APPLIED MATHEMATICS, COMPUTATIONAL SCIENCE and ENGINEERING

Proceedings of the 2014 International Conference on Applied Mathematics, Computational Science & Engineering (AMCSE 2014)

Varna, Bulgaria
September 13-15, 2014

APPLIED MATHEMATICS, COMPUTATIONAL SCIENCE and ENGINEERING

Proceedings of the 2014 International Conference on Applied Mathematics, Computational Science & Engineering (AMCSE 2014)

Varna, Bulgaria
September 13-15, 2014

All papers of the present volume were peer reviewed by no less than two independent reviewers. Acceptance was granted when both reviewers' recommendations were positive.

Series: Mathematics and Computers in Science and Engineering Series | 30

ISBN: 978-1-61804-246-0
ISSN: 2227-4588

APPLIED MATHEMATICS, COMPUTATIONAL SCIENCE and ENGINEERING

Proceedings of the 2014 International Conference on Applied Mathematics, Computational Science & Engineering (AMCSE 2014)

Varna, Bulgaria
September 13-15, 2014

Organizing Committee

Editors:
Prof. Valeri Mladenov, Technical University of Sofia, Bulgaria
Prof. Imre Rudas, Obuda University, Budapest, Hungary
Prof. Olga Martin, Politehnica University of Bucharest, Romania
Prof. Georgi Tsenov, Technical University of Sofia, Bulgaria
Prof. Panos M. Pardalos, University of Florida, USA
Prof. Martin Hromada, Tomas Bata University in Zlín, Czech Republic

Progam Committee:
Prof. Martin Bohner, Missouri University of Science and Technology, USA
Prof. Dashan Fan, University of Wisconsin-Milwaukee, Milwaukee, WI, USA
Prof. Luis Castro, University of Aveiro, Aveiro, Portugal
Prof. Metin Demiralp. Istanbul Technical University, Istanbul, Turkey
Prof. Kamisetty Rao, IEEE Fellow, Univ. of Texas at Arlington, USA
Prof. Alberto Fiorenza, Universita' di Napoli "Federico II", Napoli (Naples), Italy
Prof. Patricia J. Y. Wong, Nanyang Technological University, Singapore
Prof. Salvatore A. Marano, Universita degli Studi di Catania, Catania, Italy
Prof. Martin Schechter, University of California, Irvine, USA
Prof. Ivan G. Avramidi, New Mexico Tech, Socorro, New Mexico, USA
Prof. Michel Chipot, University of Zurich, Zurich, Switzerland
Prof. Narsingh Deo, IEEE Fellow, ACM Fellow, University of Central Florida, USA
Prof. Xiaodong Yan, University of Connecticut, Connecticut USA
Prof. Ravi P. Agarwal, Texas A&M University - Kingsville, Kingsville, TX, USA
Prof. Yushun Wang, Nanjing Normal university, Nanjing, China
Prof. Dimitri Bertsekas, IEEE Fellow, MIT, USA
Prof. Ferhan M. Atici, Western KentuckyUniversity, Bowling Green, KY 42101, USA
Prof. Anastassios Venetsanopoulos, IEEE Fellow, University of Toronto, Canada
Prof. Ravi P. Agarwal, Texas A&M University - Kingsville, Kingsville, TX, USA
Prof. Feliz Minhos, Universidade de Evora, Evora, Portugal
Prof. Mihai Mihailescu, University of Craiova, Craiova, Romania
Prof. Aggelos Katsaggelos, IEEE Fellow, Northwestern University, USA
Prof. Abraham Bers, IEEE Fellow, MIT, USA
Prof. Lucas Jodar, Universitat Politecnica de Valencia, Valencia, Spain
Prof. Jim Zhu, Western Michigan University, Kalamazoo, MI, USA
Prof. Andrei Korobeinikov, Centre de Recerca Matematica, Barcelona, Spain
Prof. Josef Diblik, Brno University of Technology, Brno, Czech Republic
Prof. Jianqing Chen, Fujian Normal University, Fuzhou, Fujian, China
Prof. Naseer Shahzad, King Abdulaziz University, Jeddah, Saudi Arabia
Prof. Sining Zheng, Dalian University of Technology, Dalian, China
Prof. Leszek Gasinski, Uniwersytet Jagielloński, Krakowie, Poland
Prof. Satit Saejung, Khon Kaen University, Muang District, Khon Kaen, Thailand
Prof. Ferhan M. Atici, Department of Mathematics, Western Kentucky University, USA
Prof. Meirong Zhang, Tsinghua University, Beijing, China
Prof. Lucio Boccardo, Universita degli Studi di Roma "La Sapienza", Roma, Italy
Prof. Tiecheng Xia, Department of Mathematics, Shanghai University, China
Prof. Lucas Jodar, Universitat Politecnica de Valencia, Valencia, Spain
Prof. Noemi Wolanski, Universidad de Buenos Aires, Buenos Aires, Argentina
Prof. Zhenya Yan, Chinese Academy of Sciences, Beijing, China
Prof. Shanhe Wu, Longyan University, Longyan, Fujian, China
Prof. Natig M. Atakishiyev, National Autonomous University of Mexico, Mexico
Prof. Jianming Zhan, Hubei University for Nationalities, Enshi, Hubei Province, China
Prof. Narcisa C. Apreutesei, Technical University of Iasi, Iasi, Romania
Prof. Detlev Buchholz, Universitaet Goettingen, Goettingen, Germany

Additional Reviewers

Matthias Buyle	Artesis Hogeschool Antwerpen, Belgium
Lesley Farmer	California State University Long Beach, CA, USA
Deolinda Rasteiro	Coimbra Institute of Engineering, Portugal
Sorinel Oprisan	College of Charleston, CA, USA
Santoso Wibowo	CQ University, Australia
Yamagishi Hiromitsu	Ehime University, Japan
Kei Eguchi	Fukuoka Institute of Technology, Japan
Shinji Osada	Gifu University School of Medicine, Japan
Tetsuya Yoshida	Hokkaido University, Japan
Xiang Bai	Huazhong University of Science and Technology, China
Philippe Dondon	Institut polytechnique de Bordeaux, France
José Carlos Metrôlho	Instituto Politecnico de Castelo Branco, Portugal
João Bastos	Instituto Superior de Engenharia do Porto, Portugal
Takuya Yamano	Kanagawa University, Japan
Hessam Ghasemnejad	Kingston University London, UK
Konstantin Volkov	Kingston University London, UK
Eleazar Jimenez Serrano	Kyushu University, Japan
Jon Burley	Michigan State University, MI, USA
Manoj K. Jha	Morgan State University in Baltimore, USA
Frederic Kuznik	National Institute of Applied Sciences, Lyon, France
Stavros Ponis	National Technical University of Athens, Greece
Ole Christian Boe	Norwegian Military Academy, Norway
Imre Rudas	Obuda University, Budapest, Hungary
Masaji Tanaka	Okayama University of Science, Japan
Francesco Rotondo	Polytechnic of Bari University, Italy
George Barreto	Pontificia Universidad Javeriana, Colombia
Dmitrijs Serdjuks	Riga Technical University, Latvia
Andrey Dmitriev	Russian Academy of Sciences, Russia
Tetsuya Shimamura	Saitama University, Japan
Francesco Zirilli	Sapienza Universita di Roma, Italy
Minhui Yan	Shanghai Maritime University, China
Valeri Mladenov	Technical University of Sofia, Bulgaria
Jose Flores	The University of South Dakota, SD, USA
James Vance	The University of Virginia's College at Wise, VA, USA
Genqi Xu	Tianjin University, China
Zhong-Jie Han	Tianjin University, China
Kazuhiko Natori	Toho University, Japan
Moran Wang	Tsinghua University, China
M. Javed Khan	Tuskegee University, AL, USA
Bazil Taha Ahmed	Universidad Autonoma de Madrid, Spain
Alejandro Fuentes-Penna	Universidad Autónoma del Estado de Hidalgo, Mexico
Miguel Carriegos	Universidad de Leon, Spain
Angel F. Tenorio	Universidad Pablo de Olavide, Spain
Abelha Antonio	Universidade do Minho, Portugal

Table of Contents

Erosion case study by Computational Fluid Dynamics (CFD) modeling and optimization *in situ* of clinker sampler probe design

Héctor Alfredo López Aguilar[1], Jorge Alberto Gómez[3], Marco Antonio Merino[3], Alberto Duarte Möller[1,2], E. Orrantia-Borunda[1] and Antonino Pérez Hernández[1],

[1]Centro de Investigación en Materiales Avanzados
Miguel de Cervantes 120, Complejo Industrial Chihuahua
Chihuahua, Chih. 31109, México

[2] Universidad Tecnológica de Querétaro
Ave. Pie de la Cuesta 2501, Col. Unidad Nacional
Querétaro, Qro. 76148, México

[3] Universidad Autónoma de Ciudad Juárez
Avenida Plutarco Elías Calles 1210
Ciudad Juárez, Chihuahua, Chih. 32317, México

[4] Universidad Autónoma de Chihuahua
Ave. Escorza 900, Col. Centro
Chihuahua, Chih. 31000, México

Abstract. This paper presents the design and modelling of a sampling probe and its erosion particle damage. Applying the simulation tool CFD (Computational Fluid Dynamics)-Fluent ANSYS 15.0, this study verifies and optimizes the dimensional configuration of the probe. The optimized device considers the cooling rate and the internal gases velocity for negative pressure generation (Bernoulli Effect) and its suitable for sampling in cement industry.The synergy with Computational Fluid Dynamics- Design of Experiments- Response Surface modelling (CFD-DOE-RS) tools, allowed the optimization of the operation of the sampler probe and verifies the enoughcooling time to prevent contamination of the specimen in contact with air to maintain its crystallographic structure. The selection of materials for the construction of the device must resist heat transfer rate and abrasive erosion occasioned for friction between the micro particles specimens that moves at high velocity in the internal walls of the device proposed.

Keywords: Bernoulli, cement, CFD, sampling probe, oxidative damage, erosion.

1 Introduction

Any industry requires the use of devices for process control and quality assurance. In cement industry the extraction of samples at high temperatures and inert atmospheres turns the extraction process into a complex activity by the potential degradation of the specimen in contact with oxygen from air. Xue [1] performed the analysis of a jet type pump,Yimer [2] through Computational Fluid Dynamics (CFD) software, which principle of operation is based on the Venturi effect [3]. This effect is widely used in the automotive, aviation and flow measurement industries [4-7] and many researchers have modelled this phenomenon by finite volume element [8-13]. In cement industry it has been used for the design and optimization of calciners [14] and to simulate the main transport processes in rotary kilns [15]; there are also patents focused on sampling systems for combustion gases from the rotary kiln. Some patents deal with volatile gases, chlorine and sulfur compounds, and for the removal of lead in the sample [16-20].

In the jet type devices during operation are subjected to friction erosion between the fluid and the surfaces, models have been developed to study this phenomenon [21]. Kumar and Shukla [22] used a finite element simulation to simulate the crater of a particle which impacts a surface and Graham et al. [23] used the **CFD** analysis to study the erosion caused by high velocity fluid. Therefore during a normal operation of the proposed probe, it is convenient the selection of certain materials. For this study anerosion simulation in finite volume, (**CFD**) **ANSYS FLUENT** was employed as a complementary analysis of the design and optimization of the extraction probe to identify risk areas.

2Materials and methods

2.1. Design considerations of specimen extraction probe.

Considering it is necessary a procedure to extract specimens during the formation process of cement clinker and keeping the structure in present phases through a quick cooling in a protective atmosphere, an extraction jet probe type is proposed. This design was based on fluid dynamics, especially on Bernoulli's principle, considering a basic structure of two tubes connected in "T" shape, by passing a non-reactive high velocity fluid by one of the tubes, a drop pressure is generated and safe extraction of samples subjected to certain atmospheresis allowed.

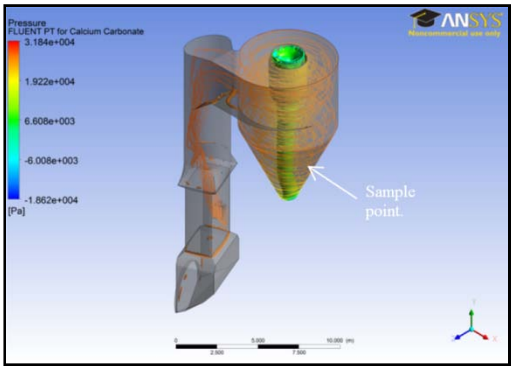


Fig. 1 Isometric view and CFD simulation inside cyclone process in cement industry.

On the other hand, in order to maintain the microstructural and chemical characteristics of the extracted samples under the mentioned extreme conditions, it is necessary a fast cooling and special-atmosphere device to avoid a reversible reaction in clinker phases or a reaction with oxygen fastened by the high temperature environment. The materials inside the cyclone (Fig. 1) are at temperatures close to 1090 K in a CO_2-rich atmosphere.

2.2. Setup and operation of the sampling probe.

For quality control in the production of cement, analysis of the samples before and after each process in the manufacture of cement clinker is necessary.

To achieve the extraction and fast cooling in a CO_2-rich atmosphere, the device shown in Fig. 2 is proposed.The device consists of an extraction tube that is introduced into the specimens' extraction gate in the cyclones (Fig. 1).

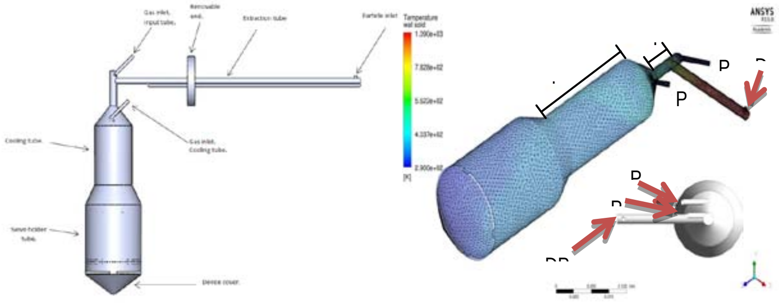


Fig. 2A) Full frontal view of the configuration of the sampling probe. B) Isometric view of the mesh of the sampling probe and lateral view with the details of the extraction tube and the gas inlets.

A flow of CO_2 (used as carrier fluid) is injected in both, the extraction and cooling inlet tube. The tangential position (Fig. 2 B) of each pivot promotes a helical flow of CO_2. Inside the cyclone, the sample rotates and enters through the hole of the collecting tube. This hole is placed facing the direction of the particles flow within the cyclone, slowing the particles by the impact with the internal wall of the collecting tube. Once the particle sample is stopped, a gas flow is applied to produce a low pressure and it helps to generate a suction effect, in which the particles captured are sending from the collection inlet tube towards the cooling tube.

A second helical effect on the cooling tube is generated by providing a CO_2 flow in the cooling inlet tube; the primary objective is to force the particles to follow a helical path toward the same cooling tube to increase the residence time.

In this way, *i)* by the second cold CO_2 flow in the cooling cone, *ii)* the sudden change in volume of the mixture of the particles with the cold carrier gas and *iii)* the helical path, the original structure of the samples is maintained inside cyclones. Therefore, the chemical and crystallographic analysis performed to the particles extracted with this invention is representative of the particles inside the extreme atmospheres in the kiln.

From the process mentioned above, the particles experiment a new volumetric expansion from the second conical section to the sieves-holder tube, where are captured by the sieves and CO_2 gases leaving the sieves-holder tube through the venting slots. After the venting slots the conical lid closes the system; the lid is removable in order to place or remove the sieves.

2.3. Simulation and dimensional optimization of the device by ANSYS - FLUENT CFD:

For the development of the present computational study, finite volume **CFD** package, **FluentANSYS 15.1** was used. To verify the operation, the diffusive behavior of gases flowing into the proposed device was modelled using the Reynolds stress model turbulence model, based on the **Navier-Stokes** equations which describe the motion of fluids [25].

To obtain the boundary conditions for the simulation of the probe, a simulation of the conditions of the internal flows in the cyclone during the manufacturing process of clinker was done. The same **CFD** software was used (Fig. 1) for this task.

The mesh used to solve the conservation equations and the final configuration of the device is illustrated in Fig. 2A - 2B, this design was patented under Mexican registration with number mx/a/2014/002336.

The simulation tool is alternated with the Design of experiments (**DOE**) and the Response Surface (**RS**) modelling; the **DOE** method is used to analyze experimental data and build empirical models to obtain the approximate representation of the physical situation, creating a table with the values of the variables to optimize. The **RS** methodology could be defined as a method to construct global approximations of the behavior of the system on the calculated results at various points in the design space. [26]

Erosion modelation.

One of the most critical wear mechanisms is erosion by particle impact. The overall correlation for the erosion rate has been established empirically [27-32]:

$$E = m_p \, C \, f(\alpha) V_p^n$$

where E is the rate of erosion (kg s^{-1}), m_p is the particle flow (kg s^{-1}), $C$is a material onstant that define the erosion resistance, *f(α)*is the impact function of the angle, is the particle velocity (m s^{-1}) and V_p is the velocity exponent, normally between 2.5 and 3.0 [32].

A low impact angles $\alpha \leq 18.5°$ the particles impact the surface removing one piece of material; the maximum erosion occurs at α = 18.5°. For impact angles higher than 18.5°, the particles impact to the surface rebounding or accumulating, small craters are produced on the surface where material is accumulated [33].

The angle factor,*f(α)*, could be calculated in relation with Finnie [34], where $f(\alpha \leq 18.5°) = sin2\alpha - 3sin^2\alpha$y $f(\alpha > 18.5°) = \frac{1}{3}cos^2\alpha$, and approximate its behavior to a piecewise-polynomial function (fig. 3)

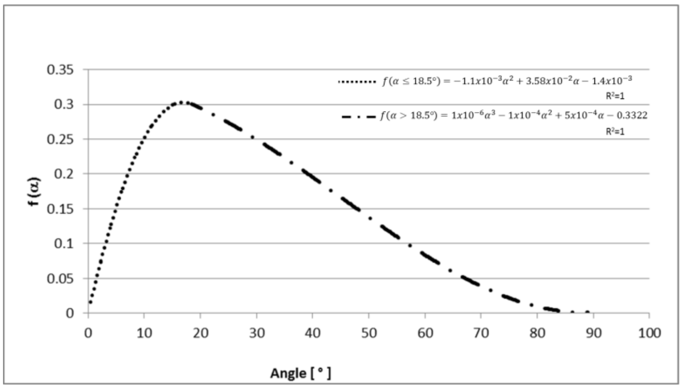


Fig. 3 Piecewise-polynomial Finnie's function.

The erosion rate (kg m^{-2} s^{-1}) on the wall is defined as [26]:

$$E_R = \sum_{p=1}^{Np} \frac{\dot{m}_p \, C(d_p) V_p^n}{A_f}$$

Where the material constant, *C(d$_p$)*, is calculated in function of the particle diameter.

Haugen et al. [30] recommends a value for *C(d$_p$)*= 2x10^{-9}for steel eroded by sand. According to the literature, the value recommended is *C(d$_p$)*=1.8x10^{-9}and*n* = 2.6 as a default constant value forangular sand (200-250µm)/ carbon steel systems, the same values that have been taken in this work.

3Results and discussion

3.1. Simulation and optimization.

In Fig. 4 A, the isotherms of the simulation are illustrated. Note that in the inlet tube, the temperature of the gases is close to 700 K. Likewise, in the outlet of the cooling tube the temperature drop near to 290 K can be observed.

The detail of the flow gases drawings is illustrated in Fig. 2 B. This picture perfectly defines the helical paths of the gases, and shows the temperature variations.

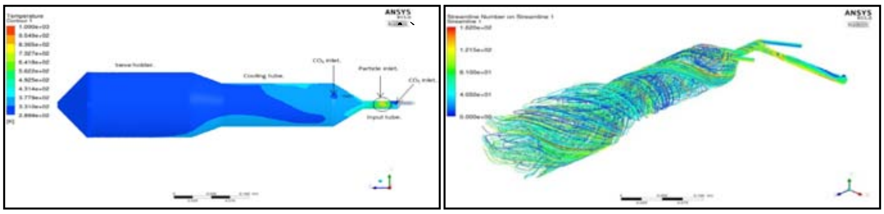


Fig. 4A) Longitudinal section of the device showing temperature contours inlet tubes, and carries cooling sieves.**B)** Detail 3D flow lines where gas temperatures shown from the inlet to the outlet of the device.

3.2 Dimensional optimization.

This design optimization is based on the construction of a response surface based on fifteen level DOE.

The parameterized variables were: the main angle between the extraction tube and the main tubeθ (fig. 4), the inlet length tube and the cooling length tube L1, L2 (fig 2 B).

The optimal design angle between the two tubes is 90° among themselves, and there is no considerable effect of the length inlet tube in the extraction rate. It was found that the length of the inlet tube has not a dependency to the cooling rate. The **SR** indicates an optimal distance for a 162.2 mm to improve the heat dissipation rate.

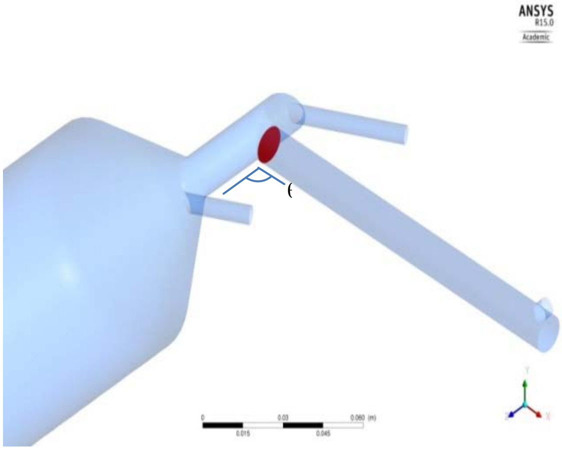


Fig. 5 Isometric probe (in red) where the surface taken as a reference for the calculation of gas velocity and the angle θ.

3. 3. Description of current sampling conditions and case study.

For the optimization of the device performance, the Rosin Rammler (**RR**) distribution model for particles in the range of the sample under study was used (Fig. 6). For the analysis of the actual particle size distribution at the laboratory, a CILAS 1180 L was used conforms to ASTM C430.

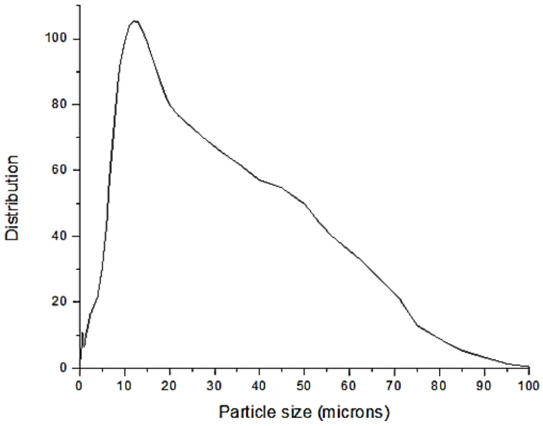


Fig. 6 Particle size distribution within the cyclone, obtained with CILAS 1180 L.

The parameters to optimize were: the gases injection angles (extraction and cooling tubes) injection pressures (Fig 2B).

To obtain the maximum velocity at the extraction inlet tube, a negative pressure in the x-axis direction will be generated by the Bernoulli effect, the optimum value obtained was -850.69 ms^{-1}, calculated on the highlighted surface in red (Fig. 5). A pivot angle of the extraction tube of 21.479° is obtained with a pressure of 0.874 GPa, and a cooling pivot angle of 28.521° with a pressure of 0.2268 GPa.

A 25levels **DOE** generated the **RS** simulation which relates the injection angles of CO$_2$with the extraction velocity in the specified area (Fig. 5). Fig. 7 shows the**SR** relationship between the pressures of both pivots (p1, p2) and the temperature at the output of the device. It can be confirmed that at the magnitudes of the pressures selected as optimal, a minimum level of temperature is obtained at the outlet of the device.

In this simulation, 99% of the path of 2220 particles (DPM) was followed, representing 1x10^6 steps of 0.01 m. The mean residence time of these particles was 0.5619 s with a standard deviation of 0.8526 s. These results show that the heat transfer (heat rate) was -6.176e10^{-15} W with a cooling rate of 1423 Ks^{-1}.

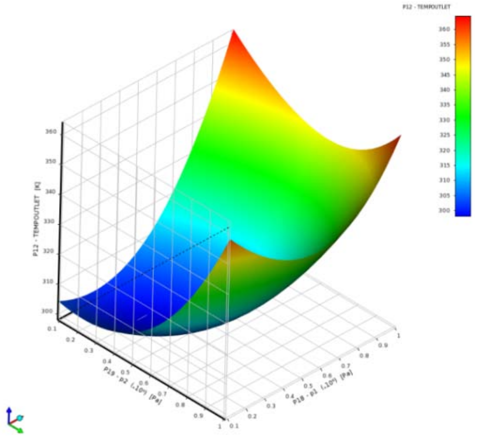


Fig. 73D graph of the pressure pivot in cooling tube (p2), the pressure pivot in extraction tube (p1) respect to outlet temperature device (TEMPOUTLET).

In this simulation, 99% of the path of 2220 particles (DPM) was followed, representing 1x10^6 steps of 0.01 m. The mean residence time of these particles was 0.5619 s with a standard deviation of 0.8526 s. These results show that the heat transfer (heat rate) was -6.176e10^{-15} W with a cooling rate of 1423 Ks^{-1}.

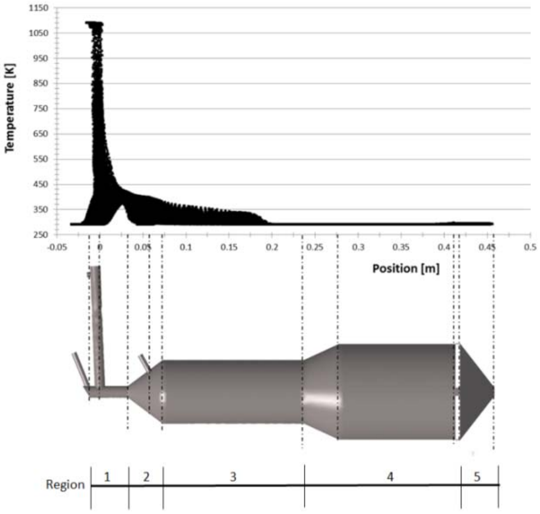


Fig. 8 Temperature behavior in each node and position of the particle within the probe.

Fig. 8 shows the temperature behavior representing the values of every node conforming the simulation domain. This figure shows the heat transfer rate of both, the particles and the gas flow. This is true since the energy transfer condition approaches a concentrated system, since it satisfies the Biot number condition; i.e. the temperature changes are the same on the particle surface and inside the particle.In regions 1, 2 and 3 a cooling ramp is identified; region 1 shows how the particles and the carrier gas tend to a thermal equilibrium while region 2 shows a conic geometry in which takes place the expansion of the particle-gas system and a second gas injection at room temperature. At this point, a complementary cooling rate observed in region 1 is generated. Finally, region 3 shows the mixture is thermally homogenized. Regions 4 and 5 contribute to the feedback of the low-pressure gases to keep the necessary turbulence of the system allowing the collection of the samples in the sieves.

3.4. Simulation of erosion rate

The images in figure 9 display the damage for erosion rate on the interior surface at the extraction tube. It is seen colored the erosion rate according to the color layer (fig. 9 A, 9B, 9C) are in different perspectives at the maximum erosion zone.

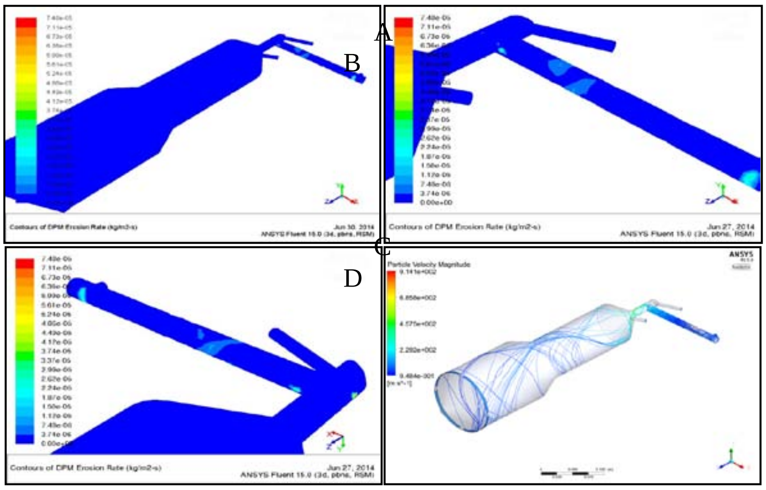

A
B
C
D
Contours of DPM Erosion Rate (kg/m2-s)
Jun 30, 2014
ANSYS Fluent 15.0 (3d, pbns, RSM)
Contours of DPM Erosion Rate (kg/m2-s)
Jun 27, 2014
ANSYS Fluent 15.0 (3d, pbns, RSM)
Contours of DPM Erosion Rate (kg/m2-s)
Jun 27, 2014
ANSYS Fluent 15.0 (3d, pbns, RSM)
Particle Velocity Magnitude
ANSYS

Fig. 9. Erosion rate profiles of the extraction probe and velocity particle track.

Once the particles enter the device through the extraction tube, some collisions occur on the front wall. This effect slow down the particles and these are extracted for the suction pressure generated by the device (fig. 9D). The particles are sent to the cooling section cone (region 2, Fig 6) and continue with the same path toward to the sieves tube. The particle impact angle is modified to achieve the critical angle within the extraction tube (fig. 9), is in this area of the probe where the maximum degree of erosion is achieved. When leaving the extraction tube and enter into the cooling tube, the particles are dispersed in a larger volume so it does not generate a measurable damage. The erosion model was found atotal erosionrate of $2.3439x10^{-3}$ $kgm^{-2}seg^{-1}$ or 0.234 $mgcm^{2}seg^{-1}$.

Conclusions.

Through the analysis of finite volume CFD, has been possible verify the correct operation of the cement clinker probe sampler at high temperatures and velocity of the particles within a cement industry cyclone, and also included an erosion analysis of this device during normal operation.

Simulation tools and the statistical analysis of the RS values contribute significantly to the design, performance optimization and materials selection for construction devices required to control the current industrial processes.In this particular study, the synergy of the **CFD-DOE-RS** tools, has allowed the optimization of the operation of the sampling device in the cement industry.

This simulation verifies the enough coolingtime to prevent contamination of the specimen by contact with air maintaining the crystallographic structure of the sample inside the cyclones. The materials for the construction of the device must resist a heat transfer rate and an abrasive wear friction between the particles moving at high velocity and temperature in the internal walls of the device. The erosion model determine the most vulnerable erosion area and the optimal materials for construction could be selected, in which angular sand in carbon steel materials was selected in this analysis for the worst case.

Acknowledgments

The authors thank the National Council of Science and Technology of Mexico for its financial support. Also, they thank the National Laboratory of Nanotechnology of CIMAV, S.C., Chihuahua, Mexico.

Conflicts of Interest

The author(s) declared there are not any conflict of interests among them or some government institutions.

References

1. S. Xue, P. Joon, K. Seung, and P. Young, “Performance comparison and erosion prediction of jet pumps by using a numerical method”, Mathematical and Computer Modelling, vol. 57, pp. 245–253, June 2011.
2. I. Yimer, H.A. Becker, and E.W. Grandmaison, “The Strong-jet/Weak-jet Problem: New Experiments and CFD. COMBUSTION AND FLAME”, vol. 124, pp. 481–502, 2001.
3. A.M. Abdulaziz, “Performance and image analysis of a cavitating process in a small type venturi,” Experimental Thermal and Fluid Science, vol. 53, pp 40–48, February 2014.

4. P. Kumar, and M.W. Ming, “A CFD study of low pressure wet gas metering using slotted orifice meters”, Flow Measurement and Instrumentation, vol. 22 pp. 33–42, December 2010.
5. J.A. Cruz, F. Sánchez, and P. Quinto, “A new correlation to determine the discharge coefficient of a critical Venturi nozzle with turbulent boundary layer”, Flow Measurement and Instrumentation, vol. 17, pp. 258–266, June 2006.
6. H. Ghassemi, and H. Farshi, “Application of small size cavitating venturi as flow controller and flow meter”, Flow Measurement and Instrumentation, vol. 22, pp. 406–412, May 2011.
7. R.K. Singh, S.N. Singh, and V. Seshadri, “Study on the effect of vertex angle and upstream swirl on the performance characteristics of cone flowmeter using CFD”, Flow Measurement and Instrumentation, vol. 20, pp. 69-74, December 2008.
8. M.T. Kandakure, V.C. Patkar, and A.W. Patwardhan, “Characteristics of turbulent confined jets”, Chemical Engineering and Processing. vol. 47. Pp. 1234–1245, April 2007.
9. A.M. Silva, J.C.F. Teixeira and S.F.C.F. Teixeira, “Experiments in a large-scale venturi scrubber Part I: Pressure drop”, Chemical Engineering and Processing, vol. 48, pp. 59–67, February 2008.
10. P.A.B. de Sampaio J. L.H. Faccini and J. Su, “Modelling of stratified gas–liquid two-phase flow in horizontal circular pipes”, International Journal of Heat and Mass Transfer, vol 51, pp. 2752–2761, December 2007.
11. D. He, and B. Bai, “Numerical investigation of wet gas flow in Venturi meter”, Flow Measurement and Instrumentation, vol 28, pp. 1–6, August 2012.
12. A.N. Johnson, J.D. Wright, S. Nakao, C.L. Merkle, and M.R. Moldover, “The effect of vibrational relaxation on the discharge coefficient of critical flow venturis”, Flow Measurement and Instrumentation, vol. 11, pp. 315–327, December 1999.
13. K.A. Ibrahim, Mofreh H. Hamed, W.A. El-Askary, and S. M. El-Behery, “Swirling gas–solid flow through pneumatic conveying dryer”, Powder Technology, vol. 235, pp. 500–515, October 2012.
14. K.S. Mujumdar, V. V. Ranade, “CFD modeling of rotary cement kilns”, Asia-Pacific Journal of Chemical Engineering, vol 3, pp. 106–118, 2008.
15. H. Mikul, M. Vujanovi, D.K. Fidaros, P. Priesching, I. Mini, R. Tatschl, N. Dui and G. Stefanovi, “The application of CFD modelling to support the reduction of CO2 emissions in cement industry”, Energy, vol 45, pp. 464-473, 2012.
16. U.S. Patent: 7,789,944 B2.
17. U.S. Patent: 4,059,019.
18. U.S. Patent 4,276,092.
19. Request patent 2008/0092739.
20. Request patent 2011/0083745 A1.
21. C. Huang, S. Chiovelli, P. Minev, J. Luo, K. Nandakumar. “A comprehensive phenomenological model for erosion of materials in jet flow”. Powder Technology, vol. 187, pp. 273–279, 2008.
22. N. Kumara, M. Shukla. “Finite element analysis of multi-particle impact on erosion in abrasive water jet machining of titanium alloy”, Journal of Computational and Applied Mathematics, vol. 236, pp. 4600–4610, 2012.
23. L. Graham, D. Lester, J. Wu. “Quantification of erosion distributions in complex geometries”, Wear, vol. 268, pp.1066–1071, 2010.
24. V. Nguyen, H. Poh, Y. Zhang. “Predicting shot peening coverage using multiphase computational fluid dynamics simulations”, Powder Technology, vol, 256 , pp. 100–112, 2014.
25. D. Montgomery. Diseño y análisis de experimentos. Segunda edición, Limusa Wiley, ISBN 13: 978-968-18-6156-8.
26. User Manual ANSYS-FLUENT 15.1

27. Tilly, GP. "Erosion Caused by Impact of Solid Particles." *Academic Press, Inc., Treatise on Materials Science and Technology* 13 (1979): 287-319.
28. Adler, WF. "Assessment of the State of Knowledge Pertaining to Solid Particle Erosion, Final Report for Army Research Office Contract No." DAAG29-77-C-0039 1979.
29. Raask, E. "Tube Erosion by Ash Impaction." *Wear* 13, no. 4 (1969): 301-15.
30. Haugen, K, O Kvernvold, A Ronold, and R_ Sandberg. "Sand Erosion of Wear-Resistant Materials: Erosion in Choke Valves." *Wear* 186 (1995): 179-88.
31. Hutchings, I M. "The Erosion of Steels by the Impact of Sand Particles.". (1984).
32. Nøkleberg, Lars, and Terje Søntvedt. "Erosion of Oil&Amp;Gas Industry Choke Valves Using Computational Fluid Dynamics and Experiment." *International Journal of Heat and Fluid Flow* 19, no. 6 (12// 1998): 636-43.
33. Keating, Anthony, and Srdjan Nesic. "Particle Tracking and Erosion Prediction in Three-Dimensional Bends." Paper presented at the Proc. of ASME FED Summer Meeting, 2000.
34. Finnie, Iain. "Erosion of Surfaces by Solid Particles." *Wear* 3, no. 2 (3// 1960): 87-103.

Electrical Brackets for IP Cameras

Milan Adamek, Dora Lapkova, Rudolf Chovanec, Petr Neumann, Miroslav Matysek

Tomas Bata University in Zlín, Faculty of Applied Informatics, Nad Stráněmi 4511
760 05 Zlín, Czech Republic
{adamek, lapkova, neumann, matysek}@fai.utb.cz

Abstract. The objective of this paper is to create an electrically-controlled bracket for analogue or IP cameras. The mechanical construction of the bracket itself and the possibilities of its movement are also described. The control device/unit assures the control of every individual part of the bracket. The primary operation of the various sections of the adjustable brackets is assured by bipolar stepper motors which are inserted into the mounting guide-rails. It also includes the design and implementation software used to control the bracket.

Keywords: camera, holder, bracket/arm, control device/unit

1 Introduction

Various sites used for installing cameras require specifically shaped brackets. Camera brackets exist in different colour and type designs. Brackets currently available on the market are designed for placement on the ceiling, walls, columns, etc. Their installation is simple and relatively quick.

2 Current camera brackets on the market

Various types of brackets are currently available on the market for reasonably low prices. The problem however is their effectiveness and the low level of effectiveness during positioning.

Fig. 1 Types of base-mount [1]

2.1 Camera brackets with rotational heads

This type represents one of many types of camera bracket, whose simplicity influences the price of other brackets offered on the market. This bracket is most often mounted on ceilings, walls, etc.

2.2 Indoor hooked bracket with swivel head

Different sites require the specific installation of brackets. Their use is relatively extensive and their price is acceptable. The holding bracket is bent into an L-shape, at the end of which is the mount for the camera. The length of leg of the bracket is usally 25 cm, and the cabling to the camera is led in the hollow space within the tube.

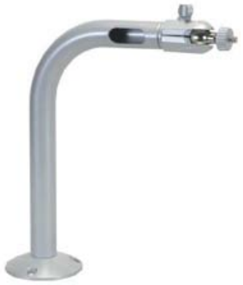


Fig. 2 Curved bracket-mount [2]

2.3 Domestic camera bracket-mounts

This is a practical bracket-mount specially developed for indoor cameras. This mount allows you to install the camera on the wall, and thus can increase the field of view of the camera. Its location versatility allows one to install the camera in places where the installation of an ordinary mounting is not suitable. The footage from the cameras is - if suitably located, much better and sharper - which is unachievable by supplementary processing of the image. Installation of the bracket is simple and quick, since the bracket is designed to ensure the security and stability of the dome camera [1].

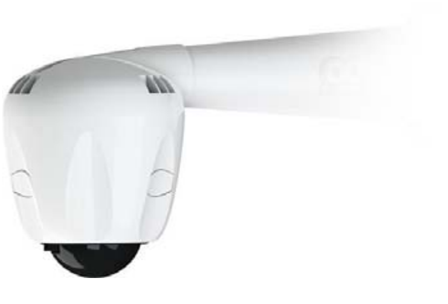


Fig. 3 Bracket mounting for dome cameras [1]

2.4 Aluminium brackets

This has to do with a strong bracket for industrial cameras, ideal for outdoor use. It can, of course, be used indoors. The main advantage is its solid construction which provides great stability and a secure mount for cameras.

Fig. 4 Aluminium bracket construction [1]

3 The construction design of our own bracket

3.1 Mechanical construction design

The bracket mounting is formed from aluminium profiles of various different sizes and wall thicknesses. Aluminium was selected for the construction due to its suitable physical properties. The design of the bracket mounting done using the VariCAD program is shown in Figure 5.

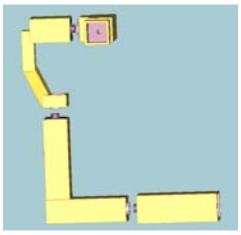


Fig. 5 Bracket-mounting design using the VariCAD programme

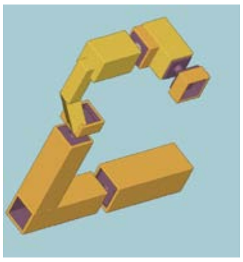


Fig. 6 Side view of the bracket mounting

Rotation of the individual components of the bracket mounting is assured through roller bearings. Roller Bearings allow the mutual relative movement of parts and the transfer of the forces and are characterized by the insertion of the rolling elements between two relatively moving elements.

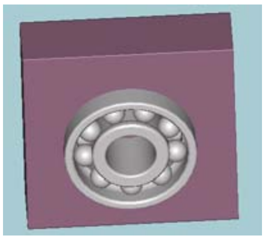


Fig. 7 A roller bearing set into aluminium material

3.2 Electrically-equipped bracket mounting

Panning and rolling of the bracket is assured by four stepper motors, which are inserted into aluminium profiles. 23HS8430 type designation bipolar stepper motors with a step angle of 1.8 ° were used for the construction [3].

Tab. 1 Basic parameters of a 23LC76 step motor

Type	Step angle	Current	Resistance	Induction	Moment	Weight
23LC76	1.8°	3A	1 Ohm	3.5 mH	180N.cm	1050g

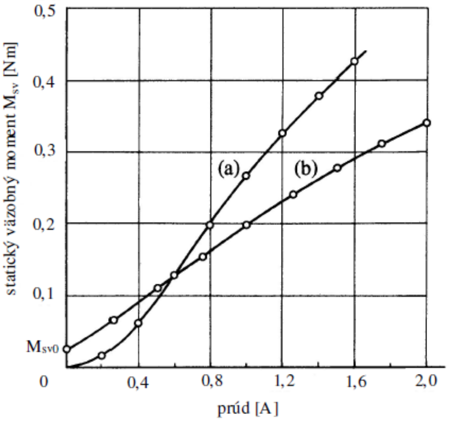


Fig. 8 Static characteristics of a step motor

Four-stroke control with two-phase magnetisation was used for the rotation of the stepper motor. It has to do with the control of a motor, with two adjacent phases switching. In this method of power supply, the equilibrium lies between the excited adjacent stator poles. Unlike four-stroke control with one magnetic phase, the rotation of the rotor is half-sized, while the step size remains unchanged. Then the time course of switching between each phase AB - BC – CD - DA is used for one direction; and switching phases AD - CD - BC - AB for the second direction to rotate clockwise [3].

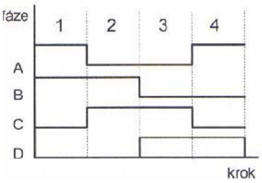


Fig. 9 Time course of a four-stroke control mechanism

4 Bracket mounting electrical rotation

Control of the step motor is assured by means of an H5controller, which controls the individual motors one after another. The controller is connected to a computer by a data cable. The computer is equipped with software which assures communications with this control device. The controller can be connected to a computer in a number of ways, e.g. USB, RS232 or even an LPT - 25 pin cable [4].

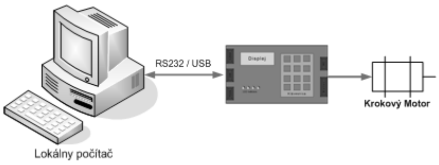


Fig. 10 The connection of a step motor [4]

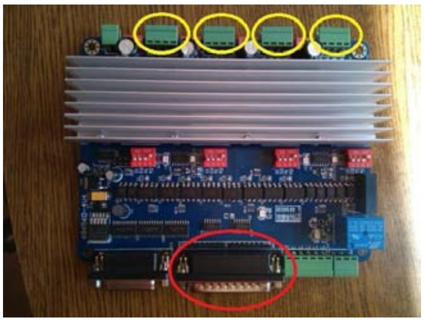


Fig. 11 The controller

The H5 Controller, which can concurrently control four step motors, also has inputs which can be connected to five different switches or various inductive loads. The inputs are protected by diodes and 1 kΩ resistor. The relay outputs can be controlled by switching a stepper motor [5].

Connection of the motors is by means of four conductors, labelled: A1+, A1-, A2+, A2 [6].

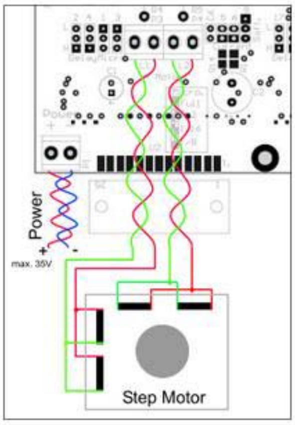


Fig. 12. Connection of a stepper motor [6]

5 Software for controlling the bracket

The MACH3program was used to control the controller, which is relatively simple for users, while at the same time ensuring minimal loss of communication at start-up. At first glance, a great range offered by the given program is obvious. All offers are grouped into a few logical groups, which are called control element families. The term control elements can be thought of as buttons and their assigned keyboard shortcuts to control not only the Mach3, but also to display information (i.e. DigitalReadOuts), tag-badges and LED indicators [7].

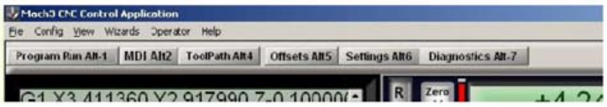


Fig. 13 Elements for switching between screens

ScreenDesigner can be used to adjust the control elements of individual screens. One can modify or suggest screens from the beginning, thus it is also possible to add various control elements to each individual screen as required.

5.1 Manual positioning using a keyboard

This program offers three regime modes for manual positioning:

- Continuous
- Stepper
- MPG

The individual modes can be selected using the JogMode, where the selected mode is indicated by a lit LED.

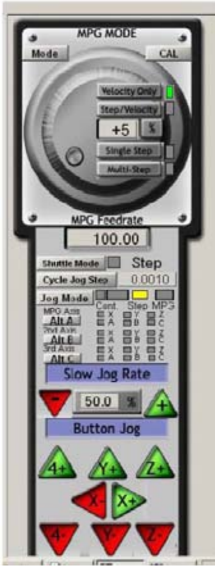


Fig. 14 Manual positioning

In the continuous mode, the bracket mounting rotates around its axis throughout the compression of the keyboard pad. The speed of movement is selected by means of the SlowJog Rate menu. Positioning speed in "continuous" is defined as the percentage of the maximum speed option values in the Slowpercentage DRO. This value can be entered within the range of 0.1% to 100%. Using the + / - buttons, one can change the value by 5%. The set positioning speed can be exceeded by just pressing the Shift key and the appropriate jogging key [8].

Apart from the LED diodes that indicate the continuous mode, the LED diode immediately indicates the activation of the maximum positioning speed [5].

6 Conclusion

The positional bracket proposed here can be operated in both internal and external environments. It is suitable for positioning analogue or IP cameras. The ideal location of the proposed bracket mounting is on the corner of a building such that the camera can be used to capture, for instance, two entrances to the building.

Acknowledgement

The authors wish to thank to the Ministry of Education, Youth and Sports of the Czech Republic (and the European Regional Development Fund for their financial support of the CEBIA-Tech No. CZ.1.05/2.1.00/03) project

References

1. Ubiquiti [online]. Bratislava, 2010, 10.1.2014 [cit. 2014-04-28] . In: http://www.ubiquiti.sk/abracam-dome-bracket-drziak-na-stenu-pre-kameru-aircamdome/
2. Eltrex: Camera systems [online]. Svidník, 2012, 2014 [cit. 2014-04-28]. In: http://www.eltrex.sk/kategoria/konzoly-na-kamery/aluminium-drziak-na-kamery-montazna/stenu-sab-06-6708/
3. Novak, Petr. Mobilné roboty. Praha: Ben - Technická literatúra, 2005. ISBN 80-7300-141-1.
4. Timko, Jan. Electrical engineering. Košice. Košice: Technická univerzita, 2008. ISBN 978-80-8073-779-5.
5. Hobby CNC [online]. Bratislava, 2012, 23.1.2014 [cit. 2014-04-29]. In: http://cnc1.eu/sk/h5controller.htm
6. Pospisilik, Martin, Kouril, Lukas, Motyl, Ivo, Adamek, Milan: Switching Power Supply for an Autonomous Monitoring System. In: 14th WSEAS International Conference on Systems: Latest Trends on Systems. 1. Greece : [s.n.], 2010. s. 431-434. ISBN 978-960_474-241-1.
7. Pospisilik, Martin, Kouril, Lukas, Motyl, Ivo, Adamek, Milan: Single and Double Layer Spiral Planar Inductors Optimisation with the Aid of Self-Organising Migrating Algorithm. In: Proceedings of the 11th WSEAS International Conference on Signal Processing, Computational Geometry and Artificial Vision. Venice : WSEAS Press (IT), 2011, ISBN 978-1-61804-027-5.
8. Electronics for transportation E4T [online]. 2010 [cit. 2013-04-28]. In: http://e4t.cz/Vyrobky/CAN4t.aspx

Communication Principles Between Client and Physical Hardware of ISES Remote Laboratory

M. Gerža[1], F. Schauer[1,2], K. Vlček[1]

[1]Tomas Bata University in Zlín, Faculty of Applied Informatics, Nad Stráněmi 4511,
CZ-760 05 Zlín, Czech Republic. E-mail: michal.gerza@email.cz
[2]University of Trnava, SK-918 43 Trnava, Slovak Republic

Abstract. The paper is focused on the analysis of communication principles between interested client and the physical hardware of ISES (Internet School Experimental System) remote laboratories. Different types of connections are allocated to use comfortably the real-time experimenting in a remote laboratory. Each ISES unit includes some communication mechanism to provide data to underling or superior unit to process it in a given way. The main reason for proper communication is to deliver control commands from clients to the physical hardware to accomplish programmed tasks in order to observe, measure and receive real physical or electrical phenomena in form of data. The ISES remote laboratory provides clients a unique educational tool for the purpose of the desired phenomena understanding. This tool is especially useful for distant students, who are often hampered to attend regular courses.

In the first chapter, a state of the art is described to explain the ISES remote laboratory concept. As the next, an analysis is performed concerning data communication needed for a cooperation of the all units involved, i.e. physical hardware, Measureserver®, Internet, local area network and client. The further chapter proposes improvements of the most sensitive communication points. Two diagnostic systems are introduced to prevent or significantly reduce occasional faults and anomalies. The first system used is the internal units diagnosis solving communication deficiencies inside of the ISES remote laboratory. The second one acts as the network traffic diagnosis, dealing with the detection, identification and quantification of anomalies, which can create congestion in network and have an ill impact on administrators or clients. The last chapter summarizes benefits of these diagnostic systems for ISES remote experiments in order to improve communication among units.

Keywords: ISES, Measureserver®, physical hardware, remote experiment, communication protocol, diagnosis, transmission

1 Introduction

The traditional methods of teaching, oriented on students at secondary schools and universities, are quite obsolete and not so broadly popular to understand taught scientific themes. The contemporary students demand higher level teaching methods, which help them to perceive phenomena in better way in the field of physics, biology, chemistry and electro-engineering. Educational materials accessibility is important as well, especially for distant students who often prefer studying scientific themes via the Internet on their computers. These coveted advantages are provided by a remote laboratory (RL) called e-laboratory. RL is built on ISES, which has been developed for educational purposes. The ISES is a complex tool for real-time operation, data acquisition, data processing and controlling physical hardware (HW). It is an open system consisting of the basic ISES hardware and ISES WIN software intended for a local laboratory but it also has an option for the remote connection called ISES WEB Control Kit available anytime and anywhere.

The RL based on ISES WEB Control Kit is perceived like the superstructure so called ISES remote experiment (ISES RE), which has been developed by Charles University in Prague. After some time, the ISES RE has been significantly improved on a higher level educational tool by Tomas Bata University in Zlín in cooperation with Charles University in Prague so called EASY REMOTE - ISES (ER-ISES) in order to simplify settings and usage for teachers.

The ISES REs are categorized to several groups according to their complexity and the level of control as the basic, complex and scientific. Each RE consists of five cooperative units like is the physical HW (apparatus consisting of the ISES panel, meters, sensors and specific experimental devices generating given phenomena), Measureserver®, ImageServer, WebServer and WebClient. More technical details about the ISES RE are available in [1] and [2]. The clarifying scheme, including the communication relationships, is presented in Fig. 1.

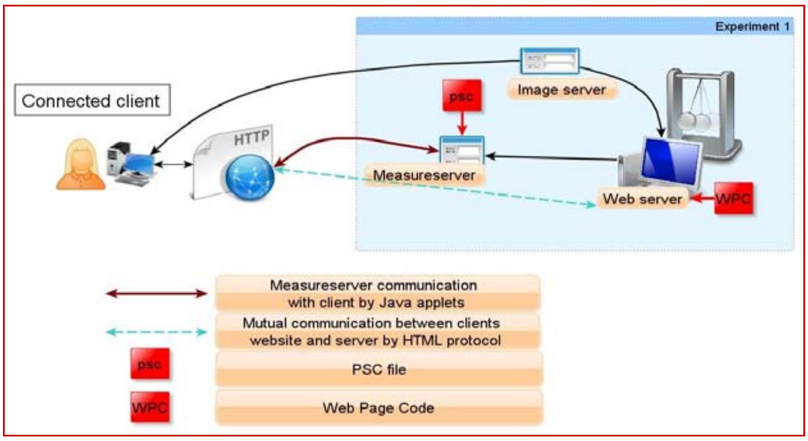

Experiment 1
Connected client
Image server
psc
HTTP
Measureserver
Web server
WPC
Measureserver communication with client by Java applets
Mutual communication between clients website and server by HTML protocol
psc
PSC file
WPC
Web Page Code

Fig. 1. Arrangement of the ISES remote experiment [3]

2 State of the art

The ISES units dispose of adequate communication mechanisms to cooperate with neighboring units to deliver requested information. Since many different types of data (signals and packets) are being processed and transmitted, so the functional concept implements the signal converting process and communication protocols.

2.1 Physical hardware

A low-level communication based principle is used between the ISES RE physical hardware and the AD/DA (Analog-to-Digital / Digital-to-Analog) convertor - 12 bits, time of conversion - 0.01 ms, installed as the PCI 1202 interface card inside an administrative computer. This device converts a continuous physical quantity (voltage) to a digital number that represents the quantity's amplitude and performs the inverse operation back to the physical quantity. All the used modules of physical HW, including the AD/DA convertor, are demonstrated in Fig. 2.

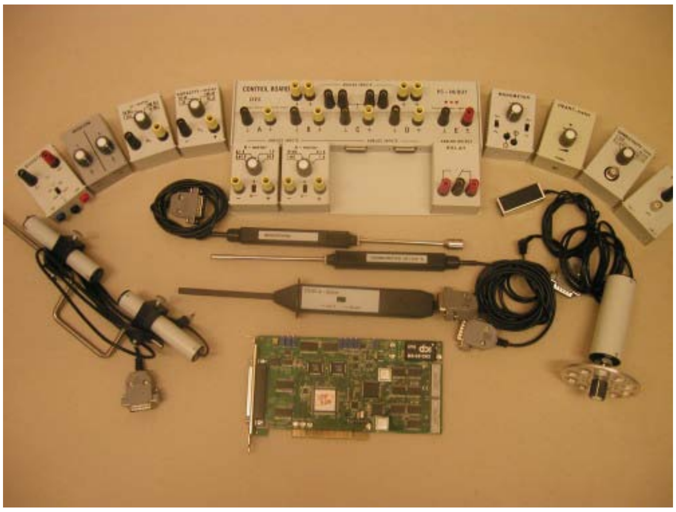


Fig. 2. ISES remote experiment including the AD/DA convertor card and a broad range of involved meters, sensors and probes [4]

2.2 Measureserver® unit

The Measureserver® (MS) is a significant software part of the ISES RE concept. It is perceived as a communication mediator between the physical HW and remote clients. The MS is constructed as the mathematical model used for designing of control programs by an external PSC program file to build a control and measurement logic.

Towards the physical HW, the MS communicates in reality with a software driver of the AD/DA convertor. It is entirely digital process based on reading data (values) directly from particular pins and writing data to respective pins which are translated by the AD/DA convertor. These pins are perceived as the inputs and outputs located on the ISES board that allows connecting particular sensors and devices into the system. The low-level operation is always ensured by the PCI1202CardPlugin.ldp plug-in (intercommunication file) loaded by the ScriptablePlugin2.ldp plug-in, which exploits the first one for its internal functioning. The ScriptablePlugin2.ldp plug-in builds the ISES RE logic by a PSC program delivered to the system by a responsible administrator. This plug-in is able to load any intercommunication file within the MS startup, but presently, the PCI1202CardPlugin.ldp is only available. The CFG configuration file, as a necessary part of MS intended for initial settings, includes a reference to the ScriptablePlugin2.ldp plug-in. A scheme of the data communication relationships among particular modules is described in Fig. 3.

When data (control and measurement commands) come from a remote client to MS, the communication is realized by the TCP/IP (Transmission Control Protocol / Internet Protocol) protocol via the Internet and then goes to Intranet (local area network) in a building where the laboratory with ISES RE resides. Such the communication requires a static public IP address of a computer hosting the MS and other important supporting services.

All commands, incoming from the entered client and physical HW on the other side, are processed by the deterministic way in a finite-state machine (FSM) realized by two involved parser mechanisms.

The first is the LR(1) parser that processes commands from the CFG configuration file for the purpose of the GUI (graphical user interface) setting. This parser is based on the static state transition tables called parsing tables, which codify the language grammar. These parsing tables are parameterized together with a lookahead terminal (lookahead establishes the maximum incoming tokens that the parser can use to decide, which rule it should use). More technical details, including several parsing examples, are available in [5] and [6].

The second one is the Recursive descent parser processing commands from the PSC program file in order to create internal data structures for ISES RE. The parser uses a general form of top-down parsing where backtracking may be involved. The parsing principle is based on the walking through a tree. More details, with a parsing example, are available in [7] and [8].

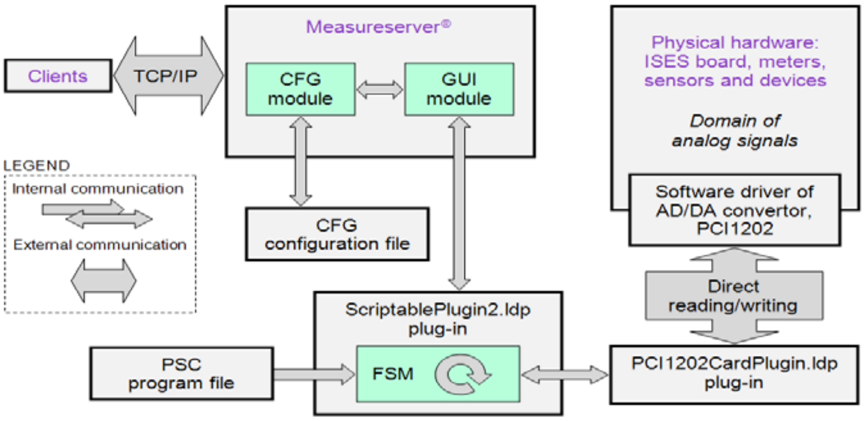


Fig. 3. Communication relationships among modules of the ISES remote experiment

2.3 Web server

This unit is called Nginx that comes into the process when client enters a web page of the ISES RE by typing an IP address or URL (Uniform Resource Locator) in any web browser (e.g. Firefox Mozilla, MS Explorer). Nginx is an open source reverse proxy server for HTTP, HTTPS, SMTP, POP3 and IMAP protocols and a web server [9].

When a client enters the ISES RE, the Nginx starts negotiating with the client and establishes a direct data communication between the MS unit and Java applet called ConnectionHub. Every applet, imported on the web page by the Nginx, uses services of the ConnectionHub to communicate with the physical HW via the MS unit.

2.4 Data network

As mentioned previously, the ISES RE uses communication protocols to negotiate with clients. When a client enters an URL of the ISES RE in a web browser to reach the physical HW, the communication starts by using the Internet Protocol Suite. After establishing the connection, initial packets enter a local area network (LAN) in the building where the laboratory resides. In the LAN, the connection is realized by Ethernet to communicate with the MS unit.

2.5 Client’s interface

It is only one interface the clients can access the ISES physical hardware, therefore the web page's design and serviceability play important role as presented in Fig. 4.

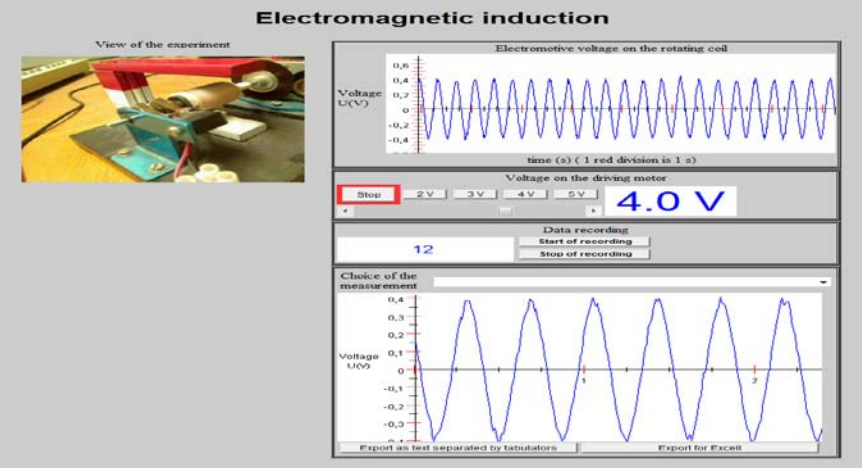

Electromagnetic induction
View of the experiment
Electromotive voltage on the rotating coil
Voltage U(V)
0,6
0,4
0,2
0
-0,2
-0,4
time (s) (1 red division is 1 s)
Voltage on the driving motor
Stop
2 V
3 V
4 V
5 V
4.0 V
Data recording
12
Start of recording
Stop of recording
Choice of the measurement
Voltage U(V)
0,4
0,3
0,2
0,1
0
-0,1
-0,2
-0,3
1
2
Export as text separated by tabulators
Export for Excell

Fig. 4. Web page of the ISES RE "Faraday's law of electromagnetic induction" [4]

3 ISES remote experiment diagnosis

A diagnostic system poses an important part of modern software and hardware applications. Contemporary applications became too complex and they communicate usually with different subsystems, therefore administrators and clients should have a comfortable diagnostic tool to maintain functioning of such the applications.

3.1 Internal units diagnosis

The ISES RE concept has many deficiencies related to the communication among particular units. The most problematic point seems to be between the MS and physical HW where the involved AD/DA convertor is important.

Presently, the MS sometimes loses connection with the ISES RE or even stops its functioning. This is a serious problem that always has to be solved by the intervention of an administrator by experience-based actions (e.g. restart of the MS, re-connection of individual hardware modules). A solution is to deploy an intelligent diagnostic system intended for the communication that should primarily eliminate all the administrator's actions because a human factor can negatively influence the ISES RE functioning. The diagnostic system will be automatically monitoring and evaluating the internal connection between the MS and the AD/DA convertor. In case of the miscommunication, an alarm report will be generated and dispatched to the remote laboratory management system (RLMS), as a new unit of the improved ISES RE. The RLMS will be acting as a supervisor authorized to restart the MS as well to recover its functioning. Furthermore, the communication between the PCI1202CardPlugin.ldp plug-in and modules (e.g. ampere-meter, voltmeter), installed on the ISES board, will dispose of the robust self-checking mechanisms. When e.g. a cold link occurs in the connector linking the pin with module, a generated alarm report will be delivered to the RLMS to inform an administrator and entered clients about existing problem that obstructs the experimenting. The scheme, shown in Fig. 5, presents a deployment of the internal units diagnosis into the MS communicating with the ISES RE.

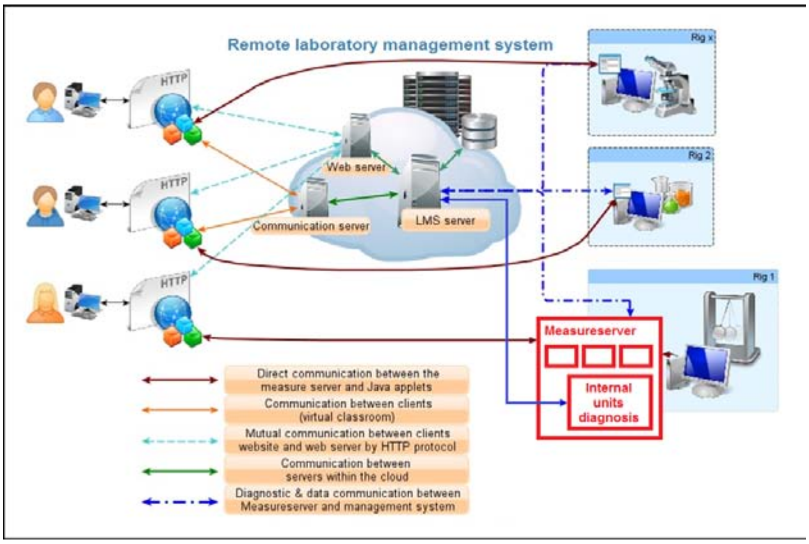

Remote laboratory management system
HTTP
HTTP
HTTP
Web server
Communication server
LMS server
Rig x
Rig 2
Rig 1
Measureserver
Internal units diagnosis
Direct communication between the measure server and Java applets
Communication between clients (virtual classroom)
Mutual communication between clients website and web server by HTTP protocol
Communication between servers within the cloud
Diagnostic & data communication between Measureserver and management system

Fig. 5. Arrangement of the improved ISES RE concept based on the remote laboratory management system and the internal units diagnosis [3]

3.2 Network traffic diagnosis

As the second problematic point appears network traffic anomalies decelerating or blocking the communication between clients and the ISES RE. Anomalies are unusual and significant changes in network's traffic levels, which can often span multiple links. It is an important problem to understand the nature of traffic anomalies in a network. Regardless of whether the anomalies are malicious or unintentional, it is needed to analyze them for the following reasons:

- Anomalies can create congestion in the network and stress resource utilization in a router, which makes them crucial to detect from an operational standpoint.
- Some anomalies may not necessarily impact the network but they can have a dramatic impact on network administrators or end clients.

It is a difficult problem because anomalous patterns must be extracted and interpreted from large amounts of high-dimensional noisy data. Hence, a general method is used to diagnose such anomalies. This method is based on a separation of the high-dimensional space occupied by a set of network traffic measurements into disjoint subspaces corresponding to normal and anomalous network conditions. The separation can be effectively performed by the coordinate transformation method called Principal Component Analysis.

An analysis of volume anomalies can be realized by using simple traffic measurements only from data links. The involved diagnostic method can:

1) detect when a volume anomaly is occurring,

2) identify the underlying origin-destination flow, which is the source of the anomaly,

3) estimate the amount of traffic involved in the anomalous origin-destination flow.

The introduced method is able to diagnose (i.e., detect, identify and quantify) both existing and synthetically injected volume anomalies in real traffic in two networks. It diagnoses the largest anomalies and does so with a very low false alarm rate [11].

3.2.1 Volume anomalies

A typical network (e.g. backbone) is composed of nodes (also called Points of Presence or PoPs) that are connected by links. An Origin-Destination (OD) flow is define as the traffic that enters the network at the origin PoP and exits at the destination PoP. The path followed by each OD flow is determined by the routing tables. Therefore, the traffic observed on each network link arises from the superposition (two signals are added together) of these OD flows.

The *volume anomaly* term refers to a sudden (with respect to time step used) positive or negative change in an OD flow's traffic. Since such an anomaly originates outside the network, it will propagate from the origin PoP to the destination PoP.

A technique is used for diagnosing the volume anomalies. If a volume anomaly propagates through the network, it should be observed on all links it traverses. Anomalies based on the OD flow are identified by observing only link counts.

The diagnosis difficulty stems in part from the fact that it uses only link data, which can be collected via SNMP (Simple Network Management Protocol). Necessary inferences must be formed about unusual events occurring in the underlying OD flows from these link data.

Examples of this difficulty are presented in Fig. 6. The top plot on each side of the figure shows an OD flow time series with an associated volume anomaly - this information is not available to the algorithms, but just to show the nature of these anomalies. The point at which each anomaly occurs is designated by a circle on the timeline. Below the timeline are plots of link traffic on the four links that carry the given OD flow. These four plots represent the data that is available to the used algorithm. The diagnosis consists of processing all link data so as to:

1) detect that at the time shown, the network is experiencing an anomaly,

2) isolate the four links shown as those experiencing the anomaly,

3) estimate the size of the spike in the OD flow.

Three observations could be performed from these examples. First, while the OD flows have pronounced spikes, the corresponding spike in the link traffic is dwarfed, and difficult to detect even from visual inspection. For instance, the traffic volume at the spike time on links, defined as *c*-*d* and *b*-*c* in Example 1, is hardly distinguishable. Second, the temporal traffic patterns may vary substantially from one link to another. In Example 2, the *i*-*f* link has a smooth trend, whereas the other links for the OD flow have more noisy traffic. Separating the present spike from the noise in the traffic on the *c*-*b* link is visually more difficult than separating the spike in the *i*-*f* link. Thus isolating all the links exhibiting an anomaly is challenging. Finally, mean traffic levels vary considerably. In Example 1, the mean traffic level on the *c*-*d* link is more than twice that of the *f*-*i* link. The varying traffic levels makes it difficult to estimate the size of the volume anomaly and hence its operational importance.

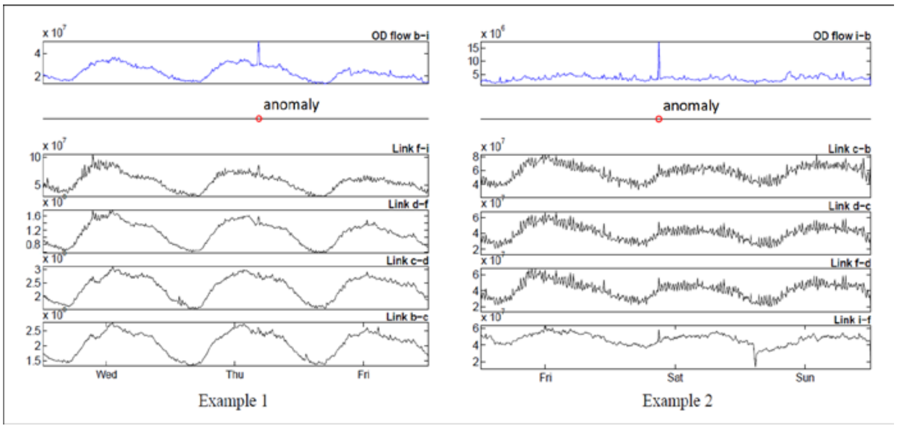


Fig. 6. Examples of anomalies at the Origin-Destination flow level (top row) that is required to diagnose from link traffic [11]

The problem of diagnosing a volume anomaly in an involved OD flow can be separated, as mentioned, into the following three processing steps:

- *Detection* consists of designating those points in time at which the network is experiencing an anomaly. An effective algorithm for solving the detection problem has a high detection probability and a low false alarm probability.
- *Identification* consists of selecting the true anomaly type from a set of possible candidate anomalies. The method is extensible to a wide variety of anomalies. However, as a first step, the candidate anomaly set is the set of all OD flows.
- *Quantification* is the problem of estimating the number of additional or missing bytes in the underlying traffic flows. The quantification is important because it gives a measure of the importance of the existing anomaly.

The diagnosis also requires the detection of an anomaly time, the identification of the underlying responsible OD flow and the quantification of an anomaly.

3.2.2 Data acquirement

The method operates on link traffic data obtained by SNMP. Traffic anomalies can last anywhere from milliseconds to hours. It can be used on data with any time granularity, e.g. to work with data binned on 10 minute intervals. Binning is a way to group a number of more or less continuous values to a smaller number of bins [10].

In order to validate data against true OD flows, a set of link traffic counts must be obtained consistent with sampled OD flow data collected from the network. To perform this, the traffic matrix estimation method is followed and a construction of the link counts is then performed from OD flow counts, which use a routing table taken from the network in operation.

3.2.3 Subspace analysis of link traffic

The diagnosis of anomalies in traffic requires the ability to separate them from normal network-wide traffic. In this subchapter, the Principal Component Analysis (PCA) is described to separate normal and anomalous network-wide traffic conditions.

The PCA is a coordinate transformation method that maps a given set of data points onto new axes. The axes are called the principal axes or principal components. When working with zero-mean data (mean value to zero), each principal component has the property that it points in the direction of maximum variance remaining in the data, given the variance already accounted for in the preceding components. As such, the first principal component captures the variance of the data to the greatest degree possible on a single axis. The next principal components then each capture the maximum variance among the remaining orthogonal directions. Thus, the principal axes are ordered by the amount of data variance that they capture.

An illustration of the difference between normal and anomalous traffic variation is shown in Fig. 7, as captured in the PCA decomposition. The figure shows sample projections of the network 1 dataset onto selected principal components. On the left, projections onto the first two principal components (*u1* and *u2*) are presented, which capture the most significant variation in the data. These time series are periodic and reasonably deterministic and clearly capture the typical diurnal patterns, which are common across traffic on all links. Note that *u1* and *u2* are roughly 180 degrees out of phase, meaning that the two can be used in linear combination to roughly construct of sinusoid of any phase. Thus the extraction of common temporal patterns via the PCA does not require the underlying traffic time series to have the same periodic phase as reflected e.g. in traffic in the same time zone. The used subspace method is able to assign these traffic variations to the normal subspace.

Presented Fig. 7 also shows projections *u6* and *u8*. In the contrast to involved *u1* and *u2*, these projections of the data exhibit significant anomalous behavior. These traffic spikes indicate unusual network conditions possibly induced by a volume anomaly at the OD flow level. The subspace method treats such projections of the data as belonging to the anomalous subspace.

A variety of procedures can be applied to separate the two types of projections into normal and anomalous sets. Based on examining the differences between typical and atypical projections, a simple threshold-based separation method has been developed to work well in practice. Specifically, a separation procedure examines the projection on each principal axis in order; as soon as a projection is found that exceeds the threshold, e.g. contains a deviation from the mean, that principal axis and all subsequent axes are assigned to the anomalous subspace. All previous principal axes then are assigned to the normal subspace. All the dimensions showing significant variance are assigned to the normal subspace when this procedure results in placing the first four principal components in the normal subspace in each case.

The traffic is decomposed on each link into normal and anomalous components after separating to the space of possible traffic measurements into the subspaces.

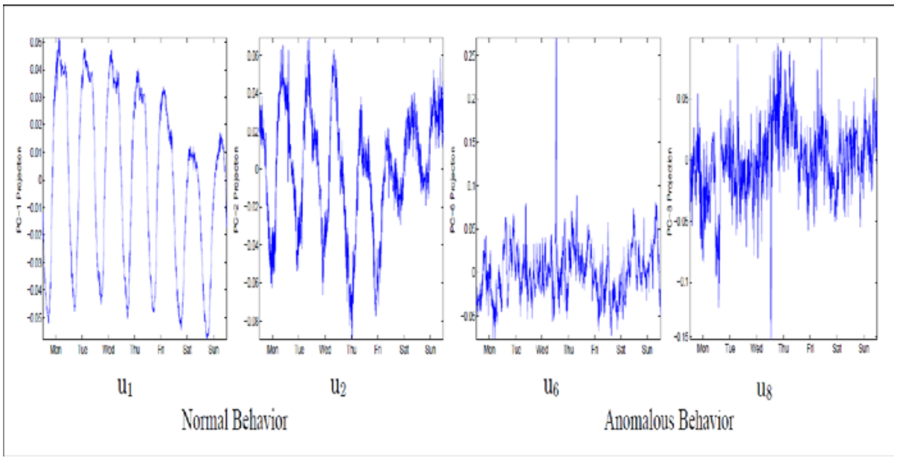


Fig. 7. Example of the projections onto principal components showing normal and anomalous traffic variation in data network [11]

3.2.4 Diagnosing volume anomalies

The methods used for detecting and identifying volume anomalies draw from a theory developed for the subspace-based fault detection in multivariate process control.

Detecting volume anomalies in link traffic relies on the separation of link traffic at any time step into normal and anomalous components. They can be also called as the *modeled* and *residual* parts of the link traffic in a network.

The key idea in the subspace-based detection step is that, once both the normal and anomalous subspaces have been constructed, this separation can be effectively performed by forming the projection of link traffic onto these two subspaces.

As the next diagnostic step is a process of the identification. In the subspace framework, a volume anomaly represents a displacement of the state vector away from the normal subspace. This state vector is expressed as a sum of the sample vector for normal traffic conditions and the magnitude of the anomaly, which is influenced by the vector defining the manner in which this anomaly adds traffic to each link in the network. The particular direction of the displacement gives information about the nature of the anomaly. Thus the approach to anomaly identification is to ask which anomaly out of a set of potential anomalies is best able to describe the deviation of state vector from the normal subspace.

When an estimation of the particular volume anomaly was formed, the last step comes into the process called quantification. This method is able to estimate the number of bytes constituting this anomaly.

3.2.4 Validating results

The validation approach is centered on answering two questions:

1) How well can the method diagnose actual anomalies observed in real data?

2) How does the time and location of the anomaly affect performance of the method?

The first question can be answered as follows. It is reached up by using the time series analysis on OD flow data to isolate first a set of true anomalies. This approach allows then evaluating the subspace method quantitatively. In particular, it allows making a measurement of both the detection and false alarm probabilities.

The second question can be answered as well. It is realized by injecting anomalies of different sizes in OD flows and applying a procedure to diagnose these known anomalies from link data. This is performed repeatedly for each time step and for each anomaly to form the picture of how diagnosis effectiveness varies with the time and location of the occurred anomaly in a network.

In each case, the performance of each step must be quantified in the following diagnosis procedure. A detection success is measured by two metrics: the detection rate and the false alarm rate. The detection rate is the fraction of true detected anomalies. The false alarm rate is the fraction of normal measurements that trigger an erroneous detection. An identification success is captured in the identification rate, which is the fraction of detected anomalies that are correctly identified. Finally, a quantification success is measured by computing the mean absolute and relative error between the estimate and the true size of all identified volume anomalies [11].

4 Functional benefits

The introduced diagnostic systems provide us an efficient solution how to avoid or reduce faults coming from some modules of the physical HW in the ISES RE. The second benefit is an elimination of the congestion in a network caused by wide traffic anomalies when clients are being connected to the ISES RE.

Both the diagnostic systems should cooperate with the RLMS that performs proper accommodation actions based on scenarios in case of detected and identified ill events occurred during the experimentation. The scheme, presented in Fig. 8, shows an implementation of the diagnostic systems as new modules into the MS unit.

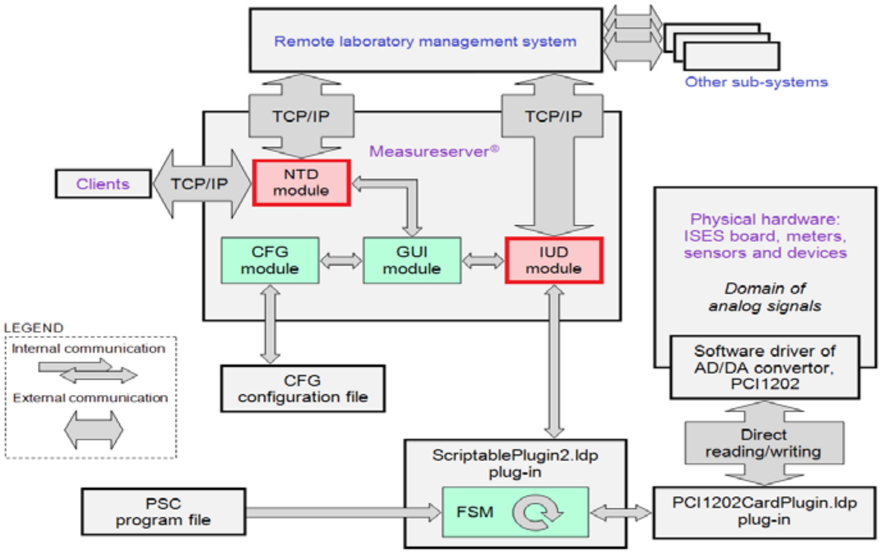


Fig. 8. Implementation of the internal units diagnosis (IUD) and the network traffic diagnosis (NTD) modules into the Measureserver® unit

5 Conclusions

This paper has presented the extensive analysis of communication among particular units of the ISES remote laboratory, and provided you possible improvements by using two diagnostic approaches. It has been the objective of our work to analyze the low-level communication to understand its basic principles. The further part of this objective has been focused on the diagnosing an occasional miscommunication of the ISES hardware modules, and wide traffic anomalies in a network. We have analyzed the suitable diagnostic approaches to implement into the ISES remote laboratory to avoid or significantly reduce such ill events during the operation.

Our conclusions may be formulated as follows.

1) The experimentation based on the ISES remote laboratory is a new approach of teaching and learning in comparison with traditional forms of education.
2) The Measureserver® is a core unit of the ISES remote laboratory responsible for communicating between clients and physical hardware modules.
3) The ISES remote laboratory exploits Ethernet that is a family of networking technologies for local area network protocols, and the TCP/IP networking model including a large group of communication protocols used for the Internet.
4) The internal units diagnosis is a suitable approach for monitoring and evaluating the internal communication between the Measureserver® and the AD/DA convertor to avoid possible faults coming from the ISES physical hardware.
5) The network traffic diagnosis fits to the wide traffic anomalies occurring in a network for the purpose of detecting, identifying and quantifying them, and to report ill events to administrators and clients using the ISES remote laboratory.
6) We also plan the improvement of these diagnostic systems concerning intelligent corrections performed when faults or anomalies come into the system.

Acknowledgment

The paper was published thanks to the Grant of the Internal Agency of Tomas Bata University No. IGA/FAI/2014/044, and partially by the Grant of the Kega Agency KEGA Agency projects No 011TTU-4/2012 and 020TTU-4/2013 and Grant of the agency APVV project No. APVV 0096-11.

References

1. ZEMAN, Petr. Software environment for integration of measured data from remote laboratory and simulation. Ostrava: VŠB-Technical University of Ostrava, 2012.
2. ZEMAN, Petr. Software environment for control of remote experiments. Ostrava: VŠB-Technical University of Ostrava, 2011.
3. KRBEČEK, Michal. ISES remote experiments configuration. Zlín. UTB ve Zlíně, Fakulta aplikované informatiky, 2013.
4. LUSTIG, František. *Internet School Experimental System iSES* [online]. Prague, Czech Republic, 2009 [cit. 2014-06-05]. Dostupné z: http://www.ises.info/index.php/en
5. Canonical LR parser: Constructing LR(1) parsing tables. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001-2014 [cit. 2014-06-05]. Available: http://en.wikipedia.org/wiki/Canonical_LR_parser

6. Parsing: Lookahead. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001-2014 [cit. 2014-06-05]. Available: http://en.wikipedia.org/wiki/Parsing#Lookahead

7. REDDY. *Top-Down Parsing, Recursive-Descent Predicative Parsing* [online]. [cit. 2014-06-05]. Available: http://www.facweb.iitkgp.ernet.in/~niloy/Compiler/notes/TDP.doc

8. WILKINSON, Leland. Recursive Descent Parser. [online]. 2008 [cit. 2014-06-05]. Available: http://www.cs.uic.edu/~wilkinson/Applets/parser.html

9. Nginx. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001-2014 [cit. 2014-06-05]. Available: http://cs.wikipedia.org/wiki/Nginx

10. Binning. *Spotfire Technology Network* [online]. TIBCO Spotfire, 2013 [cit. 2014-05-06]. Dostupné z: [18] http://stn.spotfire.com/spotfire_client_help/bin/bin_what_is_binning.htm

11. LAKHINA, Anukool, Mark CROVELLA a Christophe DIOT. Diagnosing network-wide traffic anomalies. In: *SIGCOMM '04 Proceedings of the 2004 conference on Applications, technologies, architectures, and protocols for computer communications*. New York, NY, USA: ACM, 2004, s. 12. ISBN 1-58113-862-8. DOI: 10.1145/1015467.1015492. Available: http://www.cs.cornell.edu/people/egs/cornellonly/syslunch/fall04/anomalies.pdf

Electromagnetic Compatibility of Alarm Systems

Jan VALOUCH

Tomas Bata University in Zlin, Faculty of Applied Informatics,
Nad Stráněmi 4511, 76005, Zlín, Czech Republic
valouch@fai.utb.cz.

Abstract. Alarm systems are deployed to ensure the protection of people and property in the form of an intruder alarm system, hold-up alarm system, CCTV systems, access control systems or social alarm systems. In terms of electromagnetic compatibility is necessary to address issues of the conformity assessment of products, selection of suitable components and in particular method of installation in a specific area of deployment. The aim of the article is definition of legal and basic technical requirements for electromagnetic compatibility of components of Alarm systems.

Keywords: Electromagnetic interference, electromagnetic compatibility, alarm systems, technical standards, government regulation, conformity assessment.

1 Introduction

Alarm systems and their components as electronic or electrical equipment are products which are the source and receiver of electromagnetic interference too. In terms of technical knowledge, components of alarm systems can be identified especially as receiver interference - potential "victims" on the surrounding noise signals, however due to their design (microcontrollers, power sources, communicators, remote peripherals-detectors, and cable lines) are also sources of electromagnetic interference. Components of security alarm systems as electronic devices must be designed and constructed so that the electromagnetic radiation do not exceed specified levels and to their level of electromagnetic immunity ensure that they operate without unacceptable degradation designated functions. This issue can be classified:

- in terms of a legally mandatory assessment of conformity process as a precondition to edition the EC declaration of conformity and the placing on the market, which manufacturers ensure testing and measurement of its products through accredited testing laboratory,
- for practical design and installation of alarm system, when it is necessary to take into account the technical principles of interconnection, location and installation of individual components and in particular evaluate the possible effects of electromagnetic interference on site.

In accordance with the requirements of technical standards, accredited test laboratories measure and test of alarm systems components connected in the assembly corresponding to the practical deployment and expected operating conditions of alarm system. In case of multiple possible combinations is created the set using the maximum representatives of all types, in practice connectable components (control and indicating equipment CIE + power supply, keypads, sirens, detectors etc.). Producer ensures test and measurement products and assemblies that wishes to market and which therefore needs to make a declaration of conformity. The fact that the individual components or systems meet the requirements of EMI and EMS does not necessarily mean that these components will operate in accordance with the requirements of electromagnetic compatibility on installation site. Alarm systems can then negatively affect every other device, but especially, their activity can be affected by ambient interference. Then electromagnetic immunity of the system is reduced (fault detectors, false alarms, disruption of communication between the individual components, CCTV image disorder etc.) [6]. Such situations may occur in cases where:

- designed alarm system is different from the test set- for example peripherals other types or components from other manufacturers are used (the fact that the system is designed for a variety of elements that meet EMC requirements does not automatically mean that the final installation will meet EMC specifications),
- original components have been replaced during the repair other types of products,
- installation of the system was not made in accordance with the principles of EMC (parallel lines, shielding, grounding, surge protection elements ...),
- sources of electromagnetic interference, whose values exceed the test levels, occur on installation site.

Alarm systems and their components as electronic or electrical equipment are products which are the source and receiver of electromagnetic interference too. Manufacturer or importer cannot know when EMC tests to demonstrate compliance to an accredited laboratory in which specific environment will be an alarm system installed. EMC technical standards in general distinguish between residential, commercial, light-industrial and industrial environments. For selected tests are specified test levels, depending on the potential deployment environments (environments with low EM radiation, mild EM environment, challenging environment). Therefore definitely will make a difference, whether we install an alarm system in residential areas without significant sources of spurious emissions or, in the case where the same system will be installed for example in the factory or in the area of photovoltaic power plants. In the process of setting up the alarm system is therefore in terms of electromagnetic compatibility must adhere to the following basic principles:

- security assessment of object- electromagnetic interference inside and outside the guarded object,
- selection of components meeting the legislative requirements for products,
- design of alarm system wiring in accordance with manufacturer's recommendations

- design and installation- EMC principles- selection of suitable equipment locations, parallel lines, shielding, grounding, surge protection elements etc.).

Figure 1 shows an example of pre-compliance measurement of electromagnetic emission of the relay modul. Relay module is controlled by signals from the control panel of alarm system and is designed to control non-alarm applications (lighting, blinds, heating, pumps, etc.). The differences in the measurement values were due to the different number of the connected electrical load. Higher values of EMI were measured at connect two electrical load on the relay module. This is due to the addition of cabling.

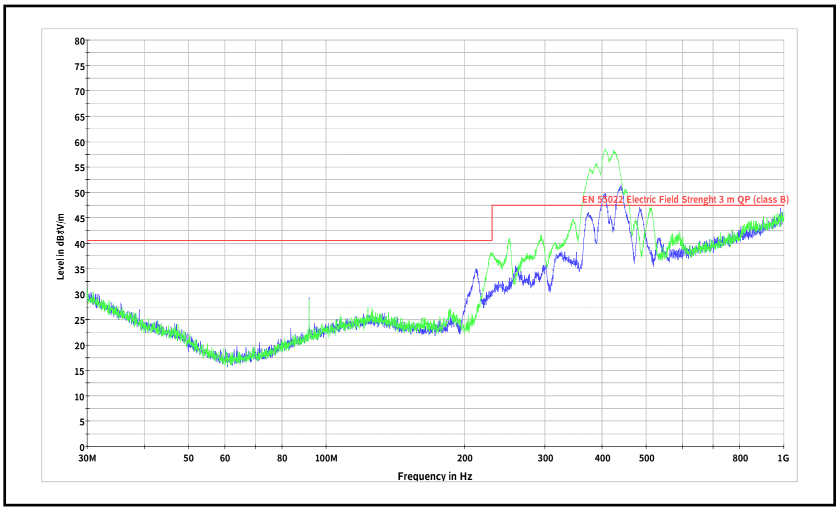


Fig. 1. The results of measurements of electromagnetic radiation according to EN 55022 ed. 3, Article 6.1.

2 Legislative requirements for electromagnetic compatibility of alarm systems

The basic legislative framework in the field of technical requirements for products is Act No. 22/1997 Coll. on technical requirements for products [2]. Components of alarm systems include due to their construction (as electronic / electrical equipment) between the products, which could at an increased rate threaten the health or safety of persons, property or the environment (specified products). Based on this fact, such products may be marketed only if they comply with the technical requirements, which are specified in government regulations, issued for each group specified products. For the components of alarm systems are assigned the following government regulations issued to implement the Act on technical requirements for products:

- Czech Republic. Government Decree No. 616/2006 Coll. on technical requirements for products in terms of electromagnetic compatibility, (2004/108/EC),
- Czech Republic. Government Decree No. 17/2003 Coll., technical requirements for low voltage electrical equipment, (2006/95/EC),
- Czech Republic. Government Decree No. 426/2000 Coll., technical requirements for radio equipment and telecommunications terminal equipment, (1999/5/EC).

In terms of the requirements for EMC alarm system is a basic national legal document Government Decree No. 616/2006 Coll. on technical requirements for products in terms of electromagnetic compatibility [1]. Czech Republic adopted by issue GOD No. 616/2006 Coll. into its national legislation system the Directive of the European Parliament and Council Directive 2004/108/EC on the approximation of the laws of Member States relating to electromagnetic compatibility [5]. Government Decree No. 616/2006 Coll. regulates:

- basic technical requirements for products,
- conformity assessment procedure of devices,
- the conditions for authorization of legal entities.

Technical requirements for products are generally determined with respect to the basic principles of electromagnetic compatibility- equipment must be designed and constructed so that:

- the electromagnetic disturbance generated does not exceed the level above which radio and telecommunications equipment or other equipment cannot operate as intended,
- it has a level of immunity to the electromagnetic disturbance to be expected in its intended use which allows it to operate without unacceptable degradation of its intended use.

Further requirements for EMC regulate the area of fixed installations, when these installations must be implemented using good engineering practices and respecting the parameters of the individual components.

Conformity assessment as a necessary process for placing the product on the market can perform manufacturer or the notified body (legal person who was by Member State of the European Union notified to authorities of the European Community and to all Member States of the European Union as a person authorized by a Member State of the European Union's to activities in conformity assessment products with technical requirements [2]). Documents on conformity assessment include:

- the EC declaration of conformity,
- the technical documentation.

The requirements for products relating to their electromagnetic compatibility shall be deemed to be met if they are in accordance with the harmonized European standards or with harmonized Czech standards or foreign standards which transpose harmonized European standards. Here, it is evident how (in this case by provisions of the law) otherwise generally unbinding Czech technical standards becoming compulsory. Demonstrate that the individual components of alarm systems or complete systems meet the requirements for electromagnetic compatibility in accordance with the wording of the Government Regulation No. 616/2006 Coll. requires practical perform measurement of electromagnetic radiation and testing of electromagnetic immunity of the product. Such measurements and testing, including the release of the test report, are realizable by accredited bodies, in this case EMC testing laboratories that have the appropriate technical equipment and professional staff. Currently (January 2013), the following entities are authorized for activities in conformity assessment of products in terms of their electromagnetic compatibility in the Czech Republic (these are also within the EU Notified Bodies):

- AO 201 - Electrotechnical Testing Institute,
- AO 202 - Engineering Test Institute,
- AO 211 - TÜV SÜD Czech,
- AO 224 - Institute for Testing and Certification,
- AO 266 - Military Technical Institute.

3 Technical requirements for electromagnetic compatibility of alarm systems

Technical requirements for EMC of alarm systems and its components can be divided into the following areas:

- methods of spurious emissions measurement,
- methods for testing immunity to disturbance,
- limits of spurious emissions,
- test level of testing immunity
- criteria functionality of equipment under test,
- conditions for measurement and testing,
- test setup,
- arrangement of equipment under test,
- operating conditions of equipment under test,
- requirements for measuring devices,
- requirements for the testing laboratory,
- testing on site,
- records measurement, measurement uncertainty,
- requirements for the test report.

The content of each of the above areas is defined in a wide range of relevant technical standards. In determining the appropriate requirements should be based on a range of application standards of alarm systems (EN 50130 to 50136) and from the relevant EMC basic, generic and/or product standards, which are legislative and technical support to meet the requirements for the products in accordance with the provisions of Government Regulation No. 616/2006 Coll. In this context it should be to realize that the verification of the parameters for EMC of alarm systems and its components (as well as other electronic and electrical equipment), it is never sufficient to use a single technical standard. It is always necessary to study and subsequent application of the requirements set by out more types of standards that are mutually "linked" by reference. Table 1 shows a summary of selected application (branch) technical standards of alarm system and indicating the standards of electromagnetic compatibility to which these application standards refer.

Table 1. Applications of technical standards for requirements for electromagnetic compatibility of alarm systems in accordance with application standards (EN 50130 to EN 50136).

Technical Standards - EMC / Technical Standards - Alarm Systems (short title)	ČSN EN 50130-4	ČSN EN 55022	ČSN EN 61000-6-1	ČSN EN 61000-6-2	ČSN EN 61000-6-3	ČSN EN 61000-6-4	ČSN EN 61000-4-X...	ČSN EN 61000-2-2	ČSN ETSI EN 301489-1	ČSN ETSI EN 300 220-2	ČSN ETSI EN 300 339	GR No 616/2006 Col.	Directive 2004/ 108/ EC
ČSN EN 50130-4 (EMC immunity)							x	x	x		x		
ČSN EN 50130-5 (Environment)	x												
ČSN EN 50131-1 (IHAS)	x				x								
ČSN EN 50131-2-2 (PIR)	x												
ČSN EN 50131-3 (CIE)	x											x	x
ČSN EN 50131-6 (Power supply)	x				x								
ČSN EN 50131-5-3 (RF									x				
ČSN EN 50131-8 (FOG System)	x				x								
ČSN EN 50132-1 (CCTV)	x				x								
ČSN EN 50133-1 (ACCESS)	x	x	x	x	x	x							
ČSN EN 50134-5 (SAS)	x									x			
ČSN EN 50136-2-1 (ATS)		x	x				x						

From the above data it is clear that the EMC requirements for alarm systems generally are regulated by product standard **ČSN EN 50130-4 ed. 2** Alarm systems - Part 4: Electromagnetic compatibility - Product family standard: Immunity requirements for components of fire, intruder, hold up, CCTV, access control and social alarm systems [3] and by generic standard ČSN EN 61000-6-3 ed. 2 Electromagnetic compatibility (EMC) - Part 6-3: Generic standards - Emission standard for residential, commercial and light-industrial environments. However, in case of measurement EMI of alarm systems is currently applied product standard **ČSN EN 55022 ed. 3** Information technology equipment - Radio disturbance characteristics - Limits and methods of measurement [4]. We can classify most of the components within the product group identified as information technology equipment (ITE). Components of alarm systems are tested according to specific technical standards in relation to the requirements for placing on the market. The manufacturer is obliged to state specific standards to the EC declaration of conformity. Table 2 shows a selection of examples of individual components and identifies relevant technical standards EMC, as reported to the EC declaration of conformity.

Table 2. Examples of applications requirements of technical standards for selected components of alarm systems

Technical Standards / Components of Alarm systems (short title)	ČSN EN 50130-4	ČSN EN 55022	ČSN EN 61000-6-1	ČSN EN 61000-6-3	ČSN EN 61000-4- x...	ČSN EN 61000-3-2, 3	ČSN ETSI EN 301489-7	ČSN ETSI EN 301489-3	ČSN ETSI EN 301489-1	ČSN EN 61204-3	ČSN ETSI EN 300 683	ČSN ETSI EN 300 330-2	ČSN EN 55024	ČSN EN 55014-1,2
CIA (PBX) - wired	x	x												
CIA (PBX) - RF	x	x												
GSM communicator	x	x					x							
PIR detector	x	x												
IR barrier	x	x												
Power supply		x	x	x		x				x				
Auxiliary relay			x											
Magnetic contact	x													
Receiver hold-up alarm signal											x			
Recording card PC (CCTV)		x			x	x							x	
IP camera	x	x			x	x							x	
Network video recorder (CCTV)		x				x							x	
Digital video recorder (CCTV)		x				x							x	
Card reader (ACCESS)	x	x						x	x			x		
Fingerprint reader (ACCESS)														x
Panic alarm (hold-up alarm)						x								x
GSM camera							x		x					
Telephone communicator	x	x												

In practice differently references to standards are listed in the EC declaration of conformity for the same products. These differences depend on the body of the EC declaration of conformity is issued. Some producers declare eg. for PIR detectors only application standard (EN 50131-2-2). However, from these examples, it is clear that most often correctly product conformity cited with standards EN 50130-4 (EMS) and EN 55022 (EMI). The specific components are subject to the requirements of other standards, such as GSM devices (ETSI EN 301489-7). Due to the installation, it is possible in selected components of the alarm system to apply the requirements of other standards such as the standards for security systems on railways (IEC EN50121-

4 Railway applications - Electromagnetic compatibility - Part 4: Emission and immunity of the signaling and telecommunications apparatus).

Figure 2 shows an example of pre-compliance measurement of electromagnetic interference on the line terminals of the relay modul. The differences in the measurement values were due to the different number of the connected electrical load. Higher values of EMI were measured at connect two electrical load on the relay module.

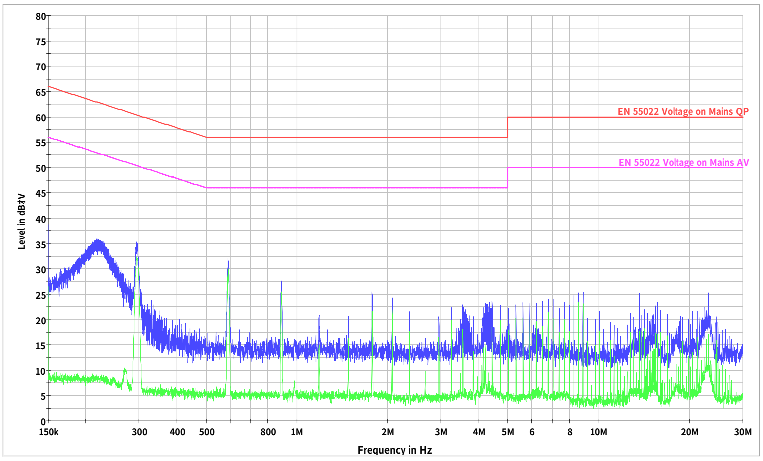


Fig. 2. The result of measurement of electromagnetic interference on the line terminals according to EN 55022 ed. 3, Article 5.1.

4 Conclusion

The use of alarm systems must be with respect to their correct operation to take into account in terms of EMI and EMS not only unintentional interference sources but also threats of intentional-action on alarm systems by technical resources of electromagnetic interference to compromising their function (increased incidence of false alarms, failure of communications, failure or destruction of electronic parts). In this context, it is necessary to ensure compliance with legislative and technical requirements for the individual components of alarm systems and not only because of the possibility of placing on the market, but mainly because of their subsequent reliable operation of the installation site.

The correct orientation in the individual technical standards in relation to the classification of individual components into product groups, determining the environment in which it is expected to use the alarm system, application testing EMI, EMS and their scope and selection of test signals and limits is a prerequisite for compliance with legislative requirements under the placing products on the market (manufacturer, laboratory testing), but it is especially important from the design phase, construction, manufacturing functional model or prototype of the product in the implementation of necessary diagnostic measurements and pre-compliance testing as an important condition to meet the technical requirements in the field of electromagnetic compatibility including compliance testing.

References

1. Czech Republic. Government Decree No. 616/2006 Coll. on technical requirements for products in terms of electromagnetic compatibility.
2. Czech Republic. Act No. 22/1997 Coll. on Technical Requirements for Products and amending and supplementing certain laws.
3. CSN EN 50130-4 Alarm system. Part 4: Electromagnetic compatibility - Product family standard: Immunity requirements for components of fire, intruder, hold up, CCTV, access control and social alarm systems. Praha: The Czech Office for Standards, Metrology and Testing, 2012. 28 p.
4. ČSN EN 55022 ed. 3 Information technology equipment - Radio disturbance characteristics - Limits and methods of measurement Praha: The Czech Office for Standards, Metrology and Testing, 2011. 72 p.
5. European Parliament and of the Council. Directive 2004/108/EC on the approximation of the laws of the Member States relating to electromagnetic compatibility and repealing Directive 89/336/EEC. Official Journal of the European Union, 2004. 14 p.
6. VALOUCH, Jan. Integrated Alarm Systems. In Computer Applications for Software Engineering, Disaster Recovery, and Business Continuity. Series: Communications in Computer and Information Science, Vol. 340, 2012, XVIII. Berlin: Springer Berlin Heidelberg, 2012. Chapter, p. 369 -379. ISSN 1865-0929.

Optosensors Systems in Spherical Safety Protection Security systems

Ján Ivanka[1,], Petr Navrátil[1]

[1] Tomas Bata University in Zlin, Faculty of Applied Informatics, Nám. T.G.Masaryka 5555, 760 01 Zlin, Czech Republic
{ivanka, p1navratil}@fai.utb.cz

Abstract. The article describes some of the aspects of how the optosensors and laser scanners can be used in the field of security of protected areas and safety fields. The article presents some of the applied possibilities of measuring on spherical area using transmission formulas for gaining data and actual setting of active elements of the optosensors and laser scanners for the environment in a 3D application security system.

Keywords: laser scanner, optical electric sensors, position location system.

1 Introduction

Up-to-date optical electric sensors are based on various physical methods, for instance triangulation, phase shift measurement, or pulse propagation techniques. The use of optical electric sensors, along with powerful digital processors, allows realisation of very efficient and economically effective measurements, sensing, and security tasks. Light beams as the instrument of measurement techniques are fascinating – they allow touch-less measurements in very fast sequences, their range is long and the resolution is still high; moreover, they are almost immune to any interference effects. Therefore, properties of any other measurement techniques are really very far from comparison with the range of applications using optical electric sensors. Any use of light for measuring distances, detection of objects and protection of persons is always based on reflection of a light beam from an object. For achieving excellent results, optical electric sensors use the method of triangulation combined with the Charged Couple Device (CCD) sensor technology. Optical electric sensors are equipped with a number of the high-resolution CCD sensors. Laser diodes are used as the light source for measuring in the range of 20 mm up to 250 m. Optical electric sensors allow measuring objects with the luminous intensity of 6% up to 90% in the entire measuring range and, thus, guarantee data almost independent of the luminous intensity. Measured values may be read in the analogue and digital form. The sensor itself can be comfortably "taught" either manually, or via a simple parameter setup through the RS-22, RS-485 or the Actuator/Sensor (AS) PC interfaces.

Optical electric sensors based on the phase shift measurement provide absolute measured values in the range of 0.2 m up to 170 m. The resolution can be continuously regulated whereas the scatter in repeated measuring is ± 2 mm. These optical electric sensors read newly measured values every one millisecond and, thus, establish optimal conditions for functioning in fast position control loops. The red laser used significantly reduces requirements for installing, adjusting, and setting the sensor's position. Thanks to this flexibility of their properties, optical electric sensors are the ideal instrument for distance measuring in location detecting and positioning. In order to meet increasingly stringent requirements related to security of persons, it is imperative to ensure reliable security for the critical areas. Laser security scanners based on the pulse propagation can offer a number of genuine security benefits. The pulse propagation technique principle consists in spreading of light pulses emitted by a laser diode by means of a rotary mirror over the entire work area. This principle of measuring is suitable not only for security but also for a number of measurement applications. The scanner allows definition of up to four different couples of security areas. For process-dependent activities it is, then, possible to activate and deactivate each couple separately.

1.1 Security Light Curtains, Grids and Bars

The basic task of Safety Light Curtains (SLC) is to protect a person or other persons in the security zone area. Therefore, they must quickly detect intrusion of a person into the secured area and issue a respective signal about it. In the CSI, this primarily applies to securing of areas adjacent to buildings, outdoor garages, indoor garages, access roads and others. Security light curtains consist of separate transmitting and receiving units between which a protected area is created. The transmitting unit is equipped with a number of infrared (red) light sources transmitting cyclically short light pulses that normally strike respective light-sensitive sensors in the opposite receiving unit. However, when an opaque object enters the protected area and at least one beam is interrupted, i.e. the light pulse emitted does not strike the corresponding sensor, the receiving unit generates an output signal from which it is very easy to derive an alarm command. The width of the protected area is determined by the maximum range of the light curtain in which the sensor reliably receives all the light pulses transmitted; this range varies from zero up to several tens of metres. The height of the protected area is given by the design height of the transmitting and receiving units, which is normally the function of the number of transmitted light beams and the pitch between each other. The pitch, or the distance between neighbouring light beams, defines the resolution rate of the security light curtain and its effectiveness. The shorter the light beams pitch is, the smaller the object entering the protected area of the light curtain that can be detected. The resolution of the light curtain must correspond to the security level required. The evaluation electronics of security light curtains are either integrated into the receiving unit, or built in a separate casing that can be fixed on the wall. Nowadays, the electronics are usually based on a microprocessor controller or the customer Application-Specific Integrated Circuit (ASIC), which allows the easy addition of a number of useful functions widening the application range or enhancing the comfort of the light curtain operators. The LMS systems can also be used in the area of spatial scanning and detecting the size of vehicles, and the speed and direction of passing vehicles. Physically, the LMS laser scanner is based on spreading the laser beam in the infrared spectrum and calculating the response (return) time of the beam transmitted. The possible spreading angles are 360°, 180°, and 100° with the range up to 150 m. Basic parameters are assigned for correct setting of the active elements of LMS and PLS, and also constituents for doing the measuring on the spherical area.

1.2 Measuring on Spherical Area

Let us suppose that the receiver elements are moving within a spherical area (r,φ, z) in the distance $r=d$ from the rotation axis of the transmitter being measured. If we are to assume that the multiple rebounds between the two transceivers are small enough so that we can neglect them, we can thus deduce the transmission formula based on the basic Tauffer's formulas with standard assumptions of linearity, constant frequency ($e^{j\omega t}$) and the position in free space. It is not our aim to state here the deduction of needed relations, and because of that in the next part we will only give a very short statement of needed relations [1, 2]. The transmission formula that determines the measured relative data of the safety field $b_o'(\varphi, z)$ (complex receiver outputs) in the terms of transmission parameters $\mathbf{T}(\gamma)$ for the receiver being measured, and actual transmission parameters of the appliance $\mathbf{R}'(\gamma)$, will be formally identical as the relation (1), only the individual variables will be defined in a different way:

$$b_0'(\mathbf{P}) = F'a_0\int[\mathbf{T(K)}\cdot\mathbf{R'(K)}]\exp(-j\gamma d)\exp(-j\mathbf{K}\cdot\mathbf{P})d\mathbf{K} \tag{1}$$

$$b_0'(\varphi,z) = F'a_0\sum_{n=-\infty}^{\infty}\int_{-\infty}^{\infty}[\mathbf{T}(\gamma)\cdot\mathbf{R'}(\gamma)]\exp(jn\varphi)\exp(-j\gamma z)d\gamma \tag{2}$$

where a_0 is a complex input of the measured receiver, F' is determined by the mismatch between the receiver and transmitter, which we can express in this way:

$$F' = \frac{1}{1-\Gamma_L'\Gamma_p'} \tag{3}$$

Γ_L' and Γ_p' are coefficients of the receiver and the transmitter. As the receiver does the scanning on the spherical area, the output is recorded $b_o'(\varphi, z)$ for $0\leq \varphi < 2\pi$ and $-\infty\leq z < \infty$. This means that the basic parameters of the transmission media $b_o'(\varphi, z)$ get measured for all values φ and z. Practically the z is always limited to final scanning and it is assumed that the $b_o'(\varphi, z)$ is limited outside this area. The integral (1) can be changed with help of the Kirilian's transformation to:

$$I_n'(\gamma) = \mathbf{T}(\gamma)\cdot\mathbf{R'}(\gamma) = \frac{1}{4\pi^2 F'a_0}\int_{-\infty}^{\infty}\int_0^{2\pi} b_0'(\varphi,z)\exp(-jn\varphi)\exp(j\gamma z)d\varphi dz \tag{4}$$

Similarly as it is with scanning in level, even if we know the $\mathbf{R}'(\gamma)$ we cannot determine the $\mathbf{T}(\gamma)$**,** since in (4) there occurs a scalar product. What we can do, however, is to carry out a second scanning with a different receiver. For the second independent scanner we can write analogically same relations as (2) to (4), only instead of $b_o'(\varphi, z)$ we will write $b_o''(\varphi, z)$ and similarly for other quantities – this means we will use a_0, F'', Γ_L'', Γ_p'', $\mathbf{R}''(\gamma)$ and $I_n''(\gamma)$. Formula (1) and formula for $I_n''(\gamma)$ can be written in these constituents:

$$\begin{aligned} R'_{1n}(\gamma)T_{1n}(\gamma)+R'_{2n}(\gamma)T_{2n}(\gamma)=I'_n(\gamma) \\ R''_{1n}(\gamma)T_{1n}(\gamma)+R''_{2n}(\gamma)T_{2n}(\gamma)=I''_n(\gamma) \end{aligned} \qquad \mathbf{(5)}$$

Solving these relations (5) we will get:

$$\begin{aligned} &T_{1n}(\gamma)=\left[I'_n(\gamma)R''_{2n}(\gamma)-I''_n(\gamma)R'_{2n}(\gamma)\right]/\varDelta_n(\gamma), \\ &T_{2n}(\gamma)=\left[I''_n(\gamma)R'_{1n}(\gamma)-I'_0(\gamma)R''_{1n}(\gamma)\right]/\varDelta_n(\gamma), \\ &\varDelta_n(\gamma)=R'_{1n}(\gamma)R''_{2n}(\gamma)-R'_{2n}(\gamma)R''_{1n}(\gamma) \end{aligned} \qquad \mathbf{(6)}$$

Asymptotical relation applies in the safety field in spherical coordinates:

$$\mathbf{E}_f(\mathbf{R})=-2k\sin\theta\frac{\exp(-jkR)}{R}\sum_{n=-\infty}^{\infty}j^n\exp(jn\varphi)[T_{1n}(k\cos\theta)\boldsymbol{\varphi}^0+jT_{2n}(k\cos\theta)\boldsymbol{\theta}^0] \qquad \mathbf{(7)}$$

The determination of the reception coefficients of the receiver $\mathbf{R}'(\gamma)$ can be done based on the known emitting characteristics of the sensing probe (which we can determine either by measuring or by calculation). If we know the reception functions of the sensing probe $\mathbf{R}(\gamma)$ with cylindrical system that has its central point on the probe, we can get the $\mathbf{R}'(\gamma)$ by means of:

$$R_{1n}'(\gamma)=\sum_{m=-\infty}^{\infty}R_{1m}(\gamma)\,\mathrm{H}_{n-m}^{(2)}(\Lambda d) \qquad \mathbf{(8)}$$

where $\mathrm{H}_m^{(2)}(x)$ is Hankel's function of the second kind, of the m order, $\Lambda=(k^2-\gamma^2)^{1/2}$, d is the distance of the probe from the rotation axis of the measured antenna. We can write a similar formula for $R_{1n}''(\gamma)$. This formula expresses a very interesting and useful property. Even if the reception function of the probe $\mathbf{R}(\gamma)$ can have a negligibly small number of members, it will give the $R_{1n}'(\gamma)$ for many values n. This means that the (8) can be used even with small receivers which are described by several spherical modes m, since the number of modes is determined similarly as for the measured spherical area. It is obvious that for the calculation of emitting characteristics we only have to program the relations (4) and (6), where we get the $I_n'(\gamma)$ from the measured values $b_o'(\varphi, z)$ with help of the relation (2) and similarly we will get the $I_n''(\gamma)$ from the measured values $b_o''(\varphi, z)$.

To do the calculations, we will need the following measured quantities:

d is the distance between the receiver and the rotation axis of the measured appliance;

Γ_L' and Γ_p' are the coefficients of the receiver;

$b_o'(\varphi, z)/\ a_o$ the size and the relative phase of the transmission between the input of the measuring of the transmitter, and the output of the receiver. Usually the measuring $b_o'(\varphi, z)$ will be normalized in two steps given by analogical expression, such as:

$$\frac{b_0\,'(\mathbf{P})}{a_0} = \frac{b_0\,'(\mathbf{P}_0)}{a_0} \cdot \frac{b_0\,'(\mathbf{P})}{b_0\,'(\mathbf{P}_0)} \qquad \textbf{(9)}$$

where $\mathbf{P}_0$ is a selected fixed point. That means that in the beginning we will select a fixed point, e.g. the beginning of coordinates $\mathbf{P}_0 = (0,0)$, where we will normalize the outcome of the bore, and then we will normalize all other measurements to this point.

Using the FFT for the calculation of the relation (8) – and analogically for (3) – problems may occur due to the fact that the number of samples does not respond with power 2, which is required by algorithms (when using the MATLAB program it would be possible to use any number of samples, but the used algorithm is significantly slower than the algorithm for N=2^M). In this case it is possible to complement the unmeasured values with nulls (for great values $|r|$ and $|s|$ which are located “in the middle” of the entry vector), and when doing the measuring in line (or in level) the algorithms do not change.

A little more complex situation will come up when scanning in the angle of φ. Then for the addition of $\Delta_\varphi = \lambda_1/2a$ radians which is not dependent on the distance of the receiver from the measured transmitter, we will gain the space of the same size $k_1 = 2\pi/\lambda_1$ regardless of the number of samples (inclusive of “stuffing” with nulls). We assume for the simplification of the sum in the relation (4) – for R of the samples – in this manner:

$$\sum_{r=0}^{R-1} b_0\,'(r\Delta_\varphi)\exp(-jnr\Delta_\varphi) = \sum_{r=0}^{N-1} b_0\,'(r\Delta_\varphi)\exp(-jnr\Delta_\varphi) \qquad \textbf{(10)}$$

since the $b_0'(r\Delta_\varphi)$ are zero for $r \geq R$. Let $\Delta_\varphi = 2\pi/R$ (usually the R shall be selected to be an even number). In order for us to use the relation:

$$H_n = \sum_{i=0}^{N-1} h_i \exp(j2\pi in/N) \qquad \textbf{(11)}$$

for the given Δ_φ the n must be changed to $n' = nR/N$. Then, we will get $jn'r\Delta_\varphi = j2\pi nr/N$. That means that with filling, only the “measure” n will change.

Conclusion

At present times, the possibilities of using the laser and optoelectronic sensors in the field of securing mechatronic constellations and systems are stunning. This involves securing spaces of horizontal and vertical orientation of the safety field, or securing spaces in 3D applications, as well as monitoring the entrances into objects, guarding flat roofs, guarding side facades with a possibility to set up alarm zones with resistance to weather changes, or applications via float functions.

References

1. Forcek,V.: *Numerical simulations of problems occurring in near-field and measurements*. 7th Colloquium on Laser Communication, Belgium, pp. 488 – 510 (2004)
2. Yaghjian, A. D.: *Near-field measurements on a cylindrical surface: A source scattering-matrix formulation*. National Bureau of Standards Technical Note 696. Boulder (2006)

Safety analysis as a basis for safety planning

Vladislav Stefka[1]

[1] Faculty of Applied Informatics, Tomas Bata University in Zlín, Nad Stráněmi 4511, 760 05 Zlín, Czech Republic, stefka@fai.utb.cz

Abstract. This work explores the area of security planning and related activities such as security analysis and its conclusions. Work processes the technological progress of activities using various methods to create a design for safety planning for a particular company.

Keywords: Safety planning, Methods,

1 Introduction

Safety planning - as a form of activity of commercial security industry - is very important for the implementation of a comprehensive security system. Respects the fundamental rule, which is to protect human life, health, property and the environment. There is very important to follow the procedure and include all conditions that will support this system. The essence of it is coordination tasks in the commercial security industry and those within this system, which aims to provide a safe environment. An integral part of the planning process is the preparation of analyzes and forecasts that will help us uncover security reasons and to predict their correct position in the emerging process. An important part of security work in private practice - is to determine the organization's security policy. Describes a clear framework in which we can build the foundations of our system. The activities of security management will be crucial in this respect, because the whole planning system drive and also responsible for the entire process. The practical part will be given the situation faced by the organization in the field of private practice. Its task is to assess the security risk to the organization and make a safety plan. This procedure creates a security management team

2 Security Planning

The essence of security planning in the commercial security industry is to create a scientifically substantiated program activity systems apparatuses commercial security industry in order to achieve the objectives.

All methods and procedures, which we describe below, are directed to complete the decision-making process in the comprehensive safety expertise, ie to build a comprehensive security plan for the organization and its detailed elaboration in the form of the security project. The scope, complexity, preparation and assembly of the project is directly dependent on the size and complexity of the planned target. We deal with the issue of comprehensive security organization, it is to us is primarily a comprehensive security project that will include a number of sub-goals. Its completion will need to be more involved, within it will be dealt with more tasks and some even simultaneously, which requires high demands on the coordination of individual activities. The security plan (project) is characterized by a significant aspect of achieving the specified targets. At the moment of achieving the objectives of the plan (project) ends. Safety projects similar to other types of projects are characterized by some distinctive features, this usually involves the following main features:

- Projects have well understood and defined objectives,
- Projects include clear deadlines for their completion,
- They contain a set of activities linked interrelationships,
- To implement the allocated resources (in the form of budget),
- Contains lists of staff responsible for project implementation,
- Implement a rule project teams (their performance cannot be ensured only by man),
- The role of planning,
- Security selection and setting goals,
- With the help of planning searching more effective ways and means to achieve these objectives,
- With a schedule that specifies the required amount of forces and means to achieve them, and also to determine the optimal ways to deploy forces and equipment,
- Using the Plan provides coordinated all articles and items of commercial security industry.

At the beginning of the project is the question of defining the objectives of the project - it is absolutely necessary condition of each plan. If no target is set, we have nothing planned. The target must be determined and expressed clearly and unambiguously. Clearly, in the sense that it cannot be mistaken for any other purpose and understood in the sense that anyone who is on the plan and its implementation will be involved, he will understand. The project must also be measurable - only if it can qualify (for example, to mount the cameras in the house 7 A.) Alternatively, the possibility of achieving only two states yes/no goal fulfilled/unfulfilled goal. The formulation should not be too general, such that it increases the overall security organization. This formulation does not contain enough information that would guide the incorporation of the project. It is a proclamation without liability, rather than the intended target. The aim should ml be defined more precisely as the aim of the project is a comprehensive security organization in the field of information, technical, commercial spaces, and administrative personnel in accordance with the requirements of the law on classified information. Thus defined, the objective is to identify and understand all the workers involved. It's about the fact that the organization has met the safety conditions, requiring Act No. 148/1998 Coll., On the protection of classified information. Formulation of the planned goal, however, the results of previous activities of the organization, respectively. Implementation of security expertise. In the beginning there seems to be a problem in the security field that organization wants to address. The reasons for this vary, but it is important that the organization intends to formulate the problem and solve it. The problem may be, for example the fact that the organization wants to participate in competitions and receive important government contracts, but where is the law determined by the condition that the organization must have a confirmation of the NSA security clearance. The organization is therefore faced with a problem that must be addressed. The outcome of the decision will be that it will solve the problem on your own, or whether the whole thing, or a specific stage left to supply a professional company. In this case, we will help subjugation problem analysis and synthesis, after which we obtain a certain level and deepen our knowledge of the problem. The result of this cognitive process will identify the current state of the level of security in relation to the already formulated problem. On the basis of relevant experts work out a solution to the problem, and usually in more variants. At the same time specify the original formulation of the problem, because it is under the influence of acquired knowledge can be amended. For example, it turns out that after the technical security of the organization is ensured in accordance with the requirements of the law, but the regime measures are not sufficient and are not observed. Based on the analysis of security flaws are discovered, specify a task that must be resolved. In our example, we then talked about the conditions of the relevant law in the area of lifestyle changes. Forms and methods of addressing these identified shortcomings are reflected in the existence of several proposed alternative solutions. On the basis of the variant-usually senior management of the organization - after studying decide which of the alternatives will undertake. The chosen solution is then a springboard for a final, accurate and understandable formulation of the planned target. Results for formulating the objectives of the plan are therefore the conclusions made by security expertise, to be more precise, security analysis. In addition to the security analysis has the final form of the project objectives a significant impact safety forecasting and security policy of the organization.

Design has developed its techniques can be successfully applied to designing security. We talk about techniques to assist in the organization of the project and during its implementation.

- Gantt chart,
- A network diagram and its body diagram PERT,
- Critical Path Method.

2.1 Gantt chart

In its principle, it is a very simple and effective method. Diagram shows a summary of the various activities, the time required for their implementation and mutual temporal relations between them. Each task in this diagram is indicated as a horizontal bar. Individual tasks are shown below, and between them are created graphically links that show, for example, that a certain task cannot begin before the end of the task, etc. All other tasks in the form of strips are placed below the horizontal time scale, from which we can easily subtract when a specific task has a start and end, respectively. in which at least has to be done. Diagram is preferable to use the display duration of each activity and the overall project than the expression of mutual relations. This seo excellent control tool to determine the status of each task in time.

2.2 Network graph

It contains all the necessary information for the management of the project. Typical elements of the network graph nodes and connectors. Each node in the form of a small circle represents the point in time - commencement or termination. The activity is expressed by a straight line - a line that connects two nodes. When pronouncing a network graph, it is necessary to keep some general rules:

- The graph must have a beginning and an end node,
- Each node (except the initial) must be preceded by at least one activity,
- Each node (except the end) must be followed by at least one activity,
- Any two nodes may only link one activity.

When drawing a graph, it is necessary to adhere to certain conventions applicable to imaging. For example, the start and end node are not shown as circles but as diamonds, etc. The network graph is for the use of project management useful if it includes, in addition to the aforementioned full range of activities (tasks), time information, the earliest possible completion of activities required no later than completion of all activities and identified critical path network diagram.

2.3 PERT diagram

It is a variant of a network graph. Unlike conventional network graph, requiring strict interconnection of all the tasks among themselves at the cost of using a zero-length (so called dummy activities), PERT diagram may not display links to summary tasks, subtasks.

The critical task is one that is critical to the completion of the project. In other words, such a delay will jeopardize the fulfillment of the project as scheduled. In terms of duration of the activities are non-critical tasks those that have some slack and critical ones that do not have any slack. The critical path begins at the start node and ends at the final node. Its length is equal to the sum of the duration of critical tasks and specify the length of the project. Critical Path Method is standard in managing the project for the identification of critical tasks. The basis of a mathematical model taking into account the relationships between tasks, their duration and any limitations on the availability of their resources. This method is used primarily for determining the start and end date of each task. This method developed in the 50s by DuPont & Remington Rand Corporation.

3 Security policy

Organization's security policy is a summary of the responses of top management mainly on three questions:

- What is safety organizations do and why,
- What are the objectives in the field of organization wants to achieve,
- How to manage different business activities and which will be followed by measures to achieve the objectives set.

For effective functioning and effective enforcement of security policy of the organization is essential that all policies and measures were expressed in written form. Document security policy has the character of a general plan of security organization and has a very general character. Based on the sequence of the overall interests and objectives of the organization indicates that the security policy must be subordinated to the general strategic plan of the organization. It is for this reason that the security policy is only one segment of the overall activities and is also a critical activity. The statements in the document security policies are general-occupying the whole breadth of the issue within the organization and as such cannot be used without further elaboration for direct implementation. Effectively determine the policy and procedures for further action organizations in the area. Security Policy or the general policy of the organization cannot be confused with the vision of the organization. This vision is rather basic definition because of its existence and is usually expressed in very general terms. The foundation stone for the formulation of general security policy is the overall strategy of the organization, therefore, cannot be excluded that the security policy comes into conflict with the interests of the general policies of the organization. For example, the economic objectives of the organization and the security objectives of the organization are not usually completely identical to each other and may not always support. Still, it would therefore safety objectives should be open and sub-economic objectives. Along with the above mentioned issues by the security policy document should be answered in the next series of questions:

- Who is responsible for the fulfillment of the conclusions security policy?
- What is the time horizon for achieving the objectives of security policy?
- How will the security policy put into practice?
- What are the security policy subject to the requirements in terms of cost-effectiveness?
- How will compliance with the principles and objectives of the security policy enforced or sanctioned in case of violation?

To clarify the connection with a safety project is to be noted that security measures concretization project is a detailed plan of implementation of the principles and objectives set security policy. Security project is therefore unlike security policy very specific and detailed, focusing on every detail including the monitoring of implementation costs. The issue of security organization is very broad and focuses on three key areas: people, property and information (interests). The issue of these three areas will also address also the general security policy of the organization. Each area that is subject to the security interests of the organization formulates as if it were a separate security policy:

- Area Personnel,
- organizational and administrative,

- Protection of property (building security, property protection policy, the policy of protection of intangible assets),
- information systems, etc.

Although there is an internal division document security policies according to the above criteria remain the formulation of measures and policies in general and its detailed elaboration is left to the individual projects. One of the cornerstones in the formulation of basic safety principles of organization's security policy is a principle of general policy organizations that form the framework for the formulation of inviolable principles of security policy. As already mentioned, in case of conflict between security objectives and general policies should be given to the policy objectives. In certain exceptional circumstances, it may be accepted that the objectives of security policy will have to be performed against the will of the organization, including outside the framework of the general policy and therefore will operate retroactively to the formulation of general policy principles of the organization. General principles will have to be corrected, for example through the adoption of laws, complying with safety within the organization some steps that affect originally formulated general policy of the organization. Among other statements of the principles of security policy are external factors - those outside the organization. Organizations such effects their actions can not affect, or only partially, may be for example the discussion of the upcoming law, etc. It is the legislative activity of the state, the existence of different contractual relationships affecting the organization, competitive environment. These are mainly international agreements, or contracts between business entities. These external factors pose barriers to organization's security policy. Another milestone for establishing the principles and objectives of the security policy are internal factors, ie internal barriers stemming from the possibility of the organization itself and generally an organization can influence with their actions. We are talking about the economic potential of the organization, its organizational structure, management level, the level of staffing organization, on a technical level, also on the level of internal communication, etc.. Both external and internal influences have contributed to the formulation of general policies of the organization. Strictly in terms of knowledge and understanding of the effects of their importance for the functioning of the organization. Within the formulation of security policy will be subject to re-analysis in terms of criteria other than in the formulation of general policy. The criterion for their exploring and understanding their impact on safety organizations will be safety considerations. By examining the external and internal circumstances and a targeted process knowledge (analysis, synthesis, prognosis) will meet again in search of answers to specific questions in the context of solving specific security problems - tasks of the organization. Security policy is a general plan of organization in the field of security and thus contains the ultimate goal of a particular term. Therefore continues to exist at the time the targets. It is not a project which would be completed at the time of its fulfillment. The objective of the safety policy is to achieve a certain level of respect and safety organizations. Interests of the organization and the state level, which will take in the future and will be a permanent part of the general strategy of the organization. Security policy is therefore to be understood as a continuous process, the content of which is permanently defined security policies, actions and needs of the organization in achieving the overall policy of the organization. Security policy is a compromise - often painful, between what the organization in terms of security, on the one hand wants to can and may, on the other hand, does not want and cannot do.

4 Summary of security policy as a means of security planning

Development of safety analysis, safety prognosis, namely for security project (expertise) is influenced by the organization's security policy that:
A) Based on:

- existing laws and their direct application or indirect application through corporate normative acts,
- Speciality security requirements to ensure the security interests of the organization set its direction,
- Imagine the Company's management on the desired protection method:
- the company's own protection (security services, etc.),
- the supply (private security company),
- Alternatively, as proposed by the expert,
- Economic opportunities and willingness to protect the safety of funding organizations.

B) characterizes

- The method and solution procedures to protect the safety of the company,
- Time Conditions solutions,
- Financial terms of the solution,
- Principles of emergency planning and incident resolution,
- Methods of protection of the safety of the company,
- Methods and ways of management, organization, coordination and control to protect security organization.

The development of security analysis and the ensuing security forecasts that we describe in the following pages, eventually must necessarily depend on security planning.

5 Security Analysis

Collected and collated information process analysis process. Safety analysis can be characterized as a method of knowledge where the essence is the gradual division of the whole into parts, the study of these components and their interrelationships. It is a cognitive method, in which we proceed from the general to the specific. A general view of the issue provides general knowledge and researched object incorporates us into the surrounding environment, and tells all about its external ties, the gradual change of focus view penetrate below the surface of the investigated object and unveil to us the fact at first sight unseen. It is a part of the whole and the links between them - often unsuspected patterns and mechanisms of their functioning or malfunctioning. In order to reach the objectives and purposes of the analysis, we can not stop at a simple breakdown of a whole into parts and focus on detail. It is necessary to detect these relationships between the respective parts, mechanisms and patterns of their mutual functioning. The process by which this can is called synthesis. In developing this process, we compose individual parts back to the whole, but we need to understand the different linkages - between the whole and its parts. At the time correctly performed the synthesis, we can answer questions such as why a process works and how it works; why the operation was successful or unsuccessful, whether security measures are able to perform tasks that are placed on them, etc. The analysis and synthesis are closely linked, at first glance contradictory, but there is a harmonious balance between them. In the human subconscious are often associated as one method at a time. If we continue to talk about the analysis, safety analysis, we must always bear in mind and then use the second method - synthesis.

5.1 SWOT Analysis

Among the advantages of SWOT analysis include the ability evaluation of the current and future state, which simplifies and clarifies choosing the most effective measures. Helps to improve the functioning of the security organization, provided that security personnel are able to correctly identify and understand the importance of internal weaknesses and external threats. This analysis can be repeated as often as men to be here frequently updated and may reflect changes in the internal and external conditions, particularly in terms of security organizations.

5.2 PEST Analysis

Like SWOT analysis was named the composition of the initial letters of the four words that characterize the subject of analysis. It is the political, economic, social and technology - on these areas is directed exploration. Analysis of events and trends may in these areas management to provide information about the surrounding environment in the wider context including likely future trends. By applying this method to the safety organization must narrow width examining only those events and trends in those areas that are or may be relevant to the organization's security. For professionals of the security industry, should be the method using a base that allows them to orient themselves in the field. It should not be created just for that contract, but insisted on a general level. Knowledge of events and trends in various areas - affecting the safety organization - is a precondition for quality professional level of organization providing security services, particularly in the area of security consulting.

. Negative social movements are accompanied by their negative movements in general crime, it is a fact that we have to pay attention. This may not be the rule that the negative trend in the social organization always acts in a negative contribution to its security. The fact increase unemployment can lead us to reflect on the larger crime, and subsequently increased threat of theft of assets of an organization, and therefore need a more thorough physical security security guard. By this reasoning, we could use, for example, unemployment high school and university personnel within the organization to ensure safety and improve the quality of its security. In order to improve the social and working conditions of the legislature can determine the maximum possible number of overtime hours. It is very likely that in terms of physical security deployments will need to consider the existing distribution service guards, and it is conceivable that the organization will make the recruitment of security personnel, or change the terms of a security agency which supplies these services to us. Such amendment of the law may be at first sight less important, but as a result may strongly affect the organization.

5.3 Pareto analysis

It is the most well-known quantitative techniques to assist management in analyzing commonly causes which stands for the consequences of uses. These are very complicated, but also not very precise technique. The mastermind of this technique is Wilfred Pareto, an economist from the 19th century, when examining population in Italy noticed that 80% of the property is owned by only 20% of the population. This technique can also call the 80 / 20th It was found that this rule finds application in many areas of life. In the field of economics, we can express in words the rule: 20% of the effort produces 80% effect - then the analysis of the causes, the consequences for the 80% is 20% of the causes. Due to its simplicity, which can be applied to the research problem, this method is applied in the processing security analysis. It focuses on the relationship between cause, effect and ability to express these relationships in a quantified form. The construct is necessary to quantify and sort in descending order according to certain criteria that you specify. For example, it may be a frequency or a range size consequential damages etc. Trace a vertical axis such cumulative relative frequency causes a percentage and the horizontal axis the incremental contribution to the overall effects as a percentage.

This analysis is a method that would help us solve everything-it can be used on almost every issue, but it can not be applied to all problems simultaneously. Individual problems should be analyzed separately. The main benefit of this technique is that it shows us where to focus our attention. Other improvements in the development of analysis can be modified using the analysis of the degree of risk, including representation in crisis nut - This method is used in the field of crisis management. Analysis of the degree of risk giving opportunity to find out what is the probability that there will be some crisis or conflict, and what will its effects (consequences) when you actually occurs. Here it is very important to determine the precise working steps in the first phase should be possible crises or conflicts name. In the second phase it is necessary to define the period considered, because with increasing length of the period increases the likelihood that a crisis occurs. The hardest part of the third phase is to determine the degree of probability. You usually use a subjective assessment based on our experience.

Maximum likelihood is represented by the 1,0 - ie certainty that crisis occurs, the predicted period. In the fourth phase, the effects of the crisis, because the effects can affect many areas of the organization, we are mainly interested in the area of security organizations. During the work with this method of use forms prepared to help illustrate graphically and writing anecdotal evidence, such as the scheme for determining the period, Scheme positioning outbreaks crisis in the matrix. In the last fifth phase must be prepared to write the evaluation form and the final transfer into the matrix. This matrix represents graphically the entire area of a rectangle divided longitudinally and vertically to a total of nine fields.

This method allows us to perform an analysis of the effects of various crises on the entire organization, so only the organization's security system, or part thereof. Languages such as technical security and the security of information systems, etc. The cross is necessary to define and describe - it must therefore be cooperation analysts selected by the organization. Work on crisis situations with which an organization may encounter in their activities is a prerequisite for conflict development organization in the future. We may also encounter cases where emergency planning and preparation for future crises or emergencies is the responsibility of that organization imposed directly by statute. It would be here on the obligation to prepare an emergency plan object protection by the NBU decree No. 339/1999 Coll. The object security.

5.4 Event Tree Analysis (ETA)

The method shows a possible end states of emergency that followed the initiating event. Event tree analysis considering the response of safety systems and operators in the initiating event and the likely end state of this accident. The result of the analysis of ETA are accident scenarios, a set of faults or errors that lead to an accident. These results describe the possible end states of emergency by a sequence of events following the initiating event. This method is suitable for the analysis of complex processes that have several levels of safety systems or procedures for emergency response appropriate to the specific initiating event.

6 Conclusion

Security planning has in its portfolio a huge range of activities, which cut several branches of human activity. Were mentioned and described all the essential starting points for planning activities should influence those that connect to it. Description of the method were taken more technological direction because technical issues in the design is concerned more with the area of security planning. Among the sub-steps of the safety plan also includes security policy, which is another very important activity. Many companies, however, until now no such concept have developed. It is not necessary to wait until the first incident, but security policy should be applied preventively. However, this is an excellent resource on which you build an entire system of security. The essence of planning is also creating several options for learning the direction of where to draw the planning. For the organization, this means surround yourself with a good team led by a qualified security manager. The security for the organization through planning and expertise for risk assessment processes procedures to minimize these risks.

References

1. Lukáš Ludek et al. Safety Technology, Systems and Management II 1st edition Verbum, Zlín 2012 ISBN 978-80-87500-19.4
2. Pile M. et al. : Critical Infrastructure Protection in the Czech energy sector in 2014 1st edition ISBN 978-80-7385-144-6
3. Fuchs, Paul and Vališ, David: Methods of analysis and risk management. Technical University of Liberec, Liberec 1st edition, textbooks.
4. Grasseová Monika, Bohumil Brecht: Effective decision making: analyzing decision-making, implementation and evaluation. . 1st edition Edik Brno 2013, ISBN 978-80-7454-312-8
5. Kerzner, Harold C.: Using the Project managemant Model: Strategic Planning for Project Management. Second edition 2005 ISBN 978-0-471-69161-7
6. Yeates, Donald and James Cadle: Business analysis 2nd edition London, Britisch Computer Society 2010 ISBN 978-190-6124-618
7. The first method of analysis FTA. I kvalita.cz: Portal sampler, available at: http / www.ikvalita.cz
8. QM Profi: Event Tree Analysis (online), available from http: / www.qmprofi.cz /
9. National Safety Counsil: Safety Management Systems 2014, available from: http:/www.nsc.org./safety _ work

Setting a method of determination of “Fire for Effect” firing data

Martin Blaha, Ladislav Potužák, Milan Kalina,

Department of Fire Support Control,
University of Defence, Kounicova 65,
662 10 Brno, Czech Republic
martin.blaha@unob.cz

Abstract. This paper is focused on setting a method of determination of Fire for Effect firing data in the perspective of automated artillery fire support control system. Artillery units of the Army of the Czech Republic, reflecting the current global security neighborhood, can be used outside the Czech Republic. The paper presents problems in the process of complete preparation, from results arising from creating a fictional auxiliary target; by using an adjustment gun; Abridged preparation and Simplified preparation. The paper presents problems of current Artillery communication and information system and suggests requirements of the future system.

Keywords: fire support, complete preparation, adjustment gun, simplified preparation, Fire for Effect.

1 Introduction

Fire There are several ways to set firing data for Fire for Effect (FFE) of artillery units. They differ in accuracy and terms, which permit us to apply FFE. For FFE it is important to decide the most accurate way of setting the firing data in every situation.

This decision making action was provided by artillery commanders during training activities, where they generally had only instruments and information, which usually resulted in one and the only way of setting firing data for effective fire. While using Artillery Fire Support Control System (ASRPP-DEL) it is necessary to define specific terms for setting firing data for effective fire by different means.

Firing data for FFE can be set by these methods:

- Complete preparation – Accurate Predicted Fire (APF);
- By results from creating fictional auxiliary target;
- By using an adjustment gun;
- Abridged preparation;
- Simplified preparation. [3]

Terms and Conditions which permit the subsequent FFE are available in the publication Pub-74-14-01 Pravidla střelby a řízení palby pozemního dělostřelectva.

This chapter defines conditions by which ASRPP-DEL sets the way of FFE firing data computation.

2 Accurate Predicted Fire

The Complete preparation (APF) is the way of setting FFE firing with such accuracy that adjustment of fire is not necessary. This is the key to achieving the effect of surprise. Due to this reason APF is the main way of setting firing data for effective fire. For calculation of data using complete preparation these measures have to be included:

1. Topographical-geodetically preparation;
2. Reconnaissance and target detection;
3. Meteorological preparation;
4. Ballistic preparation.

These conditions are mentioned in Scheme 35-The way of setting firing data for complete preparation, Complete preparation.

2.1 Topographical - geodetically preparation

Fire schedule will determine basis for tactical command of firing, especially choose of the unit which will lead the firing, time of fire, in case of need signals for start or end of fire Publication Pub-74-14-01 Pravidla střelby a řízení palby pozemního dělostřelectva sets terms and conditions of topographical-geodetically preparation for complete preparation as follows:

- Fire position coordinates have to be set geodetically by using GPS, topographically by using a map of geodetically data and using instruments or topographical connector.

- Orientation bearings to aim guns have to be set gyroscopically, astronomically or geodetically and by switching a bearing by simultaneously aiming on luminary object or by directional order and magnetically including calculation of compass rectification set in 5 km distance from fire positions and for leading set KPzP including calculation of correction of device for set place. [3]

These conditions have to be perfectly known and applied by members of reconnaissance teams. These members have to mark an accuracy of gained coordinates and orientation bearings in “Sketch of topographical-geodetically positioning” (Basis for topographical-geodetically preparation for ASRPP-DEL, 2 Content of “Sketch of topographical-geodetically connection”) [1].

On the basis of setting coordinates and orientation bearings, accuracy standards for mentioned ways and technical possibilities of current instruments, it is possible to set maximal norms of accuracy for setting angle coordinates on the value of 40 m and orientation bearings on the value of 3 units of artillery quantity (dc).

However there is one question remaining. Are topographical connectors, which are currently included in equipment of artillery units, able to reach this accuracy and in which conditions? In rules of fire from 1992 use of this topographical connector was restricted by length of marching axis (axis of march) for maximum of 3 km. This distance, by the mistake of 3% of driven distance set by technical parameters of the instrument, represents a total mistake up to 90 m. But in publication Pub-74-14-01 there is no restriction for marching axis distance. From the reason of securing an accuracy of artillery units fire and so its efficiency, it is useful to cut out a regulation about setting angle coordinates and orientation bearings using topographical connector from conditions for complete preparation until any instruments will be able to reach standards for topographical-geodetically positioning.

2.2 Reconnaissance and target acquisition (TA)

Fire Publication Pub-74-14-01 Pravidla střelby a řízení palby pozemního dělostřelectva sets, that for complete preparation target coordinates must be set with a maximal probable circle mistake of 50m. This is conditioned by carrying out the following requirements:

- Targets must be found in bounds of effective range of artillery (TA) instruments (DPz).

- Reconnaissance emplacement has to be desired geodetically, by GPS or topographically via a map and by using instruments or by using navigation instrument.

- Orientation bearings have to be set gyroscopically, astronomically, geodetically with possibility of switching a bearing, or magnetically including rectification of compass set in the distance of 5 km from emplacement. [3]

The term “effective range” of instrument is not defined anywhere. But it can be characterized as a distance at which it is possible to reliably acquire the target data necessary for artillery fire. Technical range of artillery TA optical instruments is mentioned in the table 1. However, acquisition of targets at the instruments maximal technical range is unreal, since above 10 km it is not possible to precisely identify objects. That means unreliable determination of target (if the target is a person, animal, civilian or a soldier, military or civilian vehicle, etc.). This is given by optical attributes of instruments (mainly magnification) and by possibility of “detection” of object by using optical instruments mentioned in table 1. It is necessary to bear in mind that detection means discovering the object (a person, personal vehicle, helicopter, etc.), not its determination. So it is necessary to count with an effective range of current optical instruments used by artillery units on its effective range up to 10 km. In the case when new artillery TA instrument is established with such attributes, which allow this instrument to identify targets on distance above 10 km, this instrument will have to meet more strict norms on orientation accuracy so that spatial norm for determination target coordinates will not be exceeded.

The mistake for setting coordinates of emplacement for PdPK Sněžka using navigation instrument is 0,2% of the driven distance. This means, 20ms fault of 10kms movement. A probable mistake for setting the target coordinates by using a radar type SCB 2130 L-2 is 10 m in a distance and 2 units of an artillery quantity in a direction. The mistake in distance is constant and this accuracy is invariable with increasing distance. The mistake in direction increases with increasing distance and at the distance of 15 km the mistake is of 30m. In a case where PzPK is moving on a distance of 10 km, the setting of target coordinates accuracy for complete preparation for targets in a distance above 15 km would not be allowable. If the PzPK emplacement position determination is more accurate and it is set on a value of 0,1% of driven distance, the target coordinates determination accuracy will be allowable for the target distance up to 20 km. From the mentioned dependences it is possible to deduce a relation for calculation of maximum target distance from an emplacement for PzPK Sněžka:

$$dp = ½ [50 – (0{,}002 \text{ x } d_{př})]$$

where:

dp observer distance;

½ constant, invert value of probable mistake for setting target coordinates using radar type SCB 2130 L-2 in direction (2 dc);

50 constant, characterizing maximal mistake for setting target coordinates in direction in meters, which results from maximal probable circle mistake for setting target coordinates;

0,002 constant, characterizing a mistake for setting emplacement for PsPK Sněžka coordinates using navigation instrument (0,2 %);

$d_{př}$ movement distance before taking observer emplacement by PzPK Sněžka in meters.

A calculated observer distance (dp) is possible to take for an effective range of radar SCB 2130 L-2.

The probable circle mistake for setting target coordinates, detected by radar ARTHUR in range of its technical possibilities, is 50 m including mistakes of its own positioning, which meets the requirement for APF. Effective range of radar ARTHUR is identical to its technical range. [2]

The accuracy of artillery TA instrument positioning (setting coordinates) is defined with table T-2.1 in publication Pub-74-14-01. From this publication it is clear that the artillery TA emplacement has to be pinpointed with the same accuracy as gun firing positions. This means, up to 40 ms in length and 3 units of artillery quantity in orientation direction.

In the case of compliance with the mentioned requirements, the conditions for determining target coordinates for APF are met. An artillery observer has to count on described values (target coordinates determination accuracy and artillery reconnaissance instrument positioning) and in the case of call for fire (CFF), according to CFF in ASRPP-DEL, he will declare information “accurate” or “inaccurate”, mentioned behind the figure target position.

2.3 Meteorological preparation

Fire Publication The publication Pub-74-14-01 Pravidla střelby a řízení palby pozemního dělostřelectva determines that for complete preparation, meteorological conditions have to be determined from meteorological message METC, METEO-STŘEDNÍ or METEO-STŘEDNÍ PŘIBLIŽNÁ. All these messages have to comply with spatial and time validity.

METCM is valid for distances up to 50 km and for a 4h time period. Nevertheless in the message is stated time validity, which has to be considered in the case where the time period is shorter than standard validity of 4 hours.

Table 1. The range of reconnaissance instruments

S.n.	Instrument	Parameter	Value	Note
1	Infrared camera SOPHIE	Range (target detection): - person - tank - helicopter	3 km 9 km 11,5 km	IPzS LOS, KPzP
2	Laser range-finder HALLEM II	Range	50 – 15 000 m	IPzS LOS, KPzP
3	Night vision KLÁRA	Range	2,5 km	KPzP
4	Laser range-finder VECTOR IV	Range	4 km	KPzP
5	Day overview camera	Range (detection) target:	to 5 km	IPzS LOS
6	Day aiming camera	Range (detection) target:	to 10 km	IPzS LOS
7	Infrared camera TD 92 B2	Range (detection) target:	to 9 km	PzPK SNĚŽKA
8	Laser range-finder MOLEM	Range	20 km	PzPK SNĚŽKA
9	Radio locator SCB 2130 L-2	Range (detection) target: - person - tank	9 km 33 km	PzPK SNĚŽKA
10	Laser range-finder LPR-1	Range	20 km	Substitute reconnaissance instrument (by PzPK SNĚŽKA)
11	Radio locator ARTHUR	Range: mortars, guns, rocket launchers, tactical rockets launchers	20 km 30 km 40 km	

METEO-STŘEDNÍ is valid for distances up to 10 km and for a 3 hour time period, or the distance up to 35 km and for 2 hours' time period. METEO-STŘEDNÍ PŘIBLIŽNÁ is valid only for division units, whose meteorological squad created this message and it is valid for 1 hour time period. All these norms are valid for stabilized weather conditions. ASRPP-DEL has to have available actual local time and overview of the real deployment of units, placing a great emphasis on fire positions. From meteorological messages the system gathers information about meteorological station position, about the time of processing the message and about its validity. On a basis of these mentioned entry data ASRPP-DEL automatically provides an overview about actuality of meteorological message from the time and space point of view. In a case where the time of the end of validity of the message is coming up (e.g. 30 minutes before the end of validity), it automatically sends a signal to starting probing.

2.4 Ballistic preparation

The publication Pub-74-14-01 Pravidla střelby a řízení palby pozemního dělostřelectva determines that ballistic fire conditions have to be set, especially total change of beginning projectile speed. This means that for meeting conditions for complete preparation it is necessary to determine distance correction for:

- total change of muzzle projectile speed;
- change of propellant temperature;
- cartridge case of Czechoslovakian type (alternatively of the other, newly established type);
- unpainted projectile. [3]

Into weapon set individual corrections there is included distance correction for projectile weight change.

3 Fictional auxiliary target creation – Registration fire

According to the results of fictional auxiliary target creation (FPC) it is possible to determine data for FFE with such accuracy, after which it is not necessary to adjust fire. At the same time the following restrictions have to be met:

- observer distance of created FPC cannot exceed artillery reconnaissance instruments technical possibilities (table 1);
- adjusted distance and direction corrections can be used only for projectiles with the same table corrections for fire conditions changes;
- time period of validity for values, determined by fictional auxiliary target creation is up to 3 hours;
- switch of fire by simple method can be used in the case of high-pitched trajectory fire, if the difference between the fictional auxiliary target bearing and eliminated target bearing (switching angle) equals 300 dc or if it is smaller than 300 dc, and if the difference between fictional auxiliary target topographical distance and eliminated target topographical distance equals 1 km or if it is smaller than 1 km;
- switch of fire by coefficient of fire method can be used in the case of flat and rounded trajectory, if the switching angle equals 300 dc or if it is smaller than 300 dc, and if the difference between fictional auxiliary target topographical distance and eliminated target topographical distance equals 2 km or if it is smaller than 2 km.

4 The application of an adjustment gun

A publication Pub-74-14-01 Pravidla střelby a řízení palby pozemního dělostřelectva establishment results in a statement that fire data for an effective fire can be determined by using an adjustment gun, if the fictional auxiliary target is created by one of guns of the whole battery and if a discrepancy between platoons (batteries) master guns and a battery master gun, which created a fictional auxiliary target, is known. [3] Use of ASRPP-DEL suppose directing fire from distracted fire positions and therefore from the one fire position area. And so these tasks are not performed by fire batteries but by a specific number of guns, which can be considered as one compact unit. In this case it could be possible to determine firing data for FFE by switch of fire from a fictional auxiliary target.

The determination of firing data by using an adjustment gun could be considered as a good idea, if the subordinate task force will have an assigned fire unit, which would take a different fire position than other battalion fire units.

This situation may happen in a case when it is necessary to support a task force which is performing tasks on its own direction, this means in an area where the fire cannot be directed from the main fire position area because of too long a range of fire. Then it is excluded that units from the main fire position area and assigned fire units could conduct fire into the area, where they could use results of a fictional auxiliary target creation by the second fire unit.

The distance between fire positions is also very important. However, the publication Pub-74-14-01 does not set results of fictional auxiliary targets' validity by using an adjustment gun in terms of mutual distance between units, which created a fictional auxiliary target and which will use all the results for the determination of fire data for an effective fire. For a case where it could be possible to use an adjustment gun to determine fire data by a unit located in another area, the determined process is represented in a scheme - The way of setting fire data for an effective fire, an adjustment gun. [1]

ASRPP-DEL by this way, mentioned above, finds a value of a discrepancy between all of the guns and a master gun, which had created a fictional auxiliary target. Then this value is multiplied by a table distance correction for the 1% change of a beginning projectile speed for the specific projectile, filling, topographical distance and the final value is added to adjusted corrections for a fictional auxiliary target. By this action we can get calculated distance for a target to engage. Calculated direction (calculated side divergence) is obtained by a sum of topographical direction (topographical side divergence), adjusted direction correction and the difference between derivations on an eliminated target and derivations on a fictional auxiliary target.

5 The Abridged preparation

In the publication Pub-74-14-01 it is mentioned that fire data preparation is considered as an abridged preparation, if any of all conditions are not met, or if there is data gained from a fictional auxiliary target creation used for a setting fire data and if these data are from 3 to 8 hours old. [3] In these cases, fire data for effective fire have to be set by adjustment fire. A decision-making process for considering achieving conditions is represented in a scheme - The way of setting fire data for an effective fire, using a complete preparation and according to results of a fictional auxiliary target creation. [2]

The fire data for effective fire set by abridged preparation can be used for effective fire without any adjust fire, if that fire is led by a battalion on a multiple target with a purpose of "Scotch", where conditions for complete preparation are not met within a maximum of two points and at the same time these borders are not overstepped:

- fire positions coordinates are set topographically from the map of scale 1:50 000 and by using instruments;
- orientation bearings are set magnetically including the calculation of a compass correction, set in a 10 km distance from fire positions;
- target coordinates are set by some of the ways mentioned in table T-2.1 of publication Pub-74-14-01 with the level of accuracy 1,2 or 3;
- fire meteorological conditions are set from the meteorological message METEO--STŘEDNÍ PŘIBLIŽNÁ, which is not older than 1 hour and which is used up to 1600 m height;
- there is included only the change of initial shell speed, caused by wearing out of the barrel, where corrections for changes of all shell ballistic characteristics are calculated, which are mentioned in tables for fire.

For ASRPP-DEL it is necessary for this case to exactly set the number of firing guns. From the table T-1.4 from publication Pub-74-14-01 it is clear that the battalion can have 2-3 batteries and the battery can have 6-8 guns. This means that the battalion can have 12-24 guns. For ASRPP-DEL, a principle can be formulated, that if the system sets 12 or more guns for fire on the multiple target with the purpose of "Scotch!" and if all conditions from the chapter 5 Abridged preparation will be met, it will not be necessary to do an adjust fire for the setting of fire data for effective fire.

Conditions and variants for setting fire data for an effective fire by abridged preparation are mentioned in the scheme -The way of setting fire data for effective fire, The Abridged preparation.

6 The Simplified preparation

Fire data set by simplified preparation is set extraordinarily for a battery, which in the case of ASRPP-DEL means 6 to 8 guns only if it is not possible to set fire data in another way. In the case of simplified preparation it is necessary to set firing data for an FFE by adjustment fire.

7 Conclusions

It is necessary to separate the rating of meeting the conditions for topographical--geodetically preparation. While mistakes of setting fire positions Cartesian coordinates are influencing the fire accuracy constantly with rising distance, mistakes of setting orientation bearings are reducing the fire accuracy proportionately with rising firing distance. That is why the requirement on accuracy of setting orientation bearings in relation to setting Cartesian coordinates is relatively stricter.

Conditions for a survey of a target position cannot be rated separately, because these conditions influence each other. The accuracy of setting a position of an artillery reconnaissance instrument shows itself in the accuracy of setting target coordinates.

The accuracy of artillery reconnaissance instruments and the accuracy of setting artillery TA instrument position is mutually determined. [1]

This means that the accurate detection of an artillery reconnaissance instrument position and the accurate detection of orientation bearings provides a possibility of a higher tolerance on artillery TA instruments' accuracy.

Contrarily, a more accurate observation instrument provides less accurate positioning and orientation. By expression of meeting requirements of accuracy for setting fire data by complete preparation in the part of reconnaissance and target detection the information from the artillery observer about accuracy of setting the target position is "accurate". Otherwise (the setting of a target position is "not accurate") the adjustment of fire is necessary.

Processing the data of meteorological preparation can be fully automated by the ASRPP-DEL system. The system will have all necessary data and on its basis it is able to set the validity of the meteorological message for complete preparation and if it is necessary it can also point out a need for starting new probing.

Using adjustment gun spatial standards of created fictional auxiliary target (FPC) validity, depending on distance of units both creating FPC and using FPC results, must be set.

These units will also use these results for setting fire data. Fire data for FFE on an abridged preparation basis can be set by adjustment fire or without it.

For ASRPP-DEL it is necessary to exactly set all conditions for each variant of setting fire data for effective fire.

References

[1] BLAHA, M., SOBARŇA, M. Principles of the Army of the Czech Republic Reconnaissance and Fire Units Combat using. In *The 15th International Conference „The Knowledge-Based Organization“*. Sibiu (Romania): Nicolae Balcescu Land Forces Academy, 2009, pp. 17-25.

[2] BLAHA, M., BRABCOVÁ, K. Decision-Making by Effective C2I system. In *The 7th International Conference on Information Warfare and Security*. Seattle (USA): Academic Publishing Limited, 2012, pp. 44-51. ISBN 978-1-908272-29-4

[3] Joint Forces Command, Training. *Shooting Rules and ground artillery fire control (gun, platoon, battery compartment)*. Pub-74-14-1. Prague: 2007. 256 p.

[4] *Military Strategy of The Czech Republic*. Praha: MO CR, 2008.

[5] *Long-Time Scheme of Ministry of Defence*. Praha: MO CR, 2008.

[6] *NATO Capabilities/Statements - 2018*. Brusel, 2007.

[7] *Doctrine of the Army of the Czech Republic*. Praha: MO CR, 2005.

[8] BLAHA, M., SOBARŇA, M. Some develop aspects of perspective Fire Support Control System in Czech Army conditions. In *The 6th WSEAS International Conference on Dynamical Systems and Control.* Sousse (Tunisia): University of Sfax, 2010, pp. 179 - 183.

[9] POTUŽÁK, L. *Control and Realization of Fire Support - The Cooperation of Artillery and Units of Artillery Reconnaissance during Fire Support of Forces.* Partial task - Specific research of FEM. Brno: University of Defence, 2006.

[10] *AD-6.1 Doctrine of Communication and Information systems*. Praha: MO CR, 2003.

[11] *AAP-6 NATO Glossary of Terms and Definitions* (english and french). 2009.

[12] BLAHA, M., BRABCOVÁ, K. Communication environment in the perspective Automated Artillery Fire Support Control System. In *The 10th WSEAS International Conference on APPLIED INFORMATICS AND COMMUNICATIONS (AIC '10).* Taipei, 2010. pp. 236-240. ISBN 978-960-474-216-5.

[13] BLAHA, Martin. Communication as a basic for future Artillery Fire Support Control System. In: *The European Conference of COMMUNICATIONS (ECCOM'10)*. Tenerife: WSEAS Press, 2010, p. 140-142. ISBN 978-960-474-250-9.

[14] BLAHA, Martin; POTUŽÁK, Ladislav. Decisions in the perspective Automated Artillery Fire Support. In: *Recent Researches in Applied Informatics & Remote Sensing*. Penang: Wseas Press, 2011, p. 87-91. ISBN 978-1-61804-039-8.

Determination of the kinetic model for cell line on the duration of action of an inhibitor of tyrosine kinases receptors

Corina Brînduşa[1], Cornelia Aida Bulucea[2] and Nikos E. Mastorakis[3],

[1] Faculty of Medicine, University of Medicine and Pharmacy Craiova, Romania, e-mail: corinaa_b@yahoo.com
[2] Faculty of Electrical Engineering, University of Craiova, Romania, e-mail: abulucea@gmail.com
[3] Technical University of Sofia, Industrial Engineering Department, Sofia, Bulgaria & Military Institutions of University Education (ASEI), Hellenic Naval Academy, Piraeus 18539, Greece , e-mail: mastorakis4567@gmail.com

Abstract. Transfer function as a kinetic model for tumor cell line, provides, in medical research, useful information on the evolution of the cell population during the experiment. The presence of a tyrosine kinase receptor inhibitor in the cell fraction dynamic process involves a distinct set of parameters specific to the process *in vitro*. The correlation between the evolution of cellular fraction dynamics specific to tumor cell lines, in the presence of an inhibitor, and an electric discharge process of a *RC (resistor-capacitor)* quadrupol*e* calculation can be based on the residues calculation specicific to statistical analysis. The transfer function is determined indirectly through a complex electronic structures: Quadrupole resistor-capacitance *RC* + Operational Amplifier *AO*. The calculation of such residues permits the validation of the model for the dynamics of cell fraction specific to tumor cell line *GB9B* derived from glioblastoma *GB* under the action of an inhibitor of receptors of tyrosine kinases. Such a mathematical model based on the transfer type allows highlighting the behavior of a system of type tumor cell line *GB9B* in the presence of inhibitor *GLEEVEC.*

Keywords: transfer function, GB9B, GLEEVEC inhibitor, cell line, kinetic model, operational amplifier, receptors.

1 Introduction

Study on cell lines of action of inhibitors allow the development of complex treatment configurations. Tumor cell line is a continuous line that acquires a set of specific characteristics that lead mainly to loss of contact inhibition in culture growth without the appearance of signs of aging. *GB9B* tumor cell line is derived from a glioblastoma line, *GB*.

Glioblastoma multiforme is the most common type of primary malignant brain tumors. At this type of brain tumor, one could note the unfavorable prognosis for the patient resulting in average survival / patient for about a year. Even surgery with tumor removal above 90%, accompanied by a complex chemotherapy regimen does not necessary lead to the elimination of tumor appellants. An explanation could be that endogenous tumor cells are the source of new tumor cells [1].

On the other hand it seems that *EGFR* protein occupies a role in the development of glioblastoma. It is believed that *EGFR* protein stimulates cell division, cell survival and invasion through its role as a receptor of tyrosine kinase that activates the key oncogenic pathways. Since *EGFR* disorders arising in cases of glioblastoma is inferred to *EGFR* inhibitors may be part of treatment regimens, although we have a favorable response rate of ~ *10%* of reported cases [2].

W. D. Parsons and colleagues investigated genetic alterations occurring in human glioblastoma tumor samples. These studies demonstrate the value of unbiased genomic analyses in the characterization of human brain cancer and identify a potentially useful genetic alteration for the classification and targeted therapy of GBMs [3]. It is known that human cancer cells have typically several chromosomal aberrations. We could note the nucleotide substitutions and epigenetic changes that lead to malignant transformation. In this framework the *Cancer Genome Atlas* project (*TCGA*) has imposed. The objective of this project is to evaluating on a large scale scale, by a complex analysis of molecular characteristics that occur in human cancer, so in glioblastoma [4].

Development of a chemotherapeutic regimen for tumors of type glioblastoma, *GB*, can only be done if turning the tumor lines developed from the malignant tissues collected from patients diagnosed with glioblastoma.

Initially, the inhibitor *GLEEVEC* has been used only in clinical trials for the treatment of chronic myelogenous leukemia. *GLEEVEC, (Imatinib),* is a first generation tyrosine kinase inhibitor that is used in the treatment of chronic myelogenous leukemia, gastrointestinal stromal tumors , and other cancers. In **Table 1** presents relevant data inhibitor *GLEEVEC* (see **Figure 1**) [5,6].

Table 1. Inhibitor *GLEEVEC*

Synonyms	CGP57148B, STI571, *glivec, imatinib mesilat*
Molecular formula	$C_{29}H_{31}N_{7}O.CH_{4}SO_{3}$
Molecular weight	589.71
Formulation	A crystalline solid
Solubility	DMSO (100 mg/ml)
Storage temperature / Stability	-20 ° C / 2 years

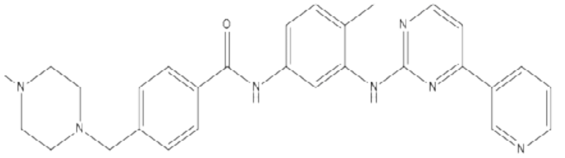


Fig. 1. Chemical formula of inhibitor *GLEEVEC,* (*STI571*)

Buchdunger E, and colleagues [7], extended the inhibitor *STI571* profile and suggest that in addition to chronic myelogenous leukemia, the *STI571* may have clinical potential in the treatment of diseases that involve abnormal activation of *c-Kit* and *PDGF* tyrosine kinases receptor.

Schindler T, Bornmann W and colleagues [8], sought to determine the structural mechanism for *STI571* inhibitor, tyrosine kinase inhibitor. The product, known as a small molecule inhibitor, is effective in the treatment of *LMC*.

For treatments of type chemotherapeutic regimens is essential the application of regimens leading to rapid improvement of the clinical status of the patient. If malignancy is desirable stagnating their development, in a first stage, followed by reduction or disappearance of them, in the later stages.

We can follow a new stage, which has interesting traits, in elaborating the strategy of optimal regimens for the patient, leading to the construction phase of a mathematical model. We approach this stage through the correlation between the evolution of the dynamics of specific cellular fraction of tumor cell lines in the presence of an inhibitor, and the electrical discharge process of an *RC (*resistor-capacitor*)* quadrupole which can be found in the structure of a complex electronic configuration. We address meaningfully an indirect construction of the mathematical model based on the known transfer function for complex electronic structure: Quadrupole *RC* + Operational Amplifier *AO*.

This study ongoing in *Clinical Research Laboratory of UMF Craiova* is emphasizing a high potential of inhibition induced by *STI 571* on the cell line *GB10,* derived from bioglastom, *GB*.

2 Material and method

Cell line *GB10* was developed on the basis of tumor sections provided by Hospital *Bagdasar Arseni* in Bucharest, in patients with glioblastoma, according to standard procedures.

Standard culture medium (Minimum Essential Medium - *MEM*) have been provided by the SIGMA – ALDRICH.(St. Louis, USA).

Fetal bovine serum (*FBS*), and antibiotics have been provided by the GIBCO, (South America) and trypsin have been provided also by the GIBCO, (South America).

GLEEVEC, (STI 571), inhibitor is present as the form of a solution of *100µM*. *GLEEVEC* has been used on cell line *GB10* in the *Laboratory CRL*.

Treatment of cells. The cell line was grown in modified standard medium MEM (which is containing 10% fetal bovine serum *(FBS)*, 1% antibiotics). The cells were grown in boards of 12 wells, and were maintained in incubator at 37°C, 95% O_2 and 5% CO_2.

At each interval of 2 days was imposed changing the standard *MEM*. The cell line was incubated for a period of 7 days. The cultured cells were detached with trypsin.

In order to determine the kinetic model *for GB10* cell line, after a incubation period, actual of seven days, it has passed to induction treatment with *GLEEVEC*

50µM in the same culture conditions (*MEM* modified). Inhibitor administration was done at an interval of *2 days*.

Cell viability. . Cell viability was determined directly at *8 hour* intervals, in marked areas, for *56h*, but can be determined using a modified MTT reduction assay. The medium was removed and fresh medium in the absence or presence of imatinib was added to the cultures. Compounds were not renewed during the entire period of cell exposure. Control cells without agents were cultured using the same conditions with comparable media changes. Compounds were not renewed during the entire period of cell exposure.

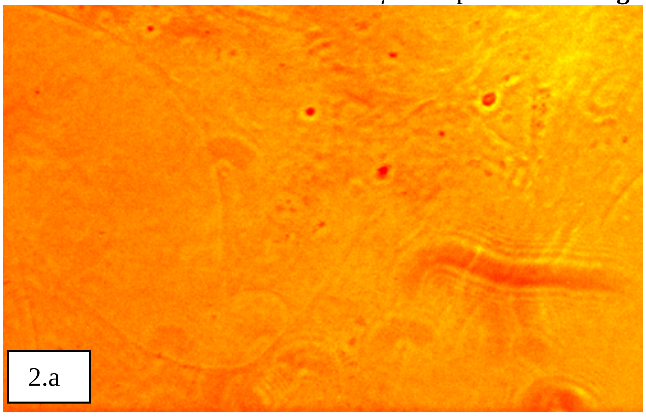
3 Results

Following the incubation process at which the cell line *GB10* has been subjected, it resulted a strong cell viability after *7* days from the start of incubation. Following the treatment with *GLEEVEC 50µM* inhibitor after the scheme depicted in ***treatment of cells*** it resulted a strong decrease in the cellular fraction of *GB10* line. Towards the end of therapy (*<3d*) the kinematic evolution revealed a cellular fraction value below *0.16*, according to **Table 2**. There have been established the system variables as: *celular fraction, f / calculation time, t.*

Table 2. Celular fraction, **f** / Tumor cell line, GB10B

Tratament day, **n**	1			2
Calculation time, **t**,(1/3d)	0	1	2	3
Celular fraction, **f**	1	0.75	0.47	0.39
Treatment day, **n**	2		3	
Calculation time, **t**,(d)	4	5	6	7
Celular fraction, **f**	0.26	0.24	0.17	0.16

Different stages in the development of a cellular tumor of cell lines *GB10* in the presence of the inhibitor *GLEEVEC 50µM* is presented in **Fig. 2.**



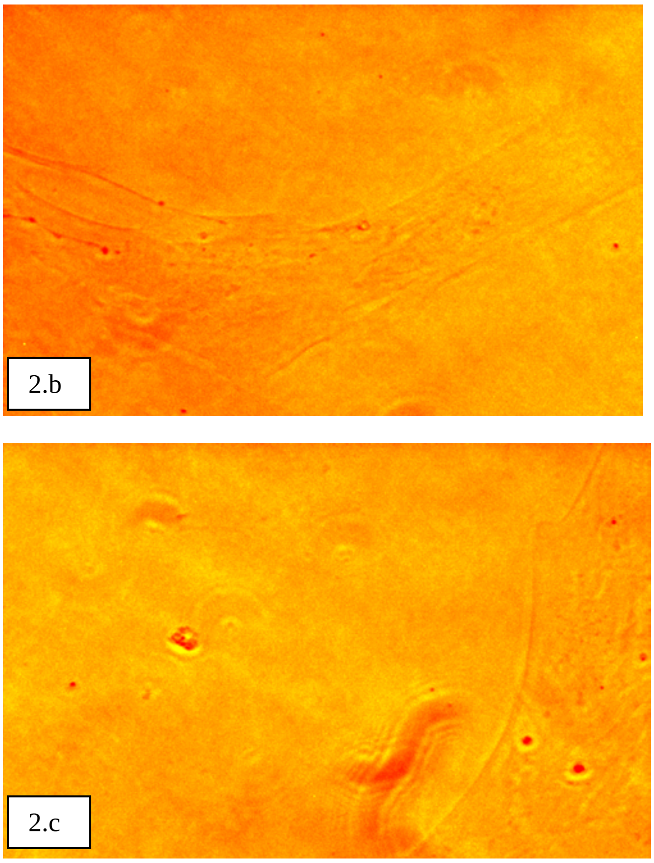


Fig. 2. Complex network of specific tumor cell line GB10.

Building of mathematical model for analyzing the cellular fraction of *GB* is performed by analogy with the electric structure of type electric pasive quadrupole. Based on complex electronic structure in **Figure 3,** mainly encompassing a quadrupole *RC*, asignal repeater A_1, and a signal noninverting amplifier A_2, we built the mathematical model through operational calculus. We have the relations:

$$0 = R\,i + \frac{1}{C}\int i dt \,. \qquad \textbf{(1)}$$

$$C\frac{du_C}{dt} + \frac{u_C}{R} = 0 \,. \qquad \textbf{(2)}$$

$$u_C(t) = \frac{1}{C}\int i dt \,. \qquad \textbf{(3)}$$

$$u_2(t)=K_1u_C(t). \tag{4}$$

The transfer function is:

$$H_{21}(p)=K_1\cdot K_2\frac{\tau}{(\tau\cdot p+1)}\ . \tag{5}$$

where:

$$\tau = RC\,. \tag{6}$$

$$K_1 = {R_4}\big/{(R_3+R_4)}\cdot \tag{7}$$

$$K_2 = 1+{R_7}\big/{R_6}\ . \tag{8}$$

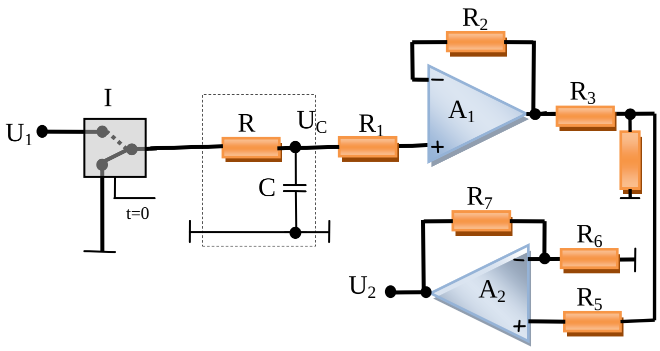


Fig. 3: Electronic structure: RC + OA.
Obs.: *- R_1, R_5 -undefined; A_1, A_2 - precision AO with input jFET; I - CND+CNI;*
- the scheme does not apply to direct measurements.

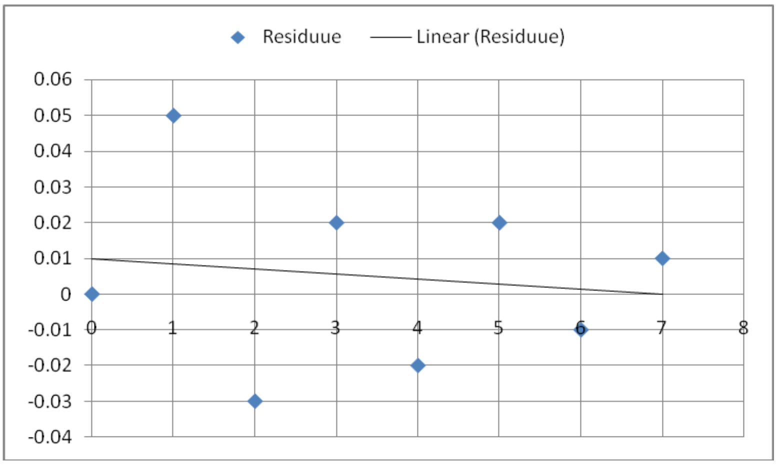


Fig. 4. Residuues Diagram

The transfer function, $H_{21}(p)$ (5) encompasses a pole, (as system stabilizing element). It is considered that the initial status of the system, corresponding to complex electronic structure ($RC + A_1 + A_2$) in **Figure 3** is the state $U_2=1V$. Loading of capacitor *C* to the value $U_C=1V$ was achieved from the voltage source $U_1>1V$, through the contactor *I*. Requiring the condition on obtaining the voltage $U_2=1V$, is imposed the choice of structural elements K_1, K_2, so as to respect the relationship: $K_1K_2=1$.

At the time moment $t=0$ the command is given in order to discharge the capacitor *C* through the resistance *R* and the contactor *I*. The voltage on capacitor *C* (and implicitly the output U_2) decreases to *0*, after a period of time depending on the time constant of quadrupole *RC*, namely $\tau=RC$.

Taking into consideration the type of the followed process, one could choose a relatively large constant value, $\tau=1d$. We can fill the second row of **Table 3** with the calculated values based on the model $\left[L^{-1}H_{21}(p)\right]_{t=0}^{t=4\tau}$. These values are predicted values in our case. The observed values are filled in the third row (the cell fraction, *f* in **Table 2**). The fourth row contains *residuues*. These represent the values of prediction error calculated as the difference between the observed and predicted values, see **Figure 4**.

Table 3. Calculation of residuues

Calculation time, **t**,(1)	0	1	2	3
Predicted values (2)	1	0.7	0.5	0.37
Observed values (3)	1	0.75	0.47	0.39
Residuue values (4)	0	0.05	-0.03	0.02
Calculation time, **t**,(1)	4	5	6	7
Predicted values (2)	0.28	0.22	0.18	0.15
Observed values (3)	0.26	0.24	0.17	0.16
Residuue values (4)	-0.02	0.02	-0.01	0.01

4 Discussion and conclusions

The cell line *GB10* (tumor cell line *GB*) was incubated in the *Laboratory LCT* in the *UMF Craiova*. The incubation process revealed a strong cell viability, accompanied by a large increase in the growth rate of the cell fraction.

After proper incubation period, cell line *GB10* followed a period of treatment and monitoring (*3 days*). Treatment was based on the inhibitor *Gleevec*. Treatment schedule consisted of injecting doses of *GLEEVEC 50μM* every *2* days after incubation. Monitoring line *GB10* was performed directly by counting the cells on marked areas, at time interval *Δt=12h*. This revealed the cellular fraction profile, emphasized by: strong decrease on line *GB10*, subjected to treatment with *GLEEVEC 50μM*. At the end of treatment (*56h*), the kinetic evolution reached a negative jump of over *84%* from the time of launch treatment initially. It is noted that in **Table 3** we worked with computation time (*turn 1*), that begins after flowing the inertia phase of the kinetic evolution of the cell line.

In another study [9] we identified a specific kinetic model of cellular dynamics fraction of glioblastoma lines, *GB*, subjected to a process of incubation and cell proliferation. Model identification in the form of transfer function was done indirectly through a complex electronic structure, (composed mainly of the *RC* quadrupole, the signal repeater A_1, amplifier/ signal inverting A_2, amplifier/ signal inverting A_3).

The transfer function of electronic structure *RC* quadrupole + operational amplifier *OA* determines forecast values for the proliferation process of tumor cells gliblastoma. Based on the analysis of residues one could accept that such a mathematical model $H_{21}(p) = H_{GB} = K_1 \cdot K_2 \cdot \frac{1}{\tau} \cdot \frac{1}{p(\tau p+1)/\tau}$ is valid for the proliferation process of the cell line,*GB9B*, of *GB* tumor cell type. Calculation of standard residues explains our choice to accept indirect construction of the mathematical model specific to this process by cell dynamic type on tumor cells *GB* [9].

Such a model allows, by generalization, an anticipation of the evolution of cell mass on continual cell lines, that is an important aspect specific to *in vitro* research.

One could note that over time gave been proposed various models of tumor cell mass increase in volume. In these models the size of the cancerous mass is measured experimentally as a volume. Another expression of cell mass dynamics is a function of the number of cells, (Norton, 1988). Such a model describes the early stage of tumor growth dynamics, in conditions that do not involve constraints of nutrition type [10].

Other work highlight a number of models describing the dynamics of tumor cell mass under the action of combinations of cancer drugs. The assessment of such effects, the establishment of therapeutic strategies is imperative in such cases. Ana Catarina Pinto and colleagues have proposed a model that establishes the correlation between drug dose and the corresponding effect, as a form of inhibited cell growth [11].

There are currently developing personalized therapies by molecular tests that are based on the identification of mutations in genes examined tumor tissue. The analyzes are performed mainly on gene *HER-2, ALK, c-MET, FGFR, PIK3CA, EGFR* [12, 13].

Further on we would look for proving that a mathematical model described by a differential equation of order *2* with concentrated parameters could be accepted for a complex process of xenobiotic absorption [14]. Within the structure of a modulated absorption system, with a target type xenobiotic, one could identify specific elements of xenobiotic compounds dissipating type and of xenobiotic compounds accumulating type. As is already told, a mathematical model depicting a xenobiotic absorption process could be a differential equation of order *2* [15,16].

Continuous and sustained pursuit of subjects which have a xenobiotic induced retardation in speech is vital in the areas of permanent and intensive monitoring. Detection and quantification of retardation induced impermanent implementation on a subject affected by a xenobiotic can be implemented by using the elements of statistical analysis, more precise by watching crowd sounds appearances interrelated groups [17,18].

We can say that the study of forced inhibition of tumor cells *in vitro* is important to building the specific mathematical model process. Construction of the mathematical model in the form of the transfer function can be obtained by analogy with complex electronic structures: quadrupole *RC + AO*.

It is possible to develop mathematical models for analyzing cellular fraction *GB* based on a so-called indirect construction process mathematical model. In our case the mathematical model for analyzing the cellular fraction *GB* was built indirectly by analogy with the mathematical model of passive *RC* quadrupole. It is important to emphasize that during the construction of such a model it is compulsory to have a mathematical model validation stage. Residuue analysis permits to validate a mathematical model of the dynamics of cellular fraction, based on the mathematical model built on complex electronic structure, namely quadrupole *RC + AO*.

The transfer function of electronic structure: quadrupole *RC + AO* determines the expected values for cellular fraction derived from glioblastoma tumor cells. Based on the analysis of residuues one can accept that such a mathematical model, $H_{21}(p) = H_{GB}(p) = \frac{K_1 K_2 \tau}{(\tau p + 1)} = \frac{\tau}{\tau p + 1}$, (under the condition: $R_4 = R_6, R_3 = R_7$), is valid for dynamic cell line, *GB10,* subjected to the action of an inhibitor of tyrosine kinases receptor, *GLEEVEC 50µM*. It is considered that the inhibitor process on tumor cells *GB* is defined by the points: *(0,1), (τ,e^{-1}), (2τ,e^{-2}), (3τ,e^{-3})*. We took into account that the inhibitor used had a high concentration leading to a high extinction tumor cells, GB, in a range of *3-4* time constants specific to the process.

Calculation of standard residuues explains our choice to accept indirect construction of the mathematical model, the specific biochemical process by type cell dynamic on tumor cells, *GB*, under the action of the inhibitor *GLEEVEC.*

References

1. Chen, J., Li, Y., Yu, T.S., McKay, R.M., Burns, D.K., Kernie, S.G., Parada, L.F.: A restricted cell population propagates glioblastoma growth after chemotherapy. Nature, 488: 522-526 (2012)
2. Purow, B., Schiff, D.: Advances in the genetics of glioblastoma: are we reaching critical mass?. Nat Rev Neurol.,5(8): 419-26 (2009), http:// www.ncbi.nlm.nih.gov/pubmed
3. Parsons, W.D., Jones, S., Zhang, X. et al.: An Integrated Genomic Analysis of Human Glioblastoma Multiforme. Science, Vol. 321, no. 5897, 1807-1812, DOI:10.1126/ science (2008)
4. Comprehensive genomic characterization defines human glioblastoma genes and core pathways. The Cancer Genome Atlas Research Network. Nature, 455, 1061-1068 (2008), http:// www.nature.com/nature/journal
5. Imatinib (mesylate) Cayman Chemical**,** https://www.caymanchem.com/catalog/13139
6. Imatinib Mesylate (CGP-57148B, STI-571), https://www.biovision.com/imatinib-571
7. Buchdunger, E., Cioffi, C.L., Law, N., Stover, D., Ohno-Jones, S., Druker, B.J., Lydon, N.B.: Abl protein-tyrosine kinase inhibitor STI571 inhibits in vitro signal transduction mediated by c-kit and platelet-derived growth factor receptors. J Pharmacol Exp Ther, 295(1):139-45 (2000)
8. Schindler, T., Bornmann, W., Pellicena, P., Miller, W.T., Clarkson, B., Kuriyan, J.: Structural mechanism for STI-571 inhibition of abelson tyrosine kinase. Science, 289(5486):1938-42 (2000)
9. Brînduşa, C.C., Dondon, P., Bulucea, C.A.: Indirect identification of transfer function specific to cell line dynamics. EMET 2014 - The 2014 International Conference on Education and Modern Educational Technologies, Santorini Island, Greece (2014)
10. Norton, L. A.: Gompertzian model of human breast cancer growth. Cancer Res., 48 , 7067–7071 (1998)
11. Pinto, A.C., Moreira, J.N., Simões,S.: Combination Chemotherapy in Cancer: Principles, Evaluation and Drug Delivery Strategies. Medicine Oncology: Current Cancer Treatment - Novel Beyond Conventional Approaches, book edited by Öner Özdemir (2011)
12. Oncompass™ for Patients | KPS, http://kpsdx.com/products/oncompass-for-patients
13. Oncompass™ for Physicians | KPS**,** http://kpsdx.com/products/oncompass-for-physicians
14. Bulucea, C.A., Rosen, M.A., Mastorakis, N.E., Brindusa, C.C., Bulucea, C.A.: Approaching Resonant Absorption of Environmental Xenobiotics Harmonic Oscillation by Linear Structures. Sustainability, doi:10.3390/su40x000x (2012)
15. Bulucea, C.A., Brînduşa, C.C., Mastorakis, N.E., Bulucea, C.A., Jeles, C.A.: Harmonic structures for environmental xenobiotic absorption kinetics, IEEEAM/NAUN International Conferences Prague on WORLD MEDICAL, Czech Republic, pp 192-196 (2011)
16. Bulucea, C.A., Mastorakis, N.E., Rosen, M.A., Brînduşa, C.C., Bulucea, C.A., Jeles A.: Enhancing Understanding of the Environmental Xenobiotics in Coal-Fired Flue Gas, Recent Researches in Environment and Biomedicine, Proceedings of the 6th International Conferences on Energy and Development Environment - Biomedicine (EDEB'12), Vouliagmeni, Athens, Greece, pp.58-67 (2012)
17. Brînduşa, C.A., Gofiță, E.: Detection and quantification of retardation induced by certain xenobiotics, WSEAS RECENT RESEARCHES in MEDICINE, BIOLOGY and BIOSCIENCE, Chania, Crete Island, Greece, pp 70-75 (2013)
18. Jeles, C.A., Brînduşa, C. C., Păsculescu, D.: Manifestations of retardation induced by certain xenobiotics. 5th INTERNATIONAL MULTIDISCIPLINARY SCIENTIFIC SYMPOSIUM, "UNIVERSITARIA SIMPRO 2012 on ENVIRONMENT AND GEOLOGY ENGINEERING, UNIVERSITY OF PETROŞANI, ROMÂNIA, pp 37-42 (2012)

Software Support of Integration of Alarm Systems

Jan VALOUCH

Tomas Bata University in Zlin, Faculty of Applied Informatics,
Nad Stranemi 4511. 76005, Zlin, Czech Republic
valouch@fai.utb.cz.

Abstract. Integration of the alarm systems is a modern way of using the current technological capability elements of intruder alarm system, camera systems, access control and hold-up alarm systems. These applications can be integrated with each other or to supplement the non-alarm systems and thereby provide simplify the automation processes in commercial and residential buildings. Integration of alarm and non- alarm applications is solved by various technical solutions, starting with a simple connection of input / output contacts to sophisticated software solutions. This article describes software integration methods of integrated alarm systems. The key output of the article is the proposal of classification of functions and methods of software integration for integrated alarm systems.

Keywords: Integrated alarm system, Software, Integration, Intruder alarm system, non - alarm application.

1 Introduction

Integration of alarm and non- alarm applications is solved by various technical solutions, starting with a simple connection of input / output contacts to sophisticated software solutions.

Integrated Alarm Systems (IAS) is defined according to relevant technical regulation ČSN CLC / TS 50398 as systems having a one or more common devices at least one of which is an alarm application [1]. The alarm application designed to protect life, property or environment:

- intruder and hold-up alarm system (I&HAS),
- closed circuit television used for security and surveillance (CCTV),
- access control system (ACS),
- social alarm system (SAS),
- fire detection and fire alarm systems (FDAS),
- environmental alarm systems and lift alarm systems.

The above systems can be integrated with each other or with non- alarm applications (lighting, heating, air- conditioning, ventilation, irrigation, building management, energy management).

At present, the issue of integration is described only in a single technical standard: ČSN CLC / TS 50398 Alarm Systems-Combined and integrated systems-General requirements. This document, as the name implies, describes only the general requirements for IAS and basic types of configurations. In terms of software integration support, document describes only the software of evaluation elements.

The software of each system may affect other software application. It is therefore appropriate to ensure the separation of software already in the design of system (separate modules and documentation). t is also appropriate to describe the possible mutual negative impacts for normal operation and fault condition of system. [1]

In terms of needs of formulation and the subsequent drafting of an integrated alarm system is an important factor of the selection of appropriate elements- method of technical solutions interconnection systems. Therefore it is necessary to categorize - to classify the different techniques of integration and to create a basic guide the preparation of implementation IAS. Classification of technical solutions of integration is also important for evaluating the effectiveness of alarm systems. Currently, this problem is not described in any of the literature or technical regulations. Selection of appropriate methods for integration is an important point of the system design as the first phase of the setting up the IAS, especially due to its feasibility, requirements for operation, adequacy of financing costs and particularly the possibility of any further expansion of the system. [2]

The technical ways of interconnecting the individual applications can be divided into the following basic groups:

- hardware methods of integration,
- software methods of integration.

The hardware (HW) methods of integration are based on the interconnection of systems through their inputs and outputs and on the technical parameters of alarm systems, which may include, in addition to the basic security functions also specific-expanding elements (modules) to control alarm or non alarm applications (lighting control, heating, access control, etc.). Hardware integration methods can be divided into the types:

- IN/ OUT integration,
- I&HAS - integration element,
- ACCESS - integration element,
- CCTV - integration element,
- Automation system- integration element.

The proposal of classification SW integration methods is presented in the following sections of article.

2 Materials and methods

The proposal of classification of functions and methods of software integration for integrated alarm systems is based on on the analysis of the following issues:

- basic forms of system integration,
- technical requirements for integrated alarm system,
- technical requirements for the process of integration of alarm applications,
- possibilities of software products,
- customer requirements for building automation.

The processing of the proposed classification is based on the analysis of the following types of documents -technical standards- I&HAS, CCTV, ACCESS, SAS, technical product specifications, installation manuals of relevant systems and their elements, legislation- definition of technical requirements for the components IAS.

Integration of alarm and non- alarm applications can generally be included in the field of system integration (although this is mainly associated with information systems), which is understood as the delivery of services based on connecting heterogeneous subsystems into one functioning whole. Basic forms of system integration are divided into the following types:

- technology integration,
- functional integration,
- integration of user interface,
- data integration,
- methodological integration.

The software products can support of the fulfillment of all the above types of system integration. The key document in integrated alarm systems is a technical standard ČSN CLC / TS 50398 Alarm systems - Combined and integrated systems - General requirements. Although the standard issued as early as 2005 and then 2009, not many interested companies (distributors, installation companies) this fact is not known or have only general information about the issue of the CEN / CENELEC, which has the status of technical specifications and its acceptance by the national standards of members of the CEN / CENELEC is not required (only an obligation to ensure notification of the existence and availability of CLC / TS 50398). The standard solves the issue of definitions of basic terms and describes basic types of IAS configuration, system requirements, requirements for documentation and training.

Technical standard ČSN CLC 50398 generally only specifies three IPS configuration:

- Type 1 can be applied for the combination or integration of two or more single-purpose (dedicated system) alarm systems and single purpose non-alarm systems that are connected to a common complementary device (Additional Facility) – i.e. a device not required by the standard (e.g., signaling panel, PC),
- Type 2A can be applied for the combination or integration of alarm and non-alarm systems that use (in accordance with the requirements of the standard) common transmission paths and common devices. Fault in any of application has no negative effect on other applications.
- Type 2B is defined well as type 2A with the difference that a fault in any of application can have a negative effect on other applications.

The technical standards (ČSN EN 5013x series) for each type of alarm applications (I&HAS, CCTV, ACS, SAS) describe the integration of very briefly. Each application must primarily comply with its own standards (I&HAS, CCTV, ACCESS, SAS, see ČSN EN 5013x series) and must meet specific requirements for system integration [3]. Common components used under integration must then comply with all relevant application standards. In the case of differing requirements of the standards must be used the most stringent requirements relating to the operation of the system.

3 Software Integration

The methods of software integration are based on linking of separate applications via a communication bus, and their control, management and visualization are providing by software products, which are installed on an external computer (server, client PC) or at unattended control centers equipped with the necessary software. Alarm systems and non- alarm applications can also be connected to the server via the network (LAN, WAN). PC client is connected to the application via the serial interface or USB port for simple applications. User access to the main functions via your computer or via mobile devices is a common element of integration with the use of software products.

Software products ensure the implementation of functions integrated alarm systems. These functions support of integration of activities, data, user interfaces and technologies. I propose the following classification of functions:

- system administration,
- programming
- user management,
- monitoring,
- visualization,
- technology Integration,
- control
- automation
- management of attendance
- registration - visits, entrances
- evaluation of events
- monitoring of events,
- logistics support.

This classification of functions is intended to support of the system design, system realization and evaluation of the effectiveness of the integrated alarm system.

Software products provide multiple functions for integrated alarm systems. From this perspective, I propose the following classification of software products to support of the integration of alarm systems:

- software of control panels of alarm systems,
- software for user administration,
- security software,

- visualization software,
- integration software.

3.1 Software of control panels of alarm systems

The Additional programs delivered to the various types or line of control panel IAS providing local or remote connection panel (control unit) with a PC in order to realize the basic functions - programming, monitoring, evaluation and event logger. These programs serve the need for installation and service companies. Here we talk about integration from the perspective of a central evaluation and event activation of control panels, that can be hardware linked to other systems.

3.2 Software for user administration

These programs ensure user settings of control units (control panel) connected systems. In the area of security is usually a control panels I&HAS, which are complemented by access control system superstructure. The user has, in addition to basic functions (evaluation, monitoring, archiving events), especially possibility:

- setting up user profiles, create descriptions of subsystems zones, terminals,
- creating time schedules of access,
- allocation and registration of identifiers (cards, fingerprints)
- filtering of event history (type, time, place, and person).

3.3 Security software

This type of software combines security and logistical functions. Software is intended to ensure an overview of the situation in buildings. Software can ensure the following tasks:

- integration of management methodology of access and entry
- records of persons and vehicles in the object
- saving of event history
- a current overview of movement of persons and vehicles in the object
- overview of the movement of assets
- asset management,
- creating a "black list" database of unwanted persons, vehicles and companies,
- combination with fire
- protection and work safety,
- records of postal items,
- automatic printing of access cards,
- visual records of processes in the object.

3.4 Visualization software

The visualization programs provide in contrast to programs for user management other comfort function- transparent visualization of system status in real time. The operator can monitor system status and controls selected functions - on / off surveillance subsystem or zone, opening doors, turning on the camera or control PGM outputs [4]. Software uses a building floor plans (buildings or outdoor space - there are also software for visualization of perimeter protection) with a graphical showing of the locations of individual components (detectors, cameras, card readers, terminals, etc.).

3.5 Integration software of systems of buildings

Interconnection of security systems and other technology of building are implemented through software product, which is installed on the server. These systems (alarm and non-alarm) are controlled by the client PC through a web browser [5]. The individual systems are connected in a LAN. Integration software is an additional service, allowing for example:

- setting the automatic links between systems, visualization of systems,
- local and remote control, systems management and users
- control activities of operator,
- management of attendance in continuity to payroll system,
- definition of roles and rights of users (employee, operator, manager, receptionist, etc.).

Failure of activities of integration SW may adversely affect the functionality of the connected systems. It is therefore for appropriate ensure integration of important system bindings by the hardware level. Integration software usually consists of separate modules that can be combined according to customer requirements (IAS, HAS, CCTV, ACCESS, FDAS, attendance, the map interface etc.)

4 Conclusion

The aim of the article was to present the proposed classification of software products and its functions for support of integration of alarm systems. SW integration methods can be classified according to their basic functions, which SW products can provide. Proposal of classification is based mainly on the analysis of technical requirements for integrated alarm systems and possibilities of software products.

The importance of the deployment of software products for the integration of alarm systems:

- central control of events and alerts in the system, the central management of user data,
- ability to integrate products from different manufacturers, the implementation of on-line service,

- reducing of false alarms,
- better overview of the situation in the building,
- obtaining before-alarm information,
- faster response to emergency events, user control and operators, operative changes of system,
- standard (graphical) user interface, reducing the cost of supervision in the building, maintenance, training, human resources, expansion the possibilities of connected devices.

The benefits of processing classification of software products and its functions to support of integrated alarm systems:

- starting material for preparation of technical report to support of the interpretation of technical standards in the field of integrated alarm systems,
- basic assumption to selection of integration methods in the design of of an integrated alarm system, [5].
- better orientation in software products to support of the integration of alarm systems,
- establishment of criteria for evaluation of the effectiveness of the integrated alarm systems,
- support of the process of comparison of hardware and software integration methods.

References

1. ČSN CLC/TS 50398:2009. Alarm systems- Combined and integrated alarm systems - General requirements. (in Czech).
2. VALOUCH, Jan. Integrated Alarm Systems - Characteristics, Importance and Requirements. In *Security Magazin.* Issue No 111, 1/2013. Praha: SecurityMedia, 2013. ISSN 1210-8273. p. 44-48. (in Czech).
3. CSN EN 50131-1 ed.2:2007. Alarm systems- Intrusion and hold-up alarm systems Part 1: System requirements. (in Czech).
4. Variant plus. SecurityView. [online]. [cit. 20131029]. Available at: <http://www.variant.cz/vyhledavani/?search=security+view>.
5. Variant Plus (2012). Product Catalog 2012-2013. Třebíč: Variant plus, 2012. 325 p. (in Czech).
6. VALOUCH, Jan. Security Technology, systems and management I. 1st ed. Luděk LUKÁŠ. Zlín: VeRBuM, 2011. ISBN 978-80-87500-05-07. Legislation of design security systems, p.171-183. (in Czech).

The Elevation of Positional Mechanisms for the Measurement of Electromagnetic Fields on Cylindrical Surfaces

Ján Ivanka[1,], Petr Navrátil[1]

[1] Tomas Bata University in Zlin, Faculty of Applied Informatics, Nám. T.G.Masaryka 5555,
760 01 Zlin, Czech Republic
{ivanka, p1navratil}@fai.utb.cz

Abstract. The paper presents a study of analysis of tolerance requirements for positioning mechanism for measuring on cylindrical surface with respect to precision of the positioning mechanism (azimuth/elevation) in the field of measuring of near and distant zones of electromagnetic fields of electro-technical devices in the anechoic chamber.

Keywords: electromagnetic compatibility, electromagnetic interference, electromagnetic susceptibility, measurements.

1 Introduction

Electromagnetic compatibility represents a science discipline dealing with the question of undesirable affecting of the function of various technical and biological systems through the action of electromagnetic field while individual system can have or need not have mutual functional relationship. For that reason, the new integrating discipline called ***electromagnetic compatibility (Elektromagnetische Verträglichkeit (EMV) in German, elektromagnitnaja sovmestimost' in Russian) with internationally recognized abbreviation EMC*** as a reflection of the necessary coexistence of electro-technical systems mutually as well as in relationship with respect to live organisms. Sometimes occurring Czech term "*elektromagnetická slučitelnost"* is not considered to be suitable by most of the Czech experts.

Electromagnetic interference (hereinafter EMI) is a process at which the energy produced by an interference source is transferred through an electromagnetic link in the interfered systems.

Electromagnetic susceptibility (EMS) is a property of equipment and systems to operate without defects or with a precisely defined acceptable effect in the environment in which electromagnetic interference is present.

Measurements of electromagnetic interference are very wide and important field. It includes measurement methods and procedures for quantitative assessment of the selected parameters in particular at the interfaces of interference sources and receivers, namely in the field of both near and distant zone. Besides measurements, the field of testing of electromagnetic susceptibility of buildings using so called interference simulators has developed quickly recently. Testing is carried out not only on the finished equipment, but mainly also during its development.

The paper provides basic pieces of knowledge about measurements of the parameters of microwave aerials in the near zone. The objective of this paper is to provide an overview of advantages and disadvantages of the measurements in the near zone and a comparison of measurements in the near and distant zones. The study is determined in EMS and EMI fields in which quite different problems are solved – programs for numerical field calculation in the distant zone including probe correction, reverse projection and gain, software for displaying calculated values, programs for control of scanning equipment and measuring instruments, hardware and apparatuses for measuring including construction of scanning equipment.

Reliable estimate of measurement errors is one the basic requirements for any measuring method; this applies in particular to the methods that use a high level of mathematical analysis such as measurements of areas in the near zone. Determination of limits of errors for any measuring system for a given combination aerial/probe/near zone may be difficult and time demanding task and mathematical complexity is the main reason of the difficultness. For that reason, attempts to bypass mathematical methods and to set the limits of errors for a general method of measuring using measurements for a certain aerial are made frequently. Results of measurements in the distant and near zones are compared when using this approach and the differences between these two methods are taken as a criterion of measurement errors in the near zone. Theoretical relationships that are important for making measurements more accurate (analysis of final dimensions of scanning for cylindrical scanning any analysis of accuracy of the scanning mechanism) are described in the paper. These relationships form a base for analysis of the tolerance requirements for positioning mechanism for measurements on the cylindrical surface with respect to the accuracy of the positioning mechanism (azimuth/elevation). The method of cylindrical scanning attracted probably the least interest in analysis of errors of all generally used scanning methods. It was assumed usually that errors will be similar like errors in planar surface, which is naturally true but it is necessary to investigate some sources of errors that have different impact. Similar analyses have indicated that errors resulting from the measuring system are main sources of errors.

2 Errors of Setting of the Measured Aerial

We will consider ***spherical (R,θ,φ) and cylindrical (r,φ, z)*** system of coordinates according to Fig. 1 for next analysis. The vertical axis (*z* axis) will usually be the axis of rotation for scanning on cylindrical surface.

It is possible to use theoretical analysis for planar scanning in the plane *x,y*, that is mentioned in [3] and [5] to estimate errors in the position of the probe in the direction of axis *z*. In case when the main bundle is approximately perpendicular with respect to *z* axis, the errors for maximum gain and lateral lobes are as follows:

$$\Delta G(\theta,\varphi)_{dB} \le \frac{8,7\Delta_z(\mathrm{rms})}{\eta D_z} g(\theta,\varphi) \text{ for the main lobe,} \qquad \mathbf{(1)}$$

$$\Delta P(\theta,\varphi)_{dB} \leq \frac{4,3\Delta_z(\theta,\varphi)}{D_z} g(\theta,\varphi) \text{ for the lateral lobes,} \qquad (2)$$

where G is aerial gain, P is relative diagram, D_z is main aerial dimension, η is efficiency of aerial aperture and Δ_z is position error in the z axis. The function $g(\theta,\varphi)$ is a ratio of diagram maximum with respect to amplitude in the considered direction. E.g. for the lateral lobe -40 dB, $g(\theta,\varphi)$ equals to 100. We consider a spectrum of errors for angles (θ,φ) in the equations (1) and (2). To eliminate a random error, errors with the same effective value (standard deviation) are considered, which is emphasized using rms denomination. When considering analysis, it is obvious that all conclusions associated with scanning in plane (error of position x, y) including the mentioned examples apply similarly. If you know the spectrum of errors Δ_z of the z position, you will get very realistic estimates of errors in the near zone. The upper limits of errors when we consider only the maximum value of errors will be created in relatively special cases.

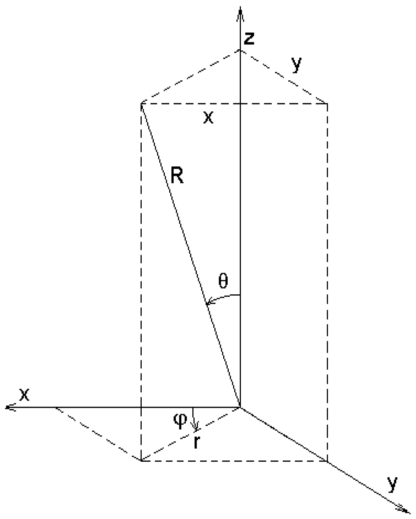


Fig. 1. Spherical system *(R,θ,φ)* and cylindrical system *(r,φ, z)*.

3 Limited Measurement Surface

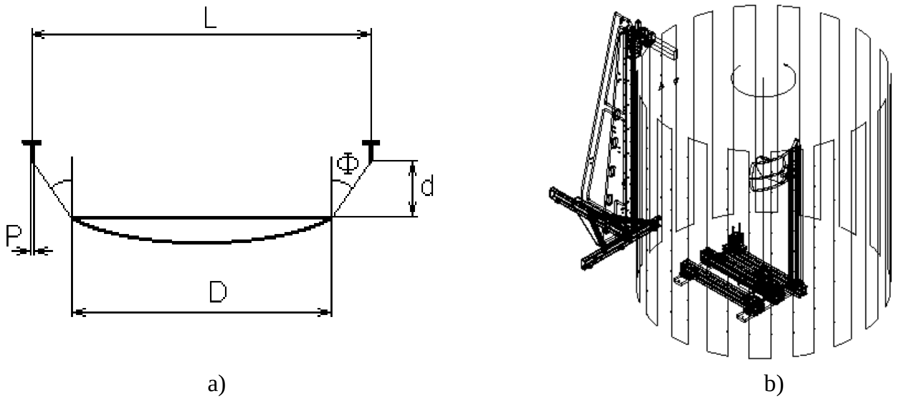
For planar scanning in the near zone, the aerial is installed in a *fixed manner* and the probe in the near zone moves along the planar surface in both x and y directions so that it is possible to scan matrices of samples of field (both amplitude and phase). Similarly, when scanning on the cylindrical surface, a matrix of samples of field for movement in z

direction and in azimuth φ is scanned. The range of scanning for measurements in the z direction indicated in Fig. 2 is important when accuracy of measurements on cylindrical surface in the near zone is considered. The size of the measured aerial and the size and location of the final scanning surface (cylinder) is defined with the critical angle Φ. Calculated emission characteristics of the aerial will be applicable in the zone between ±Φ. The following equation applies to the given scanning range L:

$$L = D + P + 2\,d\,tg\Phi\ , \tag{3}$$

where D is measured aerial diameter, P is probe diameter and d is the distance between the probe and the measured aerial. Complete angular covering can be achieved only by means of scanning on fully spherical surface in the near zone. For example, critical angle $\Phi = 70°$ can be achieved using scanning that is larger by six wave lengths on each side than the aerial aperture in the distance of two wave lengths from the aerial.

The restricted scanning area has two effects. Firstly, the resulting emission areas are applicable only inside of the zone defined in Fig. 2 for the area larger than the area aperture. This criterion is used for determination of the minimum dimension of the scanning plane for the given required zone of angles and separation distance d. As the lower limit for d is given by physical structure of the area and multiple reflections, compromise both between the maximum angular covering together with reduction of errors as a consequence of limited scanning (when small d is required) and minimum multiple reflections (when big d is required) is usually required.



a) b)

Fig. 2. Scanning range determination (a), measuring on cylindrical area (b).

Occurrence of errors for calculation even for the “applicable zone” illustrated in Fig. 2 is another effect of the limited scanning area. The following equation applies to preliminary estimate of errors as a result of the limited scanning area for measurements in planar surface:

$$\frac{|\Delta I(\mathbf{K})|}{|I(\mathbf{K})|} \le \frac{\alpha\lambda L_m b_m(\rho',\varphi_\rho)}{2S\cos\gamma_m}\frac{|I(\mathbf{K}_0)|}{|I(\mathbf{K})|}\ , \tag{4}$$

where *S* is aerial aperture area, L_m is maximum width of the scanning area, α ≈ 1 – 5 is a coefficient of amplitude drop (1 for uniform exposure, but practically not more than 4 commonly used exposures), $b_m(\rho',\varphi_\rho)$ is maximum amplitude of probe output on the edge of the scanning area with respect to the maximum probe output on the scanning area and $|I(\mathbf{K}_0)/I(\mathbf{K})|$ is a ratio of the maximum amplitude in the direction $\mathbf{K}_0$ with respect to the amplitude in the direction **K** (so called inverted value of standardized diagram in distant zone). (11) applies as the upper limit for angles up to 90°, but it can be said very approximately that the equation (4) represents a relatively reasonable estimate of the upper error for the zone of angles smaller than Φ/2 while the estimate (4) is much higher than the actual errors are for larger angles.

The mentioned equation requires less information, however, it generally provides much more higher upper limit of errors. This equation can be used according to [5] also for the aerials that are separable in the *x,y* plane only when scanning along aerial axes as was demonstrated not only theoretically but also experimentally.

$$\mathbf{E}_{o,p} = \frac{\Delta_x \Delta_y}{2\pi} \sum_{m=(-N_x/2)}^{(N_x/2)-1} \sum_{n=(-N_y/2)}^{(N_y/2)-1} \mathbf{F}(m\Delta_x, n\Delta_y) \exp\left[-j2\pi\left(\frac{om}{N_x}+\frac{pn}{N_y}\right)\right], \qquad \textbf{(5)}$$

However, it is necessary to mention that the above mentioned equation does not consider a change of phase along the scanning area periphery when measuring along the aerial axes and for that reason, it could give bigger errors in most cases. It means that it can be assumed that this equation for planar scanning can be used as upper estimate also for cylindrical scanning.

Conclusion

The paper is based on the analysis of errors made in a number of studies. All significant sources of errors were specified, all sources of errors of measurements in the near zone were measured and estimated and the shape of the function dependence of errors was determined in many cases. Combinations of individual components of errors were ascertained in order to obtain a realistic estimate of the resulting measurement errors.

References

1. Vaculíková, P., Vaculík, E.: Elektromagnetická kompatibilita (Electromagnetic Compatibility), Grada Publishing, Praha (1998)
2. Svačina, J.: Základy elektromagnetické kompatibility (Electromagnetic Compatibility Fundamentals), VUT Brno (2001)
3. Rohde & Schwarz, company documents, Test&Measurement Product, Catalog 2007/2008
4. Rohde& Schwarz, Radiomonitoring and Radiolocation, Catalog 2007/2008
5. Repjar, A. G. - Newell, A. C. - Francis, M. H.: Accurate determination of planar near field correction parameters for linearly polarized probes. IEEE Trans. Antennas Prop., AP-36, No. 6, pp. 855-768

Categorization of ITIL® Tools

Lukas Kralik, Ludek Lukas,

Tomas Bata University in Zlín, Faculty of Applied Informatics, Nad Stráněmi 4511
760 05 Zlín, Czech Republic
{kralik, lukas}@fai.utb.cz

Abstract. This paper responds to requirement to improve the orientation between offered SW, as ITIL® tools. There are really a lot of amount thus offered tools and very often leads to poor implementation of ITIL® on the basis of badly chosen tools. So this article aims to create dividing, which should facilitate choice of a suitable tool. Simultaneously, this division will serve for further work on creating a methodology for evaluation of ITIL® tools.

Keywords: ITIL®, ITIL® tools, tools categorization, IT service support, ITIL implementation.

1 Introduction

With development of information and communication technologies (ICT) and their intrusion into all sectors, gaining management and delivery of IT services different dimension and meaning. The quality of providing or managing of IT services can greatly affect the operation or performance of the company. For this reason it was introduced, the now internationally acclaimed standard known as ITIL®. It is an abbreviation for Information Technology Infrastructure Library. It is a set of concepts and practices that allow better planning, use and improve the use of IT, whether by the providers of IT services or by the customers.

The project originated in Great Britain in the mid 80s. Development of the first version lasted until 1995, and except of Great Britain it was applied and also used in the Netherlands. Since then undergone a series of changes so that it always match the current demands and conditions. Currently is ITIL® in version 3 (ITIL ® V3) and consists of five key books (titles) - hence the name for the library:

1. Service Strategy
2. Service Design
3. Service Transition
4. Service Operation
5. Continual Service Improvement

According to the general definition of tool is a means of realizing certain activities, possibly used to communicate the results of that activity. The tool is tied to a specific technology or with some real technological or social procedure (or process). Based on this definition and the current version of ITIL® v3 can say that ITIL® is an arbitrary software tool which use leads to provably improve and streamline the providing and managing IT services. The only condition is that there must be a SW. It follows that as ITIL® tool can be used even standard office software. Everything stems from its use. Many SW is described as ITIL® tool, but if not properly used so labeling it as ITIL® tool is certainly not in place

The uses of ITIL® tools are complicated due to the wide range of offered tools and often very expensive. This caused and to a certain extent still causes small and medium companies are disinterest of the use of ITIL®. On the other hand, recently is beginning to discover significant amounts of Free and Open Source SW even between ITIL® tools.

2 Categories for ITIL® tools

Due to the variety of software tools that support service management according to ITIL ® is very difficult to create and define a formal category for ITIL ® tools. The vast majority of software tools that are currently used in practice support a variety of processes. Tools focused on only one process is almost a matter of history. Categorization ITIL tools according to the current version of ITIL ® V3 is so complicated that the current version focuses on the management of IT services compared to the ITIL ® V2 was focused on the processes which allow easier categorization.

SW, which can be used as ITIL® tools, can be generally divided into three basic categories by (fig. 1):

1. Availability - way of licensing
2. Number of main functions
3. Main purpose

2.1 Division by availability

The simplest division ITIL® tools are according to availability or by the license under which it is available.

1. Proprietary SW
   - Commercial SW
   - Freeware
2. Open Source SW
3. Free SW

Proprietary SW. Also known as a closed source software is software where its author modifies licenses (typically EULA) or otherwise, the possibility of its use. For such software is usually available free source code or it is impossible free to make modifications and distribute the resulting work.

Commercial SW. It is distributed for a fee. This means that if you want to use the product, you have to pay for creators. Such software usually can only be used by the limitation of its license. It is often limited by number of installations of software simultaneously, transfer, license or right to modification of the product.

Freeware. This type of software is distributed free of charge (or for a symbolic fee type of mission cards, often the author allows (but does not require) for the satisfaction of sending a donation), sometimes is talked about the type of software licenses. Conditions for the free use and redistribution are defined in the license agreement, which is often specific to each freeware.

The freeware author retains the copyright, for example, does not allow any program modification or restrict free use only for specific purposes (eg various combinations of the following restrictions: only for non-commercial purposes, only for personal use, only the home PC, only education in schools, only charities, only specific types of equipment, just to view files generated by the actual paid software, etc..). In some cases, the author also requires free registration or restricts the manner of distribution. Some freeware can also be used in companies working on computers, but only if it is not used for the direct providing of commercial services. Freeware software is so different from Free Software or Open Source software.

Free and Open Source SW. At first sight, the differences between Free and Open Source SW minimal and for layperson it is easy to swaps between these two types of SW. The main difference is the ideology of Gross.

Open Source SW. According to the Open Source Initiative, the SW must meet several requirements. These assumptions are not restricted as it could of Open Source associate only to the obligation to provide the purchaser access to the source code of a computer program, but also include other legal relations. These are the following requirements to be met by the license terms to a computer program (the definition of Open Source version 9.1):

- Free redistribution
- Source code
- Derived works
- Integrity of the author's source code
- No discrimination against persons or groups
- No discrimination against fields of endeavor
- Distribution of license
- License must not be specific to a product
- License must not restrict other software
- License must be technology-neutral

Free SW. Free software" means software that respects users' freedom and community. Roughly, it means that the users have the freedom to use this SW. Thus, “free software” is a matter of liberty, not price. To understand the concept, you should think of “free” as in “free speech,” not as in “free beer”.

A program is free software if the program's users have the four essential freedoms:

1. The freedom to run the program, for any purpose.
2. The freedom to study how the program works, and change it so it does your computing as you wish. Access to the source code is a precondition for this.
3. The freedom to redistribute copies so you can help your neighbor.
4. The freedom to distribute copies of your modified versions to others.

2.2 Division by main purpose

Based on the experience from practice ITIL tools can be divided into seven categories according to their primary purpose.

1. Service desk
2. Monitoring, event & remote management
3. Service life cycle
4. Service portfolio and management
5. Cloud
6. Information security
7. Others

Service desk. Service Desk is the single point of contact between the service provider and users. A typical Service Desk manages Incidents and service requests and handles communication not only with users but also with the management of the company. For its correct operation are needed different tools. They are mostly integrated into a single software solution most often in the form of a portal. However, there are a number of tools aimed at specific function or process (e.g. Service Level Management - SLM).

Monitoring, event & remote management. Previously, these tools can be found under the name of NSM (Network and System Management). Allow monitoring networks and individual elements, systems, servers, applications and tracking incidents and other events by setting thresholds for optimal use of allocated resources and components. Although it is not a rule, it is integrated into the Incident Management and in most cases allows remote management.

Service life cycle. Specifically, it is a tool aimed at managing and supporting the entire lifecycle services. This area is also called the ALM (Application Lifecycle Management). But here come the tools of the field, which formally ITIL® does not cover (e.g. software development).

This type of instruments covering various platforms for developers, including support for versioning (source code revision tool), visualization platforms and different ways of testing (functional, security, load, ...) and both manual and automated.

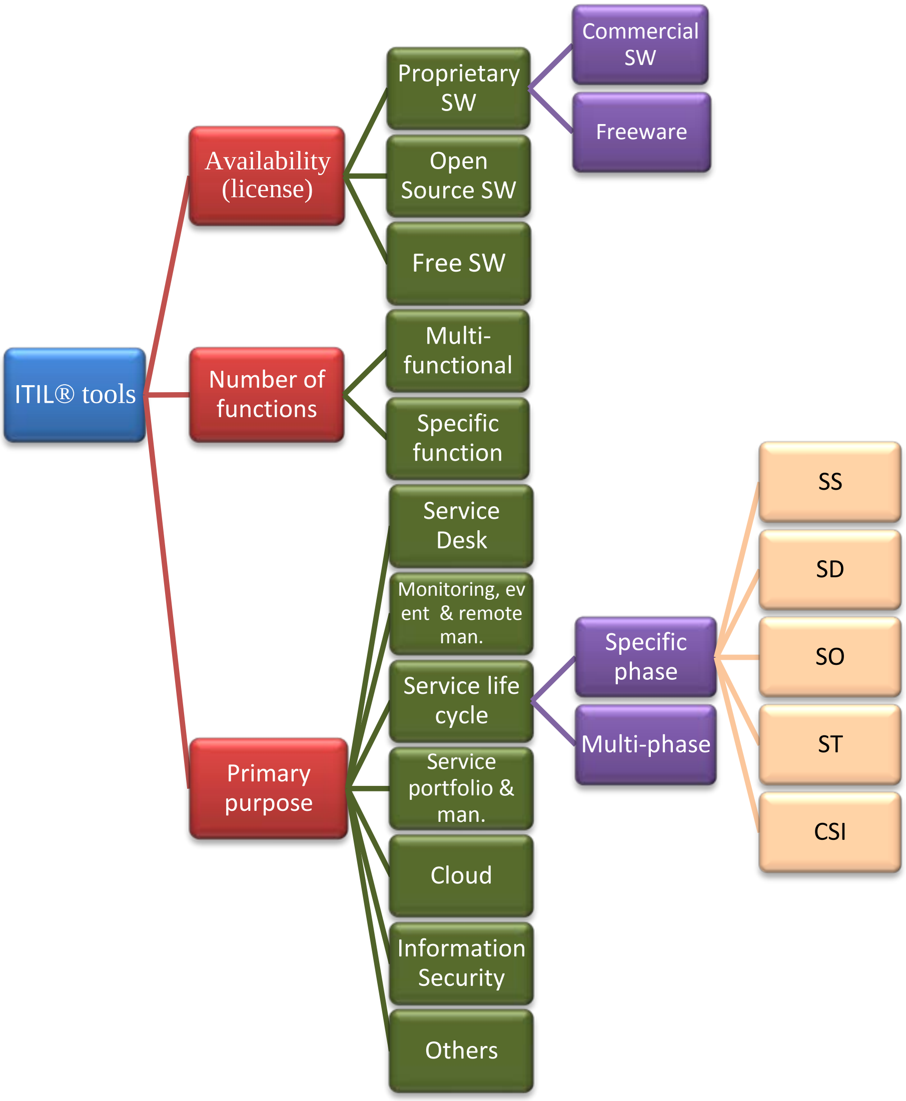


Fig. 1. Systemization of ITIL® tools

Service portfolio and management. Tools in this category helps manage and control a complete portfolio of services, projects and programs. In addition, it is support a variety of processes such as Demand Management, Project Management, Program Management, Financial Management, Time Management and Resource Management.

Cloud. In this category are tools for the management and providing services in cloud for providers, as well as for users, or customers. Tools allow offer services (ordering), activation (deployment), their providing (provisioning) and of course invoicing (billing). However intervene here even instruments from category Service Desk and all functions are integrated into a single portal solution.

With taking into account to the events at present there is a great emphasis on speed, security, automation and intuitiveness of a particular solution. This category of instruments is typically proprietary software because they are designed for producers and their HW. However, Open Source software today has actually covers a wide range of areas and also for this category is not a problem to find a representative between Open Source and Free SW.

Information security. This category includes instruments starting with the anti-virus protection, through various tools for data security and test programs (penetration tests) to tools for monitoring. When monitoring is, however, an emphasis on security attributes (data theft, hacking, data corruption, etc.). Included in this category are access control systems (Access Management), which include central authentication and authorization of users, including the use directory services to control access to network elements, mobile devices. Finally, there are also physical security management, data protection and compliance with safety standards.

3 Conclusion

Update ITIL v3 has brought a number of changes. One of them is the approach to ITIL tools. This change led to simplify the implementation of ITIL, or allow IT managers to choose from a much wider range of software tools that can be considered as ITIL tools. Use of ITIL® tools is complicated and often very expensive due to the offered a wide range of tools. This caused and to a certain extent still causes small and medium companies are disinterest of the use of ITIL®. On the other hand, recently is beginning to discover significant amounts of Free and Open Source SW even between ITIL® tools.

The aim of dividing and systemization of ITIL® tools is make the orientation in the offered SW tools not only easier, but also to prove to IT managers working in small and medium-sized companies that the use of ITIL® tools and thus the implementation of ITIL® is not a matter for only large companies and international enterprises.

Acknowledgments. This work was supported by grant No. IGA/FAI/2014/020 from IGA (Internal Grant Agency) of Thomas Bata University in Zlin.

References

1. Automated Unattended Installation in Kovárna Viva, a.s. In: International journal of computers. Oregon (USA): North Atlantic University Union, 2014, s. 7. ISSN 1998-4308.

2. KRÁLÍK, Lukáš. Searching sources and evaluation criteria for open source itil® tools. In: Mezinárodní Masarykova Konference Pro Doktorandy A Mladé Vědecké Pracovníky. Hradec Králové: Magnimitas, 2013, s. 6. ISBN 978-80-87952-00-9.
3. KRALIK, Lukas. Analysis for Automated Unattended Installation. In: Recent Advances in Automatic Control, Information and comunications: Proceedings of the 14th International Conference on Automation & Information (ICAI '13). Valencia (Španělsko): WSEAS press, 2013, s. 5. ISBN 978-960-474-316-2ISSN 1790-5117.
4. KUFNER, Vladimír. ITIL V3: Změny v klíčových publikacích. DSM - data security management. 2012, č. 2, s. 7.
5. BUCKSTEEG, Martin. ITIL 2011. 1. vyd. Brno: Computer Press, 2012, 216 s. ISBN 978-80-251-3732-1.
6. ITIL continual service improvement [online]. 2nd ed. London: TSO, 2011, xi, 246 s. [cit. 2013-07-22]. Best Management Practice. ISBN 978-0-11-331308-2. Dostupné z: http://www.best-management-practice.com
7. ITIL service transition [online]. 2nd ed. London: TSO, 2011, xii, 347 s. [cit. 2013-07-22]. Best Management Practice. ISBN 978-0-11-331306-8. Dostupné z: http://www.best-management-practice.com
8. ITIL service design [online]. 2nd ed. London: TSO, 2011, xi, 442 s. [cit. 2013-07-22]. Best Management Practice. ISBN 978-0-11-331305-1. Dostupné z: http://www.best-management-practice.com
9. ITIL service operation [online]. 2nd ed. London: TSO, 2011, xi, 370 s. [cit. 2013-07-22]. Best Management Practice. ISBN 978-0-11-331307-5. Dostupné z: http://www.best-management-practice.com
10. ITIL: service strategy [online]. London: Stationery Office, 2011, xii, 264 s. [cit. 2013-07-22]. ISBN 978-011-3310-456. Dostupné z: http://www.best-management-practice.com/
11. JAŠEK, Roman, SZMIT, Anna, SZMIT, Maciej. Usage of Modern Exponential-Smoothing Models in Network Traffic Modelling. In Nostradamus 2013: Prediction, Modeling and Analysis of Complex Systems. Heidelberg : Springer-Verlag Berlin, 2013, s. 435-444. ISSN 2194-5357. ISBN 978-3-319-00541-6.
12. JAŠEK, Roman, SZMIT, Anna, SZMIT, Maciej. Usage of Modern Exponential-Smoothing Models in Network Traffic Modelling. In Nostradamus 2013: Prediction, Modeling and Analysis of Complex Systems. Heidelberg : Springer-Verlag Berlin, 2013, s. 435-444. ISSN 2194-5357. ISBN 978-3-319-00541-6.
13. JAŠEK, Roman, KOLAŘÍK, Martin, VÝMOLA, Tomáš. APT Detection System Using Honeypots. In Proceedings of the 14th WSEAS International Conference on Automation & Information (ICAI ’13). Montreux : WSEAS Press, 2013, s. 25-29. ISSN 1790-5117. ISBN 978-960-474-316-2.
14. KRBEČEK, Michal, SCHAUER, František, JAŠEK, Roman. Security aspects of remote e-laboratories. International Journal of Online Engineering, 2013, roč. 9, č. 3, s. 34-39. ISSN 1868-1646.
15. Vala, Radek; Malaník, David; Jašek, Roman. Usability of software intrusion-detection system in web applications. In International Joint Conference CISIS ´12-ICEUTE ´12-SOCO ´12. Heidelberg: Springer-Verlag Berlin, 2013, s. 159-166. ISSN 2194-5357. ISBN 978-3-642-33017-9.

Proposal of Workplace for Testing of Electromagnetic Susceptibility – Electrical Fast Transient/Burst

Hana Urbancokova, Jan Valouch, Milan Adamek, Michal Nagy,

Tomas Bata University in Zlín, Faculty of Applied Informatics, Nad Stráněmi 4511
760 05 Zlín, Czech Republic
{urbancokova, valouch, adamek, nagy}@fai.utb.cz

Abstract. In the present the level of interference critically increases as a result of increasing amounts of electrical equipment and appliances in our environment. This interference exist in the frequency ranges from 0 Hz till hundreds GHz and possibility of mutual interference between devices is high. For this reason every electronic device should be tested if it meets the requirements for electromagnetic compatibility. Frequently sensitive electronic devices have to work in the environment with strong interference and based on their insufficient electromagnetic immunity happens many errors and unwanted situations. This type of unwanted situation is for example damage of faxes, answering machines and telephones in the storms. The reason is their low overvoltage resistance and improper or missing overvoltage protection.

Keywords: electromagnetic compatibility, electromagnetic susceptibility, immunity, fast transient, burst

1 Introduction

Electromagnetic compatibility as an individual scientific and technical discipline was established in the United States in the sixties of the 20th century. At the beginning this topic was interesting just few experts working in the military and cosmic industry. With the progress of electronic, microprocessor and communication technology the electromagnetic compatibility reach our everyday life and still more and more scientists start to study it. [1]

Electromagnetic compatibility is basically the ability of coexistence of devices and systems in the common electromagnetic environment without significant influence of their normal function. Within security alarm systems electromagnetic compatibility is important especially in the cases of mutual integration of alarm and non-alarm applications. With regard to stability of function of security systems cannot come to changes in their condition, to damage of their components or essential features by the effect of electromagnetic interference. [2]

The aim of this paper is to explain the problems of electromagnetic compatibility with a focus on electromagnetic susceptibility follow by proposal and realization of testing workplace of electromagnetic susceptibility for testing electrical fast transient/burst consistent with the basic standards of electromagnetic compatibility.

2 Terminology and Definitions

Electromagnetic compatibility (EMC) is the ability of equipment, system or device to function satisfactorily in its electromagnetic environment. In this environment are present sources of electromagnetic signals, which can have adversely effect. Electromagnetic signals can have natural or artificial character. Another part of EMC is the ability of equipment, system or device to function without introducing intolerable electromagnetic disturbances to anything in that environment.

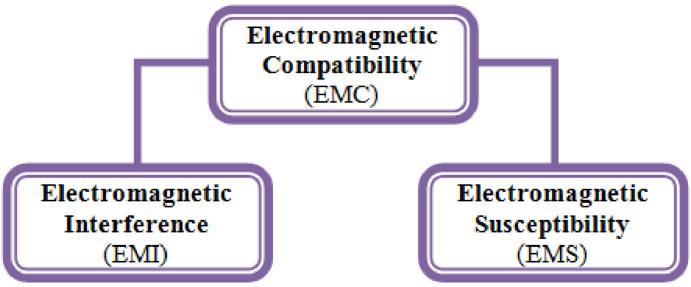

Electromagnetic Compatibility (EMC)
Electromagnetic Interference (EMI)
Electromagnetic Susceptibility (EMS)

Fig. 1. The basic breakdown of problematic of EMC

Electromagnetic interference (EMI) is the process of transmitting signal, which is generated by the source of interference, into the disturbed system. This signal is transmitted by the electromagnetic binding. Particular it is about the identification of sources of interference, their description and measurement of interference signals, identification of parasitic transmission paths and establishing of actions primarily in the resources of interference and their transmission paths. EMI deals with the causes of disturbance and their removal.

Electromagnetic susceptibility (EMS) (immunity to a disturbance) is the ability of a device, equipment or system to function without degradation in the presence of an electromagnetic disturbance. They must work without error or with clearly defined of possible influence. EMS deals with the technical measures which increase electromagnetic immunity of receivers. EMS is focused on removing the consequences of interference, without removing their causes.

By reason of proposal and realization of testing workplace of electromagnetic susceptibility for testing electrical fast transient/burst we should be familiar with the following terms and abbreviations:

- *EUT* - abbreviation of the equipment under test;
- *EFT/B* - electrical fast transient/burst;
- *Transient* is pertaining to or designating a phenomenon or a quantity which varies between two consecutive steady states during a time interval short compared with the time-scale of interest;
- *Burst* (of pulses or oscillations) is a sequence of a limited number of distinct pulses or an oscillation of limited duration; [3]
- *I&HAS* (Intrusion and hold-up systems) is a complex set of technical equipment which solve the protection against unauthorized entry to the building.

3 Normalization in the Field of EMC

Due to the impossibility of achieving absolute electromagnetic immunity of devices, systems or equipments they need to be established specific unified international standards, recommendations and EMC regulations. These documents are describing, for example unified standards and limits of the maximum permitted interference level for specific types of equipment or accurate and reproducible conditions for the measurement and verification of the electromagnetic susceptibility equipment.

Directive 2004/108/EC Electromagnetic Compatibility(EMC) (Directive 2004/108/EC repealing Directive 89/336/EEC is valid in all countries of the European Union. This directive is strictly monitored and sanctioned. It provides the general requirements of the EMC for commissioning of the equipment or system on the market. Devices are prohibited to sell, to exhibit or advertise if they do not comply requirements from the directive and there are not demonstrated its requests. Such device can be financially sanctioned and prohibited.

When we need to explain the terms related to the issue of EMC we should have the International Electrotechnical Vocabulary (IEV) IEC 60050 - Chapter 161: Electromagnetic compatibility. It describes all the basic terms. Czech version of this dictionary is CSN IEC 60050. [4]

Standards relating to EMC is multitude, but the basic sets of standards have a designation of CSN IEC 1000 and CSN EN 61000. Interference immunity is especially devoted to set of standards CSN EN 61000-4. Primarily, we follow the standard CSN EN 61000-4-4 ed. 2 Electromagnetic compatibility (EMC) - Part 4-4: Testing and measurement techniques - Electrical fast transient/burst immunity test in this contribution. Another important standard is the standard for the electromagnetic immunity for security systems CSN EN 50130-4 ed.2 Alarm systems - Part 4: Electromagnetic compatibility - Product family standard: Immunity requirements for components of fire, intruder, hold up, CCTV, access control and social alarm systems.

4 Test Levels, Equipment and Set

EFT/B represents the low-energy broadband interference pulses in the form of the groups of short transients. Usually they are created from the influence of inductances of switching processes in the power supply, signal or data networks. They may be also created by the influence of contact bounce electromechanical relays or the influence of switching high-voltage switches. Their typical characteristics are very short rising edge, short duration, low total energy (10-3J) and high repetition frequency. Generally EFT/B does not cause the direct damage to electronic equipment, but by its wide spectral range (up to approx. 200 MHz) they produce a significant high frequency electromagnetic interference. This interference is undesirable especially in numeric systems. Process EFT/B interference is similar to the work signals of the numeric devices and so it may arise an error in the transmitted signals in the numeric systems. [1]

Test conditions for testing of fast transient / burst are described in the basic standard CSN EN 61000-4-4 ed. 2 [3]. The aim of the test is to demonstrate the immunity of the EUT against fast transients, which arise at the switching contact or repeated discharge on the rebound contacts (relays, contactors, switching inductive loads). During the testing EUT is exposed to the groups of pulses containing a large number of fast transients, which are introduced to the input/output power supply, control, signal and data ports of the test devices. The interfering signal is represented by the Electrical Fast Transients grouped into groups of pulses (burst). [5]

Test levels for testing fast transient phenomena are presented in the following table. This are the test levels usable for the power supply, grounding, signal, data and control inputs and outputs of the test equipment.

Table 1. Test levels

Output testing of open-circuit voltage and repetition frequency of pulses				
Level	**On AC and DC power supply ports**		**On signal, data and control ports I/O (input/output)**	
	Open-circuit peak voltage kV	**Repetition frequency** kHz	**Open-circuit peak voltage** kV	**Repetition frequency** kHz
1	0,5	5 or 100	0,25	5 or 100
2	1	5 or 100	0,5	5 or 100
3	2	5 or 100	1	5 or 100
4	4	5 or 100	2	5 or 100
X	special	special	special	special
„X“ is the open level, which should be determined in the specifics of a particular device				

Selection of the test level is realized on the base of the expected and the most realistic of installation and environmental conditions in which the device should work. It will be followed by the immunity test of the device at these levels. Test levels are divided into 5 levels.

- Level 1: well protected environment;
- Level 2: protected environment;
- Level 3: typical industrial environment;
- Level 4: adverse industrial environment;
- Level 5 (X): Special situations which must be analysed.

The key device for testing electromagnetic susceptibility is the generator of impulses (burst), which in our case is chosen the testing device AXOS5 from Haefely EMC Technology. The main elements of the generator are:

- high voltage source (U),
- charging resistor (Rc),
- energy storage capacitor (Cc),
- high voltage switch,
- pulse duration shaping resistor (RS),
- impedance matching resistor (Rm)
- DC (direct current) blocks capacitor (Cd).

Simplified diagram involvement of the generator is shown in the following figure.

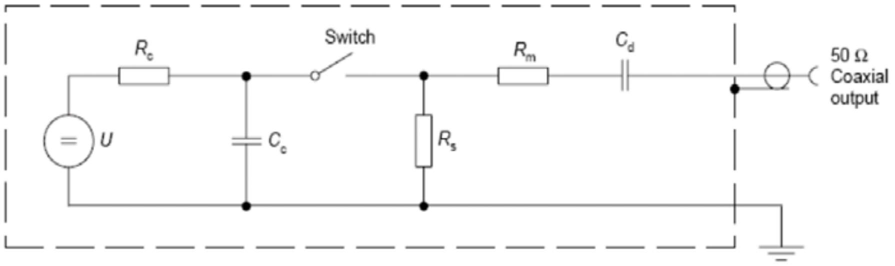


Fig. 2. Simplified diagram of the generator of the electrical fast transient/burst

For acceptance test of the input/output AC/DC (alternating current/ direct current) power supply is requested coupling/decoupling network (such as three-phase power network). Capacitive coupling clamp provide a bond of fast transient / burst into the test circuit without galvanic connecting with terminal input/output EUT, with the shielded cables or other part of EUT.

The test suite for testing EMC for electrical fast transient/burst contains the following basic test equipment:

- test generator,
- coupling equipment (network or clamp),
- decoupling network,
- ground reference plane. [3]

5 Proposal and the Design of the Workplace

The testing of the electromagnetic susceptibility of devices is performed with the help of interference simulators (EMC simulators). Based on the testing is practically verified EMS degree of the test equipment or its individual components.

For the testing of EMS are for the components of alarm systems specified tests and related test level (values of the voltage drops, test voltage, the field strength, frequency range and modulation type of interference signals etc.). These tests and test levels are determined for indoor and outdoor applications, for fixed, moving and portable devices.

On the testing device, which is a component of I&HAS - wireless relay AC82, we will perform the test in an accordance with CSN EN 50130-4 ed. 2 [6]. A time of each test is set at 1 minute. The value of the test voltage is corresponds to the level 3 according to basic standard CSN EN 61000-4-4 Ed. 2 [3], which is characterized as a typical industrial environment. There are not suppressed EFT/B in the power supply and signal circuits, industrial circuits are not completely separated from other circuits, power supply lines is not completely separated from control, signal and communication cables and moreover there are used dedicated cables for power and signal lines. [5]

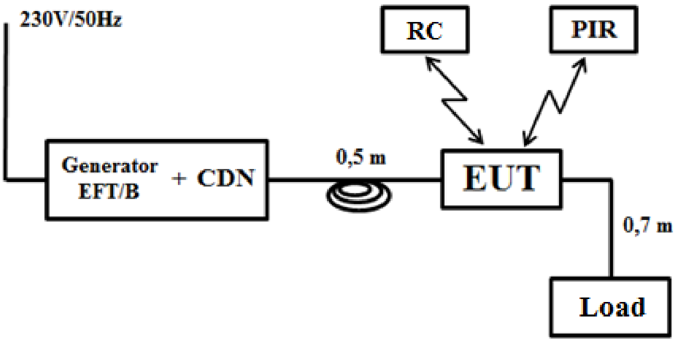


Fig. 3. Diagram of the proposed workplace for the testing EMS

Description of the testing set up shown in Fig. 3:

- Generator EFT/B + CDN (coupling/decoupling network) - testing device AXOS5;
- EUT - wireless relay AC82;
- Load - two 15W light bulbs;
- RC – remotely control RC86W;
- PIR – PIR detector JA83P.

The proposed workplace was placed on a wooden table 80 cm high, with the upper surface of 150x100 cm. Table was placed on the ground reference plane and on the entire surface of the table was also placed ground reference plane. EUT and all cables connected with the EUT were placed as described in the standard CSN EN 61000-4-4 Ed. 2 on an insulating underlay of 10 cm above the ground reference plane and at a distance of 0.5 m from the other conductive structures (e.g. walls of the room). Testing device AXOS5 was powered from the network 230V/50Hz and all the test set was properly grounded.

The parameters of the testing device AXOS5 from Haefely EMC Technology satisfy the requirements arising from the provision set of standards CSN EN 55016 Specification for radio disturbance and immunity measuring apparatus and methods. On the tested wireless relay AC82 was connected load in the form of two 15W light bulbs and EUT wirelessly communicate with the PIR detector and remotely control.

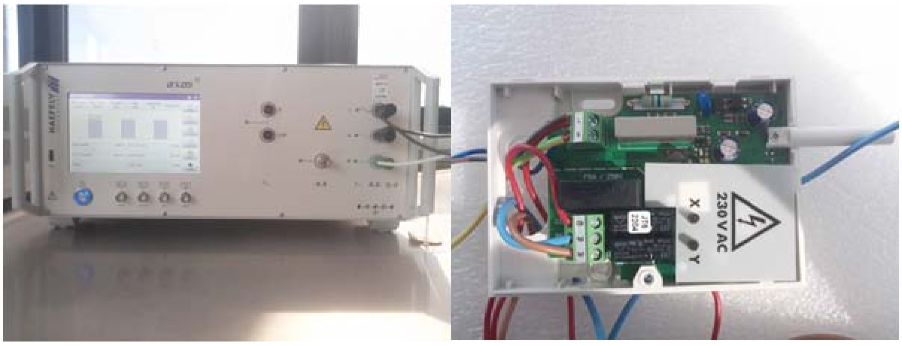


Fig. 4. On the pictures: testing device AXOS5 *(left)*, wireless relay AC82 (*right)*

At the beginning of the testing was on the EUT performed functional tests and EUT was subsequently connected to the proposed test workplace. During testing the device was monitored whether or not the EUT occur status change at any of the tested voltage peak and after each test was verified full functionality of the EUT. Repetition frequency for fast transients was set to 100 kHz, and the length of one test was 1 minute. According to the criteria for meeting the requirement in accordance with CSN EN 50130-4 ed. 2 it must not experience any damage, malfunction or change of status of the EUT during testing. Only the flashing indicator was permissible if it does not occur any residual change in the EUT. To these requirements the wireless relay AC82 complied since during testing, there were no changes in status, faults or damage to the EUT.

Table 2. Record of the measurements of the EUT

Number of measurements	Peak voltage	Regime of the EUT	Change during testing	Functionality of the EUT
1.	+ 200 V	OFF	none	full functionality
2.	+ 200 V	ON	none	full functionality
3.	- 200 V	OFF	none	full functionality
4.	- 200 V	ON	none	full functionality
5.	+ 1000 V	OFF	none	full functionality
6.	+ 1000 V	ON	none	full functionality
7.	- 1000 V	OFF	none	full functionality
8.	- 1000 V	ON	none	full functionality
9.	+ 2000 V	OFF	none	full functionality
10.	+ 2000 V	ON	none	full functionality
11.	- 2000 V	OFF	none	full functionality
12.	- 2000 V	ON	none	full functionality

6 Conclusion

Because of the impossibility of eliminating all the real or potential sources of interference signals is necessary to ensure, that the electronic equipment function properly in their presence. Great accent on the electromagnetic immunity is given to components of I&HAS. Their aim is to detect and signal the presence, ingress or attempted ingress of the intruder into the building, or the alarm status caused intentionally by the user. It is therefore important for components of I&HAS to be tested for EMS. Their trouble-free operation must be ensured not only in the residential and commercial environments, but also in the industrial environments.

Rules and processes for performing of the test of susceptibility to interference of type electrical fast transient/burst are generally described in the standard CSN EN 61000-4-4 ed. 2. EFT/B can arise when the switching contactor is repeated discharge on the rebound contacts (relays, contactors, switching inductive loads, etc.). Though EFT/B usually does not cause the direct damage to electronic equipment, it is a short overload of the circuit, which is unwanted for us. The influence of overload can arise faulty transfer of information, which for I&HAS components may cause unwanted change in the status of the equipment, or induce false alarm.

To the EMS for components of I&HAS, CCTV, access control and social alarm systems there is a separate standard CSN EN 50130-4 ed. 2, which describes more the individual immunity tests for each type of interference that they have an effect on these devices. According to this standard the EUT was exposed to the fast transients fed to the power input during the test for susceptibility to EFT/B. Test function of the EUT was performed according to the instructions before was started testing and after each one test. During the testing with different voltages of the EUT was monitored whether does not occur some change in its status. Wireless relay AC82 complied all the requirements. The EUT was fully functional during all the time of testing and at each test there was no fault or status changes.

Acknowledgments. With support by grant No. IGA/FAI/2014/052 from IGA (Internal Grant Agency) of Thomas Bata University in Zlin and the European Regional Development Fund under the project CEBIA-Tech No. CZ.1.05/2.1.00/03.0089.

References

1. SVACINA, J.: Electromagnetic compatibility: Principles and comment. University of Technology, Brno (2001), 156 p. ISBN 80-214-1873-7.
2. VALOUCH, J.: Integrated Alarm Systems. In: Computer Applications for Software Engineering, Disaster Recovery, and Business Continuity. The 2012 International Conference on Disaster Recovery and Business Continuity, Jeju Island, Korea. Proceedings. Series: <http://www.springer.com/series/7899> Communications in Computer and Information Science, vol. 340, XVIII. Berlin: Springer Berlin Heidelberg (2012). Chapter, pp. 369--379. ISBN 978-3-642-35267-9.
3. CSN EN 61000-4-4 ed. 2: Electromagnetic compatibility (EMC) - Part 4-4: Testing and measurement techniques - Electrical fast transient/burst immunity test. The Czech Office for Standards, Metrology and Testing, Prague (2005)
4. VACULIK, E., VACULIKOVA, P.: Electromagnetic compatibility of electrotechnical systems: A practical guide to technology limitations HF electromagnetic interference. 1. ed. Grada Publishing, Prague (1998), p. 487. ISBN 80-716-9568-8.
5. VALOUCH, J.: Electromagnetic compatibility alarm systems - testing and measurement of electromagnetic parameters. In: Security magazine. Ed. No. 107, 3/2012. Security Media, Prague (2012), pp. 24--29. ISSN 1210-8273.
6. CSN EN 50130-4 ed. 2: Alarm system. Part 4: Electromagnetic compatibility - Product family standard: Immunity requirements for components of fire, intruder, hold up, CCTV, access control and social alarm systems. The Czech Office for Standards, Metrology and Testing, Prague (2012)
7. VALOUCH, J.: Requirements for Alarm Systems in Terms of the Electromagnetic Compatibility. In: KRIVANEK, V. and STEFEK, A. (ed.) International Conference in Military Technology Proceeding, ICMT'13, University of Defence, Brno (2013), pp. 589--596. ISBN 978-80-7231-918-6.

Safety of database storage for remote laboratories and laboratory management system

L. Pálka[1], F. Schauer[1], [2] and R.Jašek[1],

[1]Tomas Bata University in Zlín, Faculty of Applied Informatics, Nad Stráněmi 4511, CZ-760 05 Zlín, Czech Republic. E-mail: l_palka@fai.utb.cz
[2]Faculty of Education, Trnava University in Trnava, SK-918 43 Trnava, Slovak Republic

Abstract. In spite of the fact that remote laboratories have been existing for at least three decades, virtually no attention has been devoted to the security of this new subject. The paper deals with the security of the data storage of the Datacentres (DTC), with remote laboratories working under the Laboratory Management System (LMS). Especially, the security risks for the data storage and corresponding data processing to ensure the operation of the data warehouse are described in detail.

Keywords: data security, database security, data storage, rig, remote experiments, work with data in the data warehouse, data warehouse design.

1 Introduction - Remote laboratories and laboratory management systems - state of the art

At the present stage of the development of Information Communication Technologies (ICT) there are plenty simulations and remote experiments for science and education purposes [1][3][9]. Remote experiments and informatics resources are tools that are closely related and definitely need to process and store substantial amounts of data. Data, used with remote laboratories (RL), may have the form of simple queries, data analysis, comparative analysis and data mining for associative analysis, extrapolation or predictive trend analysis. Surprisingly, in spite of the fact the RL have been existing for at least three decades [1], virtually no attention has been devoted to the security of this new ICT subject [8].

The present paper deals with the security and safeguarding of the data processed and especially stored in the DTC with remote laboratories, especially that with Laboratory Management System (LMS).

In this connection we will use the term data warehouse (DW) (see Figure 1 data warehouse functioning) [4][6], referring to a complex system that allows to collect, organize, store and share consolidated data from all available operating systems, optimized for reporting, analysis, and data archiving. Users exploit the data warehouse for reporting, in this respect synonymous for business intelligence technology, based on the use of the data and its accumulation, preservation and presentation. The working principle of the DW is that the data we need to process is first stored into the database in a raw state, then follows data classifying using OLAP[1] in data cubes l (see Figure 1) and then, using architecture model (e.g. experiments evaluation or search), and subsequent results storing and reporting.

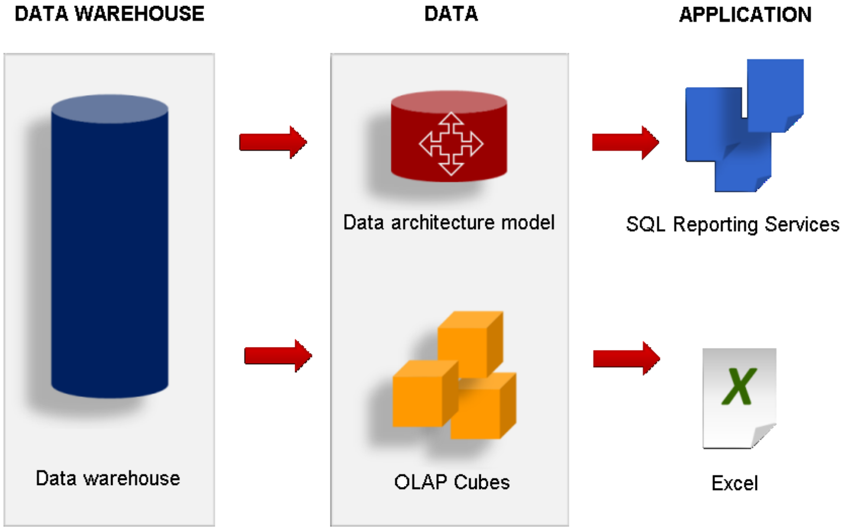


Fig. 1. Schematic representation of the data warehouse functioning.

The layout of the paper is following. In Chapter 1, the typical scheme of the communication of a typical remote experiment (RE) , built as the finite-state machine (FSM) [2], using the Internet School Experimental System (ISES) physical hardware, is described[10] (for the ease of reading we will next denote the set of the individual remote experiment by the word rig). Also, the control program compiling and the type of the data generated and transferred is shortly described. More detailes may be found in corresponding literature [2][8]

The Chapter 2 is devoted to describing the architecture Remote Experiments and the corresponding integrating management system, called for our purposes Remote Laboratory Management System (RLMS) [10]. The Chapter 3 is devoted to the actual risks, the remote laboratories are exposed. [13][14] The Chapter 4 is then focused on

[1] Online analytical processing: OLAP tools enable users to analyze multidimensional data interactively from multiple perspectives.

the corresponding security of a typical DW of a university datacentre (DTC) with LMS for remote laboratories. The final chapter 5 is oriented on prospective future warehouse security measures, followed by conclusions.

2 ISES Remote experiment (RE) and Remote laboratory management system (RLMS) – tools used

Only recently has emerged a serious problem stemming from analysis of research data. ISES is a powerful tool for process and experiments control, acquisition, collecting and data processing in real time. Let us mention the basic features of the ISES system, more detailed description may be found elsewhere [2][10]. The basis of the system is ISES board, which is available in several versions, differing depending on the number of inputs/outputs and also on type of communication with the control PC (by PCI card, USB connector, Wi-Fi). To this board are, by a unique connector, plugged in sensors like: ammeter, voltmeter, thermometer, position sensor, ohmmeter, load cell, anemometer, microphones, sonar, light gate, pH meter, conductivity meter, heart rate monitor, etc. [8]. The layout arrangement of the RE is in Figure 2.

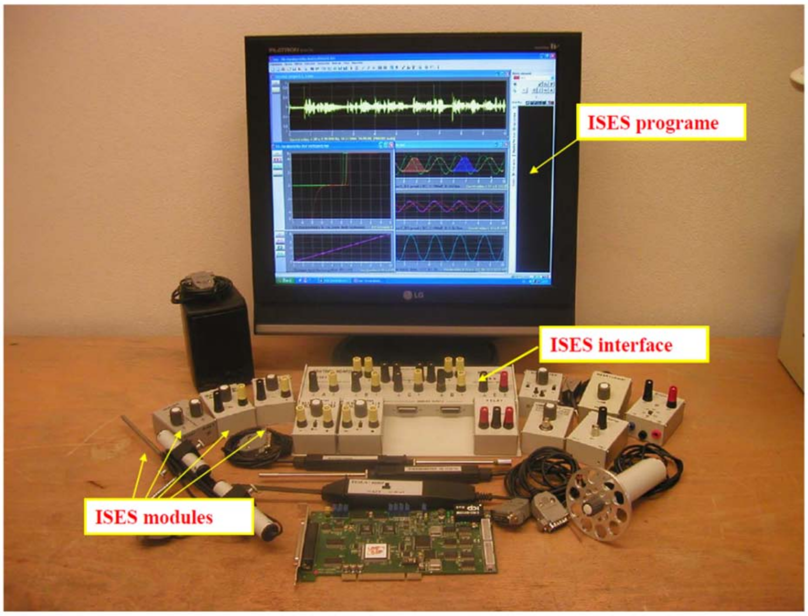


Fig. 2. ISES – Internet School Experimental System.

The most important component is the Measureserver module, functioning as finite-state machine (FSM) controlled by the controlling program of the PSC script file. The main feature of the Measureserver, is to communicate with the physical hardware and to check the setup of the ISES panel and its sensors/meters and to take care about their data collection and processing. Other parts of the system are ImageServer for life view of the remote experiment, Web server for the communication between RE and the client. Also, aprt of the RE is the communication web page as the interface communicating with the RE over the Internet by the client.

The invevitable part of the RE system is the data warehouse for the storage of data for all above systems. It is a centralized repository service to Measureserver, web server, image server and other components of the solution.

In this article we will discuss this last part of the system with respect of data security, but not only from the perspective a single RE, but of the whole RLMS. The layout arrangement of the RE is in Figure 3.

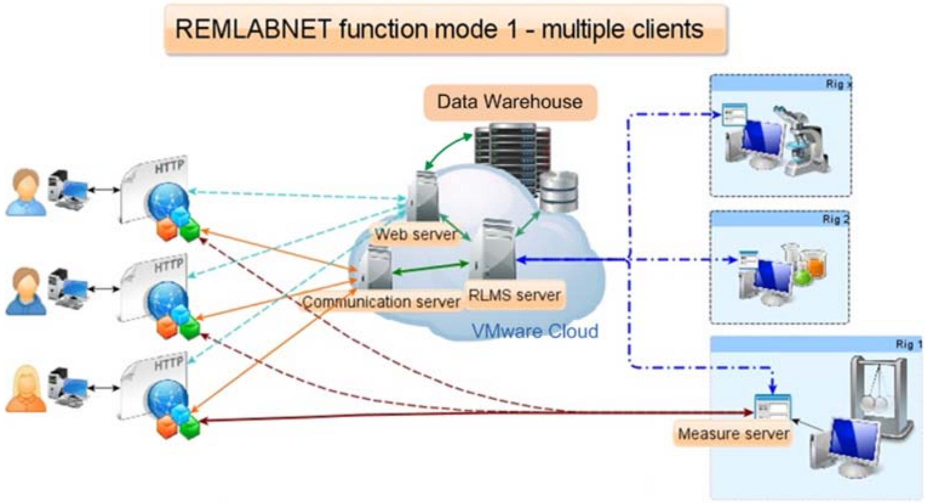


Fig. 3. REMLABNET function mode 1 – multiple clients.

A serious problem stemming from security aspects of e-laboratories has emerged only recently[]. Let us describe first the data generated and that are processed in every ISES rig working on the communication principle server-client and the functioning of the superordinate Remote Laboratory management system (RLMS). The controlling of every rig by client is enabled via Web interface, by means of which the user can perform the appropriate settings, options, and starting or stopping of the remote experiment (RE).

The measured data from the experiment delivered from the MeasureServer are stored in the data storage . RLMS is a system for a database-driven Web application. This is seen from the figure 3, where LMS is divided terms of safety in three parts. Database-driven Web applications are very common in today's Web-enabled society. LMS consist of a back-end database with Web pages that contain server-side script written in a programming language that is capable of extracting specific information from a database depending on various dynamic interactions with the user.

Remote experiments problematic is the topic of scientific activities of the group since 2005, when the first remote experiment started to be built. We relied on the enormous know-how of Assoc. Prof. F. Lustig from Department of Physics Education of Faculty of Mathematics and Physics, Charles University in Prague, where the universal and very useful modular computer oriented set Internet School Experimental System (ISES) was designed at the beginning of 90th [Lustig, F.: "Počítačem podporované školní experimenty s měřícím systémem ISES pod Windows", In: sborník MEDACTA 97 - vzdělávanie v meniacom sa svete, 404-408, Ústav didaktickej technológie, PF UKF v Nitre, Nitra, ISBN 80-967339-9-0, 1997 and Lustig, F. and Schauer, F.: "Creative laboratory experiments for basic physics using computer data collection and evaluation exemplified on the ISES", Proceedings first european conference on Physics Teaching in Engineering Education, 125-131, Copenhagen, Denmark, ed. Oehlenschlaeger, 1997].

A database architecture for Remote Experiments

A database-driven Web application for LMS has three tiers: presentation, logic, and storage. To help you better understand how Web application technologies interact to present you with a feature-rich Web experience, Figure 4 illustrates the three-tier schema.

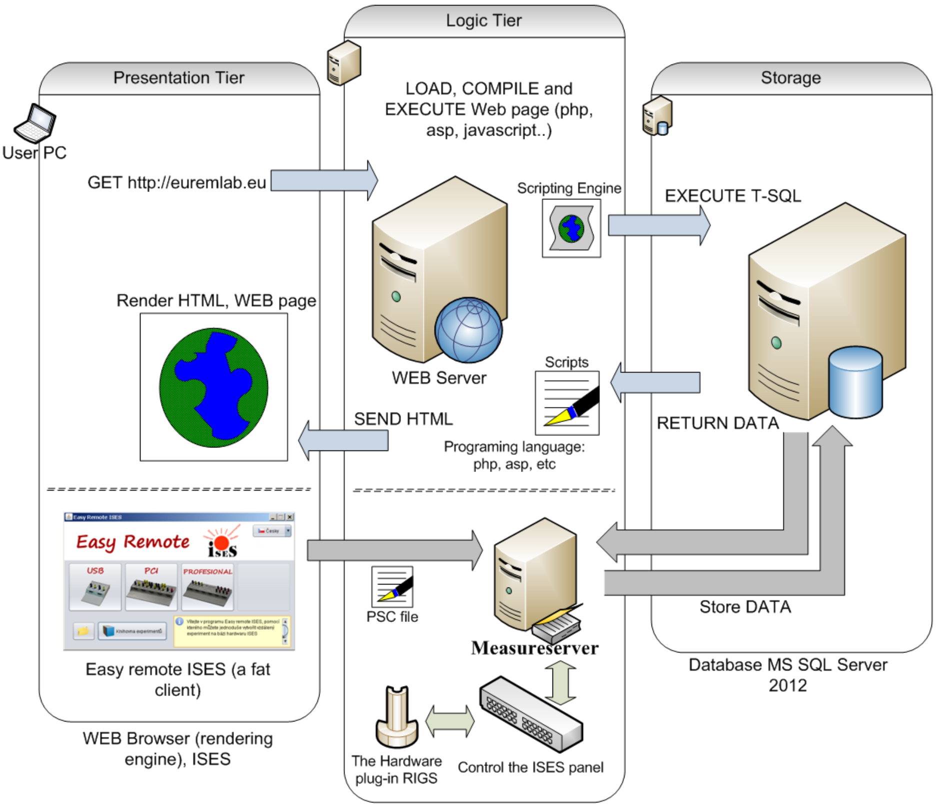


Fig. 4. Three-Tier Architecture Remote Experiments.

The presentation tier is the topmost level of the application. It displays information related to such services such as information web page about LMS, reservation system, and it communicates with other tiers by outputting results to the browser/client tier and all other tiers in the network.

The logic tier is pulled out from the presentation tier, and as its own layer, it controls an application's functionality by performing detailed processing. The data tier consists of database servers. Here, information is stored and retrieved. This tier keeps data independent from MeasureServer, reservation system and web server. Giving data their own tier also improves scalability and performance. In Figure 4, the Web browser (presentation) sends requests to the middle tier (logic), which services them by making queries and updates against the database (storage). A fundamental rule in a three-tier architecture is that the presentation tier never communicates directly with the data tier; in a three-tier model, all communication must pass through the middleware tier now. Conceptually, the three-tier architecture is linear.

In Figure 4, the user open his Web browser and connects to web page for remote experiments (http://euremlab.eu). The Web server that resides in the logic tier loads the script from the file system and passes it through its scripting engine, where it is parsed and executed. The script opens a connection to the storage tier using a database connector and executes an SQL statement against the database. The database returns the data to the database connector, which is passed to the scripting engine within the logic tier. The logic tier then implements any application or business logic rules before returning a Web page in HTML format to the user's Web browser within the presentation tier. The user's Web browser renders the HTML and presents the user with a graphical representation of the code. All of this happens in a matter of seconds and is transparent to the user.

In this slide show we describe the html code displayed on the station.

This component is represented in the LMS applications REMLABNET web server [2][16]. Web Server takes care about available ports for the LAN communication. It is a common habit by the system administrators to block all ports for security reasons except ports 80 and 443. HttpRelayServer dynamically changes communication port to that available.

We extend this model by MeasureServer. MS is most important informatics SW component of the remote experiment, functioning as finite-state machine (FSM). It communicates with the apparatus, processes the measured data and control commands. The main feature of the MeasureServer is setting of the ISES panel, the sensors/meters for data collection and processing the control commands. [16] The module dynamically responds to signals from the physical HW, as well as the commands transmitted from the client´s interface. MeasureServer has three main components - the MeasureServer core, Hardware plug-in and PSC script file. The MeasureServer core is responsible for the data and command transfer, client handling and for execution of all the controlling commands. The execution of process is controlled by the PSC script file which is directly imported to MeasureServer. The PSC script is a unique programming language specially designed for the ISES system. The PSC script is non-compliable language defining the MeasureServer's core behavior of remote experiment. The Hardware plug-in provides required functionality to control the ISES panel translating signals from/to the physical HW apparatus.

In Figure 4, the user open his rig(s) and connects to MeasureServer. The MeasureServer that resides in the logic tier loads the script (PSC file) from the file system and passes it through its scripting engine where it is parsed and executed. The MS opens a connection to the storage tier using a database connector and executes an SQL[2] statement against the database. The database returns the data to the database connector and then returns the requested data to MS. Before returning the data to the Web server. The Web server then implements any final logic (results and details of

[2] Structured Query Language: SQL is a special-purpose programming language designed for managing data held in a relational database management system.

the experiment) before presenting the data in HTML format to the user's Web browser within the presentation tier. The user's Web browser renders the HTML and presents the user with a graphical representation of the code. All of this happens in a matter of seconds and is transparent to the user.

Based on the system of RE, clients have a non-stop accessibility to enter RL through their web browser's interface connected to Internet from anywhere.[16] The most significant advantage is the real-time experimenting with the apparatus installed in a laboratory. An authorized student can comfortably communicate with the remote apparatus of the visualized RE via a web page. The apparatus promptly reacts and sends adequate responses/signals/data through particular subsystems back to the target client/student. After the completion of RE the student will arrange the data in formatted, sorted and filtered form and also in graphic charts displayed on the screen and find the corresponding answers regarding the phenomena observed.

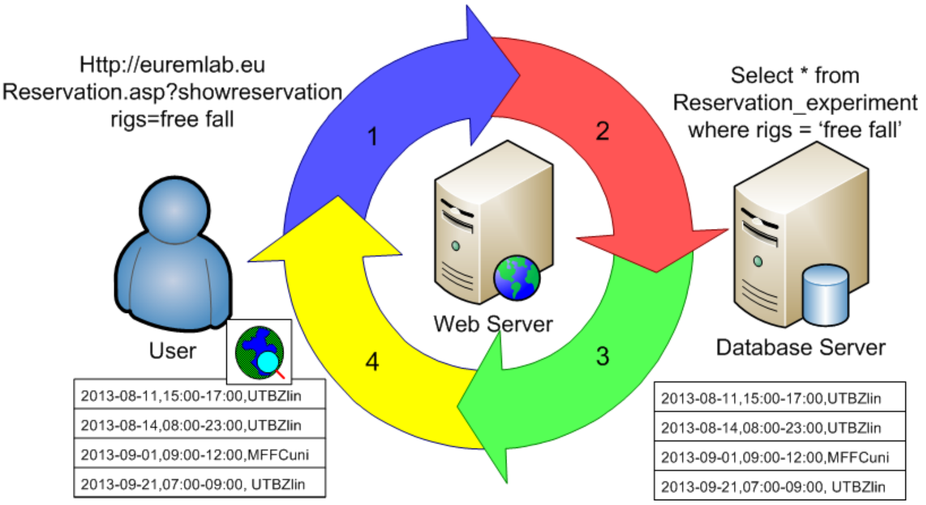
3 Database security risks of remote experiments

LMS is a specific technically sophisticated complex system. The availability of these system and the sensitivity of the data that they store and process are becoming very important. Web page that presentation LMS on Internet contains supporting infrastructure and environments use diverse technologies and can contain a significant amount of modified and customized codes. The very nature of their feature-rich design and their capability to collate, process, and disseminate information over the Internet or from within an intranet makes them a popular target for attack. Also, since the network security technology market has matured and there are fewer opportunities to breach information systems through network-based vulnerabilities, hackers are increasingly switching their focus to attempting to compromise applications.

3.1 SQL Injection of database attack

SQL injection is an attack in which the SQL code is inserted or appended into application/user input parameters that are later passed to a back-end SQL server for parsing and execution. Any procedure that constructs SQL statements could potentially be vulnerable, as the diverse nature of SQL and the methods available for constructing it provide a wealth of coding options. The primary form of SQL injection consists of direct insertion of code into parameters that are concatenated with SQL commands and executed. A less direct attack injects malicious code into strings that are destined for storage in a table or as metadata. When the stored strings are subsequently concatenated into a dynamic SQL command, the malicious code is executed. When a Web application fails to properly sanitize the parameters which are passed to dynamically created SQL statements (even when using parameterization techniques) it is possible for an attacker to alter the construction of back-end SQL statements. [15] When an attacker is able to modify an SQL statement, the statement will execute with the same rights as the application user; when using the SQL server to execute commands that interact with the operating system, the process will run with the same permissions as the component that executed the command (e.g. database server, application server, or Web server), which is often highly privileged.

It is important to have a clear understanding of how your data entry influences a SQL query and what kind of response you could expect from the server.
Figure 5 shows how the data sent from the browser are used in creating a SQL statement and how the results are returned to the browser.



2013-08-11,15:00-17:00,UTBZlin
2013-08-14,08:00-23:00,UTBZlin
2013-09-01,09:00-12:00,MFFCuni
2013-09-21,07:00-09:00, UTBZlin

2013-08-11,15:00-17:00,UTBZlin
2013-08-14,08:00-23:00,UTBZlin
2013-09-01,09:00-12:00,MFFCuni
2013-09-21,07:00-09:00, UTBZlin

Fig. 5. Information Flow during a SQL Injection Error.

If an attacker to modify the website to query the database, such as a change in url, web server just creates a SQL query, parses the results, and displays the results to the user. The database server receives the query and returns the results to the Web server. This is very important for exploiting SQL injection vulnerabilities because if you can manipulate the SQL statement and make the database server return arbitrary data (such as usernames and passwords from the Web site) the Web server has no means to verify whether the data are legitimate and will therefore pass the data back to the attacker. This is one of the most common attacks on the database and need from development to propose the necessary measures.

Of recent history

In 2011, Sony suffered a 23 day network outage after a breach of security that allowed the theft of approximately 77 million registered accounts from its PlayStation Network. It is to date the largest computer data exploit in history. A month later, hackers claimed in a press release to have stolen personal information of 1 million users from the website of Sony Pictures by a single SQL injection attack [17].

3.2 DoS and DDoS of database attack

Another attack, more difficult to prevent, is a DoS, or DDoS (Denial of Service, or Distributed Denial of Service), the overloading of a website or any kind of server with requests, for the purpose of bringing it down.
Denial of Service (DoS) is an inelegant but effective attack against web, database, and any type of public server. The goal is to overload the server with requests to crash it or make it unavailable for normal operations. A DoS is most of the time targeted towards a web server, and affects SQL server on the rebound. The first way to handle this is to protect the web server, for example, with a network firewall, which will automatically block suspicious IP addresses, or a Web Application Firewall (WAF). Here, we will provide some recipes to increase protection in SQL Server itself.
How to do it...
DoS risks are increased when you allow queries to be created dynamically in the client application, especially when you offer multi-criteria search forms. Since the user can search with any combination of criteria, it can lead to complex queries where it will take time to execute and exploit the resources of the server. A few of these queries running simultaneously can effectively decrease the performances of the whole server.

4 Security of scientific remote experiments

A greater level of baseline, hardware-enforced security features are important in all categories of remote laboratory system for part systems such as database server, MeasureServer, web server, reservation system, control system etc. These capabilities will protect the information on the device itself, and the information that is accessed from the device. They'll enable greater trust in the device, and because of this trust we'll be able to provide users of the device with access to more resources.
For LMS security, these baseline hardware security capabilities will provide help in key focus areas, including threat management, ID and access management, data protection, and remote monitoring. Some expected baseline capabilities include protected environments, encryption, hardware acceleration, enhanced recovery, and integration with security software.

4.1 SQL Injection of database based defense

SQL injection is the action of adding characters to a SQL query in order to modify its action and execute an exploit, such as getting more information, modifying data or data structures, or even getting access to the underlying operating system of the database server. [17][6][7] It can happen when a dynamic ad-hoc SQL query is built in the application code.

Let's see how it is necessary to protect the data storage LMS and what needs to be done on the website of remote experiments.

The SQL query is built dynamically in a string in web page of remote experiment in browser on client PC. [4][12][15] It leaves a possibility of something to be added to cause harm. we can find numerous and cunning ways to manipulate a query, by using SQL operators, functions, or constructs that can circumvent basic protection. For example, in T-SQL, the BULK INSERT command could be used to read the content of a file on the disk and return the result as a result set, or the xp_cmdshell extended stored procedure could be used to run Windows or even Active Directory commands. To eliminate the threat, replace those strings with parameterized stored procedures. The parameters will never be evaluated as a part of the query syntax and cannot be used for adding other behavior to it. They could still be used to get more information than expected, but not to run commands.

The best way to stay safe is to encapsulate SQL code inside parameterized stored procedures. But this sometimes defeats the first purpose of building a query dynamically: to fit a multi-criteria sear Chapter For example, if the name of the rig is part of the search, we add a JOIN to the rigs table in the query; otherwise we don't, which simplifies the query and optimizes performances.

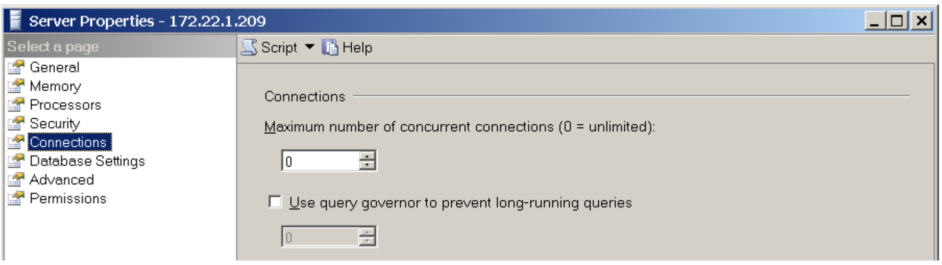
Removing the dynamic SQL is the best solution in terms of security, because there will be no chance for an attacker to inject code inside the SQL statement. The variables can now only replace values that are evaluated inside a comparison.

4.2 DoS and DDoS of database based defense

The first thing to do is to improve the quality of your code. One simple thing you can do is to ensure you have created the needed indexes on your tables, to avoid costly table scans. You can use the Database Tuning Advisor (DTA) packaged with the SQL Server client tools. You can make a .sql file containing some costly queries, and feed the DTA with it.

You can also limit the number of concurrent connections allowed on SQL Server. By default, the limit is 32,767 in MS SQL Server 2012 (the configuration value shows 0 in this case). You can change the value in the configuration pages of the instance (see the next screenshot, Figure 6) by T-SQL and set:

```
SELECT value_in_use
FROM sys.configurations
WHERE name = 'user connections';
```



Connections

Maximum number of concurrent connections (0 = unlimited):

0

□ Use query governor to prevent long-running queries

0

Fig. 6. Set restriction long-running queries.

In the previous screenshot, you can see another server configuration that could be useful: Use query governor to prevent long-running queries. If activated, the SQL optimizer will block execution of any query estimated to cost more than the number of seconds defined in the value. This is far from bullet-proof, as it is simply an estimation from the query optimizer, in pseudo-seconds (just a way of weighing plans to compare). If you choose, for example, a value of 30 seconds, it simply means that SQL server will not execute a query that it estimates costing more than 30 seconds. The actual query could finally run much faster or conversely run for hours if locks are blocking it. But it is a way to stop queries that are estimated to be heavy, and limit the risk that the server will be overloaded by a few queries.

Another way to limit resource usage is the use of Resource Governor. This addition to the SQL Server administrator toolbox is available only in the Enterprise edition. With it, you can define workload groups inside resource pools. In short, you can limit the amount of CPU and memory allocated to a group of sessions. For that, you create a classifier function that returns the name of a workload group. This function allows you to define the classification rules you want, based on SQL code, system variables, and functions (the login name, the time of day, and so on). Then you declare this function in Resource Governor along with you pools and groups.

5 Datastore in datawarehouse in the future

Let us predict, in the light of constantly developing ICT, the way of the safety precautions of the future data warehousing. Among the most growing trends, let us mention:

- Local data storage warehouseswillbe integrated into mega-integrated database centres of mega - companies such as Microsoft or Google,
- Authentication will run via a centralized authentication service USERID,
- Data scheme will be managed by mega-datacentres services and edited by higher order instruments. Thus, global consistency and the general design of structures to store and work with data will be ensured.
- Data mining will be integrated into functionalities of data protection and auditing.
- Exiting data warehouses will be more open to the needs of governmental and other institutions to control corruption and terrorism.

- Data warehouses will include integration buses and standards for reciprocal linking will be developed.
- Direct access of individuals and companies to research data warehouses worldwide for teaching, sharing information, and the like will be assured.
- Mega development of remote data centres, simulation technology centres, global centralization of knowledge and clustering into a single unit through integrators.
- Direct and audit subjected access of persons to information in the global knowledge centres (mega-integrated database centres).

6 Conclusions

This work describes a series of recommendations and procedures to secure data storage in the scheme of the data warehouse for the needs of remote laboratories. The work includes a vision for the future regarding security and direction of data warehouses, aiming to direct readers to the problems of data warehouses from all perspectives and to learn, what are the risks of today and how to comprehend security. In the course of the work on the data warehouse we learned how to realize a safety problem as well as design security. We believe, that the article sheds some light on a number of acute problems but simultaneously opened to us many other questions to consider in connection with data warehouse security. The article also describes the introduction of new terms on issues of security and shares experience in terms of theory and our practical experience.

Acknowledgments

The paper was published thanks to the Grant of the Internal Agency of UTB No IGA/FAI/2014/042. One of us acknowledges the partial support of the Slovak Research and Development Agency, project no. APVV-0096-11, the Scientific Grant Agency VEGA, project no. 2/0157/12, and the KEGA Agency projects No 011TTU-4/2012 and 020TTU-4/2013.

References

1. The whole system is detail described in the project proposal Submitted Project Grant Agency of the Czech Republic: INFORMATICS MEANS FOR GRID OF e-LABORATORIES – PROJECT REMLABNET, 2013
2. KRBEČEK, Michal. Possible_utilization_of_the_artificial_intelligence_elements_in_the_creation_of_remote_experiments. [online]. 2012, č. 1 [cit. 2013-06-26]
3. Grid Remote Laboratory Management System. Sahara Reaches Europe. 2013, č. 1.

4. Database-Level Roles [online]. 2012 [cit. 2013-06-26], http://msdn.microsoft.com/en-us/library/ms189121.aspx
5. ALEXANDER, David, Amanda FINCH, David SUTTON a Andy TAYLOR. Information Security Management Principles. 2. vyd. bcs, 2013. ISBN 9781780171753.
6. SCHULZ. Cloud and Virtual Data Storage Networking. teChapterChapterbooks, 2011. ISBN 978-1439851739.
7. Data Warehouse [online]. 2013 [cit. 2013-06-26], http://en.wikipedia.org/wiki/Data_warehouse
8. SCHAUER, František, František LUSTIG a Miroslava OŽVOLDOVÁ. Innovations 2011: World Innovations in Engineering Education and Research: Internet Natural Science Remote e-Laboratory (INTRE-L) for Remote Experiments. USA: iNEER, 2011, s. 51-68. 1. ISBN 978-0-9818868-2-4.
9. SCHAUER, František a Miroslava OŽVOLDOVÁ. Plug and play system for hands on and remote laboratories. In: Proceedings of 8th International Conference on Hands-on Science. Ljubljana: University of Ljubljana, 2011, s. 17-21. ISBN 978-989-95095-7-3.
10. KRBEČEK Michal, František SCHAUER, Roman JAŠEK. Security aspects of remote e-laboratories. Zlín: UTB ve Zlíně, Fakulta aplikované informatiky, 2012.
11. PÁLKA Lukáš,Data Warehouse services [online]. 2013 [cit. 2013-06-26], http://datawarehouse.cz/Data_warehouse
12. Data Warehouse [online]. 2013 [cit. 2013-06-25], http://www.1keydata.com/datawarehousing/datawarehouse.html
13. PÁLKA Lukáš, Methods and Tools Related to Data Security and the Protection of Microsoft SQL Servers. Zlín UTB, 2012.
14. LABERGE, Robert. The Data Warehouse Mentor: Practical Data Warehouse and Business Intelligence Insights. -: 2011. ISBN-10: 0071745327.
15. CLARKE, Justin. SQL Injection Attacks and Defense. USA: Elsevier, 2012. ISBN 978-1-59749-963-7.
16. GERŽA Michal, František SCHAUER, Roman JAŠEK. Security of ISES MeasureServer© module for remote experiments against malign attacks, Zlín: UTB ve Zlíně, Fakulta aplikované informatiky, 2013.
17. BRUCHEZ, Rudi. Microsoft SQL Server 2012 Security Cookbook. UK: Packt Publishing, 2012. ISBN ISBN 978-1-84968-588-7.
18. HARKINS, Malcolm. Managing Risk and Information Security: Protect to Enable. LLC: Apress Media, 2013. ISBN 978-1430251132.

Authors

L. Pálka, F. Schauer and R. Jašek are with the Tomas Bata University in Zlín, Faculty of Applied Informatics,
Nad Strán&mi 4511, Zlín, CZ- 760 05, Czech Republic (l_palka@fai.utb.cz, fschauer@fai.utb.cz, jasek@fai.utb.cz).

Published as resubmitted by the authors 29 June 2014.

Design of a Software Tool for Mobile Application User Mental Models Collection and Visualization

Radek Vala, Roman Jasek, David Malanik

Tomas Bata University in Zlin, Faculty of Applied Informatics, nám. T.G.Masaryka 5555, CZECH REPUBLIC
{vala, jasek, dmalanik}@fai.utb.cz

Abstract. Mental model is a fundamental term in human-computer interaction (HCI). The process of HCI creates different qualitative levels of user experience (UX) which can be determined by the quality of communication between a technological product (the system) and a user of this product. The level of user experience is indirectly derivable from measurement of different qualitative and quantitative aspects of the interaction (achievement of objectives, satisfaction, comfort, time required to perform the task). The user experience is the key factor which determines the popularity of web or mobile applications and software applications in general. During the HCI, the user is unconsciously comparing his mental model (own idea of functionality) with the system image (the real graphical user interface – GUI). The distance between the user's mental model and the system image should be minimal. Creation of successful GUI requires a real user-application interaction testing and statistical evaluation of the testing data. This paper describes a design of a software tool for user mental model collection and visualization in the area of mobile applications with emphasis on context of the HCI.

Keywords: conceptual model, mental model, mobile application design, system image, user experience, user interface.

1 Introduction

Recently, more and more mobile applications developers are facing the question of proper graphical user interface design. Area of mobile application development is rapidly growing along with increasing number of mobile applications users. According to Flurry Analytics [1], overall mobile applications use in 2013 growth by 115% year-over-year and it is expected that this trend will continue.

In segment of native application development, there is possible to follow guidelines for GUI design related with some specific platform. But these guidelines are describing only fundamental patterns or use cases. In contrast with web application UI design, there is a noticeable lack of studies and research in the area of mobile application design. Moreover, if we consider the hybrid mobile application development, a large amount of user interface design frameworks is not strictly following particular platform UI guidelines and achieving a successful mobile application design is not therefore a simple task.

The interaction between a user of mobile application and a graphical user interface could lead to some misunderstandings, errors and frustration from inability to achieve a goal. Designer is able to prevent this situation with a good UI design with respect to the user mental model (UMM).

By the user-application interaction, a user is comparing his UMM (complex idea of how the system works) with the system image (application GUI). If the distance between this two models is too high, it means that the design is confusing and users may not be able to accomplish their goals.

Good UI of a software application (system image) should help a user to create a productive UMM of the system. [2] This paper discuss best practices for consideration by a designer creating a conceptual model of an application and a software tool for UMM collection and evaluation.

2 Mental Models in Software Design

In the area of human-computer interaction (HCI) there are defined fundamental terms describing and simplifying the human computer recognition process.

2.1 Mental Models

The term Mental Model was firstly introduced by Craik [3], but in the 80th it became the fundamental part of terminology of the newly established field of cognitive science. According to Norman [4] and Krug [5], UMM is the key factor in user's perception of an object functionality and behavior. Users of an object are creating in their minds a simplified model that describes their ideas how the object works, or how to interact with it.

2.2 Conceptual Models

By the process of developing a software application, a conceptual model is created by the designer. This conceptual model reflects designer's understandings of the task and tools and abstractly describes the functionality of the system and its relations. [6] This model should be good understandable for end user and should focus on key functionality of the application. [7]

2.3 System Image

User of a software application compares unconsciously by working with GUI objects, own idea about virtual environment functionality, with real GUI objects which are creating the system image. In simplicity, by the process of HCI, user compares own mental model with the system image. [8]

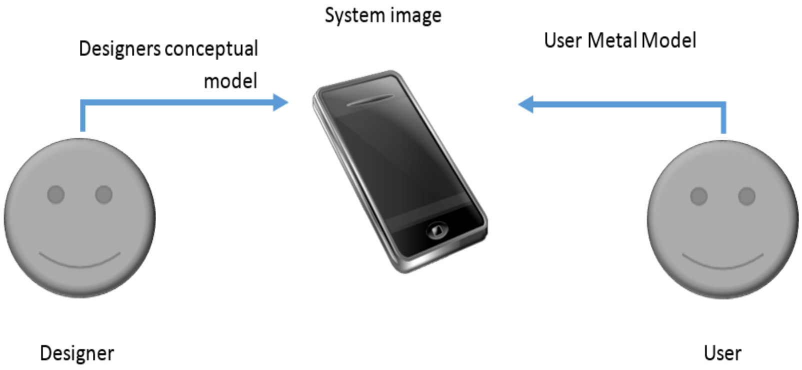


Fig. 1. Relation between conceptual model, user mental model and system image.

3 Conceptual Design Best Practices

Good conceptual model is an essential part in development process of successful software application. [9] Therefore application designer should consider following best practices published by IBM Corporation.

3.1 Simplicity

Mental models are the simplified image of reality, therefore GUI should simplified the key functions of the system. This key functions should be highlighted, lesser-used functions should be in background.

3.2 Familiarity

Users in general have some prior knowledge and using this knowledge, they are creating own mental model. The GUI should allow them to build on this knowledge.[10] The process of creation an adequate mental model, can be strengthen if the user is able to apply prior experience gained from the real world.

3.3 Availability

Because human beings are better at recognition then recall, GUI should contain visual stimulus, to fast identification of an object functionality.[10]

3.4 Feedback

GUI should provide continuous feedback about the results of actions.[4] Using appropriate feedback is possible to support user's mental model creation.[10] Positive feedback is good for strengthening current user's mental model, whilst using the negative feedback is possible to adapt the model.

4 Proposed Software Tool – MeMo2Ap

In order to assess the accuracy of the conceptual models, it is necessary to obtain a general UMM of specific application and to evaluate the extent to which these two models fits. Collecting the user models can be very costly activity and requires special commercial software or a test observer.

This paper describes a design of a context focused software solution for mobile application user mental models collection and visualization (named MeMo2Ap). Before the design of this software tool, these goals were formulated:

1) Simple implementation
2) Easy preparation of test scenario
3) Context focus (target application, target device)
4) Distributed test deployment
5) Results visualization and simple evaluation

To meet this objectives, hybrid mobile application development approach was chosen. Within this approach it is possible to use web technologies which are easy to implement and moreover it is very easy to distribute the test application to end users using URL address. In other way it is also possible to wrap the test application by wrapper technology, such as PhoneGap [11] and publish it on official distribution channels.

4.1 Principles of Testing and Data Collection

Hybrid mobile application MeMo2Ap is a client-server application which is able to perform a testing scenario and observe users touch gestures. Testing scenario contains 1 to N test cases, while the test case is determined by a test screen, description of user task to perform, and success area, where user should touch to complete the task. If the user touches the success area, the test was successful in other case, the test failed.

Testing result is immediately sent from client mobile device to database table on the server. Timestamp, vertical and horizontal position of the touch gesture are stored. This communication between client and server is established using JSON web service. The main advantage is the possibility of distributed testing and simple delivering to end testers.

4.2 Technologies Used for MeMo2Ap

As for server side, PHP programming language and MySQL database was chosen. The server was developed using QCubed [12] – open-source rapid application development framework, which uses ORM technology [13] and code generation [14] to accelerate the development process.

MySQL database was designed using open-source visual database designer MySQL Workbench 6.0 by Oracle (www.mysql.com/products/workbench/). Database table names and relations are shown in Figure 3.

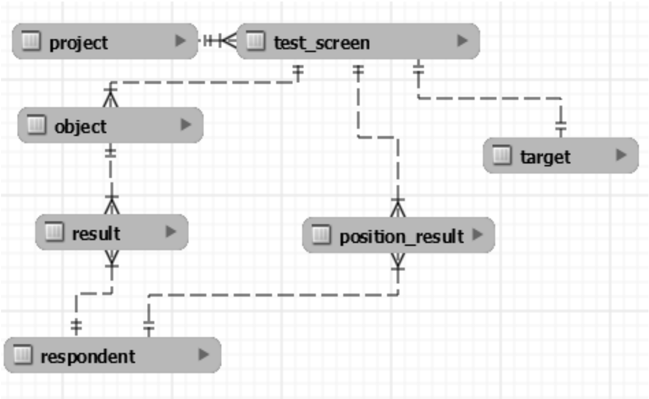


Fig. 2. MeMo2Ap database table relations.

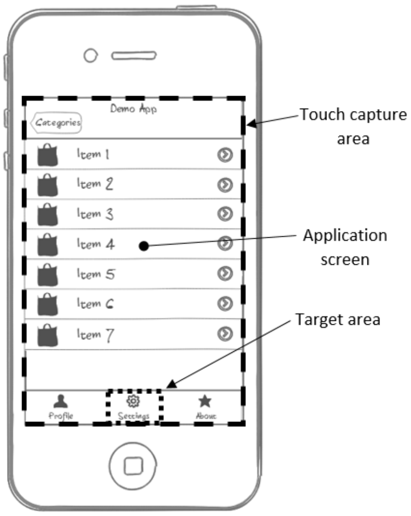


Fig. 3. Visualisation of target area within test screen.

The server side consists of the tests administration area (automatically generated QCubed Form Drafts [15]) and web services for the mobile client. The client side is created using web technologies – HTML, CSS, JavaScript, jQuery and jQuery Mobile and it is possible to process the application in a mobile browser or a Web view within a native mobile application using Phonegap wrapper [11].

4.3 Proposed methodology of collecting user's mental models using MeMo2Ap

Using MeMo2Ap testing software is possible to create test scenarios in following way:
1) New testing project with specific name and identifier is created using server administration tool.
2) Within this project, new testing scenario can be created.
3) Testing scenario consists of 1 to N testing screens. Each testing screen is represented by PNG graphic file and is possible to prepend user task text which is shown as a modal dialog window, before the test screen.
4) When the project testing scenario consists of at least 1 test screen, it is possible to run the script for setting target area (Fig. 4). Setting the target area is done using drag & drop technology, by the administrator.

Once the test scenario is set, the user testing can be performed remotely, if needed (Figure 5) and the testing results are obtained in real time.

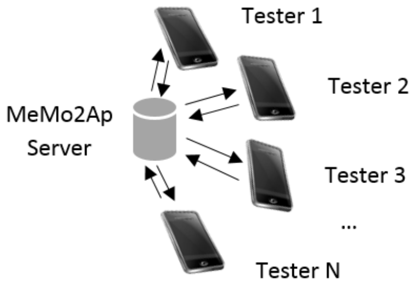


Fig. 4. Distributed testing using client-server architecture.

Using MeMo2Ap testing software from tester point of view:

1) Competition of initial form (information about gender, preferred platform, experience…)
2) Reading a user task.
3) Longer tapping the area to complete the task.

Points 2) and 3) are repeating for each test screen.

4.4 Testing Results Visualization and Evaluation

Once testing is complete (or during the testing), visualization can be displayed using MeMo2Ap software tool (Figure 5). Each test screen is overlaid with testing results with successful touches in green and unsuccessful touches in red color. There is also obvious the frequency of tapping into particular area, from the color density.

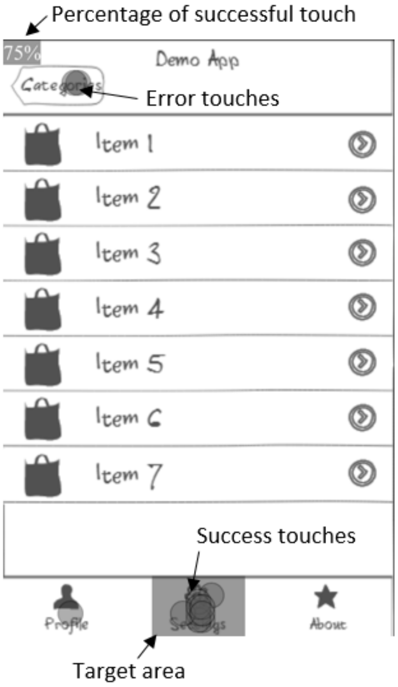


Fig. 5. Visualization of testing results.

In the left corner of each test screen, there is available the numerical information about successful tests in percent. Percentages are given by a success percent sP (1) of each test screen, where tT is number of total test count and sT is number of successful taps in target area.

$$sP = \left(\frac{sT}{tT}\right)\cdot 100 \quad (1)$$

5 Method ofIncrementalGUI Design Using Mental Models

Creating a mobile application with usable, attractive and especially understandable design can provide higher sales and growing numbers of users. On the other hand, bad user experience makes an application unsuccessful.

During the application design phase, conceptual model of the app is created. This conceptual model produces the system image with which the real user interacts. Inaccurate system image do not support creation of correct mental model of the user.

With respect to user mental model linked with specific application screen, it is possible to rearrange and redesign problematic parts and redo the tests. Comparing the results between the first system image and the redesigned system image is possible to highly improve the user experience.

After the testing, a successful threshold for each test screen should be set up. If the success percentage of the test screen is lower than the threshold, design improvements are necessary. Another test should contain the improved test screen and again the success percentage is evaluated.

Better mobile design with high user experience can be achieved using this incremental testing (Figure 6).

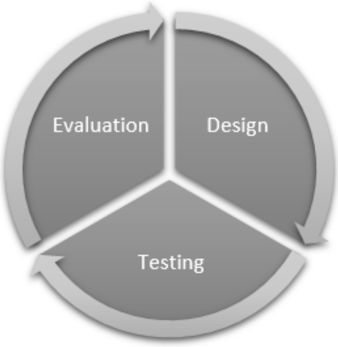


Fig. 6.UI design with incremental testing.

6 Future Research

Software tool MeMo2Ap for collecting mobile application user’s mental model was developed as an open-source and allows easy creation of test scenarios, which are focused on evaluation the accuracy of conceptual models. Using this tool and incremental mehod of GUI desing testing, an improvement in UX could be achieved.

In future research commonly used GUI patterns could be tested and the extent to fit user’s mental model could be evaluated. It is also possible to search for the error dependence on user preference for specific mobile platformby using patterns linked to another platform.

Another interesting area is the creation of proper user mental modelsupported by appropriate UI techniques, such as overlap help. Research can be conducted with two testing groups – users who have not seen the overlap help and those who have seen the overlap help in prior.

7 Conclusion

Method of collecting mobile application user’s mental models using the proposed software tool MeMo2Ap was introduced in this paper and best practices for mobile application GUI design were discussed. The software tool was designed as an open-source client-server application, to meet these goals: Simple implementation, easy preparation of test scenario, context focus (target application, target device), distributed test deployment, results visualization and simple evaluation.

Using the MeMo2Ap tool, the success rate of each test screen is reflecting the correctness of the conceptual model and if the correctness is insufficient it is possible to improve it with incremental design enhancing and testing.
Also opportunities for further research, such as established GUI pattern success rate testing and evaluating or supporting methods of creation the proper user mental model are mentioned in chapter 6.

Acknowledgment

The research work was performed to financial support by the European Regional Development Fund under the Project CEBIA-Tech No. CZ.1.05/2.1.00/03.0089.

References

1. S. Khalaf. (2014). *Mobile Use Grows 115% in 2013, Propelled by Messaging Apps.* Available: http://blog.flurry.com/bid/103601/Mobile-Use-Grows-115-in-2013-Propelled-by-Messaging-Apps. Last accessed 2014-03-04.
2. J. Preece. *Human-Computer Interaction*. Reading MA: Addison-Wesley, 1994.
3. K. Craik.*The nature of explanation*, Cambridge University Press, 1943.
4. D. A. Norman. *Design of everyday things*. Rev. and exp. ed. New York: Basic Books, 2013, xviii, ISBN 978-046-5050-659.
5. S. Krug *Don't make me think!: a common sense approach to Web usability*. Indianapolis, Ind.: Que, 2000, ix, ISBN 07-897-2310-7.
6. J.Johnson, A. Henderson. *Conceptual models: core to good design*. San Rafael, Calif., 2012. ISBN 978-160-8457-496.
7. D. A. Norman. *Design of everyday things*. Rev. and exp. ed. New York: Basic Books, 2013, xviii, ISBN 978-046-5050-659.
8. D. A. Norman, S. W. Draper.*User centered system design: new perspectives on human-computer interaction*. Pbk. ed. Boca Raton, FL: CRC Press, 1986. ISBN 978-089-8598-728.
9. J. Johnson, A. Henderson. *Conceptual models: core to good design*. San Rafael, Calif., 2012. ISBN 978-160-8457-496.
10. IBM Corporation (1992). *Object-Oriented Interface Design: IBM Common User Access Guidelines*. Indianapolis IN: QUE.R. W. Lucky, “Automatic equalization for digital communication,” *Bell Syst. Tech. J.*, vol. 44, no. 4, pp. 547–588, Apr. 1965.
11. Adobe Systems Inc. (2014). *About the Project.* Available: http://phonegap.com/about/. Last accessed 2014-03-04.
12. QCubed. (2014). *Welcome to QCubed!.* Available: http://qcu.be/content/welcome. Last accessed 2014-03-04.
13. K. Roebuck. *Object-relational mapping: high-impact strategies - what you need to know*. S.l.: Emereo Pty Limited, 2011. ISBN 978-174-3044-759.
14. G. Rossini. *Rapid Application Development with Qcubed*. Gianni Rossini.
15. Form Drafts [online]. [cit. 2014-03-25]. Available from: https://github.com/qcubed/framework/wiki/Form-Drafts.

Proposal of Evaluation ITIL® Tools

Lukas Kralik, Ludek Lukas,

Tomas Bata University in Zlín, Faculty of Applied Informatics, Nad Stráněmi 4511
760 05 Zlín, Czech Republic
{kralik, lukas}@fai.utb.cz

Abstract. This paper responds to requirement to improve the orientation between offered SW, as ITIL® tools. There are really a lot of amount thus offered tools and very often leads to poor implementation of ITIL® on the basis of badly chosen tools. So this article aims to create dividing, which should facilitate choice of a suitable tool. Simultaneously, this division will serve for further work on creating a methodology for evaluation of ITIL® tools.

Keywords: ITIL®, ITIL® tools, tools categorization, IT service support, ITIL implementation, multicriterial evaluation.

1 Introduction

With development of information and communication technologies (ICT) and their intrusion into all sectors, gaining management and delivery of IT services different dimension and meaning. The quality of providing or managing of IT services can greatly affect the operation or performance of the company. For this reason it was introduced, the now internationally acclaimed standard known as ITIL®. It is an abbreviation for Information Technology Infrastructure Library. It is a set of concepts and practices that allow better planning, use and improve the use of IT, whether by the providers of IT services or by the customers.

ITIL® is a collection of books in the form of extensive and widely available manual for IT service management. The experiences and recommendations have become best practices. Provide sufficient flexibility to adapt the recommendations from books ITIL® requirements and needs of a specific corporation. ITIL® provides a free available framework, covering the entire cycle of IT services. ITIL® is suitable for all companies that operate IT services. As a framework, ITIL® is full of tips, warnings, knowledge, omissions, instruction, warnings and things to do or not do. One of the greatest benefits of ITIL® is a fact that it is based on experience of others.

According current version of ITIL® v3 is possible to say that ITIL® tool is an arbitrary software tool which use leads to provably improve and streamline the providing and managing IT services. There is only one condition – it must be a SW.

The uses of ITIL® tools are complicated due to the wide range of offered tools and often very expensive. This caused and to a certain extent still causes small and medium companies are disinterest of the use of ITIL®. On the other hand, recently is beginning to discover significant amounts of Free and Open Source SW even between ITIL® tools.

2 Evaluation Criteria

On the market is really wide range of Free and Open Source ITIL® tools and orientation between them is very difficult. This problem is also related to selection of the most appropriate tools for a specific company. Therefore, below are defined and described the basic criteria for selection and evaluation of these tools. However, it is important to say that each company may have different requirements and other criteria. So, same tool is useful for one company and at the same time might be useless for another company.

Basic criteria for Free and Open Source ITIL® tools are divided into several groups:

1. Product Functionality
2. Requirements for Free and Open Source Project
3. Specifications
4. User friendliness

2.1 Product Functionality

Criteria relating to the functionality vary by application category. A large number of features do not necessarily mean that the application is better than competing product with a shorter list of features. This point cannot be assessed quantitatively as a measurable criterion of selection, but rather as an overview which may apprise readers and provide them information about the basic functions of the product.

2.2 Division by main purpose

Open source project is meant organizing and managing a group of people who are involved in the development of the product.

- Duration of the project; version in which the product is available.
- License, under which the product is offered.
- Activity on the mailing lists - community
- Option of commercial support.
- Appropriate documentation - is the absence of the necessary documentation was in the selection of appropriate tools stumbling block relatively large number of projects. The basic requirement in this case, I consider the existence of technical documentation and user documentation.
- Demo applications.

1.3 Specifications

Most of the Free and Open Source products use of ready-made programs usually also available under any other Free or Open Source licenses. This covers programs such as the Apache web server, or database servers MySQL, PostgreSQL, e-mail servers Postfix and so on.

Technical parameters are therefore a considerable amount and in particular, for each of this software may vary. Therefore, it is evaluation only directly influenced by the following parameters:

- HW requirements
- Supported operating systems - Cross-platform
- Integration with other SW
- Difficulty of configuration

Other parameters such as licenses, programming language, etc. are given only as a parameter list and have only informative value to the end user, which can serve to more specific evaluation according to the requirements of the specific company.

1.4 User friendliness

User friendliness is the main parameter that affects the user's ability to learn to work with a new product and use all functions. Improperly designed user interface can greatly influence user's work.

Evaluation of this criterion is very subjective and based primarily on practical experience. At the same time here enter localization - the used language and of course the entire GUI (Graphic User Interface). Some tools are merely for the Command line.

2. Evaluation of ITIL® tools

The rating is divided into 2 parts. The first part is evaluated on the basis of defined criteria. The second part of the evaluation is intended for basic evaluation by users; this means that the use of the tool led to increase efficiencies in managing of the provision of IT services. This project is primarily focused only on the first part and is intended to provide basic guidance on valuation of available Free and Open Source ITIL ® tools. At the same evaluation procedure in the first section can also serve as a guide or template for creating a custom evaluation according to specific needs and requirements of the company to any SW, not just for ITIL ® tools.

$$\mathbf{H} = [(\textstyle\sum_{\boldsymbol{i}=\mathbf{1}}^{\boldsymbol{n}} \mathbf{K_i} \cdot \mathbf{V_i})/\mathbf{5}] * \mathbf{100} \ [\%] \qquad (1)$$

H overall rating
K_i i-th criterion
V_i stength of i-th criterion
n number of the criteria

Evaluation of the first part is according to the above equation (1). It is the degree of fulfillment of the essential requirements for the Free and Open Source ITIL ® tools. The procedure is as follows:

1. On the basis of the tables establishing a rating for the basic criteria.
2. Obtained values are multiplied by the strength of standardized criteria according the table.
3. New standard ratings of criteria are added together.

Overall rating is expressed as a percentage - the sum of the standardized criteria is divided by 5 (the highest possible score for each criterion) and then multiplied by 100.

3 Conclusion

Due to the widespread of information and communication technologies, which today affects absolutely all human activity is the IT management absolute necessity. ITIL® framework has deal whit this issue with more than 20 years of experience. It gathers the best experience in IT management and provides advice and tips on how companies can improve overall IT management efficiency.

The main objective of the project was to design a procedure for evaluating Free and Open Source ITIL ® tools. Licenses for commercial products are often going up to the order of hundreds of thousands of Czech crowns. And even so there is no guarantee that the product purchased for a particular company is the right solution. Another option is to choose from Free or Open Source solutions. However, they are on the rise and each year comes a large amount of new projects. Not all of them have high quality and have a future. Another fact is the absence of a database or a web portal, which would be devoted to the issue. Based on these fact was created project about the evaluation of Free and Open Source ITIL® tools.

Acknowledgments. This work was supported by grant No. IGA/FAI/2014/020 from IGA (Internal Grant Agency) of Thomas Bata University in Zlin.

References

1. Automated Unattended Installation in Kovárna Viva, a.s. In: International journal of computers. Oregon (USA): North Atlantic University Union, 2014, s. 7. ISSN 1998-4308.
2. KRÁLÍK, Lukáš. Searching sources and evaluation criteria for open source itil® tools. In: Mezinárodní Masarykova Konference Pro Doktorandy A Mladé Vědecké Pracovníky. Hradec Králové: Magnimitas, 2013, s. 6. ISBN 978-80-87952-00-9.
3. KRALIK, Lukas. Analysis for Automated Unattended Installation. In: Recent Advances in Automatic Control, Information and comunications: Proceedings of the 14th International Conference on Automation & Information (ICAI '13). Valencia (Španělsko): WSEAS press, 2013, s. 5. ISBN 978-960-474-316-2ISSN 1790-5117.

4. KUFNER, Vladimír. ITIL V3: Změny v klíčových publikacích. DSM - data security management. 2012, č. 2, s. 7.
5. BUCKSTEEG, Martin. ITIL 2011. 1. vyd. Brno: Computer Press, 2012, 216 s. ISBN 978-80-251-3732-1.
6. ITIL continual service improvement [online]. 2nd ed. London: TSO, 2011, xi, 246 s. [cit. 2013-07-22]. Best Management Practice. ISBN 978-0-11-331308-2. Dostupné z: http://www.best-management-practice.com
7. ITIL service transition [online]. 2nd ed. London: TSO, 2011, xii, 347 s. [cit. 2013-07-22]. Best Management Practice. ISBN 978-0-11-331306-8. Dostupné z: http://www.best-management-practice.com
8. ITIL service design [online]. 2nd ed. London: TSO, 2011, xi, 442 s. [cit. 2013-07-22]. Best Management Practice. ISBN 978-0-11-331305-1. Dostupné z: http://www.best-management-practice.com
9. ITIL service operation [online]. 2nd ed. London: TSO, 2011, xi, 370 s. [cit. 2013-07-22]. Best Management Practice. ISBN 978-0-11-331307-5. Dostupné z: http://www.best-management-practice.com
10. ITIL: service strategy [online]. London: Stationery Office, 2011, xii, 264 s. [cit. 2013-07-22]. ISBN 978-011-3310-456. Dostupné z: http://www.best-management-practice.com/
11. JAŠEK, Roman, SZMIT, Anna, SZMIT, Maciej. Usage of Modern Exponential-Smoothing Models in Network Traffic Modelling. In Nostradamus 2013: Prediction, Modeling and Analysis of Complex Systems. Heidelberg : Springer-Verlag Berlin, 2013, s. 435-444. ISSN 2194-5357. ISBN 978-3-319-00541-6.
12. JAŠEK, Roman, SZMIT, Anna, SZMIT, Maciej. Usage of Modern Exponential-Smoothing Models in Network Traffic Modelling. In Nostradamus 2013: Prediction, Modeling and Analysis of Complex Systems. Heidelberg : Springer-Verlag Berlin, 2013, s. 435-444. ISSN 2194-5357. ISBN 978-3-319-00541-6.
13. JAŠEK, Roman, KOLAŘÍK, Martin, VÝMOLA, Tomáš. APT Detection System Using Honeypots. In Proceedings of the 14th WSEAS International Conference on Automation & Information (ICAI ’13). Montreux : WSEAS Press, 2013, s. 25-29. ISSN 1790-5117. ISBN 978-960-474-316-2.
14. KRBEČEK, Michal, SCHAUER, František, JAŠEK, Roman. Security aspects of remote e-laboratories. International Journal of Online Engineering, 2013, roč. 9, č. 3, s. 34-39. ISSN 1868-1646.
15. Vala, Radek; Malaník, David; Jašek, Roman. Usability of software intrusion-detection system in web applications. In International Joint Conference CISIS ´12-ICEUTE ´12-SOCO ´12. Heidelberg: Springer-Verlag Berlin, 2013, s. 159-166. ISSN 2194-5357. ISBN 978-3-642-33017-9.

Analysis of Direct Punch with a View to Velocity

Dora Lapkova, Milan Adamek

Tomas Bata University in Zlin
Faculty of Applied Informatics
Nam T.G. Masaryka 5555, 760 01 Zlin
Czech Republic
{dlapkova, adamek}@fai.utb.cz

Abstract. This paper is focused on analysis of a direct punch which was chosen from many striking techniques of professional defence. The analysis is aimed to find the velocity and dependences of this velocity on input parameters. Our goal was to find out if the velocity is suitable physical value for analysis of the direct punch. During the experiment a high-speed camera Olympus i-Speed 2 was used. For data analysis two pieces of software were used – i-Speed Control Software and MINITAB. 30 participants took part in this experiment. The results are presented in this paper – especially dependence mean velocity on time and difference in velocity between genders.

Keywords: Direct punch, Professional defence, Velocity, Gender Differences

1 Introduction

Physical protection has a very long history and it belongs among basic parts of effective protection of people and property. Human factor is very important for data analysis and for quickly solving some unexpected situation. For these people professional defence training is necessary for effective work. During the training the participants are taught to stop attacker, to neutralize an attack or to solve conflict situations.

The striking techniques are one of the basic elements of the majority of combat sports [2], martial arts [5] or combat systems [9]. In these techniques the striking energy [8] is transferred through arms, legs or head. In this paper the direct punch velocity is closely analyzed. The direct punch is delivered by the arm following a direct line. The hitting area is a closed fist [11]. The aim is to stop the attacker and increase distance between the defender and an attacker. In the following experiment the punch was delivered by the back hand (see Fig. 1).

The aim was to measure the velocity of direct punch and then to find out dependence of velocity on inputs parameters – a training level, body's height and weight and a gender.

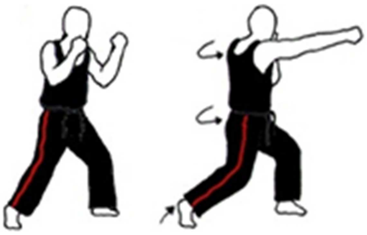


Fig. 1. Direct punch [11]

2 Measuring station

A high-speed camera Olympus i-Speed 2 was used for measuring of velocity. This camera has CMOS 800x600 sensor, full resolution recordings to 1000 fps (fps = frames per second) and 33000 fps maximum recording speed. We used recording speed 1000 fps. [1, 4, 6]

During this experiment we used only one camera, so we choose direct punch from all striking techniques because only this punch is made directly. The result is that during the whole movement of the hand we have had a focused image.

The measuring station consists of a punching bag and a construction of its suspension. Paper with two perpendicular lines was stuck on the right of the punching bag. Horizontal line was for leading the hand during movement. The aim of the vertical line was to determine the beginning of data analysis. The result was that the all direct punches were measured in the same distance from punching bag. This distance was 60mm. The end of the measuring was at the moment when the movement of the hand was stopped in axis “x” – the deformation of punching bag was at the maximum.

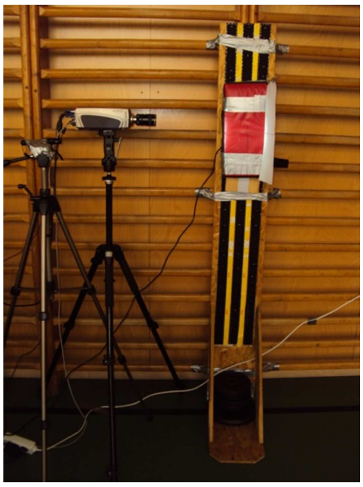


Fig. 2. Measuring station with the camera and the punching bag

3 Experiment

The total of 30 participants took part in the experiment; 24 men and 6 women. Based on the previous training and experience the participants were divided into following three groups:

- Untrained – These people have never done any combat sport, martial art or combat system. They have no theoretical knowledge of the striking technique. The technique was presented to these people before the experiment for safety reasons. Noted further as UTM (for men).
- Mid-trained - These people have the theoretical knowledge of striking techniques and they have attended the Special physical training course for at least six months. The course is focused on self-defence and professional defence. Noted further as MTM (for men) and MTW (for women).
- Trained – These people do some combat sports, martial arts or a combat system for longer than two years. Noted further as TM (for men).

During the experiment each person made one strike (Except one man from training group. He did two strikes.). During the measurement the target was positioned in such manner that the center of the punching bag was in line with the striking person´s shoulder. That way the punches have the maximum velocity and force (as there is no decomposition of force or velocity into the other axes). The person was made to stay at the same place for the whole experiment. Any unnecessary movement (e. g. lunge etc.) would lead to data distortion.

Reflective markers with diameter 10mm have been stuck on the hand of each person.

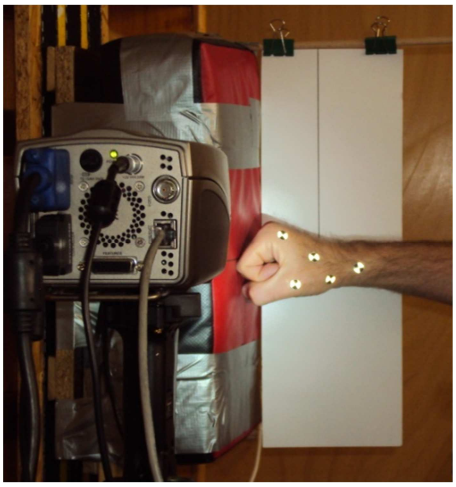


Fig. 3. Reflective markers

4 Results

For data analysis we used i-Speed Control Software. It is used for image analysis and for work with images – modification of contrast, brightness etc. On the basis of sequential labelling of markers on hand the software it is able to calculate the velocity of the hand. The rate of images (1000 fps) and the distance of markers between two images are known.

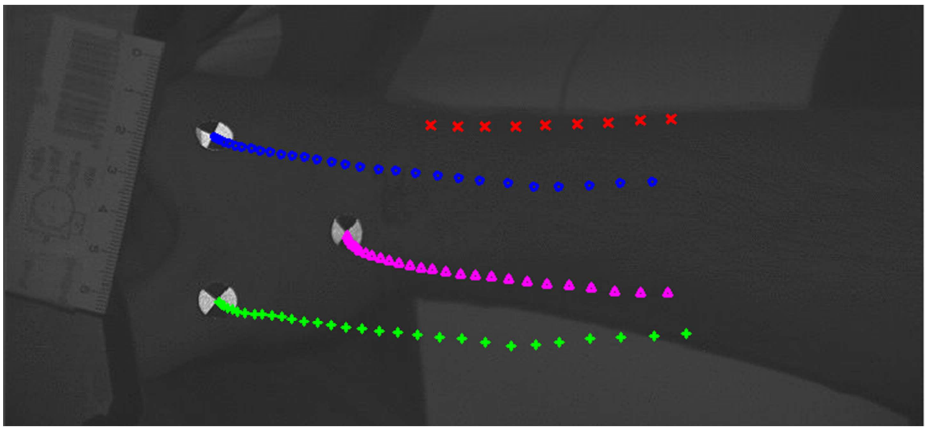


Fig. 4. I-Speed Control Software

For velocity analysis we used software MINITAB. It was possible to find out dependence of the mean velocity on time, dependence of the maximum velocity on body's height and weight, dependence of the maximum velocity on training level and also on gender.

Fig. 5 shows dependence of the velocity on time. There are clear differences among signals due to the training level and the gender. The aim was to find out a simple statistical classifier which would helps us to classify people on basis of their training level. Possibilities are the maximum of velocity and its standard deviation (Table 1).

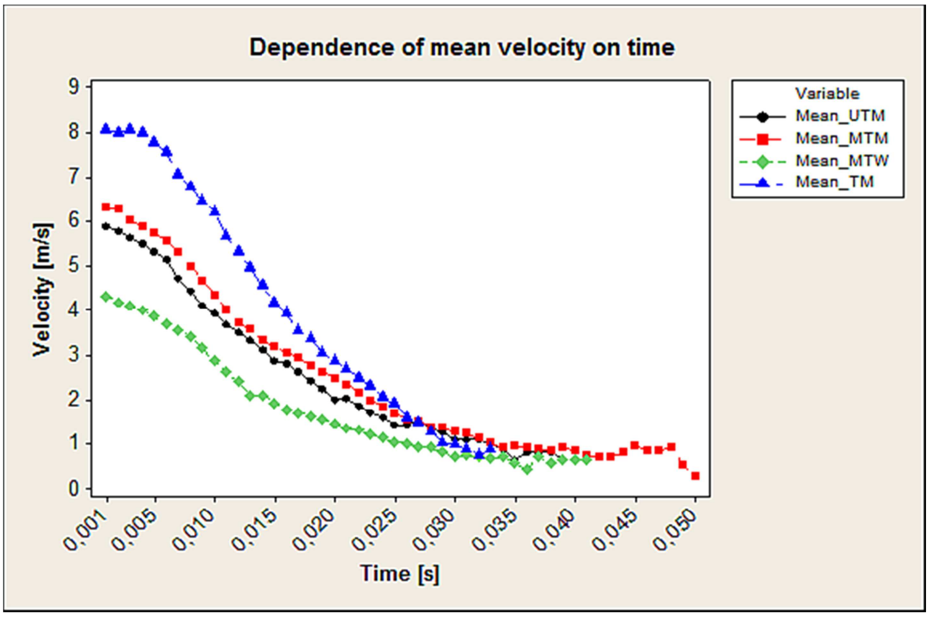


Fig. 5. Dependence of mean velocity on time

Table 1. Results overview

	Mean	StDev	CoefVar	Minimum	Median	Maximum	Number of samples
UTM	3,169	1,6269	51,85	0,8354	2,916	5,989	8
MTM	2,848	1,8631	65,65	0,4849	2,474	6,325	13
TM	4,203	2,545	60,13	0,727	3,705	8,109	4
MTW	2,0223	1,239	61,05	0,4493	1,663	4,347	6

Very important part of experiment was to find out if it is possible to determine dependence of maximum velocity on body’s height and weight. This is so important because it is expected that tall men with bigger weight would have stronger punch than small and thin men.

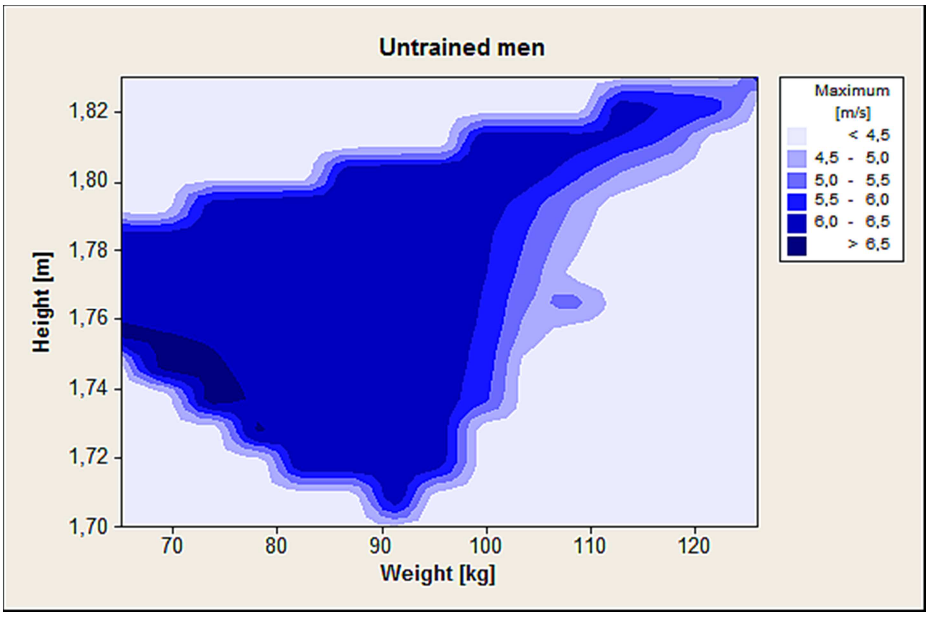


Fig. 6. Dependence of maximum velocity on body's height and weight for untrained men

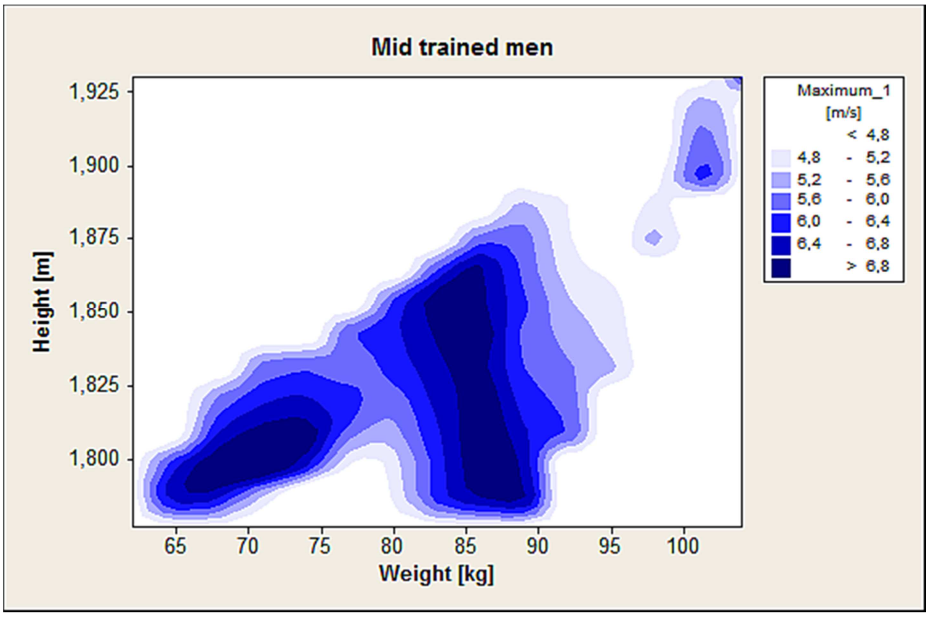


Fig. 7. Dependence of maximum velocity on body's height and weight for mid trained men

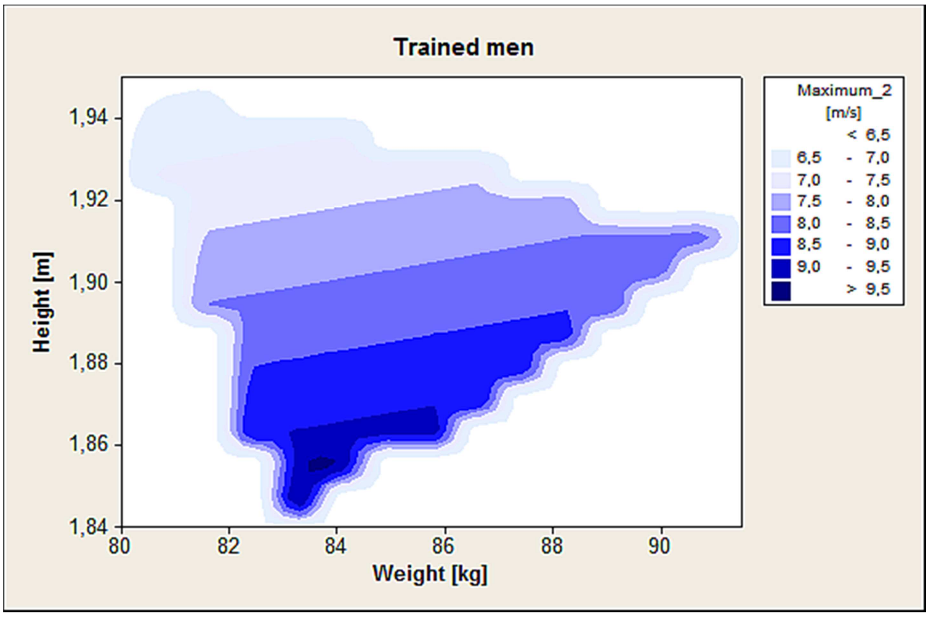


Fig. 8. Dependence of maximum velocity on body's height and weight for trained men

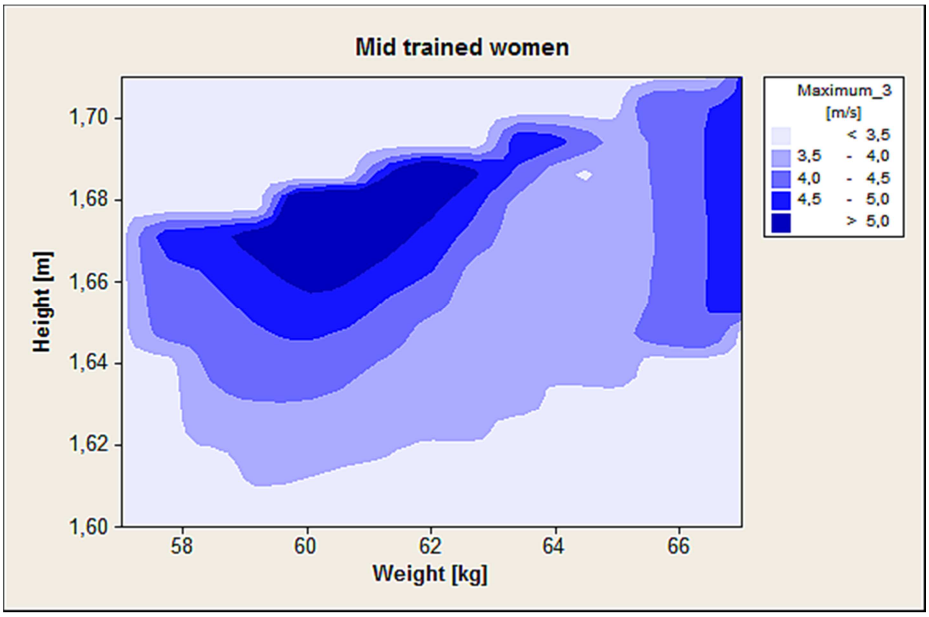


Fig. 9. Dependence of maximum velocity on body's height and weight for mid trained women

It can be seen there is no evident dependence of the maximum velocity on body's height and weight. Only in category of trained men there is a trend of bigger maximum velocity with lower height. In category of untrained men there is a trend of bigger maximum velocity with lower height and also with lower weight.

5 Conclusion

The experiment was focused on analysis of direct punch with a view to velocity. The high-speed camera Olympus i-Speed 2 and software i-Speed Control Software and MINITAB were used. The results are measuring of velocity in time and the maximum velocity. The aim was to find dependences of velocity on input parameters such as body's height and weight, gender and training level. It can be stated that there is a big difference between genders on the same training level. Dependences on body's height and weight are not evidential. The future experiment will be focused on gathering larger sample of people and then we can establish if some dependence exists.

Acknowledgments. This work was supported by the Internal Grant Agency at TBU in Zlín, project No. IGA/FAI/2014/036 and by the European Regional Development Fund under the project CEBIA-Tech No. CZ.1.05/2.1.00/03.0089.

6 The References Section

1. Baroň, M.: Measurement and evaluation of high-speed processes using high-speed camera system Olympus i-SPEED 2. Zlín, 2010. Thesis. Tomas Bata University in Zlin. Advisor doc. Dr. Ing. Vladimír Pata
2. Blower, G.: Boxing: Training, Skills and Techniques. Crowood, 2007
3. Bolander, R.P., Neto, O.P., A. Bir, C.: The effects of height and distance on the force production and acceleration in martial arts strikes. Journal of Sports Science and Medicine [online]. 2009, roč. 8, s. 47-52 [cit. 2012-06-27]. Available: http://www.jssm.org/combat/3/9/v8combat3-9.pdf
4. Chiu, H., Shiang, T.: A NEW APPROACH TO EVALUATE KARATE PUNCH TECHNIQUES. [online]. [cit. 2012-06-27]. Available: http://w4.ub.uni-konstanz.de/cpa/article/viewFile/4052/3751
5. Gianino, C.: Physics of Karate: Kinematics analysis of karate techniques by a digital movie camera. Latin-American Journal of Physics Education, 2010, 4.1: 5
6. Kolomaznik, Petr. Methodology of fast and stochastic mechanical process research. Brno, 2008. Thesis. Brno University of Technology. Advisor doc. Dr. Ing. Vladimír Pata
7. Lapkova, D., Pluhacek, M., Adamek, M.: Computer Aided Analysis of Direct Punch Force Using the Tensometric Sensor. In: Modern Trends and Techniques in Computer Science: 3rd Computer Science On-line Conference 2014 (CSOC 2014). Springer, 2014, s. 507-514. ISBN 978-3-319-06739-1.ISSN 2194-5357
8. Lapkova D., Pospisilik M., Adamek M. and Malanik Z.: The utilisation of an impulse of force in self-defence. In: XX IMEKO World Congress: Metrology for Green Growth.Busan, Republic of Korea, 2012, ISBN: 978-89-950000-5-2
9. Levine, D., Whitman, J.: Complete Krav Maga. 2007

10. Pešek, J.: High speed digital imaging system I-Speed 2 and its application. Brno, 2008. Bachelor's thesis. Brno University of Technology. Advisor doc. Dr. Ing. Vladimír Pata
11. Reguli, Z.: Inovace SEBS a ASEBS: Inovace bakalářského studijného oboru Speciální edukace bezpečnostních složek a navazujícího magisterského studijního oboru Aplikovaná sportovní edukace bezpečnostních složek. BIOMECHANIKA ÚPOLOVÝCH SPORTŮ A BOJOVÝCH UMĚNÍ [online]. 2011, Available: http://www.fsps.muni.cz/inovace-SEBS-ASEBS/elearning/biomechanika/biomechanika-upolovych-sportu

Modernization of artillery reconnaissance

Jiří Šotnar, Michal Carbol, Martin Blaha

Department of Fire Support Control,
University of Defence, Kounicova 65,
662 10 Brno, Czech Republic
martin.blaha@unob.cz

Abstract. The paper contains description of modernized artillery reconnaissance set LOS –M. It summarizes technical achievements which were made during the modernization process and it highlights the main advantages of the device. There is pointed out to importance of artillery reconnaissance and fast information flow. This is realized through modernized computers, software and generally through technical equipment. The modernization process is result of permanent need for better results and performance.

Keywords: artillery reconnaissance, reconnaissance device and vehicle, information flow, observing device, detection of targets.

1 Reconnaissance set LOS – M

All currently used means of artillery reconnaissance have during determination process of reconnaissance data specific limitations. These limitations can be solved by adding additional reconnaissance devices or resources, or their modernization throughout artillery reconnaissance system so that new devices are not doubling existing activities, but increasing the level of its quality.

Therefore, chief of artillery of the Czech Armed Forces adopted and already partially implemented projects related to modernization of artillery reconnaissance, both in yielding sets as well as in reconnaissance sets. By modernization or by inclusion of new devices will be cover the full spectrum of artillery reconnaissance tasks.

During the development of artillery reconnaissance devices is necessary to pay attention to connecting devices and their possibility of passing the real data to the required distance and in the required format. [5]

One of the first devices of artillery reconnaissance, which is currently undergoing modernization, is the observation set LOS. Its modernized version is called LOS - M.

LOS - M device is part of the fire control system of an artillery unit, which replaces an artillery observer. We count with its deployment mainly on exposed areas of the battlefield, where the standard observer of artillery fire control system would be exposed to unreasonable risk, primarily in terms of shelling enemy firing means, or from the viewpoint of chemical warfare agents, respectively other form of contamination of the surrounding environment. The LOS-M device will also be preferably used at forward positions, which will be quickly stationed, or that are inaccessible to artillery observers and also for the securing the critical areas and objects, both civilian and military.

Observing device LOS-M has, in practical terms, benefits that due to extensive computer support for operator activities in comparison to the current level of artillery observers fire control system workplaces, significantly increases the efficiency of management of reconnaissance activities of the artillery forces.

Due to integrated connecting means is better communication between mechanized forces and artillery. LOS - M reconnaissance device allows by its modular concept prospective expansion to other exploration sensors and subsystems.

The design and the possibility of changing system operators LOS-M allows virtually continuous combat operations of artillery observer throughout the reconnaissance system.

Used subsystems for the reconnaissance and their relative configurations, allows to create reconnaissance equipment with long-range detection and identification of targets. Established SW structure largely taking into account operator comfort and allows modifications to the requirements and the experience of the user. LOS-M system is also equipped with a simple kit for conducting spare reconnaissance.

For the crew are intended four places. Original driver's seat was retained. Place behind a driver is designed for a substitute or an advanced forward air controller posts (FAC). Commander´s workplace and integrated operator station is located to the left and right of the tower.

2 Function

LOS - M device allows, among other functions, to perform all tasks of the artillery observer fire control system ie.:

- Allows to search targets and determine their coordinates with high precision, day or night, and transfer them to superior.
- Plans and requires artillery and mortar fire.
- Correcting the results of shooting at different methods
- Coordinates the fulfillment of firing tasks of the artillery and mortar units in conjunction with combat activity of supported mechanized units.
- It provides the communication with the superior fire support coordinator and also fire control section and batteries.
- Allows monitoring of the tactical situation and enemy units on a digitized map, displaying areas of interest.
- It provides a connection to the commander of supported mechanized unit.
- It allows determination of their own stand and navigation using GPS.

3 Upgraded sensory subsystem

Upgraded sensory subsystem consists of the following components that are built into the sensory head:

- TV camera MERLIN-2;
- TV camera HK-170;
- Thermal imaging camera LIRC 640;
- LDM 38 laser rangefinder;
- INU TALIN 3000;
- Laser marker.

TV camera MERLIN-2

It is a color / monochrome (Day & Night) TV camera that is designed for close, especially for remote optical reconnaissance for the day and at dusk.
Detection of 16 km;
Reconnaissance 5 km;
Identification of 2.5 km.

TV camera HK-170

This is a TV camera mounted monochrome CCD sensor, which can be used as a sensor reconnaissance and combat means of orientation in the field, the field reconnaissance, to search and detect targets during the day and at dusk.
Detection of 10 km;
Reconnaissance 3,5 km;
Identification of 1.5 km.

LIRC 640 Thermal Camera

It is a thermal Module 3 generation operating in the spectral range to 10 micron.
Detection of 9.0 km
Reconnaissance of 3.0 km
Identification of 2.0 km

Laser rangefinder LDM 38

It is a high performance module eye safe laser rangefinder. It features a ruggedized compact design and is designed for installation in military applications.
Minimum distance measuring 100 m
Maximum distance measuring 20,000 m
Accuracy of distance measurement ± 5 m

Laser marker

It will provide marking of the observed target for other units that are equipped with observation devices operating in a narrow band near IR region of the spectrum.

4 Software

Application software will provide two basic modes of research:

- Viewing Mode
- Monitoring Mode

Viewing mode will be used to reconnaissance of the field and will be fully dependent on the operator's activities, ie. It is integrated in the operator´s workplace, he will operate reconnaissance subsystem by his instructions and will concentrate on field observations.

Monitoring mode will automate surveillance activities in the form of programmed activities, which will perform autonomously without operator intervention. The operator defines interest points, which will focus sensory subsystem, and after running the tracking mode, image sensors scan the set area. The monitored area can also set motion detection area, the system will automatically inform the operator of its integrated workplace disruption of any monitored area.

5 The following facts

Artillery Reconnaissance set LOS - M is supplemented, as opposed to the original type, by surveillance subsystem of the commander, who will provide him an overview of the vehicle's surroundings full 360 ° both in the day and at night. This subsystem is solved by integration of camera modules on the outside of the vehicle and display elements of the system on the commander's inside. [8]

The modernization of reconnaissance device will also replace existing radios for modern radios fully compatible with radios used by other NATO armies. The vehicle has been fully implemented by system BVIS-V, which is the basic communication node of today's military devices in the Army.

The big advantage is the replacement of the original yielding electric generator, which is built into the body of the vehicle and will apply without taking out. It is equipped with a means of air conditioning units that ensure suitable working environment and service deployment in climatic conditions quite different from those on which the original reconnaissance vehicle was designed.

It is also calculated with a modifying of software, to ensure a smooth transition of operators between the upgraded reconnaissance set and other reconnaissance sets with the modernization or development, is expected in the future. [10]

For the modernization of LOS set has been extensively used test subsystems that are used in the vehicle PANDUR, especially in the reconnaissance version KBV-Pz. This is complete integrated reconnaissance subsystem, which will make extensive use of components and subsystems identical with integrated reconnaissance system KBV-Pz, which greatly simplifies the logistics of LOS-M set.

Reconnaissance LOS-M device is assigned to the degree of artillery unit at the same level as an artillery observer, respectively artillery reconnaissance team. Inclusion of set LOS – M in the structure of artillery sections intended for direct fire support is subordinated to the appropriate commander, or it is subordinated to the commander of a mechanized unit for which this reconnaissance vehicle is destined. [9]

If artillery fulfills tasks of general fire support is the inclusion of LOS-M device directly subordinated to the commander of the section.

6 Conclusion

Modernization of reconnaissance set LOS was focused on advancement of the overall utility performance to the level of today's modern reconnaissance systems and was also focused on eliminating the existing gap, which was particularly manifested during its deployment in international missions of the Czech Armed Forces.

References

[1] *Military Strategy of The Czech Republic*. Praha: MO CR, 2008.

[2] *Long-Time Scheme of Ministry of Defence*. Praha: MO CR, 2008.

[3] *NATO Capabilities/Statements - 2018*. Brusel, 2007.

[4] *Doctrine of the Army of the Czech Republic*. Praha: MO CR, 2005.

[5] BLAHA, M., SOBARŇA, M. Principles of the Army of the Czech Republic Reconnaissance and Fire Units Combat using. In *The 15th International Conference „The Knowledge-Based Organization"*. Sibiu (Romania): Nicolae Balcescu Land Forces Academy, 2009, pp. 17-25.

[6] *AD-6.1 Doctrine of Communication and Information systems*. Praha: MO CR, 2003.

[7] *AAP-6 NATO Glossary of Terms and Definitions* (english and french). 2009.

[8] BLAHA, M., BRABCOVÁ, K. Decision-Making by Effective C2I system. In *The 7th International Conference on Information Warfare and Security*. Seattle (USA): Academic Publishing Limited, 2012, pp. 44-51. ISBN 978-1-908272-29-4

[9] BLAHA, M., BRABCOVÁ, K. Communication environment in the perspective Automated Artillery Fire Support Control System. In *The 10th WSEAS International Conference on APPLIED INFORMATICS AND COMMUNICATIONS (AIC '10).* Taipei, 2010. pp. 236-240. ISBN 978-960-474-216-5.

[10] BLAHA, Martin. Communication as a basic for future Artillery Fire Support Control System. In: *The European Conference of COMMUNICATIONS (ECCOM'10)*. Tenerife: WSEAS Press, 2010, p. 140-142. ISBN 978-960-474-250-9.

[11] BLAHA, Martin; POTUŽÁK, Ladislav. Decisions in the perspective Automated Artillery Fire Support. In: *Recent Researches in Applied Informatics & Remote Sensing*. Penang: Wseas Press, 2011, p. 87-91. ISBN 978-1-61804-039-8.

A Recommender System using Collaborative Filtering and K-Mean Based on Android Application

Kunyanuth Kularbphettong[1, a], Sunisa Somngam[2,b], Cholticha Tongsiri[3,c] , and Pattarapan Roonrakwit[4,d]

[1,2]Suan sunandha Rajabhat Univesrsity, 1 Dusit, Bangkok, Thailand
[3,4]Silpakorn University, CAT Tower 8 floor, Bangkok, Thailand

kunyanuth.ku@ssru.ac.th, sunisa.so@ssru.ac.th, ctongsiri@gmail.com,ajpui20@hotmail.com

Abstract. The objective of this research is to develop the diamond recommendation system by using K-Means and Collaborative Filtering techniques. The prototype system suggests users automatically in order to maximize users' satisfaction. The system design and development will be in the form of Android (android operating system). We illustrate the methodologies and experimental results of this system. In this project, it was divided the result by the research purposes into 2 parts: developing the Mobile application for diamond recommender users and evaluating and testing the system. The results showed that the experts and users are satisfied with the system at a good level. The guide to buying diamonds actually works.

Keywords: Recommendation system, K-Mean, Collaborative filtering, Android

1 Introduction

With the advance technologies, there is an overwhelming amount of information available in the world and it is very difficult for customers to find the suitable products. To provide needed information, recommender system is the application of knowledge used to make a decision to users and it is a significant component to the businesses. Many recommendation systems were developed for use in industry and education that aim to create a list of suggestions and provide information to help customers for choosing the products. For instance, a Grundy system [1] is the first recommendation system that described models of users by using stereotypes and the result shown that user modes are effective in guiding its performance.

Collaborative Filtering is one of the significant techniques used in recommender systems to suggest products and services for customers on e-Commerce systems. This approach advices user based on the preferences of similar users and it generally analyzes relationships between users and products or services to identify the user product/service associations [2]. Ratings were given by customers to catalog items/products and users who have similar tastes will have similar tastes in the future

[3]. The number of items associated with users is evaluated the accuracy of a collaborative filtering approach. There are two types of collaborative filtering: user-based and item-based. User-based collaborative filtering predicts user's preference items from rating preference of similar users in the past and item-based collaborative filtering depends on the similarity items and this approach is based on the user rating history to indicate the ratings pattern [4]-[5].

Also, recommendation system is interested to researcher because the results of this research cause to effect in many fields and it is divided in 3 categories according to the suggested method as follows: Collaborative filtering, Content-base recommendation, and Hybrid approaches. In this paper, we present the prototype of mobile application for recommendation users by using K-Means and Collaborative Filtering techniques because Collaborative Filtering approach is sensitive with sparsity rating data in small group of users. Hence, K-means and Collaborative Filtering approaches were adapted in this project to reduce the sparsity rating problem. Furthermore, user preferences were considered to enhance the quality of this prototype.

The remainder of this paper is organized as follows. Section 2 presents related works and research methodologies used in this work. Section 3 we describe the system architecture based on the purposed model and section 4 shows the results of this experiment. Finally, the conclusion and future research are presented in section 5.

2 The Methodologies

2.1 Collaborative filtering (CF)

Collaborative filtering (CF) is one of the most effective and successful techniques of recommender systems. This technique uses the relevant feedback from other similar users to predict or recommend to other users. Amazon.com [6] is the most famous recommendation system. This recommendation system incorporates a matrix of the item similarity. In order to find the similarity of the users, the Pearson's correlation coefficient is used to compute similarity between user$_a$ and user$_u$

$$C_{a,u} = \frac{\mathrm{covar}(r_a, r_u)}{\sigma_{r_a} \sigma_{r_u}} \tag{1}$$

where $C_{a,u}$ is the Pearson's correlation coefficient between user a and user u

r_a and r_u is the received score from user a and user u

$$\mathrm{cov\,ar}(r_a, r_u) = \frac{\sum_{i=1}^{m} (r_{a,i} - \bar{r}_a)(r_{u,i} - \bar{r}_u)}{m} \tag{2}$$

Let $r_{a,i}$ and $r_{u,i}$ are the received score of product i from user a and user u

$\bar{r}_a$ and $\bar{r}_u$ are the average of score product from user a and user u
and m is the number of the co-rated items

According to Herlocker et al [7], they suggested to weight user similarity and computed a prediction by performing a weighted average of deviations from the neighbor's mean.

$$p_{a,i} = \bar{r}_a + \frac{\sum_{u=1}^{n} (r_{u,i} - \bar{r}_u).w_{a,u}}{\sum_{u=1}^{n} w_{a,u}} \tag{3}$$

where $p_{a,i}$ is the prediction for item i of user a
n is the number of neighbors
$w_{a,u}$ is the similarity weight between user a and user u

2.2 K-means

K-means is one of the simplest unsupervised learning algorithms for clustering data. The procedure follows a simple and easy way to classify a given data set through a certain number of clusters (assume k clusters) fixed a priori [8]. This algorithm aims at minimizing an objective function, in this case a squared error function. The formula of Euclidean distance is as follows:

$$j = \sum_{j=1}^{x} \sum_{i=1}^{x} \left\| x_i^{(j)} - c_j \right\|^2 \tag{4}$$

where $\left\| x_i^{(j)} - c_j \right\|^2$ is a chosen distance measure between a data point $x_i^{(j)}$ and the cluster centre c_j, is an indicator of the distance of the n data points from their respective cluster centers

3 The Experimental Setup

In this section, we described an overview and detail of the proposed system. we collected data from 150 users and each user was asked to fill out his/her personal profile including age, gender, income, type of jewelry, style, diamond shape and preferences. K-means was used to cluster into 3 groups of users by measuring distance from a point centriod Euclidean. Then collaborative filtering step calculated the similarity among each user and selected a user that is similar to the current users from finding the similarities and then the rating data is processed to predict the value prediction. Finally, the system will present the results by selecting from the highest rating for the current user.

4 The Results

In this project, it was divided the results by the research objectives into 2 parts: developing the mobile based on K-Means and Collaborative Filtering techniques and evaluating and testing the application.

4.1 Developing the mobile application

In this section, to develop the mobile application, Fig 1 and Fig 2 were shown the results of mobile application.

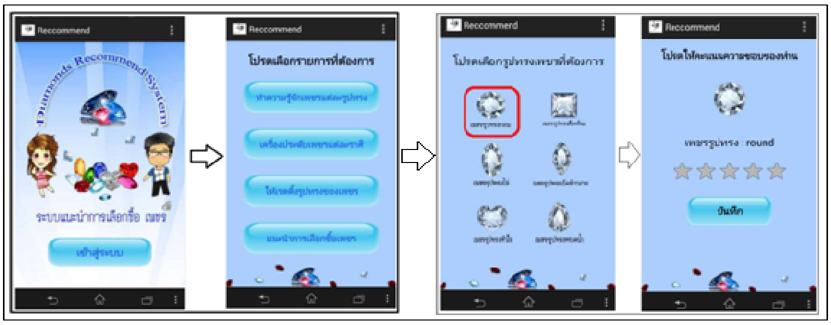


Fig. 1. The main page of application

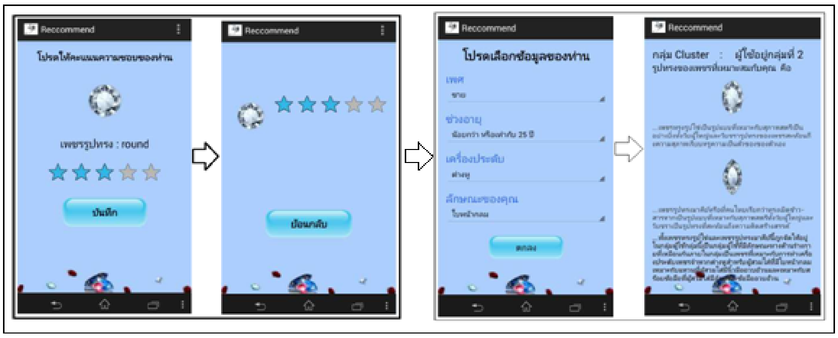


Fig. 2. The results page of application

4.2 Evaluating and testing the application

Black box Testing and Questionnaires by 5 experts and 150 users were used to evaluate and test the qualities of this application. Respondents were asked to rate the recommendation results and the rating score was from 1 to 5. Black Box testing is the testing approach that focuses only on the outputs generated in response to selected inputs and execution conditions and the internal mechanism of a system or component is ignored [9]. Black box testing was assessed in the error of the project as following:

functional requirement test, Function test, Usability test, Performance test and Security test.

Table 1. The results of Black box testing

	Experts		Users	
	$\bar{x}$	**SD**	$\bar{x}$	**SD**
1.Function Requirement Test	4.46	0.51	4.22	0.56
2. Functional Test	4.2	0.57	4.27	0.64
3. Usability Test	4.16	0.55	4.25	0.59
4. Performance Test	4.00	0.50	4.33	0.63
5. Security Test	4.25	0.47	4.19	0.54

Functional Requirement Test is evaluated the satisfaction on the ability of the system so as to meet the needs of users and functional test was used to evaluate the accuracy of the system. Usability test is a measurement of the suitability of the system. The performance of the system is assessed the processing speed of the system in Performance Test. Finally, Security test was evaluated the security of the system and Table 1 and Fig 3 were shown the results of Black box testing.

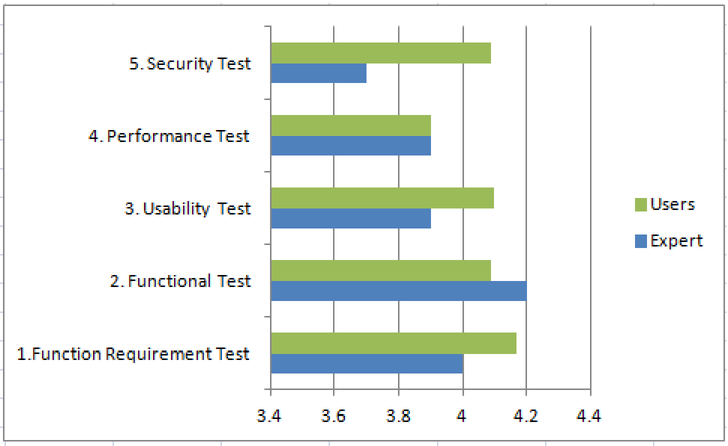


Fig. 3. . The results of Black box testing

The results showed that the Diamond recommender system based on Mobile application was satisfied the requirements of users. Means for 5 experts and 150 users were 4.2 and 4.25 respectively.

5 Conclusion

In this work, we proposed the diamond recommendation system by using K-Means and Collaborative Filtering techniques based on Mobile Application. This system provides more suitable recommendation information to users. K-means was used to cluster optimal groups and Collaborative filtering produced recommendation results based on user's voting and preferences. The initial results showed that our approach is successfully generated the recommendation results matching with the group of users. As for the future work, we need to explore more reasonable other technologies to apply in this project to enhance the quality and quantity of services to users.

6 Acknowledgements

The authors would like to thank Suan Sunandha Rajabhat University for scholarship support this project.

References

1. Rich, "User Modeling via Stereotypes," Cognitive Science, vol. 3,no. 4, pp. 329-354, 1979.
2. Y. Hu, Y. Koren, and C. Volinsky, "Collaborative filtering for implicit feedback datasets", ICDM'08. Eighth IEEE International Conference on, pp. 263–272, 2008
3. Dietmar Jannach, Markus Zanker and Gerhard Friedrich, "Tutorial: Recommender Systems", International Joint Conference on Artificial Intelligence Beijing, August 4, 2013.
4. Ricci F, "Mobile Recommender Systems", International Journal of Information Technology and Tourism, Vol. 12, No. 3, pp. 205-231, 2011.
5. Su, X., Khoshgoftaar, T.M., X. Zhu, and R. Greiner, "Imputation-Boosted Collaborative Filtering Using Machine Learning Classifiers", Proceedings of the ACM symposium on Applied Computing, pp. 949-950, 2008.
6. Greg Linden, Brent Smith, Jeremy York, "Amazon.com Recommendations Item-to-Item Collaborative Filtering", "IEEE Internet Computing", IEEE Computer Society, vol. 7, no 1, pp 76-80, January 2003.
7. MacQueen, R., "Some Methods for classification and Analysis of Multivariate Observations" Proceedings of 5-th Berkeley Symposium on Mathematical Statistics and Probability, Berkeley, University of California Press, vol.1, pp.281-297, 1967.
8. Herlocker JL, Konstan JA, Borchers A and Riedl J, "An algorithmic framework for performing collaborative filtering", In: Hearst MA, Gey F and Tong R, eds., Proceedings of the 22nd International Conference on Research and Development in Information Retrieval (SIGIR'99). ACM Press, New York, pp. 230–237, 1999.
9. Laurie Williams. "Testing Overview and Black-Box Testing Technique

Local flood warning systems and application possibilities

Jakub Rak[1] , David Sevcik[2], Blanka Svobodova[3], Jan Strohmandl[1],

[1] Faculty of Logistics and Crisis Management, Tomas Bata University in Zlín, Studentské nám. 1532, 686 01 Uherské Hradiště, Czech Republic
Jakub Rak jrak@flkr.utb.cz, Jan Strohmandl strohmandl@flkr.utb.cz
[2] Faculty of Applied Informatics, Tomas Bata University in Zlín, Nad Stráněmi 4511, 760 05 Zlín, Czech Republic
David Sevcik, dsevcik@fai.utb.cz
[3] Faculty of Technology, Tomas Bata University in Zlín, nám. T. G. Masaryka 275, 762 72 Zlín, Czech Republic
Blanka Svobodova, bsvobodova@ft.utb.cz

Abstract. The article describes possible technical systems within the field of flood protection, which serve as remote monitoring and detection of floods. It is focused on local flood warning systems, methods of measuring water surface and discharge flows with the possibility of remote transmission and processing by means of a gauging station, special software, and other support elements. The conclusion includes a description of the use of these stations within the process of emergency management and protection of the population.

Keywords: Flood Protection; Population Protection; Emergency Management; Information Systems.

1 Introduction

The development of society, constructions, agriculture, and industrial production leads to hazards and risks associated with it. These hazards include extraordinary events caused by humans as well as natural extraordinary events. Natural extraordinary events are natural disasters, which cause extensive damage and harm in many countries, including the Czech Republic. Floods are ones of these disasters. Not only does damage and loss affect property and districts but also the lives and health of the population. Floods, in particular, are one of the most serious problems in the Czech Republic as regards natural disasters. According to [1], the flood in 1997 in the Czech Republic caused damage of 2.25 billion Euros (based on the current conversion rate) and claimed 60 human lives. The flood affected 536 municipalities and the damage represented about 3.5 % of GDP in the respective year. Also in the following years the floods caused extensive damage to the country. Specifically, it was in 2002 when the flood claimed 17 lives and caused damage of 2.6 billion Euros (based on the current conversion rate). In total, the floods in the Czech Republic claimed 123 lives

ISBN: 978-1-61804-246-0

and caused damage of 6.15 billion Euros (based on the current conversion rate) between 1997 and 2010. Due to the number of fatalities and the extent of damage it is necessary to develop methods for flood protection. The prompt detection of flood is necessary for the timely deployment of protection systems.

2 Problem Formulation

Owing to the seriousness of flooding and the extent of damage and harm, the issue of flooding became a part of Czech legislation. In particular, the flood protection and related problems are provided for by the regulations: Act No. 254/2001 Coll., "the Water Act"; Act No. 239/2000 Coll., on the Integrated Rescue System, and some other regulations. Furthermore, security bodies and bodies responsible for protection of the population together with Management of water flows also gives great awareness to floods.

2.1 Floods

The flood can be defined as substantial temporary rise of the water surface caused by abrupt discharge flows or temporary constriction of a river bed, particularly in the event of ice formations. [5]

Based on the course of floods and time of their formation, they can be divided as follows:

- winter and spring floods,
- summer floods caused by persistent regional rainfall,
- summer floods caused by short term intensive rainfall,
- winter floods caused by ice formations.

The extent of flooding and resulting damages and harm are affected primarily by the following factors [6]:

- persistent rainfall, torrential rains, intensive thaw with rain causing melting of snow and releasing of ice,
- capacity and condition of the river bed,
- resistance and sufficient height of flood banks along the watercourse against surging and flowing water, and resistance of dikes against overflowing,
- influence of retention of waterworks (reservoirs, ponds, polders) and other technical protections (weirs, flood banks along watercourses, etc.),
- influence of the retention capacity of the land,
- built-up areas and the use of floodplains,
- timely notification of flood hazards;
- operative administration of water management processes during floods,
- precautions for the protection against floods.

2.2 Protection against floods

From the perspective of time, the protection against floods and coping with them can be described as follows. Precautions taken:

a) prior to the occurrence of floods;

These precautions include, for instance, construction changes to river beds, construction of protective elements, such as waterworks and weirs, preparation of flood protection plans, etc.

b) in the event of floods;

Evacuation of affected persons, building of improvised flood banks, water barriers, etc.

c) after the flood;

Cleaning and decontamination of affected areas, regeneration of the area, revitalization, etc.

The protection against floods is administrated by the flood protection authorities in all three periods of time.

Flood protection authorities. In the Czech Republic the protection against flood is administrated by the flood protection authorities that within their territorial scope provide services for the preparation for flood management, organization and control of all relevant actions during flooding as well as in the period immediately after the flood, including management, organization and control of other participants involved in flood protection. Activities of flood protection authorities are governed by flood protection plans. Status and activities of flood protection authorities are specified at two time levels:

a) off-flood protection authorities:

- municipal bodies and bodies of municipal districts in Prague,
- local authorities of municipalities with extended powers; authorities of municipal districts established by the Statute of the City of Prague,
- regional authorities,
- The Ministry of the Environment; provision for the preparation of rescue operations falls within the competence of the Ministry of the Interior.

b) protection authorities during the flood:

- flood commissions of municipalities; flood commissions of municipal districts in Prague,
- flood commissions of municipalities with extended powers; flood commissions of municipal districts established by the Statute of the City of Prague,
- flood commissions of regions,
- Central Flood Commission.

2.3 Detection of the flood origin

In order to implement protective measures it is important to obtain information about the actual origin of the flood. This information can be acquired during the flood or within a short period prior to its origin (before the arrival of a flood wave).

As stated by [2], the acquisition of information in advance (dozens of minutes up to 2 hours) significantly lowers the probability of loss of human lives and it helps to protect their property to some extent.

Specifically, timely detection of floods is crucial for the so-called “flash floods”. For these floods it is not possible to use conventional methods of a weather forecast given to a small size of the affected area and the speed of the formation. Detection by means of these methods is quite difficult and unusable in practice. The local warning systems for individual rivers installed directly in the relevant areas are one of the means of “early detection.” The description of a similar system and its implementation within the municipality with extended powers in Uherské Hradiště can be found in Chapter 3

3 Problem Solution

Local systems for early warnings can efficiently be used for monitoring and giving timely notification to flood protection authorities and population within the areas at risk of flash floods. This system is a comprehensive summary of technical and software equipment that serves for detection of approaching floods. Timely detection enables acquiring some time for the implementation of protective measures.

3.1 Materials and methods

For testing of the system for timely warnings against floods at the territory of MEP UH, a gauging station composed of a universal registration and control unit M 4016-G3 with an integrated GSM/ GPRS modem, RS232 interface and pressure sensor of water surface PTX 7500 was used. In order to control the station the “MOST” software was used; this software enables the overall setting of all necessary parameters for the station. Apart from the “MOST” software also the “web viewer of measured data” was employed. This web interface serves for limited settings of the station and for storing and displaying outputs of measurements.

The system of timely warning is based on the method of continuous measurements of water surface and the wireless transmission to the server, or mobile station (mobile phones).

Some municipalities in the territory of the MEP Uherské Hradiště face similar problems. A similar system, its components and problems connected to its implementation within the municipality with extended powers in Uherské Hradiště is described in this contribution.

Implementation and engagement of the system within the processes of flood protection is quite difficult. The implementation of the system in the territory of the MEP Uherské Hradiště and its testing was accomplished as follows.

3.2 Local systems for early warnings

Implementation of the local system for early warnings consists of following steps.

Gauging profile. The first step of installation is the choice of an appropriate gauging profile, in other words finding a suitable place for installation.

The suitable profile must comply with the basic requirements, which are in particular:

- distance from the area at risk,
- power supply,
- firm attachment,
- GSM network coverage.

On selection of the suitable profile the actual installation of individual parts of the system was accomplished.

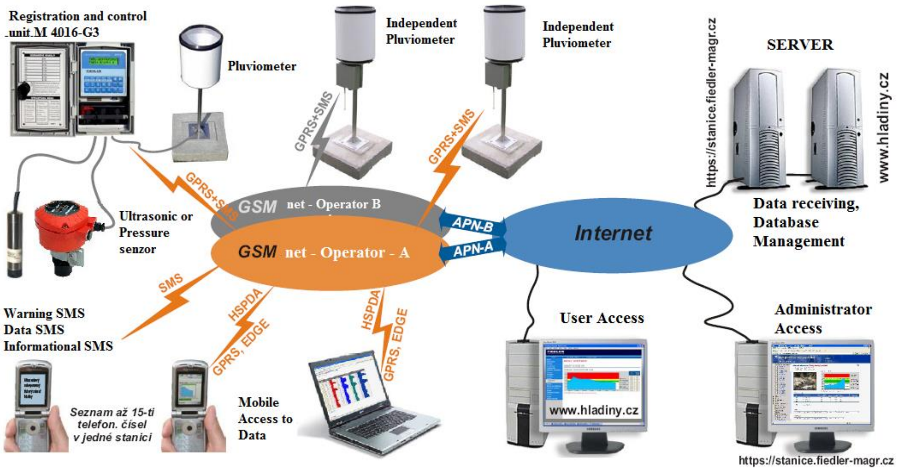


Fig. 1. The scheme of Local systems for early warnings [4]

Installation of individual parts of the system and their interconnection. The main parts, which included the registration and control unit M 4016-G3 together with the pressure sensor of water surface PTX 7500, were mounted on the fixed part of the bridge structure. The sensor was placed below the water surface at a height of 0.5 m above the bottom of the river (this height protects the sensor from fouling). The registration and control unit was mounted on a lighting column at a height of 2 m above the top edge of the bridge in a metal protective casing. Mounting it on a lighting column enabled connection to the source of electrical energy and thus ensured a permanent power supply (12 V). In the event of a power outage the station is equipped with a rechargeable battery. The battery allows operating up to 48 hours. In order to connect the station with the sensor a RS232 bus was used.

For the actual application of the system, the station was connected to the server by means of the GSM network (through data SMS messages). Individual parts of the system and their interconnection are very apparent in Fig. 1.

Scanning the water surface of the watercourse. Scanning of the water surface is provided by a pressure sensor PTX 7500, which operates on the principle of scanning the pressure of the water column above the sensor. The sensing part is thus located under water surface in a place that reduces the likelihood of fouling.

Discharge flow calculation – the water level. In order to calculate the discharge flow a graphical-numerical method consisting of the manual measurement of water flow rates by means of floats was employed [5]. Based on the examination of the bottom of a suitable gauging profile, a model of this profile was created (see Fig. 2). Furthermore, bridge pillars were integrated into the model and subsequently, a cross sectional area of the water surface was calculated. To calculate the surface, the data from the gauging station was used, namely the water level.

The following section of the article describes the process of detection of regular discharge flow.

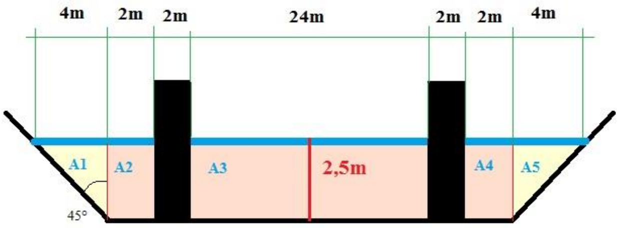


Fig. 2. The gauging profile model

The regular discharge flow was calculated based on formula No. 1, where Q is the resulting discharge flow in [m^3*s^{-1}], F is the surface of the cross sectional area of the water surface in [m^2] and V$_S$ is the velocity of the discharge flow in [m*s^{-1}]. The resulting discharge flow is 43.2 [m^3*s^{-1}]. In order to reduce the influence of measurement errors, the velocity of the discharge flow was measured 10 times and subsequently the average value V$_S$ was calculated (see the equation No. 2). These values are specified in Tab. 1.

$$Q = F * V_S \tag{1}$$

$$V_S = \frac{\sum_{k=1}^{10} V_x}{10} \tag{2}$$

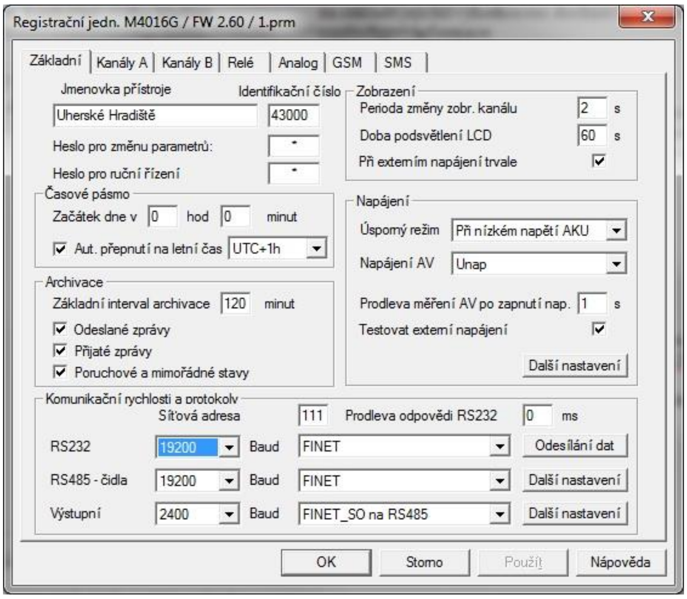
By means of the calculation, the value of the average discharge flow of water in the place of the gauging profile was acquired. Consequently, based on the average discharge flow it is possible to derive an equation for determining the standard flow, namely on the basis of changes in water surface and velocity of discharge flow.

Table 1. The table of the velocity of the flow for equation 2

Experiment	1	2	3	4	5	6	7	8	9	10	V$_S$
Vx [m*s^{-1}]	0.6	0.55	0.5	0.55	0.5	0.55	0.5	0.6	0.55	0.5	0.54

$$\begin{gathered} V_S = 0{,}54\ [m*s^{-1}] \\ Q = 80*0{,}54 \\ Q = \mathbf{43.2}\ [m^3*s^{-1}] \end{gathered} \tag{3}$$

Implementation of outputs of the system. The actual installation of the local system for early warnings is only one of the basic steps in protection against floods. Nevertheless, the following steps included in the implementation of the station's outputs are also significant. The outputs can be connected to a desktop software application. However, in order to ensure a quick response, the connection to the web application and particularly to the mobile GSM stations (mobile phones) is more convenient. Owing to this connection it is possible to report on the imminent hazard within one minute. In particular, notification by means of the GSM gateway is the main advantage of this system. Communication is based on the GSM module (gateway) employing a user's SIM card (the station then works as a standard GSM station - the mobile phone). By means of this device, the signal is transmitted through the public mobile network to the user (desktop application, web application or GSM station). Owing to the universal registration and control unit M 4016-G3 it is possible to set up required alarm values whose evaluation serves for reporting alarms or process information.


Registrační jedn. M4016G / FW 2.60 / 1.prm
Základní | Kanály A | Kanály B | Relé | Analog | GSM | SMS
Další nastavení
Odesílání dat
OK
Storno
Použít
Nápověda

Jmenovka přístroje: Uherské Hradiště
Identifikační číslo: 43000
Heslo pro změnu parametrů: *
Heslo pro ruční řízení: *

Časové pásmo
Začátek dne v 0 hod 0 minut
☑ Aut. přepnutí na letní čas UTC+1h

Archivace
Základní interval archivace 120 minut
☑ Odeslané zprávy
☑ Přijaté zprávy
☑ Poruchové a mimořádné stavy

Zobrazení
Perioda změny zobr. kanálu 2 s
Doba podsvětlení LCD 60 s
Při externím napájení trvale ☑

Napájení
Úspomý režim: Při nízkém napětí AKU
Napájení AV: Unap
Prodleva měření AV po zapnutí nap. 1 s
Testovat extemí napájení ☑

Komunikační rychlosti a protokoly
Síťová adresa 111
Prodleva odpovědi RS232 0 ms

RS232	19200	Baud	FINET
RS485 - čidla	19200	Baud	FINET
Výstupní	2400	Baud	FINET_SO na RS485

Fig. 3. The software application for system management

Once the limit values are reached and evaluated by the gauging station, the alarm signal is transmitted to the server and individual mobile stations.

The universal registration and control unit M 4016-G3 has 20 relays that allow the connection of up to 20 input devices. Apart from the sensors for water surface (e.g. PTX 7500), it is possible to connect rain gauges and other technological equipment. Owing to this fact, the station can be used as a comprehensive weather unit. Warnings and informational SMS can then be sent from each input separately.

4 Conclusion

Local systems for early warnings enable a significant increase in the quality of protection against floods. They are important for the protection against the so-called “flash floods” as well as common types of flooding. The manner of their use is fully dependent on the location of their installation and nature of the watercourse. The actual installation is constrained by several conditions that allow obtaining accurate and useful data. Ideally, it should be possible to acquire information on the high probability of flooding several hours in advance. In real-life situations, however, it is possible to obtain warnings in advance of dozens of minutes up to an hour.

Nevertheless, the local systems for early warnings using the gauging station and GSM information transmission have one major disadvantage. This disadvantage is the dependence on the functionality of the GSM networks. At present however, the risk of failure of GSM networks is acceptable because of two reasons. The first reason is a high reliability of GSM networks only with occasional failures due to network overload. The second reason is vital for public administration, whose staff, in the Czech Republic, is responsible for dealing with the flood situation. There are the so-called “emergency SIM cards” that operate within GSM networks even when the service is blocked for ordinary users. The probability of malfunction of GSM networks is thus minimal.

Another advantage of employing local systems for early warning is their relatively low price and the possibility of obtaining real-time data.

The previously described characteristics were verified during a test installation and operation of the gauging station in Uherské Hradiště. Results obtained from the installation, and the operation of it proved it to be a highly reliable system. However, they also revealed a possible large deviation when determining discharge flows. A possible approach for improving accuracy in discharge flow measurements is a topic for further research. An area worth further research appears to be the interconnection of outputs of the gauging station with SW applications, or technological equipment. This interconnection could lead to the possible extension of the gauging stations and their outputs.

Acknowledgments. This paper is supported by the Internal Grant Agency at TBU in Zlin, projects No. IGA/FAI/2014/035, IGA/FAI/2014/041 and IGA/FT/2014/001

References

1. Bumerl, M.: Hydrology. Veseli nad Luznici, (2003)
2. Kubat, J., Cekal, R., Danhelka, J., Matousek, V.: The technical guidance for implementation of flood warning service, Czech Hydrometeorological Institute, (2012)
3. M4016-G - Registration and control unit, Telemetric station, Flow meter, (User manual 1.3), FIEDLER-MAGR, http://www.fiedler-magr.cz, (2011)
4. FIEDLER-MAGR, http://www.fiedler-magr.cz
5. Sene, K.: Flood warning, forecasting and emergency response. Berlin: Springer, (2008)
6. Adamec, V.: Flood control and civil protection. Ostrava: Association of Fire and Safety Engineering, (2012)

Service Design According ITIL® with RAD Approach

Veronika Vesela, Lukas Kralik

Tomas Bata University in Zlín, Faculty of Applied Informatics, Nad Stráněmi 4511
760 05 Zlín, Czech Republic
{vvesela, kralik}@fai.utb.cz

Abstract. This paper responds to requirement to improve the orientation between offered SW, as ITIL® tools. There are really a lot of amount thus offered tools and very often leads to poor implementation of ITIL® on the basis of badly chosen tools. So this article aims to create dividing, which should facilitate choice of a suitable tool. Simultaneously, this division will serve for further work on creating a methodology for evaluation of ITIL® tools.

Keywords: ITIL®, ITIL® tools, tools categorization, IT service support, ITIL implementation.

1 Introduction

ITIL presents extensive and generally available manual for IT service management in a form of collection of books. The experiences and recomendations included by ITIL have become the best pracices. Those practices provide enough flexibility to accommodate the recommendation of the ITIL books to its needs and also to the needs of particular organization. The ITIL provides freely available scope which includes whole cycle of IT services. The ITIL is suitable for all companies operating in IT services (fig. 1). The ITIL is for example full of advices notices knowledge and warnings and also full of lessons what to do and what to not do. Standarts like ISO 9000 or ISO/IEC 20000 and models for property administration are used in practice cause they all have been proved relevant for service proveders. One of advantages of ITIL is the fact that it is possible to gain experience from experiences of the others.

2 IT Service Design

Service Design is a relatively new industry, which sees the functionality and form of services from the perspective of the user. "Apply tools and design methodologies for intangible products, ie services for the purpose of producing solutions that are useful, usable and attractive from the perspective of the customer, competitive and efficient from the perspective of providers". It combines many different disciplines such as marketing, corporate strategy, human resources or IT

2.1 ITIL® Service Design

Service design is one phase of ITILs® life cycle. It provides manuals for design and development of services and processes. It also presents design methods and principles which can help to transfer strategic objectives into the portfolio of the services and service assets. Service design responds to the needs of business user or targeted client and it is based round defined strategy of the company (Service Strategy). So it includes many functions processes and procedures, not only service design itself.

- Design coordination
- Management of the services catalogue
- Management services layers
- Capacity management
- Availability management
- IT service community management
- Information security management
- Supplier management
- Metrics definition

Whole process of design and deployment of the new service consists of few partial phases.

1. Strategy
2. Design
3. Transaction
4. Operation

However all these phases are solved complexly because Service Design does not focused on each individual parts. Thats the reason why the ITIL® (mean Service Design) should be completed with other techniques and practices. In this case is appropriet to use AGIL techniques or even better choice a RAD (Rappid Application Development).

2.2 Rapid Application Development

It is methodology oriented to objects themselves and it is able to simplify software development. The RAD includes some tools and procedures which are based on AGIL methodology. Those tools and procedures can be used to software development, which is their primary objective also can be used to development of systems products and processes. The RAD reduces the time for planning and focuses its potential into the development itself. The methodology consists of four basic aspects – methods tools management and people. If there is something wrong with one part it has influence on the development speed and quality. The method has a list of tasks and particular structure of work progress (workflow). This procedure is designed to achieve the highest possible speed of development. Functional prototype can be designed very quickly by using these procedures. Also there is still possibility to do any changes in the prototype. The prototype is used very often for software development also for development of new systems products web pages etc. More precisely it's used in every case where it is needed to see a basic structure of application and its mode of operation. If it's already able to meet our requirements or some changes have to be done. The prototype also allows the cooperation of more developers and involves the client into the development process and product testing.

Dominant tools supporting Rapid Application Development methodology are tools generating application code. These are mostly the tools supporting teamwork development called CASE. The tools selected by developing team should be able to process the system requirements and creates functional database and most of the application code.

This leads to the following requirements:

- The tool must produce a code which has multilayer structure.
- It generates prototype without the need of direct typing of the code.
- It allows modifying the generated code.
- It can be used in whole development.
- It must not cause more troubles than benefits.

Advantages and disadvantages of Rapid Application Development

Advantages of the RAD method:

- Shorter developing time
- Creation of the functional prototype which can be easily modified
- Feedback of the final user and cooperation with him
- There is possibility of creation of powerful developers team

Disadvantages of the RAD method:

- It needs very experienced developers
- Lack of know ledges and use of the RADs tools and procedures
- Incorrectly chosen tools

3 The Life Cycle Comparison for Rapid Application Development and ITIL®

The development of any application service or system has a certain life cycle. Mostly it starts with putting together requirements of the final user and realistic requirements which can be fulfilled. Selection of the right procedure and method for the developing is based on those requirements. When the ITIL and the RAD methodologies are compared so we can see if they are able to cooperate together, we can see that there is a certain similarity in their life cycle.

First step of both methodologies is planning and strategy selection. There is a little difference at the next step. The steps that are divided into two blocks in ITIL methodology are executed at the same time in RAD methodology. The RAD performs operations like draft design, group discussion, development itself, testing and consultation with final user in one phase of its life cycle. On the other hand the ITIL has similar steps divided into two phases. So there is an advantage of RADs involvement into the ITIL methodology of IT service development. Differences of both life cycles (ITIL® and RAD) are compared in next table (Table 1.)

Table 1. Comparison of RAD and ITIL® V3 life cycles

Rapid Application Development		**ITIL® V3**	
Planning	* Identification of requirements * Compilation a team of developers * Strategy	*Service strategy*	* Identification of requirements * Source links * Terms and Conditions * Strategy
Development	* Appearance design * Group discussion with JAD * Product development * Testing * Consultation with the user	*Service design*	* Packed of service models * Standards * Architecture * Models of the solution
Transition	* Service Operation * Application Operation	*Service Transition*	* Updated packages of service models * Test Solutions * Deployment plans
		Service Operation	* Operational plans * Service Operation

5 Conclusion

The best advantage of combination of both methodologies is reduction of time. Because the functional prototype of the application is ready quite soon and it is constantly improved. Another important advantage is communication with the final user and his evolvement into the developing process. The cooperation is based on AGIL methodology.

Acknowledgments. This work was supported by grant No. IGA/FAI/2014/020 and IGA/FAI/2014/053 from IGA (Internal Grant Agency) of Thomas Bata University in Zlin.

References

1. Automated Unattended Installation in Kovárna Viva, a.s. In: International journal of computers. Oregon (USA): North Atlantic University Union, 2014, s. 7. ISSN 1998-4308.
2. KRALIK, Lukas. Analysis for Automated Unattended Installation. In: Recent Advances in Automatic Control, Information and comunications: Proceedings of the 14th International Conference on Automation & Information (ICAI '13). Valencia (Španělsko): WSEAS press, 2013, s. 5. ISBN 978-960-474-316-2ISSN 1790-5117.
3. ITIL service design [online]. 2nd ed. London: TSO, 2011, xi, 442 s. [cit. 2013-07-22]. Best Management Practice. ISBN 978-0-11-331305-1. Dostupné z: http://www.best-management-practice.com
4. JAŠEK, Roman, SZMIT, Anna, SZMIT, Maciej. Usage of Modern Exponential-Smoothing Models in Network Traffic Modelling. In Nostradamus 2013: Prediction, Modeling and Analysis of Complex Systems. Heidelberg : Springer-Verlag Berlin, 2013, s. 435-444. ISSN 2194-5357. ISBN 978-3-319-00541-6.
5. JAŠEK, Roman, KOLAŘÍK, Martin, VÝMOLA, Tomáš. APT Detection System Using Honeypots. In Proceedings of the 14th WSEAS International Conference on Automation & Information (ICAI '13). Montreux : WSEAS Press, 2013, s. 25-29. ISSN 1790-5117. ISBN 978-960-474-316-2.
6. KRBEČEK, Michal, SCHAUER, František, JAŠEK, Roman. Security aspects of remote e-laboratories. International Journal of Online Engineering, 2013, roč. 9, č. 3, s. 34-39. ISSN 1868-1646.
7. Vala, Radek; Malaník, David; Jašek, Roman. Usability of software intrusion-detection system in web applications. In International Joint Conference CISIS ´12-ICEUTE ´12-SOCO ´12. Heidelberg: Springer-Verlag Berlin, 2013, s. 159-166. ISSN 2194-5357. ISBN 978-3-642-33017-9.
8. HOLMAN, Jan. Srovnání RAD platforem Seam Forge a Spring Roo. Brno, 2013.
9. ProjectManagement.com - Process/Project RAD - RAD - Rapid Application Development Process. In: Process/Project RAD - RAD - Rapid Application Development Process [online]. © 2014 [cit. 2014-06-25]. Dostupné z: http://www.projectmanagement.com/content/processes/11306.cfm
10. IT Service Management and ITIL Training: Introduction and Overview - The Cisco Learning Network. In: MARCUS, Ann. IT Service Management (ITSM) and ITIL [online]. 20.6.2011, 31.10.2011 [cit. 2014-06-25]. Dostupné z: https://learningnetwork.cisco.com/docs/DOC-12010
11. JELÍNEK, Jan. Spolupráce metodik ITIL a RUP. Praha, 2008. Dostupné z: http://student.vsmie.cz/~jelij5ap/itil.html
12. GRÁC, Marek. Rapid Development of Language Resources. Brno, 2013. Dostupné z: http://is.muni.cz/th/50728/fi_d/thesis.pdf
13. TANG, Raymond. Rapid Application Development. The University of Hong Kong, 12.8.2006. Dostupné z: http://matlesiouxx.free.fr/Cours/HKU/Courses/CSIS0404/Lecture%202/HKU2006_%282b%29_Rapid_Application_Dev.pdf
14. SHARP, Alec. Workflow modeling: tools for process improvement and applications development. 2nd ed. Boston: Artech House, c2009, xx, 449 s. ISBN 978-1-59693-192-3.

Software Application of Mathematical Modeling of Critical Infrastructure Element Resilience

Martin Hromada[1], Ludek Lukas[2]

[1] Faculty of Applied Informatics, Tomas Bata University in Zlín, Nad Stráněmi 4511, 760 05 Zlín, Czech Republic, hromada@fai.utb.cz
[2] Faculty of Applied Informatics, Tomas Bata University in Zlín, Nad Stráněmi 4511, 760 05 Zlín, Czech Republic, lukas@fai.utb.cz

Abstract. Software application of mathematical modeling of critical infrastructure element resilience is one of the security research project "The critical infrastructure element and sector resilience evaluation system" outcome. In the article the basic mathematical relations will be expressed from the perspective of internal structure of software application with relevant visualization. Application will be presented as a logical expression and algorithm use as an outcome of developed critical infrastructure resilience evaluation methodology.

Keywords: Critical Infrastructure, Resilience, Software Application, Mathematical Modeling,

1 Introduction

In the process of mathematical application of critical infrastructure resilience evaluation software application development was the resilience evaluation methodology selected. Methodology application is seen and represent the approach and phase of critical infrastructure element resilience evaluation, where the resilience is understood „The ability of systems, infrastructures, government entities, businesses, and society to adapt to adverse events, to minimize the impact of such events (keeping the system running), and also to anticipate future adverse events and be able to prevent them." (CRN Report, Focal report 6, Risk Analysis, Resilience – trends in Policy and Research)[1]

2 Critical infrastructure element resilience evaluation methodology algorithms

Critical infrastructure elements and elements system resilience evaluation respects the principles of critical infrastructure resilience evaluation. Depending on the purpose, the evaluation should be done as an external or internal resilience of critical infrastructure element or elements. It should be based on knowledge of nature and basic functional, technological and spatial attributes of the evaluated critical infrastructure elements.

Multi-criteria evaluation is one of the appropriate methods for evaluating the resilience of critical infrastructure element and system. This method allows implementation of a comprehensive evaluation of relatively independent indicators and parameters. It uses a semi-quantitative expression of the size of the individual indicators. Its disadvantage is a lower level of resilience level performance. It allows to rate a critical infrastructure element in an appropriate range of resilience levels. The result of evaluation unfortunately does not specify how long the element of critical infrastructure can withstand the influence of negative factors. The advantage is the evaluation of the protection measures quality in relation to identified threats.[2]

Critical infrastructure element resilience evaluation includes the following phases:

a) System analysis of evaluated critical infrastructure element
b) Analysis and Risk assessment
c) Determination of evaluated areas of security/safety
d) Determination of the attributes and indicators calculation
e) Calculation of critical infrastructure element resilience
f) Evaluation of critical infrastructure element resilience.

In the next part of article we will express only those methodology parts whose are most important in relation to mathematical modeling of resilience evaluation in the context of software application development.

2.1 Analysis and Risk assessment

Analysis and risk assessment is in the context of above-mentioned methodology two steps process where we use:

1. Semi-quantitative risk analysis,
2. QARS analysis

In the first instance, the risk is semi-quantitatively expressed by the relationship:

$$R = P * N \tag{1}$$

where:

R - Risk value,
P - The probability of threats application,
N - Is the impact value.

In risk and vulnerability evaluation process is necessary to use relevant methodology for the expression of the mutual relationships and interdependencies between identified risks. For this purpose, the QRAC (qualitative risk analysis by risk importance correlation) methodology was selected.

The importance of this method is especially in connection with the diversification of risk based on level of risk activity (the risk ability or potential to cause further risks) and passivity (possibility that the risk may be caused by other risks) in relation to other risks.

The process of implementation of the QRAC analysis is multi-steps process, where in the first step the list of risk is created. The next step is focused on the expression of importance relations and interdependencies between the identified risks in the form of spreadsheet correlation.

Table 1 List of Risks

	Index	1	2	3	4
Index.	The Threat Of	High temperature	Lightning	Tree fall	Operating error of third parties
1	High temperature	x			
2	Lightning	1	x	1	0

x - Reflects the fact that the risk itself cannot cause,

1 - Is the real possibility that the risk Ri may cause risk Rj,

0 - Expresses a condition where there is no real possibility that the risk Ri may cause risk Rj

To calculate the coefficients of the relationships and interdependencies we apply:

$$C_A R_i = \frac{\sum R_i}{x-1} \qquad C_P R_i = \frac{\sum R_i}{x-1} \qquad (2)$$

where:

$C_A R_i$ is the value of activity coefficient,

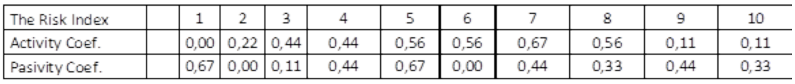
$C_p R_i$ is the value of passivity coefficient,

$\sum R_i$ is the sum of risks,

x - total number of risk,

After adding values to the correlation table for the tree fall risk, the horizontal axis (activity coefficient) and vertical axis (passivity coefficient) after using equations has following parameters:

Table 2 Coefficients and risk index



The Risk Index		1	2	3	4	5	6	7	8	9	10
Activity Coef.		0,00	0,22	0,44	0,44	0,56	0,56	0,67	0,56	0,11	0,11
Pasivity Coef.		0,67	0,00	0,11	0,44	0,67	0,00	0,44	0,33	0,44	0,33

Subsequently, the values were plotted in the graph, which ultimately enables the most significant risks in term of its potential (high activity and passivity potential).

For the risk evaluation or for the process of determinig the most significant risks, must be the graph divided into segments that diversify risks according their significance. To divide the grapf into 4th segments is necessary to define S1 and S2 lines that divide the graph itself and the risks to the segments where it is assumed that in the first segment will be 80% if major risks.

To express the parameters for line S1 and S2 we use the equations:

$$S_{1/2} = C_{A/P\max} - \frac{(C_{A/p\max} - C_{A/P\min})}{100} * 80 \qquad (3)$$

where:

$C_{A\max}; C_{A\min}$ Minimum and maximum values of activity coefficient,

$C_{P\max}; C_{P\min}$ Minimum and maximum values of passivity coefficient,

Then the lines are implemented into the graph and we divide the risks by 4 segments that represent the level of risks:

1. I. Segment - Primarily significant risks – the highest activity and passivity coefficients,
2. II. and III. Segment – Secondary significant risks,
3. IV. Segment – Tertiary significant risks – low value of activity and passivity coefficients,

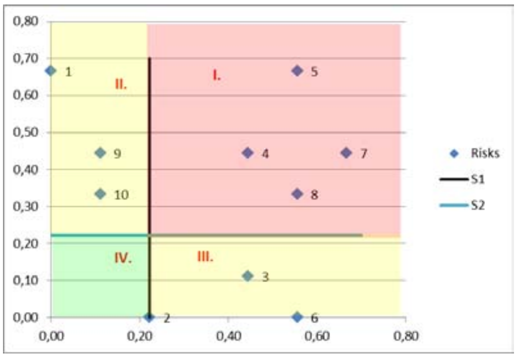


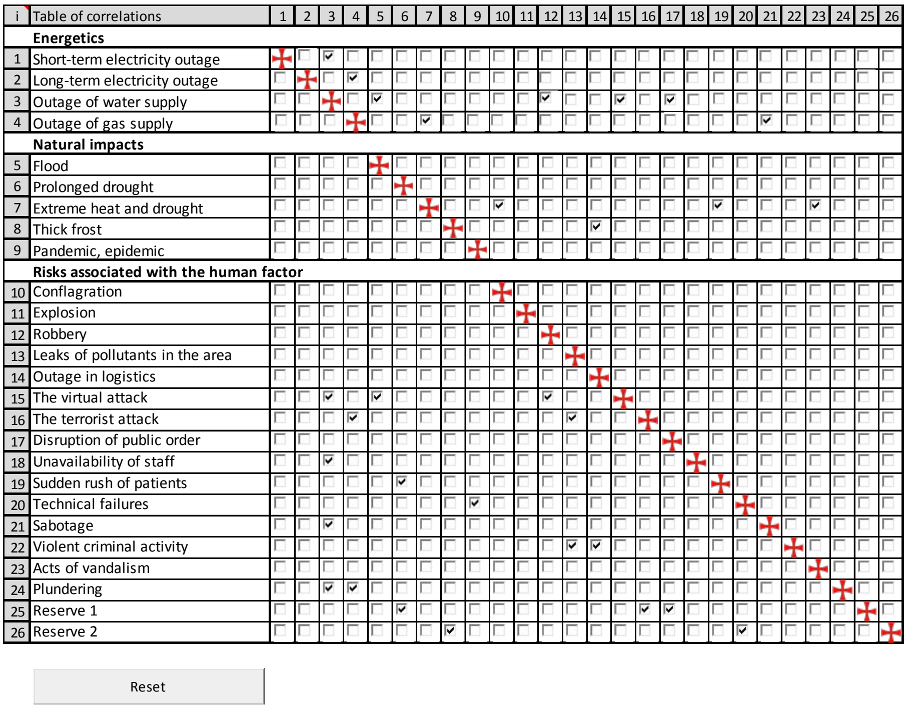
Figure 1 Graph division to 4 segments

This process allows us to divide risks by the highest potential in relation to system functionality degradation due to domino efect, which can be seen as expression and evaluation of vulnerability (parameter Vi)[3,4].

2.2 Software application

In relation to above-mentioned, the second step of risk analysis and assessment is the risk the list of risks creation. This method is based on the use of simple mathematical equations. In connection with this fact the excel calculator was selected, mostly to easy editing and graph work. Resulted table was:

Table 3 Risks correlation table



i	Table of correlations	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
	Energetics																										
1	Short-term electricity outage	✚	☐	☑	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
2	Long-term electricity outage	☐	✚	☐	☑	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
3	Outage of water supply	☐	☐	✚	☐	☑	☐	☐	☐	☐	☐	☐	☑	☐	☐	☑	☐	☑	☐	☐	☐	☐	☐	☐	☐	☐	☐
4	Outage of gas supply	☐	☐	☐	✚	☐	☐	☑	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☑	☐	☐	☐	☐	☐
	Natural impacts																										
5	Flood	☐	☐	☐	☐	✚	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
6	Prolonged drought	☐	☐	☐	☐	☐	✚	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
7	Extreme heat and drought	☐	☐	☐	☐	☐	☐	✚	☐	☐	☑	☐	☐	☐	☐	☐	☐	☐	☐	☑	☐	☐	☐	☑	☐	☐	☐
8	Thick frost	☐	☐	☐	☐	☐	☐	☐	✚	☐	☐	☐	☐	☐	☑	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
9	Pandemic, epidemic	☐	☐	☐	☐	☐	☐	☐	☐	✚	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
	Risks associated with the human factor																										
10	Conflagration	☐	☐	☐	☐	☐	☐	☐	☐	☐	✚	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
11	Explosion	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	✚	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
12	Robbery	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	✚	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
13	Leaks of pollutants in the area	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	✚	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
14	Outage in logistics	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	✚	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
15	The virtual attack	☐	☐	☑	☐	☑	☐	☐	☐	☐	☐	☐	☑	☐	☐	✚	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
16	The terrorist attack	☐	☐	☐	☑	☐	☐	☐	☐	☐	☐	☐	☐	☑	☐	☐	✚	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
17	Disruption of public order	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	✚	☐	☐	☐	☐	☐	☐	☐	☐	☐
18	Unavailability of staff	☐	☐	☑	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	✚	☐	☐	☐	☐	☐	☐	☐	☐
19	Sudden rush of patients	☐	☐	☐	☐	☐	☑	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	✚	☐	☐	☐	☐	☐	☐	☐
20	Technical failures	☐	☐	☐	☐	☐	☐	☐	☐	☑	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	✚	☐	☐	☐	☐	☐	☐
21	Sabotage	☐	☐	☑	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	✚	☐	☐	☐	☐	☐
22	Violent criminal activity	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☑	☑	☐	☐	☐	☐	☐	☐	☐	✚	☐	☐	☐	☐
23	Acts of vandalism	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	✚	☐	☐	☐
24	Plundering	☐	☐	☑	☑	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	✚	☐	☐
25	Reserve 1	☐	☐	☐	☐	☐	☑	☐	☐	☐	☐	☐	☐	☐	☐	☐	☑	☑	☐	☐	☐	☐	☐	☐	☐	✚	☐
26	Reserve 2	☐	☐	☐	☐	☐	☐	☐	☑	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☑	☐	☐	☐	☐	☐	✚

After the process of table fulfillment and the use of appropriate mathematical background the resulted graph and risks segmentation was:

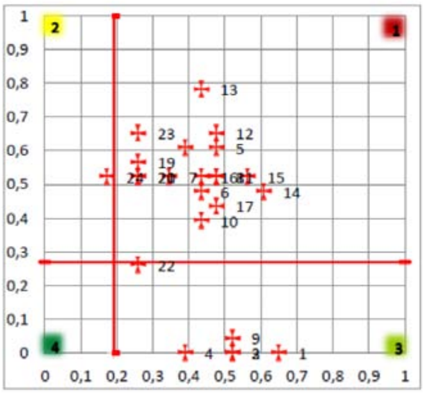
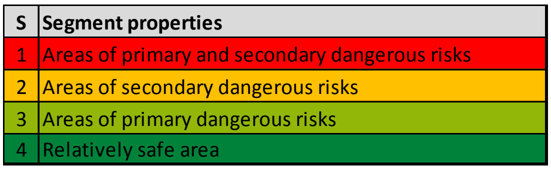


Figure 2 Risks correlation graph

where:



S	Segment properties
1	Areas of primary and secondary dangerous risks
2	Areas of secondary dangerous risks
3	Areas of primary dangerous risks
4	Relatively safe area

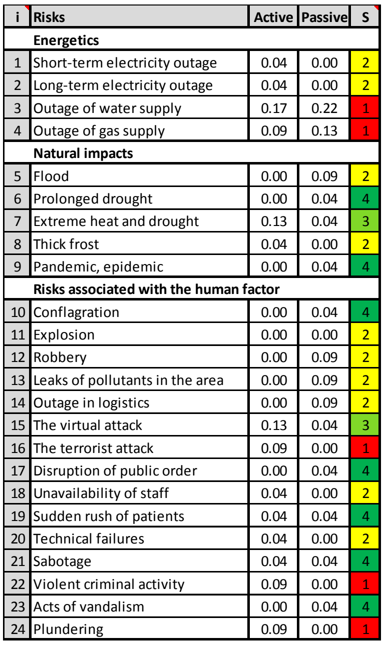
Figure 3 Segment properties

For the process of determining the value respectively the risk coefficient/parameter H_{Rzi} we select risks, which can be considered critical - located in I. Quadrant of QARS. These risks value is seen through first phase of risk assessment and analysis, which takes into account the degree and significance of the impact of the selected risks to the system. For the determination of the risk value we applied relationship:

$$H_{RZi} = \frac{H_{Ri}}{H_{Ri\max}} \qquad (4)$$

where:
H_{RZi} - is the risk value of i-th risk in range <0,1>
H_{Ri} - is the original risk value expressed in the first phase of the risk analysis
H_{Rimax} - the maximum attainable risk value within the value range.

After the select values of risks components, the final list for evaluation of critical infrastructure element risk value is presented:



i	Risks	Active	Passive	S
	Energetics			
1	Short-term electricity outage	0.04	0.00	2
2	Long-term electricity outage	0.04	0.00	2
3	Outage of water supply	0.17	0.22	1
4	Outage of gas supply	0.09	0.13	1
	Natural impacts			
5	Flood	0.00	0.09	2
6	Prolonged drought	0.00	0.04	4
7	Extreme heat and drought	0.13	0.04	3
8	Thick frost	0.04	0.00	2
9	Pandemic, epidemic	0.00	0.04	4
	Risks associated with the human factor			
10	Conflagration	0.00	0.04	4
11	Explosion	0.00	0.00	2
12	Robbery	0.00	0.09	2
13	Leaks of pollutants in the area	0.00	0.09	2
14	Outage in logistics	0.00	0.09	2
15	The virtual attack	0.13	0.04	3
16	The terrorist attack	0.09	0.00	1
17	Disruption of public order	0.00	0.04	4
18	Unavailability of staff	0.04	0.00	2
19	Sudden rush of patients	0.04	0.04	4
20	Technical failures	0.04	0.00	2
21	Sabotage	0.04	0.04	4
22	Violent criminal activity	0.09	0.00	1
23	Acts of vandalism	0.00	0.04	4
24	Plundering	0.09	0.00	1

Figure 4 Risks assessment list

2.3 Correlation value

Determination of correlation coefficient K$_s$ is an important aspect that expresses the position of the linkages and dependencies in CI within the critical infrastructure system. Generally speaking, the main linkages and dependencies areas are:

a) Logical linkages and dependencies,

b) Physical and dependencies,

c) Territorial linkages and dependencies.

To determine the value of correlation parameter the relationship is applied:

$$K_s = \frac{\sum Si}{S_{\max}} \tag{5}$$

where:

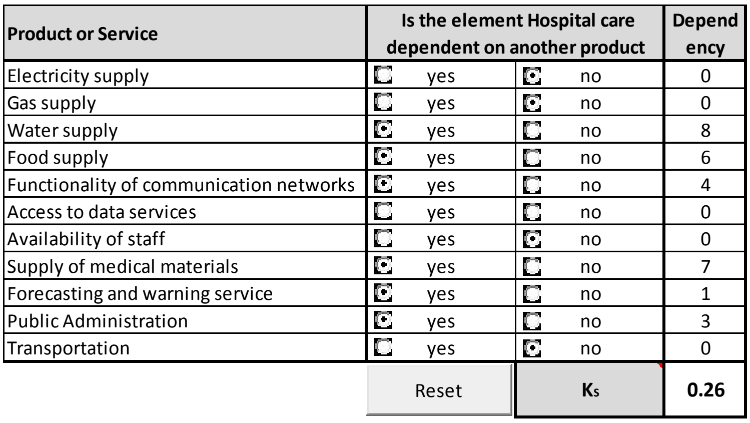
K$_s$ - correlation parameter value

Sum Si - the sum of the dependence degree of the i-th CI elements groups to other CI areas

S$_{max}$ - is the maximum value of corelation

2.4 Software application

After the mathematical expression of correlation value parameter the final list for critical infrastructure element correlation value calculation was:



Product or Service	Is the element Hospital care dependent on another product		Dependency
Electricity supply	○ yes	● no	0
Gas supply	○ yes	● no	0
Water supply	● yes	○ no	8
Food supply	● yes	○ no	6
Functionality of communication networks	● yes	○ no	4
Access to data services	○ yes	● no	0
Availability of staff	○ yes	● no	0
Supply of medical materials	● yes	○ no	7
Forecasting and warning service	● yes	○ no	1
Public Administration	● yes	○ no	3
Transportation	○ yes	● no	0
	Reset	K_s	**0.26**

Figure 5 Correlation value

2.5 Robustness coefficient evaluation

The robustness expressed by K$_{RO,}$ represents strength, durability, resistance to deformation. It is the ability to resist and withstand the effects of negative events without significant function degradation. In this methodology is the element robustness divided into structural robustness and security robustness. These two areas respectively their expression formulates a relationship for the evaluation of the system robustness:

$$K_{RO} = K_{RZ} * K_{SR} \tag{6}$$

where:
K_{RO} - is the robustness coefficient,
K_{RZ} - is the structural robustness coefficient,
K_{SR} - is the security robustness coefficient.

2.5.1 Security robustness coefficient evaluation

Evaluation of security robustness coefficient K_{RZ} in relation to the evaluation of resilience is seen in a wider context. Security robustness coefficient expresses the extent and quality of the critical infrastructure element security in connection with identified risks. Individual measures according to the nature and effect are grouped into specific areas of security. It is an area of physical security, information security, administrative security, personnel security, etc. For each type of critical infrastructure elements should the responsible entity recommend the different security areas. The security robustness coefficient basically consists from:

- level of physical security M_{FB} - which is an expression of the extent and quality of the measures taken in the critical infrastructure element physical security,
- level of information security M_{IB} - which is an expression of the extent and quality of the measures taken in the critical infrastructure element information security,
- level of administrative security M_{AB} - which is an expression of the extent and quality of the measures taken under the critical infrastructure element administrative security,
- level of personal security M_{PB} - which is an expression of the extent and quality of the measures taken in the critical infrastructure element personnel security.

It is obvious the selected areas of security in context of critical infrastructure element protection and resilience would have different weights (importance), so it was necessary to define it by:

$$V_i = \frac{\sum v_i}{K_v} \tag{7}$$

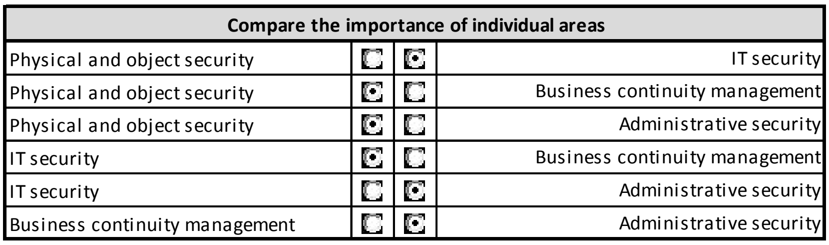
Where:
V_{FB} – physical security weight,
V_{IB} – information security weight,
V_{AB} – administrative security weight,
V_{PB} – personnel security weight,

For security robustness evaluation process has been formulated following relationship [5]:

$$K_{RZ} = M_{FB} * V_{FB} + M_{IB} * V_{IB} + M_{AB} * V_{AB} + M_{PB} * V_{PB} \tag{8}$$

2.5.2 Software application

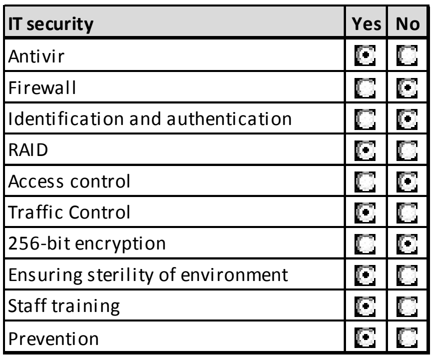
In relation to software application of security robustness expression we used comparison of selected security areas importance by Fullers triangle:



Compare the importance of individual areas			
Physical and object security	○	●	IT security
Physical and object security	●	○	Business continuity management
Physical and object security	●	○	Administrative security
IT security	●	○	Business continuity management
IT security	○	●	Administrative security
Business continuity management	○	●	Administrative security

Figure 6 Security areas importance comparison

and selected security areas checklists fulfilment:



IT security	Yes	No
Antivir	●	○
Firewall	○	●
Identification and authentication	○	●
RAID	●	○
Access control	○	●
Traffic Control	●	○
256-bit encryption	○	●
Ensuring sterility of environment	●	○
Staff training	●	○
Prevention	●	○

Figure 7 Selected security area checklist

2.5.3 Structural robustness coefficient evaluation

The evaluation process is represented by scoring of the main attributes that determine the magnitude of the structural robustness. The structural robustness coefficient K_{SR} varies in the interval 0.8 – 1. Structural robustness coefficient K_{SR} expresses the influence of topological structure, complexity and other properties or characteristics of the deterioration of protective measures effect of evaluated critical infrastructure element. If the coefficient of structural robustness K_{SR} is lower, the more attention should be paid to emergency preparedness. Main attributes by which the evaluation of the structural robustness should be performed include:

- type of topological structure,
- complexity,
- number of key technologies
- flexibility
- redundancy
- perimeter protection.

The values of topology index I_t, complexity index I_s, key technologies index I_{kt}, flexibility index I_f, redundancy index I_r and perimeter protection index I_{po} were based on special methodology which will be presented in software application of this part of robustness evaluation.

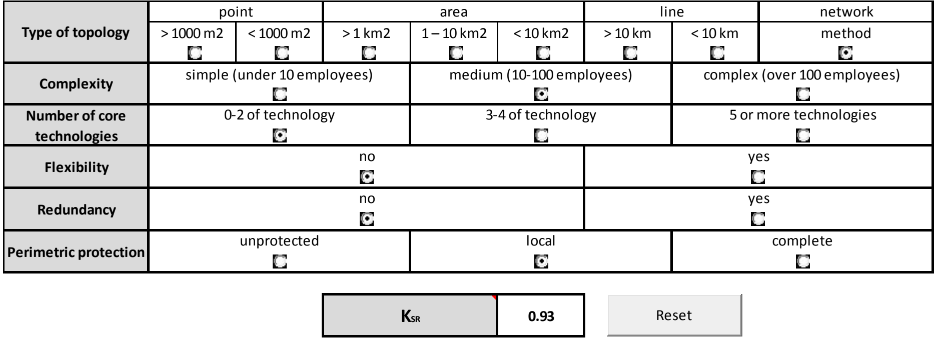
The resulting coefficient of structural robustness K_{SR} is calculated using a formula which respects the "Pareto rule"

$$K_{SR} = 0{,}8 + \frac{I_t + I_s + I_{kt} + I_f + I_r + I_{po}}{60} \tag{9}$$

K_{SR} - structural robustness coefficient[5]

2.5.4 Software application

Software application of structural robustness evaluation is divided into two parts. First is the highest hierarchical level and it is presented by following:

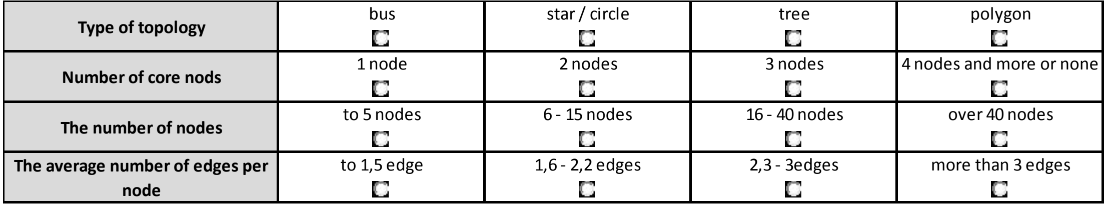


Type of topology	point		area			line		network
	> 1000 m2 ○	< 1000 m2 ○	> 1 km2 ○	1 – 10 km2 ○	< 10 km2 ○	> 10 km ○	< 10 km ○	method ●
Complexity	simple (under 10 employees) ○			medium (10-100 employees) ●			complex (over 100 employees) ○	
Number of core technologies	0-2 of technology ●			3-4 of technology ○			5 or more technologies ○	
Flexibility	no ●					yes ○		
Redundancy	no ●					yes ○		
Perimetric protection	unprotected ○			local ●			complete ○	

K_{SR}	0.93	Reset

Figure 8 Structural robustness evaluation

In case, that the topological type is a network, it is necessary to fulfill additional information by following table:



Type of topology	bus ○	star / circle ○	tree ○	polygon ○
Number of core nods	1 node ○	2 nodes ○	3 nodes ○	4 nodes and more or none ○
The number of nodes	to 5 nodes ○	6 - 15 nodes ○	16 - 40 nodes ○	over 40 nodes ○
The average number of edges per node	to 1,5 edge ○	1,6 - 2,2 edges ○	2,3 - 3edges ○	more than 3 edges ○

Figure 9 Additional table for network structural robustness evaluation

2.6 Preparedness coefficient evaluation

Preparedness of critical infrastructure element expresses its ability to restore its function after its degradation by the effects of negative factors (risks). Preparedness is evaluated through the preparedness parameter/coefficient K_{PR}, which can be understood as an expression of the ability to adequately reaction respectively response to the outbreak of an emergency or incident as well as the ability to recover and return to desired system functionality.

Mathematical expression of preparedness of the selected CI element is given by:

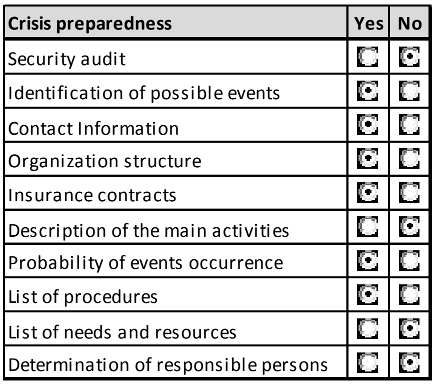
$$K_{PR} = \frac{K_r + K_p + K_i}{3} \tag{10}$$

where:

K_r - coefficient of identified risks accuracy,
K_p - CI subjects crisis preparedness plan quality coefficient,
K_i - CI subjects crisis preparedness plan implementation quality coefficient,

2.7 Software application

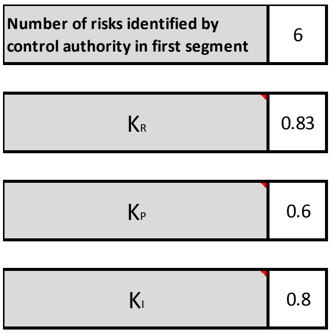
Each part (defined coefficients) of the preparedness coefficient had different check list, so we present the example of selected one and the final software application of critical infrastructure element preparedness coefficient evaluation.



Crisis preparedness	Yes	No
Security audit	○	●
Identification of possible events	●	○
Contact Information	●	○
Organization structure	●	○
Insurance contracts	●	○
Description of the main activities	○	●
Probability of events occurrence	●	○
List of procedures	●	○
List of needs and resources	○	●
Determination of responsible persons	○	●

Figure 10 Crisis preparedness plan quality coefficient

and the final software application of critical infrastructure element preparedness coefficient evaluation:



Number of risks identified by control authority in first segment	6
K_R	0.83
K_P	0.6
K_I	0.8

Figure 11 final preparedness coefficient evaluation

2.8 Critical infrastructure element resilience evaluation

It is obvious that the multi-criteria evaluation should relate to the areas of security, which have a positive impact on the level of resilience (robustness and preparedness), including their components. Each area of security, having a positive impact on the robustness and preparedness should be assessed in relation to the established standards (criteria), for selected area through checklists. A comprehensive evaluation requires expressing the value (coefficient) of the risk and its relationship and impact to the value of resilience in relation to selected element or sector of critical infrastructure. This highlights the fact that the total value of resilience under evaluated system is the average value of resilience in relation to i-th risk. For a complex multi-criteria evaluation of selected CI element or elements resilience was established mathematical relationship:

$$ODP = \frac{\sum ODi}{xi} \qquad (11)$$

where:

ODP - selected CI element resilience value
ODi - CI element resilience value in relation to selected i-th risk
xi - number of selected risks
Mathematical expression of CI elements resilience in relation to the i-th risk:

$$ODi = \frac{(1 - H_{RZi}) + (1 - K_S) + (K_{RO} * V_{RO} + K_{PR} * V_{PR})}{3} \qquad (12)$$

where:

H_{Rzi} - the value of i-th risk,
K_s - correlation parameter,
K_{RO} - robustness parameter,
V_{RO} - robustness weight,
K_{PR} - preparedness parameter,
V_{PR} - preparedness weight,

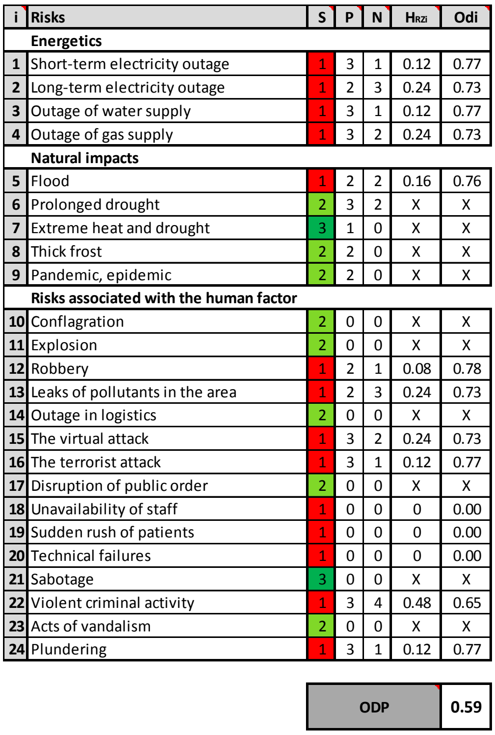
Equations (1- H_{Rzi}) and (1- K_s) reflect the fact, that risk and correlation value negatively affect the value of the critical infrastructure element resilience.

The presented facts are the basis for the final evaluation of the critical infrastructure element or group of elements resilience in the relevant sector.

The final qualitative evaluation will be presented in software application part of final critical infrastructure element resilience evaluation.

2.9 Software application

For final critical infrastructure element resilience evaluation were above-mentioned facts and mathematical expressions used and they were presented by following:

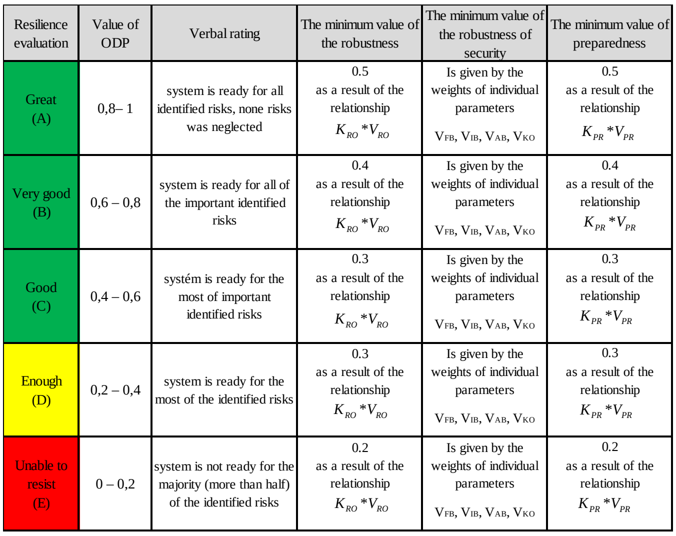


i	Risks	S	P	N	H_{RZi}	Odi
	Energetics					
1	Short-term electricity outage	1	3	1	0.12	0.77
2	Long-term electricity outage	1	2	3	0.24	0.73
3	Outage of water supply	1	3	1	0.12	0.77
4	Outage of gas supply	1	3	2	0.24	0.73
	Natural impacts					
5	Flood	1	2	2	0.16	0.76
6	Prolonged drought	2	3	2	X	X
7	Extreme heat and drought	3	1	0	X	X
8	Thick frost	2	2	0	X	X
9	Pandemic, epidemic	2	2	0	X	X
	Risks associated with the human factor					
10	Conflagration	2	0	0	X	X
11	Explosion	2	0	0	X	X
12	Robbery	1	2	1	0.08	0.78
13	Leaks of pollutants in the area	1	2	3	0.24	0.73
14	Outage in logistics	2	0	0	X	X
15	The virtual attack	1	3	2	0.24	0.73
16	The terrorist attack	1	3	1	0.12	0.77
17	Disruption of public order	2	0	0	X	X
18	Unavailability of staff	1	0	0	0	0.00
19	Sudden rush of patients	1	0	0	0	0.00
20	Technical failures	1	0	0	0	0.00
21	Sabotage	3	0	0	X	X
22	Violent criminal activity	1	3	4	0.48	0.65
23	Acts of vandalism	2	0	0	X	X
24	Plundering	1	3	1	0.12	0.77

ODP	0.59

Figure 12 Final resilience evaluation

Qualitative expression of critical infrastructure element resilience evaluation is represented by:



Resilience evaluation	Value of ODP	Verbal rating	The minimum value of the robustness	The minimum value of the robustness of security	The minimum value of preparedness
Great (A)	0,8– 1	system is ready for all identified risks, none risks was neglected	0.5 as a result of the relationship $K_{RO} *V_{RO}$	Is given by the weights of individual parameters V_{FB}, V_{IB}, V_{AB}, V_{KO}	0.5 as a result of the relationship $K_{PR} *V_{PR}$
Very good (B)	0,6 – 0,8	system is ready for all of the important identified risks	0.4 as a result of the relationship $K_{RO} *V_{RO}$	Is given by the weights of individual parameters V_{FB}, V_{IB}, V_{AB}, V_{KO}	0.4 as a result of the relationship $K_{PR} *V_{PR}$
Good (C)	0,4 – 0,6	systém is ready for the most of important identified risks	0.3 as a result of the relationship $K_{RO} *V_{RO}$	Is given by the weights of individual parameters V_{FB}, V_{IB}, V_{AB}, V_{KO}	0.3 as a result of the relationship $K_{PR} *V_{PR}$
Enough (D)	0,2 – 0,4	system is ready for the most of the identified risks	0.3 as a result of the relationship $K_{RO} *V_{RO}$	Is given by the weights of individual parameters V_{FB}, V_{IB}, V_{AB}, V_{KO}	0.3 as a result of the relationship $K_{PR} *V_{PR}$
Unable to resist (E)	0 – 0,2	system is not ready for the majority (more than half) of the identified risks	0.2 as a result of the relationship $K_{RO} *V_{RO}$	Is given by the weights of individual parameters V_{FB}, V_{IB}, V_{AB}, V_{KO}	0.2 as a result of the relationship $K_{PR} *V_{PR}$

Figure 13 Qualitative expression of resilience evaluation

3 Conclusion

It obvious that for an objective resilience evaluation of the selected critical infrastructure element group or sector is needed the establishment of security standards and requirements which are sectorial specific, assuming their definition and acceptance of a leading governmental authority. Previous text and whole article discuss about software application of mathematical modeling and expression of critical infrastructure element resilience evaluation using simple approach and resilience evaluation methodology application implementation to the excel calculator environment. We know that critical infrastructure resilience evaluation problematic is more complex and difficult but it is necessary to make a first step. This should be seen as a beginning of our future research work.

Acknowledgement

This work was supported by the European Regional Development Fund under the project CEBIA-Tech No. CZ.1.05/2.1.00/03.0089.

References

1. CRN Report, Focal report 6, Risk Analysis, Resilience – trends in Policy and Research, Commisioned by the Federal Office for Civil Protection Zurich, pp.25. April 2011
2. ASME INNOVATIVE TECHNOLOGIES INSTITUTE, LLC, . All-hazard risk and resilience : Prioritizing Critical Infrastructures Using the RAMCAP Plus Approach. 1. New York : ASME, 2009. 155 p. ISBN 978-0-7918-0287-8
3. HROMADA, M., LUKAS L., Conceptual Design of the Resilience Evaluation System of the Critical Infrastructure Elements and Networks in Selected Areas in Czech Republic, The twelfth annual IEEE Conference on Technologies for Homeland Security (HST ’12), will be held 13-15 November 2012 in Greater Boston, Massachusetts. Pp. 353-358, ISBN 978-1-4673-2707-7
4. HROMADA M., Knowledge sharing in the risk analysis proces in energy sector, 3rd EU-US-Canada Expert Meeting on Critical Infrastructure Protection (CIP) May 22nd – 23rd 2012, Brussels
5. HROMADA, M., LUKAS L., The Status and Importance of Robustness in the Process of Critical Infrastructure Resilience Evaluation, The 13th annual IEEE Conference on Technologies for Homeland Security (HST ’13), held 12-14 November 2013 in Greater Boston, Massachusetts. Pp. 589-594, ISBN 978-1-4799-1533-0
6. Vugrin E.G., Warren D.E., Ehlen M.A., Camphouse R.C., A Framework for Assessing the Resilience of Infrastructure and Economic Systems, In: Sustainable and Resilient Critical Infrastructure Systems, 1st Edition, pp. 84-85,April 2010,ISBN 978-3642114045

Testing The Security in Analog Intrusion And Hold-up Alarm Systems

Adam Hanáček, Martin Sysel,

Tomas Bata University in Zlín, Faculty of Applied Informatics, Nad Stráněmi 4511
760 05 Zlín, Czech Republic
{hanacek, adam}@fai.utb.cz

Abstract. The first part of the paper is focused on current situation in the field of intrusion and hold-up alarm systems and on the description of requirementsthat have to be accomplished. The main part of the work deals with testing the security of analog intrusion and hold-up alarm system and necessity to digitalize communication between a control and indicating equipmentand each element. In case of possibility to disconnect the detector without notifying the control and indicating equipment, the lots of objects would be threatened by robbing. In the conclusion, there are discussed the results of the paper and future recommendations.

Keywords: Intrusion alarm system, hold-up alarm system, detector, control and indicating equipment

1 Introduction

The designation “intrusion and hold-up alarm system”(I&HAS) was introduced by the norm named CSN EN 50 131-1 ed 2. in 2010. The main contrast lies in unification of the previous norm CSN EN 50 131 – 1 (intrusion alarm system) and CSN EN 50 131-5 (hold-up alarm system). [1]

The main purpose of an intrusion and hold-up alarm system consists in protection of life, health and properties. The acronym IAS (intrusion alarm system) is used in cases of finding out of intrusion of an intruder into the protected object by the system. The acronym HAS (hold-up alarm system) is used in cases of alarm activation intentionally.[1]

Currently it is prospective to utilize analogs, digitals or wireless control and indicating equipments(CIE)for object security. The digital systems are the most appropriate from the viewpoint of protection against sabotage and interference. Nevertheless, the price of digital systems is approximately five times more expensive than the price of analog systems. The advantage of wireless connection between a CIE and detectors in comparison with wire connection lies in simple installation and higher level of protection against sabotage; however, the main disadvantage lies in highersusceptibility to interference and increased acquisition costs. An analog system is very often used for protection of the object for the lower price of each element.

IAS is applied for protection of family houses, cottages, flats, companies, banks and so on. The main purpose of IAS includes discovering a presence of unauthorized person in secured object and sending an information about intrusion into an object to a mobile phone or to an alarm receiving center. Nowadays, sending alarm message of the object intrusion to mobile phone is the most often used; however, it is necessary to realize an importance of each minute in case of intruding into the object and it is important to check the object as soon as possible.

The work is divided into three parts. The first part describes each element of intrusion and hold up alarm system, the second part describes the testing of whole system. The last part of the work is focused on the results and on possible threatement of objects and subjects in case of using analog intrusion and hold up alarm system.

The main parts of intrusion and hold-up alarm system contains:

- Control and indicating equipment
- Hold-up devices
- Detectors
- Keypad
- Output devices
- Alarm transmission system
- Device for receive an alarm message

Control and indicating equipment

Control and indicating equipment is elemetary component of intrusion and hold-up alarm system. It controls an activity of all components conntected to I&HAS, provides the power for whole system, evaluates signals from keypad, saves an alarm history to a memory, receives an alarm signals and sends an alarm information by using alarm transmission system to predetermined place if the object is disturbed.

The control and indicating equipment of I&HAS is divided on wireless or metalic. The main benefit of wireless connection between a control and indicating equipment and components consists in simpy installation; however, the advantage of metalic connection consists in lower risk of false alarm caused by interference.

Hold-up device

Hold-up device is facility, which is used for inducing an alarm intentionally by activation of public or hiden hold-up device.

The usage of hold-up devices are the most common in banks, where they are used for intentional alarm activation by their employess, caused by treading or pressing of hold-up device.

Detector

Detector is component of intrusion and hold-up alarm system. The main purpose consists in guarding of predefined area and sending an alarm information to thecontrol and indicating equipment in case of disturbing.

Microwave, ultrasound or passive infrared detectors for guarding an area, glassbreaks for detections of broken window and magnetic contacts for detection of openning the door or window are the most often used detectors.

Intrusion alarm keypad - intrusion alarm keypad isused not only for placing in guarding state, but also for programming of whole system.
Alert indication - signalization equipment usually represents optic or sound signalization and its purpose lies in frightenning an intruder and in informing of surrounding area about object´s disruption.
Alarm transmission system - it is possible to transmit an alarm messages from the secured object to alarm receiving center or to mobile phone by alarm transmission system.
Other used terms
False alarm-an alarm caused by defect of electronic componentsor by otherfailureof the detector. [2]
Digital communicator- a part ofthe alarm system,whichforms an outputinterface for transmittingmessages betweenI&HASand alarmtransmission network. [3]
Periodiccommunication -"Periodic" means, that at leastone reportshould has been realised in predefined interval to ensure, thatcommunication works. [4]
Expander- an electronic equipmentused toextend the functionality ofI&HAS. [5]
Interconnection- resources, that help messagesor signals with transmission between componentsI&HAS. [6]
Subsystem –a part of an I&HAS located in a clearly defined part of the supervised premises capable of independent operation. [7]
Zone - assessed area where abnormal conditions may be detected.[8]

2Testing of Analog Intrusion and Hold-up Alarm Systems

This chapter describes the procedure of testing if it ispossible to disconnect thedetector without noticing by the control and indicating equipment. All testingis basedon the fact,that eachcontrol and indicating equipment has to have a timeinterval,during whichthe resistance changeis notrecorded. Nevertheless, acording to thestandards this time interval cannotexceed 400ms. The next condition, which has to be fulfilled, is that the tolerance of closed resistor is between 20-35%.

2.1 Connection of Analog Control and Indicating Equipment to Each Component

Connection of each part to control and indicating equipment is shown in figure 1. Each analog security system has 6, 8, 16 or 32 analog zones and each detector is connected to a zone using a circuit, which has to be closed by terminating resistor to provide protection against sabotage.

The principle of analog I&HAS consists in measuring the resistance of each circuit. Each detector has one alarm contact and one tamper contact connected to the circuit.

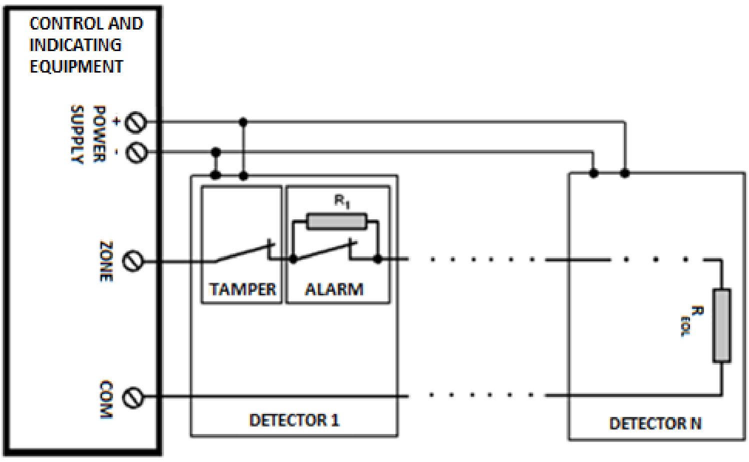


Fig. 1.Connecting of analog detectors to the I&HAS

2.2 Measuring of theVoltage on theTerminating ResistorandConnecting ofa Voltmeter

Firstlyit is necessary toinsulatethe conductor onrelevantcircuit.

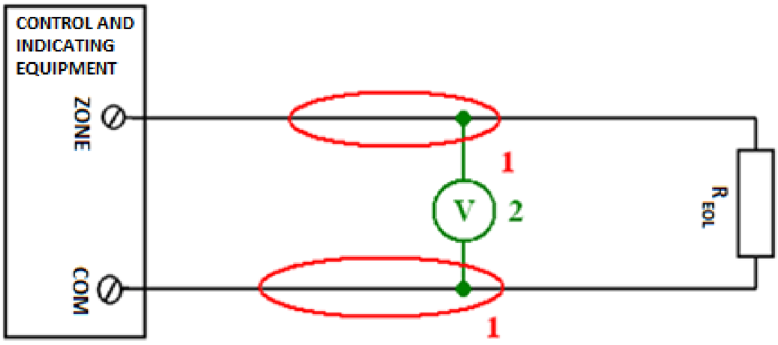


Fig. 2. The area where it is necessary to insulate a conductor

Connecting of a voltmeter shown in figure2 is identified by green color and thenumber2. There is pictured a parallel connection of a voltmeter for determining a voltage on theclosed resistor.The most frequently usedvalue ofthe closed resistoris1 kΩ. But there also exist control and indicating equipments, that they are possible to change their ready state to 1100 Ω, 2200 Ω, 4700 Ω or 5600 Ω.

2.3 Ammeter Connecting

Ammeter connecting is shown by light green color and by number 3 in figure 3. The ammeterisconnected to a switchto the circuit between nodes“A” and “D”.

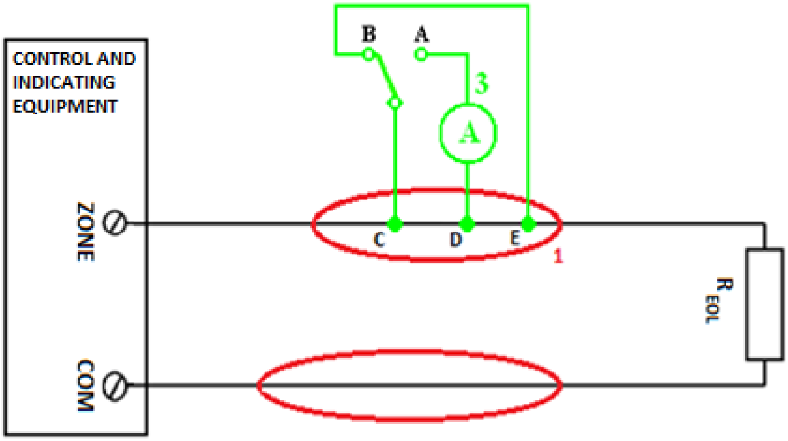


Fig. 3. Ammeter connecting 1

The next step of connecting an ammeter to the circuit consists in disconnecting the conductor between nodes “C” and “D”. Further, it is necessary to put the switch to position “A”. The situation is pictured in figure 4. Once the switch is set to position “A”, the ammeter displays the value of current, which flows through the resistor. Further, it is necessary to disconnect the conductor between nodes “B” and “E”.

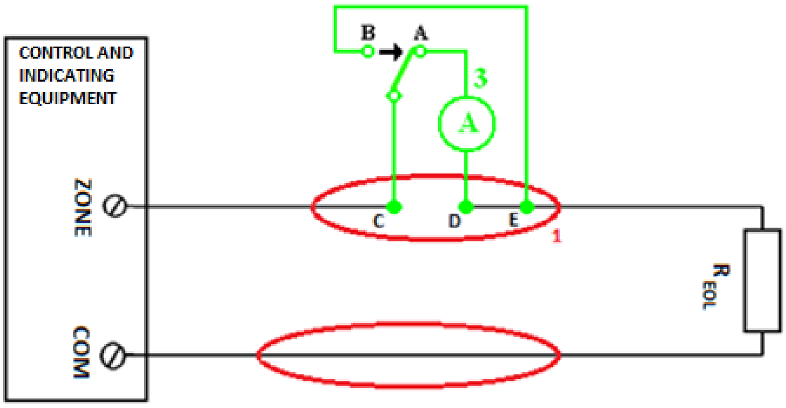


Fig. 4. Ammeter connecting 2

2.3 Closed Resistor Connecting

Purplecolorin figure5 showsthe resistor “R_A“ connected to the nodes“B”and“E”, which replaces the closed resistor. The value of the resistor “R_A“ was calculated from the current and voltage values, that were measured in the previous points.

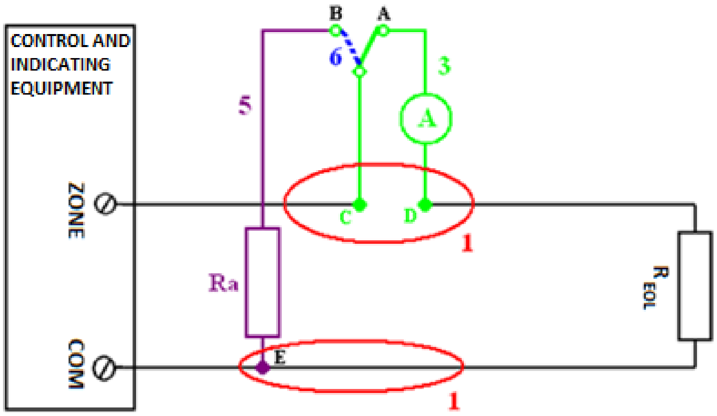


Fig. 5. Closed resistor connecting

2.4 Changing the Switch to Position “B”

Changing the switch to position “B” is pictured by blue color and the number 6 in the figure 5. This change causes, that the current doesn´t flow through the closed resistor anymore, but flow through the resistor “R_A”. Switching has to be fast to the CIE doesn´t note this short interruption. After this switching the CIE will not respond to any change in detector´s connected to the circuit.

2.5 Process of Testing and Summary of Results

All testing was realized on the CIE named DSC 6000. The detector was connected to the circuit via connection described in the previous chapter. The equipment used for testing are control and indicating equipmentnamed DSC 6000, keypads, voltmeter, ammeter, switch, detectors, conductors and resistors.

The procedurewas applied10 times, while the CIEdid not noticedisconnection of the detector 8 times. Procedure success is equal 80%. However, for testing was used ordinary switch. It ispossible to usemore suitableswitches, for which the switching takes less time. This way it could be possible to increase the efficiency of described procedure. The procedure, which enables the disconnection of the detector without noting by the CIE, is effective if an intruder gains access to the circuit. However, according to the standards the connection between the CIEand detectors doesn´t has to be protected against a sabotage and also doesn´t has to be placed in the armed zone. This situation can cause a threat of many objects. In practice, the analog detectors are used for security of cottages, garages, houses, flats, etc. Thus we are discussing about security of level 1, 2 and 3. According to the standards there is a duty to notice a delay, modification, replacement or loss of signals or messages only in security level 4. Therefore, there shouldn´t be used analog control and indicating equipments in security level 4.

3Conclusion

The whole workwas focused on theprotection of analog control and indicating equipments against sabotage and on the need of digitalization of data transfer between the control and indicating equipment and detectors.

Presented resultsdescribed in the chapter "Process of Testing and Summary of Results" shows that it is possible to disconnect the detector of analog intrusion and hold-up alarm system without noticing by the control and indicating equipment. This fact enables to trick the security devices and gain the access to a secured object without any knowledge of security code. But the burglary also depends on knowledge of circuits that connect the control and indicating equipmentwith detectors and on finding a way, how to get to these circuits. Due to the fact that the connection between components don´t have to be in secured zone, the possibility mentioned above can happen easily. Currently, analog control and indicating equipmentsbelong to the most often used, because of the low price of their parts and of their good interference immunity; however, the analog systems cannot be recommended for building security. In the fieldof analogintrusion and hold-up alarm systems there would be appropriate to digitize the transfer minimally between analog elements or utilize already used digital systems despite their higher acquisition costs.

Acknowledgments. This work was supported by grant No. IGA/FAI/2014/020 from IGA (Internal Grant Agency) of Thomas Bata University in Zlin.

References

1. ČSN. *EN 50131-1 ed. 2*. Praha: Úřad pro technickou normalizaci, 2007, 40 s.

2. ČSN. *EN 50131-7*. Praha: Úřad pro technickou normalizaci, 2010, 48 s.
3. ČSN. *EN 50131-1 ed. 2*: *ZMĚNA A1*. Praha: Úřad pro technickou normalizaci, 2010, 12 s.

4. ČSN. *EN 50131-1 ed. 2*: *ZMĚNA Z2*. Praha: Úřad pro technickou normalizaci, 2011,
20 s.
5. HORNÍK, Jan. *Model zabezpečení inteligentního domu*. Praha, 2010. Bakalářská. ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ.
6. KINDL, Ing. Jiří. *Projektování bezpečnostních systémů*. Zlín, 2007. ISBN 978-80-7318-554-1. Učební text vysokých škol. Univerzita Tomáše Bati.
7. ČERNÝ, JUDr. Josef a Ing. Ján IVANKA. *Systemizace bezpečnostního průmyslu I*. Zlín, 2006. ISBN 80-7318-402-8. Učební text vysokých škol. Univerzita Tomáše Bati.
8. EN 50131-1. *Alarm systems - Intrusion and hold-up systems*. Brussels: rue de Stassart 35, 2006.

Security Risks of Java Applets in Remote Experimentation and Available Alternatives

Petra Špiláková[1], Roman Jašek[1] and František Schauer[1, 2],

[1] Tomas Bata University in Zlín, Faculty of Applied Informatics, Nad Stráněmi 4511,
760 05 Zlín, Czech Republic
[2] Trnava University in Trnava, Faculty of Education, Priemyselná 4,
P. O. Box 9, 918 43 Trnava, Slovak Republic

Abstract. Java is a widely used multiplatform programming language, which we used to create ISES (Internet School Experimental system) control software of remote experiments spread across the Internet. However recently, due to the security constraints, we have been forced to change our original concept with the main goal is to find the suitable substitute for Java applets in controlling ISES remote experiments. The contribution describes the Java security model and its holes, which can be abused by the hackers´attacks. In finding a suitable choice we pay attention to the programming languages such as JavaScript, ActiveX and Dart, their comparison and selection of the best alternative.

Keywords: ActiveX, Dart, Java applet, Java security, JavaScript, ISES remote laboratory, Security holes.

1 Introduction

In this article we deal with the safety issues of Java applets and alternatives to replacing them. This issue directly affects us because in our Internet School Experimental system (ISES) remote laboratories, where Java applets have been used for remote control of ISES experiments. In 2002, when the first remote experiment "*Water level control*", was designed, and made available on the page http://kdt-14.karlov.mff.cuni.cz/en/mereni.html, the most appropriate method of the transformation from laboratory experiments to real remote experiments, Java applets were used. It was then the best solution for the authors of the ISES remote experiments (RE) [1], [2], [3] because Java applets recorded in these years its biggest boom with the brightest prospects for the future.

Unfortunately due to the security threats that are currently occurring on the Internet, it is not possible to continue along Java lines. The situation requires Java applets to be replaced by other approaches. Therefore, we started to analyze various replacement alternatives how to renew controlling programs for the ISES experiments in the most appropriate manner so as to preserve its functionality and to avoid security hindrances.

The days when the Local Area Network (LAN) was the most widely used are behind us. Now, most Local Networks have been connected directly to the Internet, which means the security issue is more important than ever before. We need to try to protect our data with advanced security mechanisms such as firewalls, secure shells, virtual private networks and a lot of other means, discussed later in this article. Connecting computers together in a network allows computer users to share devices, files, data, programs, and each others' computational resources. In most cases pages are not only purely static but contain a lot of dynamic content that extend their functionality and design. On the creation of dynamic content and Internet communication many toolsare used, among others, JavaScript, PHP, CSS styles, and of course Java. Thanks to the development of information and communication technology (ICT) and many others the number of users connected to the Internet is growing at an increasing rate every year. Along with these abilities and large numbers of connected computers it comes to the question about computer security.

2 Java Language

This chapter introduces the language Java with the main attention paid to its security policy.

There has been a lasting a problem of writing cross-platform applications. As a result, the platform independent programming language Java, its first public version was introduced at the SunWorld conference in 1995which was later in 2010 bought by Oracle Corporation [4].Java works on the general principle that the majority of the code is automatically downloaded from the network and runs on your computer. Java can be run on a computer that has a Java Virtual Machine (JVM) installed. Because Java byte code runs on the Java Virtual Machine, it is possible to run Java code on any platform [4]. The Oracle Corporation provides on its website the following describe of the Java programming language: Java is a high-level language. It is simple, object oriented, distributed (your system can directly interact with an object in the remote host), multithreaded, dynamic, architecture neutral, portable, high performance, robust secure [5].

Java can be used to create two different kinds of programs, which are applications and applets, the main differences are that the applet needs to run under the control of a browser, whereas the application runs stand-alone, with the support of the virtual machine . Next, let us discuss the Java applets from the point of security view.

3 Java Applets

Let us have first a definition of the Java applet, as it is defined on Oracle website [5]. “The Java applet is a special kind of Java program that a browser enabled with Java technology can download from the internet and run. The applet is typically embedded inside a web page and runs in the context of a browser. The applet must be a subclass of the *java.applet.Applet* class. The *Applet* class provides the standard interface between the applet and the browser environment. “ There are two main types of applets either sandbox applets (unsigned) or privileged applets (signed). Sandbox, applets which are considered untrusted are run in a security sandbox. Privileged applets can either run in the sandbox, or can request permission to run outside the security sandbox and have extensive capabilities to access the client. Applets loaded over the network are usually considered to be untrusted code whereas local applets are considered to be more trustworthy. Implementing the security restrictions is the responsibility of the *java.lang.SecurityManager* class about which will be discussed below [5], [4].

3.2 Parts of the Sandbox Model

The default sandbox consists of three interrelated parts: *Verifier*, *Class Loader*, and *Security Manager*. These parts must work perfectly because if any of the three parts crashes, the whole security system crashes, leaving the door wide open for attack.

The Security Manager depends on Class Loaders to correctly label code as trusted or untrusted. Class Loaders also shield the Security Manager from spoofing attacks by protecting local trusted classes making up the Java API. On the other hand, the class loader system is protected by the Security Manager, which ensures that an applet cannot create and use its own Class Loader. The Verifier protects both the Class Loaders and the Security Manager against language-based attacks meant to break the VM. All in all, the three parts intertwine to create a default sandbox.

The Java security model was subsequently extended to include more parts in new versions of the Java. First came the *java.security* package later came *Access Controller*, *Code Source* etc. [4].

The Verifier

As we said from the beginning the Java is cross-platform language through the use of bytecode. Java bytecode is verified before it can run. The Verifier provides a first part of defense against malicious codes that could be dangerous to users. This verification scheme is meant to ensure that the byte code, which may or may not have been created by a Java compiler, plays by the rules.

Thus, class files which contain bytecode are verified, Java automatically examines untrusted code before it is allowed to run. If the Verifier finds any problem with a class file, it throws an exception and the class file never executes.

The process of the verifying is divided into two major steps: internal checks that check everything that can be checked by looking only at the class file itself and runtime checks that confirm the existence and compatibility of symbolically referenced classes, fields, and methods.

The validated bytecode satisfies conditions that the class file has the correct format and proper length; stacks will not be overflowed or underflowed; bytecode instructions all have parameters of the correct type; no illegal data conversions occur; private, public, protected, and default accesses are legal; and that all register accesses and stores are valid [4].

As it is known, the length of time which it takes for a launch of the Java applet is no too short. Many people are thinking falsely that it is caused by downloading the applet from the internet to user's computer. In this time a connection to the Internet is reasonably fast so the part that takes the longest time is verifying code.

The Class Loader

The Class Loader is used to load the Java code from the network. Class loaders perform two functions. First, class loader finds the bytecode which VM needs to load for a particular class of the applet and it undergoes to the bytecode control by the Verifier. Second, class loader defines the namespaces seen by different classes and how those namespaces relate to each other. Problems with namespace management have led to a number of serious security holes. The Applet Class Loader is the most important part of the Java security model [4].

The Security Manager

The third part of the base Java security model is the Security Manager. The job of the Security Manager is to keep track of who is allowed to do which dangerous operations. A standard Security Manager will disallow most operations when they are requested by untrusted code, and will allow trusted code to do whatever it wants.

The Security Manager is a single Java object that performs runtime checks on dangerous methods. The Security Manager can veto the operation by generating a SecurityException. It makes the final decision as to whether a particular operation is permitted or rejected. When a dangerous call is made to the Java library, the library queries the Security Manager. These queries use a set of methods that check access. The Security Manager is installed in each JVM only once.

Responsibilities of the Security Manager are that it prevents installation of new class loaders; it protects threads and thread groups from each other; it controls the execution of other application programs; it controls the ability to shut down the VM; it controls access to other application processes; it controls access to system resources such as print queues, clipboards, event queues, system properties, and windows; it controls file system operations such as read, write, and delete; it controls network socket operations such as connect and accept; it controls access to Java packages, including access to security enforcement classes [6].

The CodeSource

The CodeSource encapsulates the code's origin, which is specified as an URL, and the set of digital certificates containing public keys corresponding to the set of private keys used to sign the code.

The AccessController

The java.security.AccessController class is used for deciding whether access to a critical system resource should be allowed or denied, based on the security policy currently in effect; for marking code as privileged, thus affecting subsequent access determinations; for obtaining a snapshot of the current calling context, so access-control decisions from a different context can be made with respect to the saved context.

3.3 Types of security attacks

Java applets can be subjected to potential hacker attacks. Now follows a brief description of four of many possible attacks, namely - attacks that deny legitimate use of the machine by hogging resources, - attacks that modify the system, - attacks that invade a user's privacy, - attacks that antagonize a user and attacks called Zero-day attacks [7].

Denial of Service Attacks

A Denial of Service Attack abbreviated DoS attack, is an attempt to make interrupt or suspend services of a host connected to the Internet.

The DoS attack belongs to less seriously attacks because this attack consumes only system resources and can slow your computer or your network connection considerably. For example, attacks may involve completely filling a file system, hogging all possible screen space, allocating all of a system's memory, creating many high-priority threads, or using all available file pointers [6].

The Java sandbox does not protect against DoS attacks. Therefore, we should not allow applets which come from suspects and unverified sources [4].

System Modification

This type of attack is the most severe class of attacks. It is able to intrusion into the system itself and consequences of these attacks can be critical and dangerous. Applets that implement such attacks are attack applets.

System modification attacks may modify the contents of memory, create, modify, or delete files, directories, database entries, kill processes or threads and install malware as is trojan horse, worm, back door and many more to the user computer.

Invasion of Privacy

This type of the attack includes disclosing information about a user or host machine that should not be published. The forging mail can also be perceived as an attack to privacy. Especially if we value our privacy or we have some confidential files on the computer, this attack may be a very annoying issue.

Antagonism

The most commonly we encounter with this type of attack. There are attacks that merely antagonize or annoy a user. For instance, antagonism applets are able to play unwanted sound files, open a large number of new windows simultaneously, etc.

Zero-day attacks

Zero-day vulnerabilities in computer science marking attack or threat that tries to exploit computer vulnerabilities, refer to a hole in the software that is unknown to the vendor. This security hole is then exploited by hackers. Zero-day here does not indicate the number or the number of days, but the fact that the user is at risk, until a patch is still in the works to fix bugs (ie, the zero day).

Let's now look at specific examples of security attacks. Attacks are listed chronologically by date of publication.

Targeted attacks to chemical companies, named *The Nitro Attacks,* started in **July 2011** and continued into September 2011. The 29 companies in the chemical sector and another 19 in various other sectors, primarily the defense sector were affected by this attack.The attackers first researched desired targets then sent two types of mail. If the mail was targeted to a specific recipient it contained invitation to meeting. Or if the mail was being sent to a broad set of recipients the email claims to be an update for some piece of commonly installed software. In both cases the mail contained attachment with a malicious Trojan called PoisonIvy which was included in a zipped file with the password. The PoisonIvy allowed access to other computers in the company workgroup. They could copy the content, and upload the information to servers external to the compromised organization. The purpose of the attacks was likely industrial espionage, and the attackers appear to have been seeking intellectual property, including design documents, formulas, and manufacturing processes, for competitive advantage. The source of the attack was identified as a computer system that was a virtual private server (VPS) located in the United States. The system was owned by an individual named Covert Grove from China [8].

An indisputable advantage of the Java language is a cross-platform but this can easily be exploited to an attack as a good example is following Java applet malware. In **April, 2012** the infection volume is reported at over 600,000 computers with Mac and Windows operating systems. This threat proceeds in three phases. First, Java Applet malware is loaded. Second, if the threat is running on a Mac operating system, it downloads a dropper type malware written in Python. Or if the threat is running on a Windows operating system, it downloads a standard Windows executable file dropper. This Trojan only checks whether it is the required operating system. Finally, one of two back door Trojans depending in OS is dropped on to the computer. These Trojans can download files, open a remote shell, upload files, send informations about CPU details, disk details, memory usage, etc. [9].

July, 2013 Symantec published a campaign is targeting government agencies by sending phishing emails with a malicious attachment in the form of the Java remote access Trojan (RAT). Cyber criminals use recent hot media topics to entice users. In this case they used the news coverage surrounding the NSA surveillance program PRISM. The phishing email contains two legitimate non-malicious PDF documents and one Java file named US National Security State. The most of targets were located in the United States [10].

July, 2013: The target of the attack could also be the SIM card (Subscriber Identification Module) which is present in all mobile phones. Every smart card is responsible for the unique identification number known as the IMSI (International Mobile Subscriber Identity) and also for handling the encryption when communicating with the telephone network. If an attacker send a cleverly crafted silent binary SMS update message over-the-air (OTA) to the mobile phone although the device will refuse the unsigned message but it will answer with an error code signed with the 56-bit DES private key. After the private key is deciphered, an attacker can sign malicious software updates and send them through OTA updates to the mobile phone. For instance, malicious applets can send premium text messages, reveal the geo-location of the device or misuse of payment systems [11].

November, 2013 Symantec has discovered a new back door worm-type threat which targets servers running Apache Tomcat. The Apache Tomcat is an open source web server and servlet container developed by the Apache Software Foundation (ASF) and based on Java language. Servers are quite valuable targets, since they are usually high-performance computers. Back door type Trojan horses and worms enable the attacker to control a computer remotely. Infected computers could be used to attack other Tomcat servers by sending the malware to them and this would lead to DoS attacks [12].

In early **January 2014**, on a website of a major Japanese book publisher and distributor, of books, magazines, comics, movies, and games was encountered a malicious iframe leading to another website hosting an exploit kit. This malware is intended for the purpose of stealing information and located in Japan. The malware monitors open windows for two online banking sites, three online shopping sites, three Web mail sites, three gaming/video websites and fourteen credit card sites. Most providers of these sites are aware of the security risks and have implemented additional layers of protection and verification for their online customers. It is not surprising that contested pages belonged to regional firms that had not done sufficient safety measures [13].

February, 2014 a new spam campaign appeared in the form of the Java remote access Trojan (RAT) known as JRAT. The spam email's sender claims that they have attached a payment certificate to the message and asks the user to confirm that they have received it. An attachment with the file name Paymentcert.jar was actually a malicious Trojan virus. The Windows, Linux, Mac OS X and Solaris computers are threatened by RAT. This attack affected the most individuals in the United Arab Emirates and the United Kingdom [14].

The incidence of vulnerabilities

As mentioned Java programs run in the sandbox which is responsible for a security. Since Java is so widespread is not surprising that there are constantly incidence of security breaches and are used to hacker attacks. Therefore, the Oracle is continuously working on improving its product. The Critical Patch Updates (CPU) are published on their web every 3 months starting from January. Exceptions are updates that needed to be done immediately, given the severity of the security risk. In addition the CPU are published on the website the Common Vulnerabilities and Exposures (CVE). Common Vulnerabilities and Exposures is a dictionary of common names for publicly known information security vulnerabilities. CVE includes just one vulnerability and makes it easier to share data across separate network security databases and tools, but where CPU can contain multiple CVE.

In the figure 1 can be seen the bar graph of the number of vulnerabilities (Security Alert, Critical Patch Update Advisory or Security Alert) by year, based on data mentioned by Oracle. The graf includes data to the April 18, 2014 [15], [16].

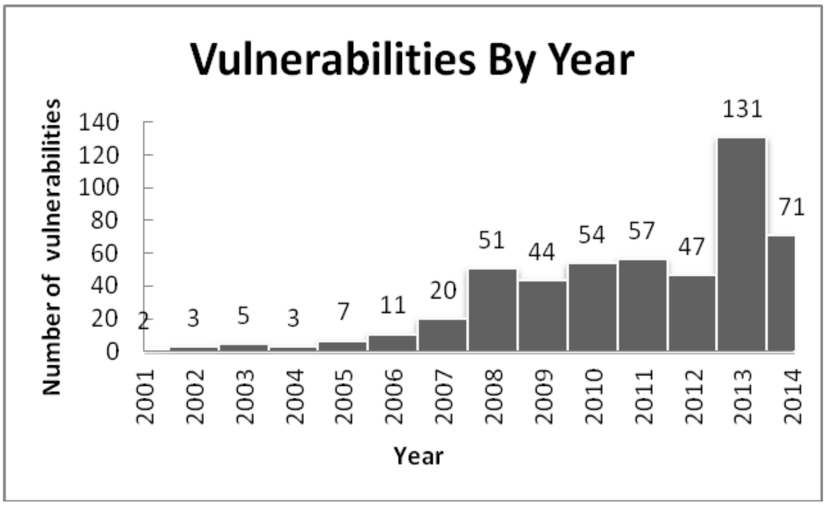


Fig. 1. Graph of the number of vulnerabilities by year [15]

It can be seen that with increasing numbers of users and extension of the Java is also an increasing number of security vulnerabilities discovered because hacker attacks occur more frequently.

4 Alternatives for Security Improvement

Next, let us analyze alternatives of programming environments with whome it is possible to replace control Java applets of experiments.

4.1 JavaScript Language

JavaScript was developed by Brendan Eich while working for Netscape Communications Corporation. It was first introduced in 1995 under the name of LiveScript. However, due to marketing purposes it was renamed JavaScript. JavaScript’s official name is ECMAScript, which is developed and maintained by theECMA (European Computer Manufacturer's Association) International organization. Today, JavaScript is a trademark of Oracle Corporation.

JavaScript (JS) is scripting dynamic and object-oriented language designed primarily for adding interactivity to Web pages and creating Web applications.

A common misconception is that JavaScript is similar or closely related to Java. There are few similarities between Java and JavaScript. For instance, both have a C-like syntax. They are both object-oriented and typically sandboxed. Also, JavaScript was designed with Java's syntax and standard library in mind. JavaScript's standard library follows Java's naming conventions, and JavaScript's Math and Date objects are based on classes from Java 1.0, but similarities end there.

Key differences between Java and JavaScript:

- Java is an OOP programming language while JavaScript is an OOP scripting language.
- Java creates applications that run in a virtual machine or browser while JavaScript code is run on a browser only.
- Java code needs to be compiled while JavaScript code are all in text.
- Java is loaded from compiled bytecode; JavaScript is loaded as human-readable source code.
- They require different plug-ins.
- Java has an implicit this scope for non-static methods, and implicit class scope; JavaScript has implicit global scope.
- Java has static typing; JavaScript's typing is dynamic. In dynamic typing, a variable can hold an object of any type and cannot be restricted [17].

JavaScript **can** perform the following operations:

- It has access to the computer's clock and can pull the appropriate data.
- It can collect information about the browser.
- It can be used to validate forms data or input.
- It can create cookies.

- It can manipulate the Document Object Model (DOM) where the HTML DOM is the official W3C standard for accessing HTML elements.
- It can create various dynamic HTML elements, such as it can interactive change all the HTML elements, all the HTML attributes, CSS styles, can remove, add new HTML elements and attributes, can react to all existing HTML events and can create new HTML events in the page.

JavaScript **cannot** perform the following operations:

- It cannot write to files on the server without the help of a server side script. JavaScript can send a request which can read a file but it cannot write to a file unless the file called on the server actually runs as a script to do the file write for you.
- It cannot access databases unless you use Ajax and have a server side script perform the database accesses for you.
- It cannot read from or write to files in the client. The only exception to this are cookies.
- It cannot close a window if it didn't open it.
- It cannot access web pages hosted on another domain.
- JavaScript cannot protect your page source [17].

JavaScript is among the top ten most popular and most widely used programming languages in the world. According to the TIOBE index JavaScript is placed in the ninth place in front of it are placed languages in the following order C, Java, Objective-C, C++, C#, (Visual) Basic, PHP, Python.

The TIOBE Programming Community index is an indicator of the popularity of programming languages. The ratings are based on the number of skilled engineers world-wide, courses and third party vendors. Popular search engines such as Google, Bing, Yahoo!, Wikipedia, Amazon, YouTube and Baidu are used to calculate the ratings [18].

The unquestionable advantages of JavaScript are that JavaScript code can be run on the web, on computers, servers, laptops, tablets, smart phones, and more, Javascript is a relatively easy language and simple to learn, JavaScript is very fast because any code functions can be run immediately instead of having to contact the server and wait for an answer. JavaScript runs on an Internet browser therefore the users do not need special software or downloads to view it.

Disadvantages include security issues as with all programming languages. JavaScript, providing a high degree of functionality at the expense of security. JavaScript can easily be used to carry out denial of service and invasion of privacy attacks. For instance JS can track a surfer's history, secretly keeping tabs on all sites visited by a user and reporting back to a collection site, read directory listings, learning about a Web surfer's file system and reporting back to a collection site, steal files, mailing the stolen goods back to an attacker, etc. [4].

4.2 Dart Language

Dart is an open-source Web programming language which was developed by Lars Bak and Kasper Lund who work in the Google. It was first introduced in October

2011 at the GOTO conference in Aarhus. Dart is a class-based, single inheritance, object-oriented language with C-style syntax.

Dart was developed to eventually replace JavaScript. Until then, in order to run in mainstream browsers, Dart code is compiled into JavaScript using the dart2js compiler. This resulting code is compatible with all major browsers with no specific browser adoption of Dart being required. Code written in Dart can, in some cases, run faster than equivalent code hand-written using JavaScript. Dart code can be run without compilation to JavaScript if we use the Chromium web browser that includes the Dart VM, called Dartium. Dartium is intended as a development tool for Dart applications and it should not be used as a primary browser.

In order to completely replace the JavaScript it is necessary that Dart virtual machine placed in browsers. But now creators of the Dart encounter with criticism and negative feedback. In any case, it is only a matter of time before a Dart finds its place among programming languages. As is known Google is among one of the largest corporations which its products constantly improves and develops. Thus Dart has great potential for the future [19].

4.3 ActiveX Environment

An ActiveX is not a programming language it is a set of technologies and tools for Internet Explorer developed by Microsoft in 1996. It is based on two earlier Microsoft technologies called Component Object Model (COM) and Object Linking and Embedding (OLE).

An ActiveX control is a small program similar to a Java applet. It can be created in any programming language that recognizes Microsoft's Component Object Model such as C, C++, Visual Basic, Java and more. ActiveX control is a control using Microsoft ActiveX technologies which are commonly used in Windows operating system.

The ActiveX approach relies on digital signatures, ActiveX controls can be digitally signed by a developer, distributor, certifier or someone who vouches for the code. ActiveX controls have almost unlimited access to the operating system. With this function comes a certain risk that it may damage software or data on your computer.

Because there was a large amount of harmful ActiveX controls, Internet Explorer version 7 and above displays a warning every time a site attempts to use an ActiveX control. It is up to the user to decide whether or not the request comes from a trustworthy source. Either you trust the code completely and allow it to run unhampered on your computer, or you don't.

Compared with Java applets, ActiveX control has two main disadvantages. First, Java has the ability to run untrusted code fairly safely due the sandbox. Second, Java applets can be run on all platforms, whereas ActiveX controls are a priority limited to Windows environments. Web browsers like Google Chrome, Safari and Firefox do not support ActiveX controls by default due to security concerns. Users of these browsers can download extensions through which ActiveX will be run. But there are not extensions for all environments [20], [21].

5 Discussion and Conclusions

In this paper, we deal with the security issues, namely security of Java applets and options for their replacement by other tools. We may conclude that each of the aforementioned languages have their advantages and weakneses. Some are more appropriate for our purposes than others. Due to the security measures of Java applets, which the Oracle Corporation develops, the formation of the control web page of remote experiments is very limiting for us. The user is also constantly harassed by the authorization to run of applets and by the reinstalling the JVM on his/her computer. With each new release of Java, a number of new serious security holes have been discovered. Every new features introduce new security holes. Consecutively, we decided to abandon the concept of making experiments using the Java, and we were looking for new acceptable alternatives. We reviewed some programming languages and we take into consideration their functionality, limitations, simplicity, and main assumptions of the usability today and in future too. Since remote experiments are made available through the website to users, we focused on languages that can create elements which are executable on web browsers. The user is not exposed to a duty to install any hardware and code is running under different operating systems.

As was mentioned earlier Dart has great potential but is yet at an early stage when it slowly gets into the consciousness of programmers and the general public. Dart programming language, we have not opted for our purposes solely because it is relatively new language, and if there were any problems it would not be easy to solve because there are still scarce professional resources. And also we did not want to risk the possibility that it completely disappeared.

ActiveX is not suitable for our purpose because it is dependent on the platform used and we want to avoid platform dependency. Our aim is to create website for remote controlled experiments that will be user friendly, accessible, and making no demands on the software. Thereby ActiveX can be excluded.

We may formulate following conclusions:

- to abandon the concept of making experiments using the Java, and we were looking for new acceptable alternatives for our ISES RE.
- The optimal solution seems to be the JavaScript. It needs less programming skills and it enables easy implementation to the web page of the experiment.
- JavaScript widgets are the most often offered on the Net as completely functioning items, which can be simply grabbed from the web and be used for your purposes. It has been In use already a couple of decades and it looks like it will be for a long time.
- Use of JS is advantageous over Java applets in that it is much easier and more robust language, it can also be run on mobile phones, tablets, etc.
- JavaScript code is running faster than Java code because it does not need much time for compiling and security checking.
- JavaScript code is also much smaller than the corresponding bytecode file.

Acknowledgments. The paper was published thanks to the Grant of the Internal Agency of UTB No IGA/FAI/2014/034. One of us acknowledges the partial support of the Slovak Research and Development Agency, project no. APVV-0096-11, the

Scientific Grant Agency VEGA, project no. 2/0157/12, and the KEGA Agency projects No 011TTU-4/2012 and 020TTU-4/2013.

References

1. Schauer, F., Lustig, F., Dvořák, J., Ožvoldová, M.: Easy to build remote laboratory with data transfer using ISES—Internet School Experimental System. In: European Journal of Physics, 2008, vol. 29, pp. 753--765, ISBN 978-0-9741252-9-9.
2. Lustig, F.:Jak si jednoduše postavit vzdálenou laboratoř na internet (How to simply build a remote laboratory on the Internet). In: Veletrh nápadů učitelů fyziky (Exchange idea shop of Physics teachers), pp. 9 -- 19. Brno (2004)
3. Schauer, F., Ožvoldová, M., Lustig, F.: Integrated e-learning - new strategy of the cognition of real world in teaching. In: World Innovations in Engineering Education and Research iNEER. pp. 119—135. USA (2009)
4. McGraw, G., Felten, E.:Securing JAVA – Getting down to business with mobile code. John Wiley & Sons, Inc. (1999)
5. Oracle Corporation, http://docs.oracle.com/
6. Flanagan, D.: Java in a Nutshell. 2nd Edition, pp. 628, (1997)
7. Gerža, M., Schauer, F., Jašek, R.: Security of ISES Measureserver® Module for Remote Experiments against Malign Attacks. In: International Journal of Online Engineering (iJOE). Vol 10, No 3. pp. 4-10. (2014)
8. Chien, E., O'Gorman, G.: The Nitro Attacks - Stealing Secrets from the Chemical Industry. Technical report (2011)
9. Katsuki, T.: Both Mac and Windows are Targeted at Once. Symantec Corporation, Official Blog (2012)
10. Lelli, A.: Rise of the Java Remote Access Tools. Symantec Corporation, Official Blog (2014)
11. Wueest, C.: Hijacking SIM Cards through Over-the-Air Updates. Symantec Corporation, Official Blog (2013)
12. Katsuki, T.: All Your Tomcat Are Belong to Bad Guys? Symantec Corporation, Official Blog (2013)
13. Symantec Security Response: Popular Japanese Publisher's Website led to Gongda Exploit Kit. Symantec Corporation, Official Blog (2014)
14. Payet, L.: JRAT Targets UK and UAE in Payment Certificates Spam Campaign. Symantec Corporation, Official Blog (2014)
15. Oracle Corporation, Official website, http://www.oracle.com/technetwork/topics/security/whatsnew/index.html
16. Oracle Corporation, Official Java website, https://www.java.com
17. Chapman, S.: What Javascript Can Not Do. http://javascript.about.com/
18. TIOBE Company: TIOBE Index for June 2014. http://www.tiobe.com/index.php/content/paperinfo/tpci/index.html
19. Dart.https://www.dartlang.org/
20. Roos, D.: How ActiveX for Animation Works. http://entertainment.howstuffworks.com/activex-for-animation1.htm
21. Microsoft, Protect yourself when you use ActiveX controls. Official webpage, http://www.microsoft.com/security/default.aspx

Laboratory Robotic Systems for the Security Industry

Petr Navrátil[1,], Ján Ivanka[1]

[1] Tomas Bata University in Zlin, Faculty of Applied Informatics, Nám. T.G.Masaryka 5555,
760 01 Zlin, Czech Republic
{ivanka, p1navratil}@fai.utb.cz

Abstract. The article deals with the use of service robots in the security industry. The required service activities of such service robots in this area should meet are defined and examples of two specific laboratory mobile robots that may find use in this field are shown. The description of the design, assembly of these mobile robotic systems and the software development of supporting algorithms, enable leading mobile robot kit for its own trajectory is also included.

Keywords: Mobile service robot, wi-fi, Bluetooth, Arduino, servomotor, security industry.

1 Introduction

Recent trends of world development in the field of service robots show the considerably wide spectrum of possibilities of service robots application. Currently, there is a constant increase in service robots used in the area of security. The main reason for the application of robotic systems (service robots) for the security services is to reduce risks and potential losses, threatening the implementation of the activities and procedures associated with these services [1].

Robotic systems are technically capable and sufficiently technically equipped to enable them to get to the places and spaces that might be inaccessible to humans and dangerous in terms of the threat to life and health or human could not control by their abilities (the influence of environmental factors).

Application area of the robotic system is given by the required service activities. In the case of security services is all about guarding a building, survey and inspection, monitoring crowd spills of dangerous substances, environment mapping. Activities related to security are associated with the occurrence of risks. These include the risks associated with the performance of routine inspection procedures specified objects (vehicles, passengers, material objects, etc.), the action to be taken against the identified objects, the processes associated with the monitoring of specific areas and objects [2, 3].

Robotic systems represent specific solutions for the requirements of the security industry. Considering the range of possible tasks that can perform robotic systems in this area, it is necessary when choosing a suitable type of robot to take into account several important parameters according to which you can decide what type of mobile robot used for intended type of operation.

The implementation of robots in the commercial security industry is the expected consequence of their development. The robotic system can replace humans in activities that threaten them to life and health, but also may serve as a potential source of information for visitors (day mode). Due to the continuous development of new technologies and control systems, we can meet with robots that are able to carry out their activities without the presence of the operator. In this case, the robot is fully independent in the performance of its tasks and partly in their maintenance (battery charging, reporting the failure to the operator). The stated capabilities challenge for the deployment of robotic systems in commercial security in guarding objects and buildings, survey and inspection activities, monitoring the crowd.

In some cases, the human presence is indispensable. In particular, it is a crisis situation, the robot is able during its service record undesirable status or potential danger, but it is not able to effectively deal with. This situation must the robot report to head office or responsible person who decides to contact the employee to solve the situation [4].

An example might be an intruder penetration into the protected territory. The robotic system can reliably detect the intruder, but has no resources to forced intruder to leave the locations (without executing the proposed action), or held it until the police arrival. Some effort on the robot's ability to resolve conflicts with humans lies in the equipment of robot with audio output through which robot is able to highlight the person action illegitimacy, or to intimidate warning signals.

An important requirement for robots in the security services is mobility. Mobility is the ability to move in an environment is not defined in advance (external, internal urbanized and natural, water, air environment). Mobility of the robot is thus dependent on the particular method of implementation of the movement in a given environment. Additional important parameters that affect the use of the robot to perform a given task may be: technical characteristics (dimensions, weight, continuity of the movement, etc.), operating parameters (traffic ability, operation costs), and energy requirements (power supply durability and capacity, operating time). [5, 6]

The reason for deployment of the robotic system should be primarily the quality of detection undesirable phenomenon (occurrence of persons in the prohibited area, presence of hazardous materials, etc.), and also expensive costs of activity of the human factor (security services staff).

2 Description of the Laboratory Mobile Robots

The mobile laboratory robots are designed as an open platform to allow for additional expansion of others appropriate components (sensors, effectors) as required service tasks. Motion control of both robots is possible through an appropriate communication interface. The robots are designed to verify their properties at a given service tasks. The following chapters provide a brief description of the laboratory service mobile robots.

2.1 Laboratory Mobile Double Track Robot

The robot consists of six smart actuators with time incremental control for each wheel separately, wireless webcam Axis 206W and access point ASUS WL – 560g. Four servomotors are used for steering motion control system of the wheels; two are used for camera control in two directions. Controlling the robot is allowed through serial interface RS232. The serial interface is used to transmit control data and setup instructions to the actuators. The system is extended for wireless communication modules, consisting of the radio modems, connectable to the serial port of the personal computer and the radio module Hőft & Wessel. The software consists of a set of instructions for communication between the PC and the robot. The whole system was designed so that it can be used as an appropriate teaching tool in laboratories dealing with teaching robotics.

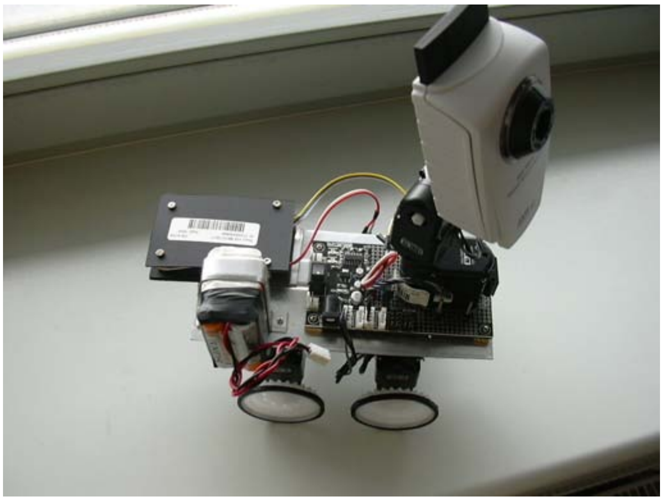


Fig. 1. Laboratory mobile double track robot.

2.1.1 AI-Actuator 1001

AI ACTUATOR-1001 is an action member for robot controlling. It consists of a driving unit, a small gear, the control unit and measuring unit. Power unit consists of a DC motor. The control unit consists from a single-chip processor, which provides also the control of DC actuator and communication with the surroundings by asynchronous serial interface RS-232 with TTL level communication signal.

The actuators can be combined into a single series in the network. In this case, form one branch of the four actuators connected in series wheels and the second branch consists from the two actuators for camera control movement in two axes. AI-Actuator receives instructions via RS-232 line. [7]

2.1.2 Motherboard MSC-BPT232

Motherboard MSC-BPT232 (see Fig. 2) is intended for management and control of the AI-actuator 1001. It contains serial port connector CD3pin (M) (1), integrated circuit MAX232 (2), battery connector (3), connectors for connecting AI actuator (4). Supply voltage ranges from 6 to 11V.

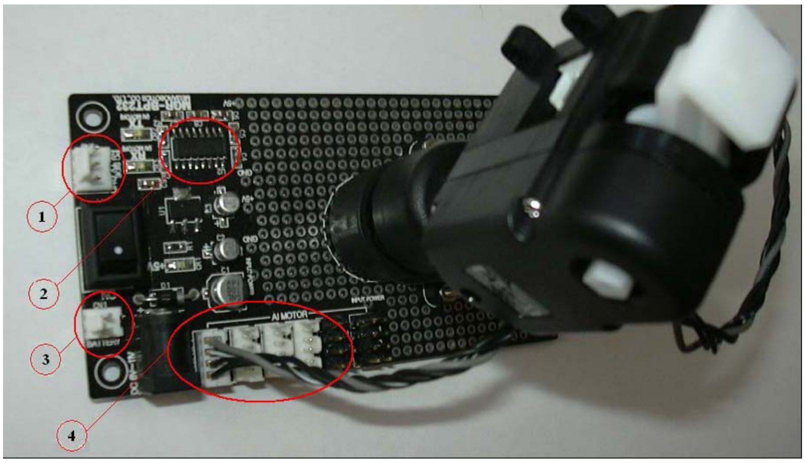


Fig. 2. Motherboard MGR-BPT232.

From Fig. 2 shows that the motherboard is used the most common RS232 connection; the cable has only three wires. Integrated circuit is a MAX232 TTL to RS232 converter. [7]

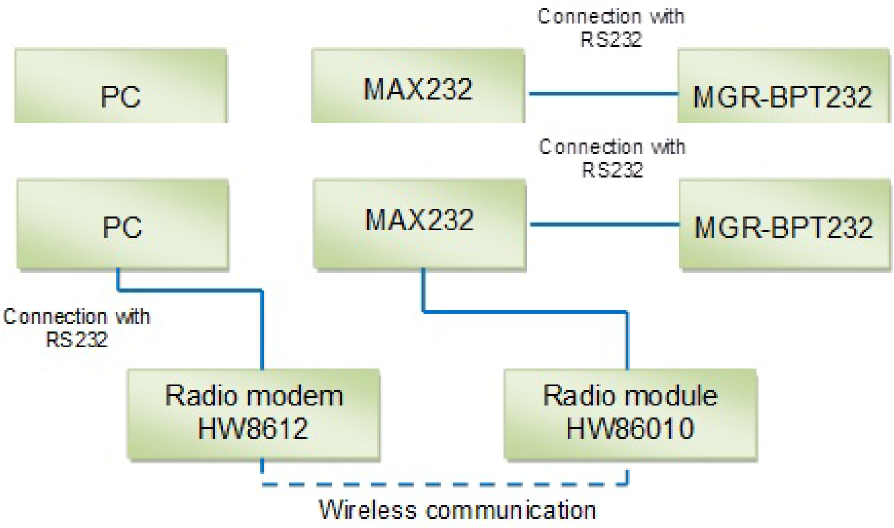
2.1.3 Web Camera AXIS 206W and Access Point ASUS WL-530 g Wi-Fi

Axis 206W has a built-in wireless 802.11b, it can therefore be placed almost anywhere, even where no network connection. In fact, the only limitation is power distribution. Due to its size and weight and also because of its mobility, the camera showed an ideal solution for mobile robot camera system. Image processing is secured by a CMOS sensor. The camera provides Motion JPEG images captured at 30 frames per second at resolutions up to 640x480 pixels. It has a built-in web server which makes possible to track and manage use a standard Web browser. The camera communication range is up to 150 meters. The camera is intended for indoor use.

2.1.4 Radio Module HW86010 and Radio Modem HW8612

For wireless communication between the motherboard of the robotic system MSC-BPT232 and personal computer were selected radio modules HW86010 and radio modems HW8612. Wireless communication architecture is shown in Fig. 3.

HW86010 radio module from the company Höft & Wessel working in the DECT band 1880.064 - 1898.208MHz (unlicensed band). The module includes RS232 interface for bi-directional data transmission (baud rate up to 115200 bit/s), PCM interface to connect standard ISDN and PBX systems, auxiliary functions for I2C and analog inputs and outputs for voice transmission. Radiofrequency power is 250mW, the possibility of using two internal and one external antenna. The range is about 300 meters in free space, 60 meters in the build-up area. Modem can be connected directly with the motherboard MSC-BPT232.



Fig

2.1.5 Implementation software - realization

The generated application is used mainly for input trajectories, where the robot will move. Entering task is to navigate the robot to a prescribed trajectory. The basic function of the program is therefore fitting curve trajectories of several points. The user then enters the coordinates of start and end points, determine the number of interlace points and also enter their coordinates. The program fits these points a curve of user's choice, by which the robot will move. Another option is to enter the coordinates of the trajectory break points, according to which the robot will move directly (by straight lines). Advantage of the system, where each wheel has its own control is that it enables the robot 180-degree turns in place. Another option is a last opportunity to let the robot to perform the movement in the closed curve such as a circle. The application also includes the option of manual control of movement forward, backward and turning left and right.

Created application software is open and arbitrary modifications can be made. It is possible for example a simple way to test own algorithms for motion control and extend the capabilities of created robot. The robot can be connected to a wireless IP camera. Camera movement is controlled in two axes using two intelligent engines. The camera communicates with the PC via a wireless router. Capture video from the camera is easy. On the basis of picture taken from camera it is possible do the analysis and subsequently control the movement of the robot.

2.2 Laboratory Mobile Tracked Robot

Mobility subsystem is implemented as a belt chassis. The chassis contains gearbox with two DC motors. Due to the used type of locomotion robot motion control is realized by differential steering. The motors are controlled by an intelligent controller Sabertooth 2x5, which allows differential control two DC motors and receives commands via the serial interface in TTL level. In order to detect obstacles, the robot is equipped with ultrasonic sensors. Control instructions for the navigation of robots are coming from the superior system via Bluetooth to a control unit consisting of Arduino development kit. Information about the status of the robot is shown on the LED display. The development kit Arduino Uno represents the control unit.

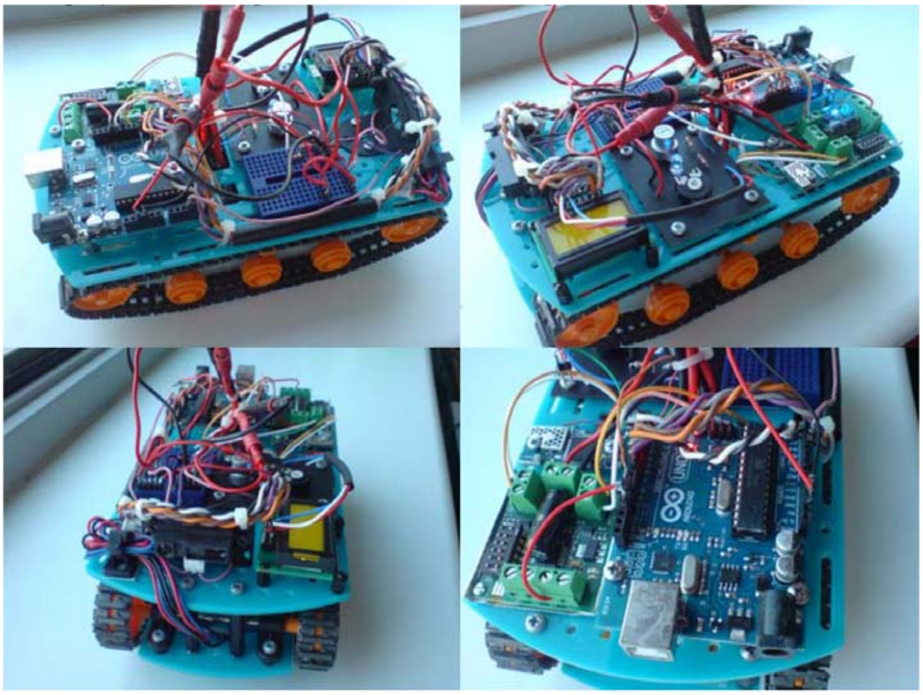


Fig. 4. Laboratory mobile tracked robot.

2.2.1 Arduino Uno

The control subsystem is implemented using a development kit Arduino Uno. The Arduino Uno is a microcontroller board based on the ATmega328. It has 14 digital input/output pins (of which 6 can be used as PWM outputs), 6 analog inputs, a 16 MHz ceramic resonator, a USB connection, a power jack, an ICSP header, and a reset button. It contains everything needed to support the microcontroller; simply connect it to a computer with a USB cable or power it with AC-to-DC adapter or battery to get started. The Arduino Uno can be powered via the USB connection or with an external power supply. The power source is selected automatically. External (non-USB) power can come either from an AC-to-DC adapter or battery. The Arduino Uno can be programmed with the Arduino software.

2.2.2 Sabertooth 2x5

The control part of the mobility subsystem is realized through intelligent driver Sabertooth. Sabertooth 2X5 is the motor driver for differential-drive robots. Sabertooth provide possibility to control two brushed DC motors and incorporates soft current limiting and thermal protection. The Sabertooth allows control two motors with: analog voltage, radio control, serial. It has independent and speed+direction operating modes, making it suitable controller for differential drive robots. To control DC motors serial interface was used. The motion control instructions are sent through serial line in TTL level.

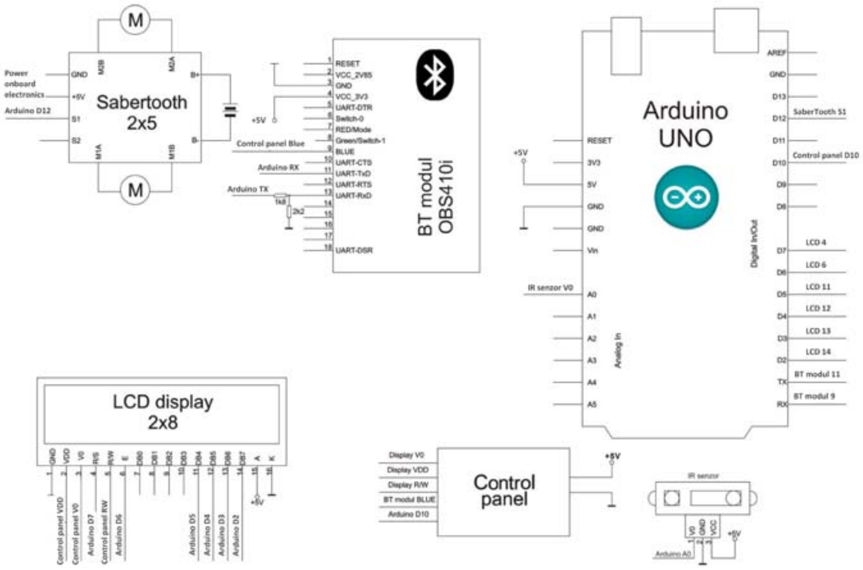


Fig. 5. Interconnection of robot modules.

2.2.3 BlueTooth Serial Port Module OBS410i

For wireless communication between the Arduino Uno and personal computer (or any other device with Bluetooth communication support) BlueTooth Serial Port module OBS410i were selected. The module includes RS232 interface for bi-directional data transmission, the possibility of using internal and external antenna. The range is about 150 meters in free space, 75 meters in the build-up area. Module OBS410i can be connected directly with the Arduino Uno board serial interface with TTL logic. Bluetooth module operates at 2.4 GHz, can be powered by 3-6V. To communicate with the Arduino configuration 8N1 (8 data bits, no parity, 1 stop bit) was used and 9600 baud rate.

2.2.4 Implementation software - realization

The microcontroller on the Arduino Uno board is programmed using the Arduino programming language (based on Wiring) and the Arduino development environment (based on Processing). Arduino projects can be stand-alone or they can communicate with software running on a computer. In the development environment was created several program to demonstrate the behavior of the robot. These include program for robot remote control using a computer or mobile phone (or any other device with Bluetooth communication support) and program solving partial autonomy in robot motion – bypassing obstacles.

4 Conclusions

Service robotic systems are used everywhere where the environment is hazardous to humans, difficult to obtain or even unavailable. Robotic systems contribute to the efficiency of solving various tasks. Sphere and the scope of robotic systems are still disseminated. There is constant evolution, which aims to improve the various elements of robotic systems, which in effect forms an ideal system for the performance of a service task. The robots are generally immune to tiredness, sleep, insufficient light and etc. In these conditions it is possible for the robot performs many tasks that would have been very difficult or insoluble for humans. Due to the fact that proposed robotic systems are open for modifications, it is possible to additionally mount the other necessary appropriate elements (e.g. sensors) for the implementation of different types of service tasks. Presented laboratory robotic systems enable development and testing, the properties and behavior of two different modes of locomotion, the possibility of their control, programming and navigation in laboratory conditions.

References

1. Kárník, L.: Využití servisních robotů v nestrojírenských aplikacích. Vysoká škola báňská: Technická univerzita, Ostrava (2010) (The Use of Service Robots in non-engineering Applications)
2. Smrček, J., Kárník, L.: Robotika, Servisné roboty, Navrhovanie, konštrukcia, riešenia, Košice (2008) (Robotics, service robots, design, construction, solutions)
3. Kárník, L.: Praktické aplikace servisních robotů. Vysoká škola báňská, Technická univerzita Ostrava (2011) (Practical Applications of Service Robots)
4. McKerrow, P. J.:Introduction to Robotics. Addison-Wessley, Sydney (1991)
5. Schilling R. J.: Fundamentals of Robotics. Analysis and Control, Prentice Hall, Englewood Cliffts, New Jersey (1990)
6. Craig, J.: Introduction to robotics : mechanics and control. Upper Saddle River, Pearson/Prentice Hall, N.J (2005)
7. PC interface board for MGR-BPT232 MANUAL, http://megarobot.net/manual_download/MGR-BPT232_manual.pdf
8. AI MOTOR 1001 - MANUAL ver. 1.02, http://www.megarobot.net/cj/manualy/megarobotics/AIMotor1001_manual.pdf

A Proposal of Camera System for Measuring of EMC Parameters of Information Technology Equipment

Michal Nagy, Jan Valouch, Hana Urbancokova

Tomas Bata University in Zlín, Faculty of Applied Informatics, Nad Stráněmi 4511
760 05 Zlín, Czech Republic
{mnagy, valouch, urbancokova}@fai.utb.cz

Abstract Information technology equipment and their the partial components are electronic devices, i.e. products that are potential sources of electromagnetic interference, while their proper operation are compromised by interfering emission of electromagnetic environment of the installation site. Product conformity assessment involves measuring and testing of parameters electromagnetic compatibility. The key outcome of the article is the proposal of the camera system, which represent the technical assistance for the EMC testing of information technology equipment.

Keywords: information technology equipment, equipment under test, electromagnetic compatibility, camera system, shielding.

1 Introduction

Information Technology Equipment (ITE) represent in accordance with the wording technical standard EN 55022 ed.3 (CSN, 2011), any device whose primary function is input, storage, display, retrieval, transmission, processing, switching, or control data and telecommunication messages. Such the device can be equipped with one or more terminal ports typically operated for information transfer. ITE devices are powered with an input voltage, which is not exceeding 600 V. In practice, we include between these devices for example personal computers, laptops, printers, switches, modems, routers, IP phones, VoIP gateways, IP set top boxes, etc.

Construction the equipment of Information technique include (such as electrical / electronic equipment) between products, which could increasingly threaten the health or safety of persons, property or the environment (specified products). Based on this fact, such products may be marketed only if they comply with the technical requirements that are specified in government regulations, issued for each group of specified products. Basic national legal document of requirements for EMC of information technology equipment is Government Order 616, 2006 on technical requirements for products relating to their electromagnetic compatibility. Once the products meet the requirements of that, comply with the requirements of the relevant technical standards (Government Order 616, 2006).

Product of information technology equipment must comply with terms of electromagnetic compatibility requirements of the following technical standards:

- EN 55022 ed. 3 Information technology equipment-Radio disturbance characteristics - Limits and methods of measurement,
- EN 55024 ed. 2 Information technology equipment - Immunity characteristics - Limits and methods of measurement.

Within the measurement of electromagnetic emissions for information technology equipment are carried out the tests:

- Measurement of radiated interference,
- measurement disturbance (noise voltage at the line terminals, unbalanced interference on telecommunication ports).

Testing electromagnetic immunity of information technology equipment mainly includes the following types of tests:

- Electrostatic discharge,
- radiated electromagnetic field,
- disturbance indicated by high-frequency fields,
- fast transients,
- slow surge,
- dips and short interruptions of mains supply.

ITE products are further tested by measuring the emissions of harmonic currents and verification of an installation for distribution system of low voltage.

Measurement and testing is performed according to the standards of standardized methodologies in testing laboratories. Measurement of radiated disturbances is performed in anechoic / semi anechoic chambers, respectively. at the test site in open space OATS-Open Area Test Site. Testing electromagnetic immunity in the test radiated high-frequency electromagnetic field would be due to the high intensity of the generated field is also carried out in shielded chambers. In the case of large systems or equipment, the measurements are carried out on site. (Valouch, 2012).

In the case of measuring and testing equipment in anechoic / semi anechoic chambers is an operator located outside the chamber and he doesn't have an ability to monitor the status of the equipment under test. Therefore, it is necessary to equip these spaces by shielded camera system, which ensures the monitoring of the state of the equipment under test with respect to:

- The risk of damage to the equipment under test while turntable is moving,
- monitoring changes in operating conditions of the test equipment when exposed to artificially generated interfering signals,
- risk of malfunction or damage to the equipment under test by the effect of artificially generated interfering signals.

The following part of the paper describes a proposal for implementation of CCTV in a semi anechoic chamber.

2 Materials and Methods

The camera system will be operating in an environment with strong electromagnetic field, so the selection of high-quality IP camera is very important. It must also be equipped with night vision, because inside the anechoic chamber are a poor lighting conditions during the measurements. I focused on the selection of PTZ dome cameras with the possibility of recording and zoom for better orientation in space. Operator must watch the test equipment for its proper functioning (eg, flashing indicator light) and therefore must have a high resolution camera, FullHD at best. Data output from anechoic chamber is implemented via an optical cable through the penetration panel; therefore camera should have the output directly to the optical cable. In this a case, media converter which implementing a conversion to fiber optic cable, would was unnecessary. The optical cable also has far better properties to the area with strong electromagnetic interference than metallic cable. Unfortunately, the cameras with such output are highly specialized and their prices are around CZK 150,000 and up. That's why I chose a cheaper alternative for my design of camera system. The quality camera with metallic data output and transfer to the optical cable by media converter. Other requirements for IP camera are quite common and during the selection isn´t a problem with them.

The camera which is chosen for design the camera system is Merit Lilin, IPS5184S. This camera meets the above requirements and its image is shown in Figure 1.

Fig. 1. IP camera IPS5184S

3 Results - Solution Design

3.1 Solution Design of Shielding Box

As soon as you want to put the camera into a shielded anechoic chamber, you must reduce the level of emission of electromagnetic signals to a minimum; thereby decrease their effects on the ongoing measurement. At the same time, the camera must maintain its functionality, even in extremely unfriendly electromagnetic environment. For these purposes, is suggested a shielding box made of stainless steel with a wall-thickness of 1 mm. There is also a hole which is located at the front of the box for the camera lens. The camera will be mounted into the box by a bolt (fig. 3).

All leaks or openings are affecting the overall effectiveness of the shielding box, and therefore is requires careful welding of the edges, the large hole on the front side is overlaps by using a conductive material and the space between the cover and the box is sealed. The cost of producing a shielding box represents approximately 1,800 CZK.

In order the hole for the camera lens, there arise are two conflicting requirements. Firstly, the hole must be electromagnetically shielded as much as possible, while maintaining correct transparency sufficient for the camera. This objective is achieved by using the technology similar to that used in a microwave oven, which employs using a conductive metal foil with holes much smaller than the wavelength of the test signals is. Anechoic chambers are usually designed to test the frequency range approximately from 26 MHz to 18 GHz which roughly corresponds to wavelengths from 11.5 m to 1.66 cm. The metal foil is attached to the shield box by means of a rectangular stainless steel strip of the same thickness as the box walls have. The second option is a strip of foil attached by a screw connection.

Electromagnetic sealing the opening between the box and the cover is provided by metal contact strips supplied by Laid Technologies, a company specializing in the production of elements for electromagnetic shielding (fig. 2).

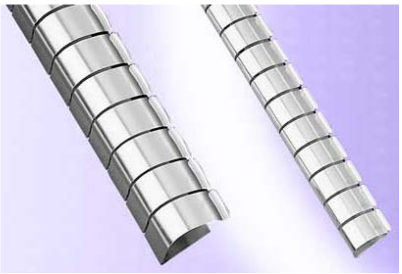


Fig. 2. Sample of strips from all-purpose series, type 97-538

Model of shielding box is shown in Figure 3, cabling for IP camera leads at the bottom of the shielding box through a hole.

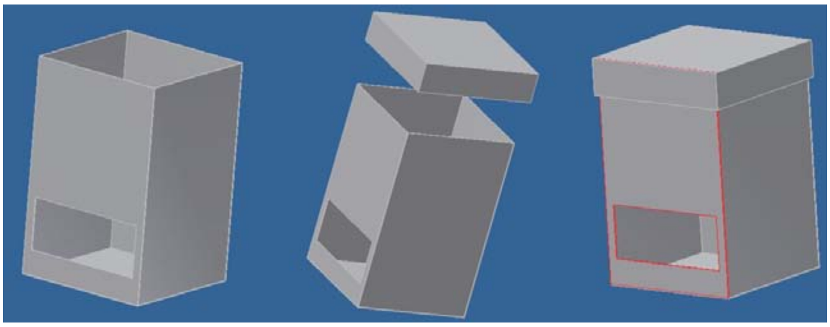


Fig. 3. Sample of modeled shielding box with a lid

ISBN: 978-1-61804-246-0

3.2 Solution Design of Rack

Shielding anechoic chamber is completely covered from the inside by absorbent material and a larger portion of the chamber is covered by absorption pyramids. Therefore is inadmissible to interfere in any way to the integrity of the walls. This would mean automatic loss guarantee from the manufacturer. IP camera can´t be attached in the ceiling or elsewhere in the room just for that reason and must be placed in the room with its own rack. The rack in terms of electromagnetic compatibility and construction of anechoic chamber is designed from polypropylene, which is one of the most common plastics; the sample is shown in Fig 4.

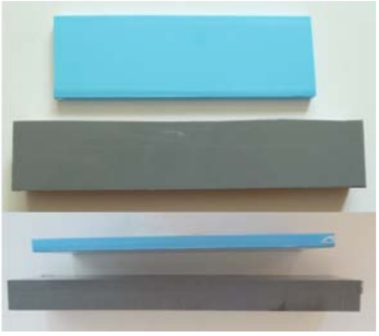


Fig. 4. Sample of rack´s material

The cost of production of the rack is 1650 CZK. Layer thickness is 6 mm (Fig. 4 - blue pattern), the size of the base is 400 mm, and thickness of base is 15 mm (Fig. 4 - brown pattern) due to the stability of the entire rack. Depending on the strength of the entire structure can change the size of the base. The shielding box will be inserted from the top, so also the rack will be provided with a lid. It is important so that both openings for the lens were the same height. This is ensured by two rails inside the rack. The shielding box is placed on them and their height is calculated so that the two holes coincide. Model of rack is shown in Figure 5. The far left of the picture is rack without lid. Second from left is a view from the bottom and you can notice a hole in the pedestal. The hole is required for cabling or also if anything fell into a rack that is an easy way to simply pulled out. Third from the left is the rack with the lid on top and far right is a detail of upper part with the lid. One of the rails for the shielding box is seen through the opening for the lens.

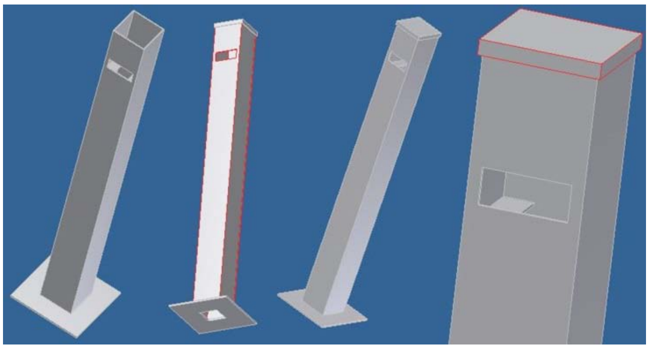


Fig. 5. Rack modeled from multiple perspectives

Rack height is determined by the requirement to camera view. The camera will control a measured device in the anechoic chamber, which may be smaller and lie on the table at a certain height. The camera must have a good view of the device at all times. Therefore the camera should be placed in minimum height of 170 cm. How can put together the entire assembly of the shielding box and the rack is shown in Figure 6.

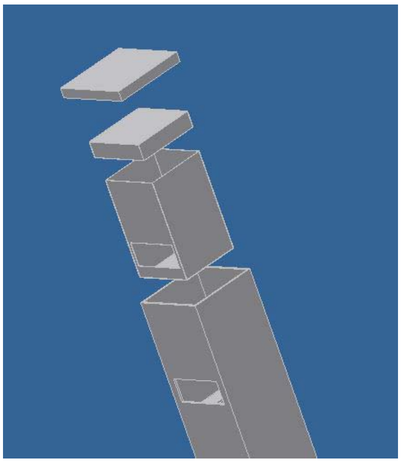


Fig. 6. Modelled rack with folding shielding box for camera

3.3 Proposed location

Location of rack with IP camera must always be chosen so as to have as little impact on the results in an anechoic chamber. The rack shouldn't stand in the direction of the antenna radiation, or even between the antenna and test equipment. In this case, would occur to undesired reflection of electromagnetic waves, before they hit into the absorbent material of the pyramids and lose much of its energy. Therefore, the expected best place for the rack is in a corner behind an antenna, as illustratively shown in Figure 7.

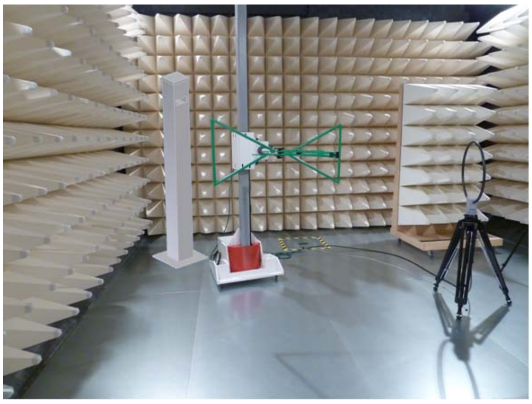


Fig. 7. The proposed location of the rack

3.4 Camera power

The camera needs a 24V AC for its operation. Part of the cameras is a power adapter with power cord. However, I would recommend replacing a cable for a shielded one, which then leads across the floor to the bottom of the rack and through it directly into the camera.

3.5 Data connections to IP camera

Optical fiber as the data cable is preferable due to its electromagnetic compatibility during a data transmission. So, the ongoing measurement does not represent an additional source of interference and is highly resistant to external electromagnetic activity. The transfer from a metallic cable to an optical cable can be used for example, media converter AT-MC102XL (fig. 8). It is a media converter from ethernet network cable UTP to 2x optical fibers MM (multimode). Max. length of fiber is 2000m. Wavelength is 1310nm. Metallic connector is RJ45. Optical connectors are 2x SC. The power adapter is included. The dimensions are 95 mm x 105 mm x 25 mm (length x width x height). Supply voltage is 12V DC. So, together with power cable for the camera also leads a cable for power supply media converter and I would recommend replacing the cable for the shielded cable. The price of this media converter is CZK 2,064.

Fig. 8. Media converter AT-MC102XL

The best location for media converter is in the rack and due to its small size is not excluded the possibility that lay directly at the bottom of the shielding box. But then is necessary to calculate the dimensions of media converter during the design of the box.

4 Conclusion

Tab. 1 shows the approximate pricing of the proposed camera system. The final price is 47 191 CZK including VAT. The most expensive item is the purchase of high-quality IP camera, which would meet the requirements for placement in anechoic chamber. The result price is without cabling.

	Produkt	Cena včetně DPH
1	IP kamera, Merit Lilin, typ IPS5184	41 772 Kč
2	Výroba stínícího krytu	1 755 Kč
3	Výroba stojanu	1 650 Kč
4	Media konvertor AT-MC102XL	2 064 Kč
	Celkem:	47 191 Kč

Tab 1. Price list of the proposed camera system

The shielding box main task is protection IP cameras from destruction due to strong electromagnetic fields. The measurements taken with an older IP camera MIP-6430-2 showed high levels of electromagnetic radiation in the frequency range from 30 MHz to 2 GHz (Fig. 9). The IP camera is comply with the standard EN 55022 (emission information technology equipment), but at some frequencies has very high amounts of radiation and that is an important finding. This measurement shows that results of next measurements of electrical equipment will be significantly affected by the location of old IP camera into the anechoic chamber without the shielding box.

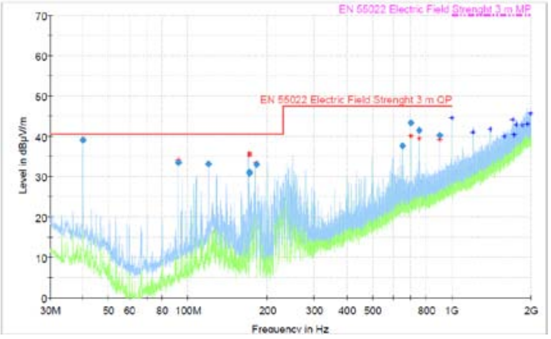


Fig. 9. The measurement result in the test range

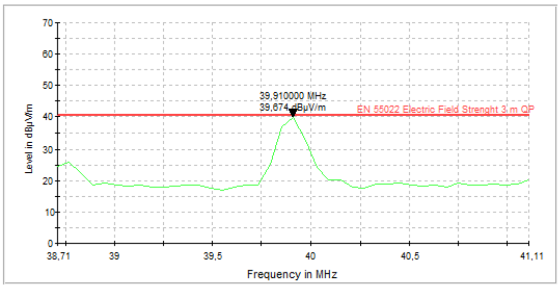


Fig. 10. Detail of the peak on 39.91 MHz

But the recommended camera Merit Lilin (type IPS5184S) is far more modern and more suitable for industrial environments than the old tested camera. So this measurement will end probably much better with the recommended camera.

Acknowledgments. With support by grant No. IGA/FAI/2014/060 from IGA (Internal Grant Agency) of Thomas Bata University in Zlin and the European Regional Development Fund under the project CEBIA-Tech No. CZ.1.05/2.1.00/03.0089.

References

1. VACULIK, E., VACULIKOVA, P.: Electromagnetic compatibility of electrotechnical systems: A practical guide to technology limitations HF electromagnetic interference. 1. ed. Grada Publishing, Prague (1998), p. 487. ISBN 80-716-9568-8.
2. CSN EN 55022 ed. 3 Information technology equipment-Radio disturbance characteristics - Limits and methods of measurement. The Czech Office for Standards, Metrology and Testing, Prague (2006).
3. VALOUCH, J.: Integrated Alarm Systems. In: Computer Applications for Software Engineering, Disaster Recovery, and Business Continuity. The 2012 International Conference on Disaster Recovery and Business Continuity, Jeju Island, Korea.

Proceedings. Series: <http://www.springer.com/series/7899> Communications in Computer and Information Science, vol. 340, XVIII. Berlin: Springer Berlin Heidelberg (2012). Chapter, pp. 369--379. ISBN 978-3-642-35267-9.

4. VALOUCH, J.: Electromagnetic compatibility alarm systems - testing and measurement of electromagnetic parameters. In: Security magazine. Ed. No. 107, 3/2012. Security Media, Prague (2012), pp. 24--29. ISSN 1210-8273.
5. SVACINA, J.: Electromagnetic compatibility: Principles and comment. University of Technology, Brno (2001), 156 p. ISBN 80-214-1873-7.
6. CSN EN 50130-4 ed. 2: Alarm system. Part 4: Electromagnetic compatibility - Product family standard: Immunity requirements for components of fire, intruder, hold up, CCTV, access control and social alarm systems. The Czech Office for Standards, Metrology and Testing, Prague (2012)
7. VALOUCH, J.: Requirements for Alarm Systems in Terms of the Electromagnetic Compatibility. In: KRIVANEK, V. and STEFEK, A. (ed.) International Conference in Military Technology Proceeding, ICMT'13, University of Defence, Brno (2013), pp. 589--596. ISBN 978-80-7231-918-6.

Lighting Measurement Methods related to Intelligent Video Surveillance System Evaluation

Jiri Sevcik and Petr Svoboda

Tomas Bata University in Zlin, Faculty of Applied Informatics, Department of Security Engeneering, Nad Stráněmi 4511, 760 05 Zlín, Czech Republic
jsevcik@fai.utb.cz, psvoboda@fai.utb.cz;

Abstract. The percentages of the areas which are covered through Video Surveillance Systems are continuously increasing. The various evaluation techniques are utilized in order to manage their effectiveness. The comparison study of lighting measurement possibilities are provided in this research paper. Magnitude and reason of such measurement is discussed in the initiate part. The second part is aimed to presentation of methods and instruments utilized for measurement. The particular results obtained within the two case studies are provided in final section.

Keywords: Intelligent Video Surveillance System, Lighting measurement methods, comparison study, evaluation, Image functional properties.

1 Introduction

One of the key functional properties of Intelligent Video Surveillance System (IVSS) is their image acquisition capability. Although the IVSS effectiveness is influenced by complex variety of factors, the most important are lighting conditions within the scene exposed. This fact is obvious even from camera working principle. The Image Acquisition properties of the cameras are continuously increased by the IVSS manufacturers on one hand, but the effectiveness of the IVSS could be increased throughout the exact specification of influencing conditions on the other hand. Moreover, Image Acquisition is an initial step within the image capturing process which means, that all next steps are influenced by the quality of input signal generated under particular conditions applied. Final scheme exposed scene lighting conditions could be managed even within IVSS design process, where two approaches could be utilized:

- Empirical (based on “know how” of particular system designer),
- Exact (based on measurable values).

Appropriate assessment of lighting conditions is closely related also to intrinsic and extrinsic calibration of the camera.

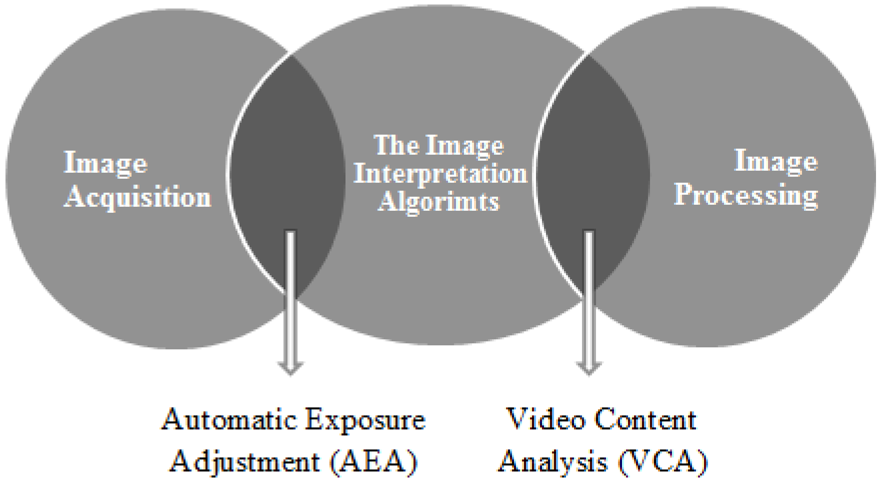


Image Acquisition
The Image Interpretation Algorimts
Image Processing
Automatic Exposure Adjustment (AEA)
Video Content Analysis (VCA)

Figure 1: Image Interpretation Algorithms utilization

The Image Interpretation Algorithms are utilized in order to increase evidence value of image sequence captured by the system. These functions are well known as an Automatic Exposure Adjustment tools. Although particular research papers discussed evaluation of the Image Acquisition process [1], the majority were aimed to evaluation of overall architecture of the system [2], including all functional blocks such as Image Acquisition, Connections, Image Processing, Activity and data management, connections with other systems, the system and data integrity.

Content of this research paper is logicaly divided into four chapters. In the initial chapter the incident and reflected lighting intensity measurement methods are described in detail. The description of measuring instruments is provided in next chapter and the results taken from two case studies are presented in final chapter of this research paper.

2 Exposed scene lighting characteristics measurement methods

Three approaches to the lighting intensity measurement are utilized for the purposes of IVSS proposal procedure.

- Incident illumination intensity measurement,
- Reflected illumination intensity measurement,
- Histogram expertise technique.

Measurement of lighting is sophisticated engine to the exposure conditions establishment process. In case of IVSS it is necessary to divide exposed area to partial block. Advantage of this solution consists in establishment of concrete lighting level in particular partial block of the scene and its monitoring within the day. There is possible to settle severity of the scene exposed in light of the dynamic range, which is important parameter for equipment solution. Illumination is a photometric magnitude which is defined as a luminous flux incident on particular surface. Its base value is Lux. The illumination intensity is in virtue of following equation:

$$E = \frac{\Delta\Phi}{\Delta S} = \frac{I}{r^2} \qquad (1)$$

Where [E] = Lux (lx), $\Delta\Phi$ - luminous flux, ΔS - is exposed area, I – luminance, r- range between surface and source of illumination.

Nonetheless, the equation before is usable only if the lighting incident vertically on the surface, but this case is not so common. More frequent is other case, when the lighting incident angle-wised randomly. Then is in virtue of following equation:

$$E = \frac{I \cdot \cos\alpha}{r^2} \qquad (2)$$

Where α - randomly wised angle of lighting incident.

Considering equations above is obvious, that illumination intensity is depended on range between source and illuminated object and on the lighting incident angle. Common illumination levels are illustrated via next table 1:

Table 1: Common real-life illumination levels

Illumination intensity [lx]	Level of illumination within exposed scene
100 000	Direct sunlight
50 000	Sunny weather
5 000	Overcast
500	High quality illuminated surface etc. office
300	Minimal illumination needed for reading
100	Insufficiently illuminated surface
60	Day illumination of aisles
15	Quality illuminated streets at night time
10	Evenfall
5	Common illumination of off-street
2	Minimal security illumination

1	Sunset
0,3	Full moon
0,1	Overcast moon illumination
0,001	Common stars illumination
0,0001	Low stars illumination

Alternative method of lighting characteristic is reflected illumination intensity measurement. Instead of incident illumination intensity, where the lighting beams coming on surface are gathered for measurement, in case of reflected illumination intensity are the lighting beams reflected from surface utilized and evaluated. This method has several advantages, but also similar number of disadvantages. Main advantage consist in their ability to take into account the reflection characteristic of materials which are situated in exposed scenery. The lower accuracy of measurement is then disadvantage on the other hand. Both of introduced methods are usable before the IVSS´s design itself, nonetheless the last one, the histogram expertise is based on revision of existing camera views. Core contribution of lighting characteristic is to specify dynamic range severity of the scene. The difference between the lightest and the darkest point within the image. The absolute magnitude is defined through this relationship, whereas the total amount of lighting occurring on the image sensor is described. The maximal amount of shades, which image sensor could recognize is then defined as a contrast value. Borders of image sensor are stated by capacity of each photo-sensitive cell and also the noise generated. The exposure value are established in EV magnitudes as a difference of the lightest EV in opposite to the darkest EV.

3 Measurement instruments description

Two types of measurement instruments were used within the experiment. The first one is a representative of lux meter category Sonel LXP 1. The second instrument which were used is able to measure incident and also the reflected illumination, this capabilities are at disposal by expose meter Sekonic LITEMASTER L-478DR. Technical parameter of each are illustrated via tables 2 and 3.

Table 2: Digital Luxmetr Sonel LXP 1 technical specification

Display	Multifunctional LCD	
Measuring scales	400,0 lx 4000 lx 40,00 klx 400,0 klx	40,00 fc 400,0 fc 4000 fc 40,00 kfc
Measuring rate	1,3 lx / sec	
Interrelations (lux / fc)	1 lx = 0,09190304 fc	

	1 fc = 10,76391 lx fc = foot candle
Internal memory	99 measuring results
Data logger	16000 values
Supply voltage	9 V (accumulator)
Dimensions	170 x 80 x 40 mm
Weight	390 g

Table 3: Sekonic LITEMASTER L-478DR technical specification

Measuring methods	Incident | Reflected
Special functions	Brightness difference | Memory
Lighting measuring	Ambient | Flash
Measuring scale (EV)	-27,9/+55,8EV
Sensitivity	3 - 409 600 ISO (1/3EV)
Iris	f/0,5 - f/161,2
Exposure time	30min - 1/64000 sec.
Frame per sec	1 až 1000 fps
Aperture angle	1-358°
Candela/m2	1,0-980 000
Supply voltage	2x AAA Accumulator
Dimensions	57x140x26mm
Weight	130 g

4 IVSS Lighting Characteristic Measurement Case Study

Incident and reflected illumination intensity is influenced by several aspects:

- weather conditions within the scene (overcast, semi-bright, bright weather),
- time of measurement (three hours interval between single measurements),
- camera position considering sun position (sunrise, sunset),
- considering shadows (dropped by buildings, trees,
- positioning and timing of artificial lighting.

4.1 Illumination intensity with homogenous conditions within the particular levels of detail

Because of the similarity of results taken within the particular levels of detail of the scene, the time of measurement and weather conditions dependence were utilized as main grading criteria. Measured results are digestedly illustrated via following figures:

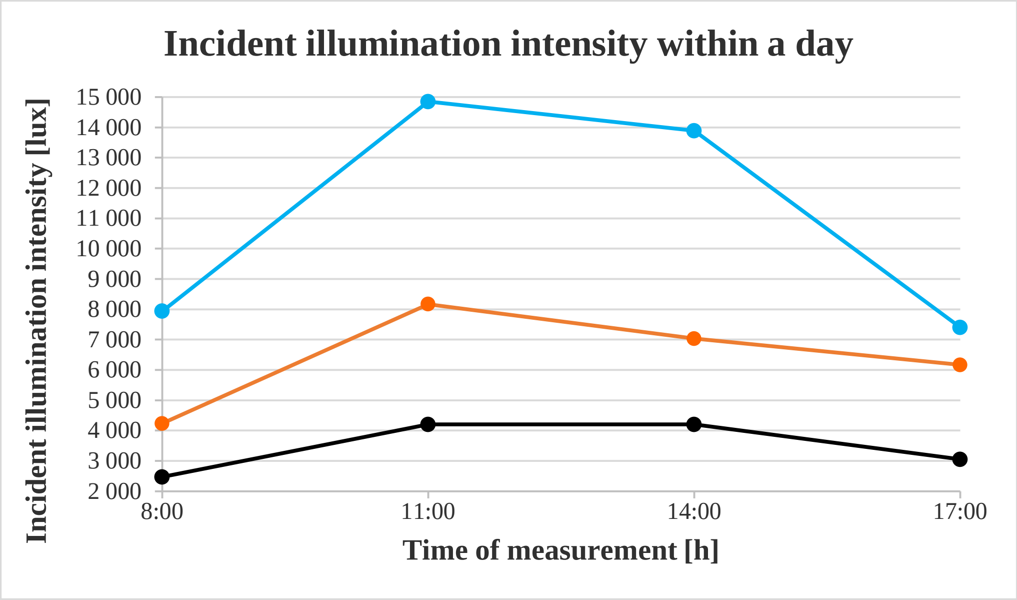


Figure 2: Incident illumination intensity within a day

Where bright weather is represented by blue line, semi-bright is represented by orange line and overcast is represented by black line. Technical ways of interconnecting the individual applications can be divided
into the following basic groups:

- hardware methods of integration,
- software methods of integration [3].

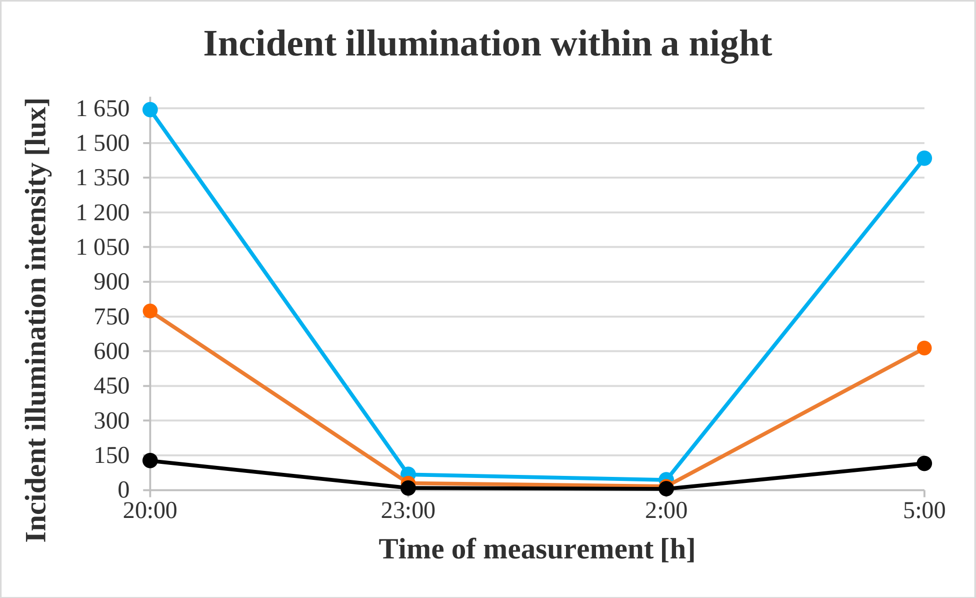


Figure 3: Incident illumination within a night

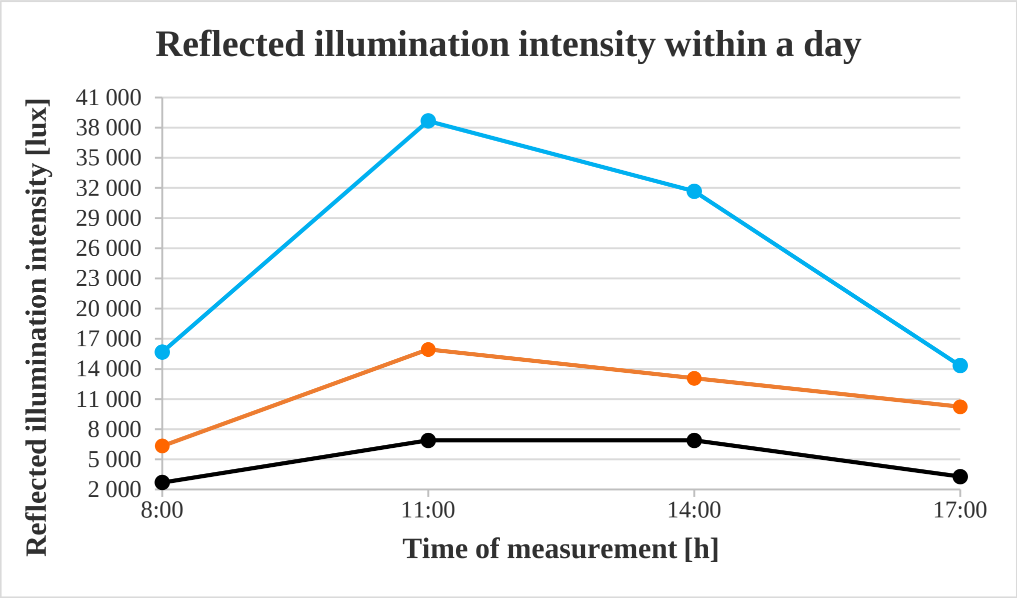


Figure 4: Reflected illumination within a day

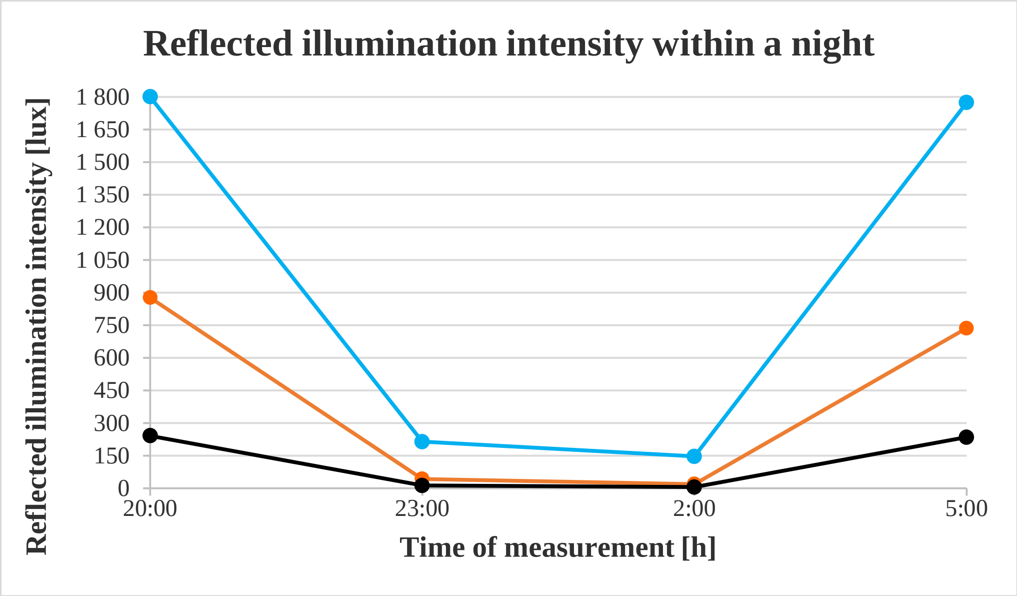


Figure 5: Reflected illumination within a night

From figures n.2, 3, 4, 5 is obvious, that characteristics of incident and reflected illumination were not significantly different. The most distinct aberrancy was investigated when measurement was accomplished during sunny weather. In these situations a value of reflected illumination was slightly higher. It is important to mention, that the most significant value differences were measured within a day. Form the results is obvious, that the reflected illumination measurement method is effective and more precise, when the highly contrastive scene is investigated. When it is necessary to measure dynamic range disposals, the reflected lighting method is considerably useful, within the IVSS design process. However, this comparison study is helpful mainly for definition of measurement methods for complex IVSS evaluation methodology, which should be proposed within the thesis of the first author of the paper.

5 Conclusion

Well known methods of illumination level measurement were utilized for purposes of IVSS design in this research paper. Recent approaches and methods used were recapitulated in the first part of the paper and then the specifications of methods used for the purposes of this research were interpreted in detail. The description of measurement tools were provided in next section. Finally the main contribution is included in four sections, where the results comparison study is provided and discussed. Larger data pattern will be published in extended version of the paper. Where the other measurement approaches will be provided.

References

1. Aldridge JJ994, CCTV Operational Requirements Manual JSDB Publication 17/94, ISBN 1 85893 335 8.
2. Raaty, T.D., "Survey on Contemporary Remote Surveillance Systems for Public Safety," Systems, Man, and Cybernetics, Part C: Applications and Reviews, IEEE Transactions on, vol.40, no.5, pp.493, 515, Sept. 2010.E. H. Miller, "A note on reflector arrays (Periodical style—Accepted for publication)," IEEE Trans. Antennas Propagat., to be published.
3. VALOUCH, Jan. Integrated Alarm Systems. In Computer Applications for Software Engineering, Disaster Recovery, and Business Continuity. The 2012 Internationa Conference on Disaster Recovery and Business Continuity, Jeju Island, Korea. Proceedings. Series: http://www.springer.com/series/7899 Communications in Computer and Information Science, Vol. 340, 2012, XVIII. Berlin: Springer Berlin Heidelberg, 2012. Chapter, p. 369 - 379. ISBN 978-3-642-35267-9.
4. Ashani, Z., "Architectural Considerations for Video Content Analysis in Urban Surveillance," Advanced Video and Signal Based Surveillance, 2009. AVSS '09. Sixth IEEE International Conference on, vol., no., pp.289, 289, 2-4 Sept. 2009 doi: 10.1109/AVSS.2009.112.
5. EN 50 132-7. Alarm system - CCTV surveillance systems for use in security applications - Part 7: Application guidelines. B - 1000 Brussels: Management Centre: Avenue Marnix 17, 2011.W.-K. Chen, Linear Networks and Systems (Book style). Belmont, CA: Wadsworth, 1993, pp. 123–135.
6. Pavlidis, I.; Morellas, V.; Tsiamyrtzis, P.; Harp, S., "Urban surveillance systems: from the laboratory to the commercial world," Proceedings of the IEEE , vol.89, no.10, pp.1478,1497, Oct 2001
7. HROMADA, M., LUKAS L., Conceptual Design of the Resilience Evaluation System of the Critical Infrastructure Elements and Networks in Selected Areas in Czech Republic, The twelfth annual IEEE Conference on Technologies for Homeland Security (HST '12), held 13-15 November 2012 in Greater Boston, Massachusetts. Pp. 353-358, ISBN 978-1-4673-2707-7
8. HROMADA, M., LUKAS L., The Status and Importance of Robustness in the Process of Critical Infrastructure Resilience Evaluation, The 13th annual IEEE Conference on Technologies for Homeland Security (HST '13), held 12-14 November 2013 in Greater Boston, Massachusetts. Pp. 589-594, ISBN 978-1-4799-1533-0

University network with REMLABNET and communication among individual datacenters

P.Beňo [1,2], F.Schauer [1,2], K.Vlček [1]

[1] Faculty of Applied Informatics, Tomas Bata University in Zlín,Czech Republic
[2] Centre of the information systems and Department of Physics, Faculty of Education
Trnava University in Trnava, Slovak Republic

Abstract. The paper deals with communication among individual datacenters (DTC) in the university network with remote laboratories, organized into Laboratory management system (LMS). We want to show the use of modern technologies for communication among individual DTCs, especially for the communication of individual experiments, or rigs, their communication model and the technique, based on the fiber optics. This new concept, so called Wavelength division multiplexing (WDM), uses multi wavelength approach for the communication on a single optical fiber.

Further, we deal with the main causes of a possible communication breakdown among DTCs, between the client and the cloud and among individual experiments and cloud and suggest corresponding solutions for their elimination. We consider the cloud consisting of the whole bulk of communication, among its all blocks, virtualized machines (VMs), data processing, their content, sharing and access planning to individual rigs. At present the most spread model of the failure elimination is the artificial built in redundancy of active and passive component parts of the communication network.

Keywords: *remote labs, physical labs Cloud computing, virtual, platform, datacenter, communication among datacenters, disk storage, risk, security, Cisco, VMWare, disaster recovery, backup, archiving, network, availability, WDM, communication, router, switch*

1 INTRODUCTION AND STATE OF THE ART OF REMOTE LABORATORY MANAGEMENT SYSTEMS

Our work is aimed at the inclusion of the inherent element of any modern contemporary university network - the remote laboratories spread across the Internet on the communication scheme server-client [01] and their communication with individual datacenters (DTC), the university network (UN) and the laboratory management SYSTEM (LMS) [02, 03]. The data center is a facility used to house computer systems and associated components, such as telecommunications and storage systems. It generally includes redundant or backup power supplies, redundant data communications connections, environmental controls (e.g., air conditioning, fire suppression) and security devices [04]. All these communication and data processing and storing activities are the goal of our team at TBU in Zlin, as we try, accordance with the EU FP7 activities to setup the LMS of our own with all related activities included with the working name REMLABNET [05]. Our work on LMS consists of several SW and HW solutions, starting from the reservation system for individual experiments, scheduling system, data storage of experiments and supporting material for clients, network traffic, server usage and their security, etc. (see Figure 1). Let us describe the communication in the depicted cloud and start with the individual components. First of all this is a rig. Rig is the cumulative name of the experiment itself, the physical SW and HW, as well as the informatics HW and SW, creating remote experiment, communicating, by means of special protocols, mediating the remote experiment to clients. In our design model of the LMS (Figure 1) are three new types of communications. The first communication is with Remote experiments (RE) servers in the cloud (brown colour). This communication is between DTC and each experiment (rig). The second channel of communication is the transfer of information between the management and Measure server of the rig (blue colour). This channel of the communication will also provide diagnostics of individual experiments, remote repair of their malfunctioning and finally, scheduling of the experiments as well. The last, third channel of communication is communication with the client. Clients proceed to experiment via the communication server (light brown colour).

Important part of the whole communication network of the university are individual DTC and their mutual communication (green colour). A DTC may be considered composed of all components in form of the cloud, with whom communicates clients to individual rigs executing network strategy, server platform, data storage, data compressing or data packing etc.

This work describes communication among DTCs with Laboratory Management System (LMS) with remote laboratories. In the Figure 1 is this part depicted as a part of the DTC, composed from communication and networking in the middle, the part between experiments (rigs) and clients. This DTC is a part of our cloud serving as LMS system for arbitrary from outside connected and communicating both rig server and client, working under the general communication scheme server-client. The whole cloud and thus the LMS system is a black box both for rig's administrators and clients, which is advantage from the security point of view, because knowledge about this part can be the security hole.

In our work we want to present the design of the Laboratory management system (LMS) and its communication, which is a primary part of our work. LMS executes all communication, data manipulation, data transfer or conversion and in the last but not least mediate data to clients of the rigs.

LMS system in the cloud forms a virtualization platform with virtualized machines (VMs) for managing all experiments and supported services. Supported services are web servers, communication servers, or scheduling servers in cluster node for better availability.

On top of this, we elaborate in this work also the part of the communication among individual DTCs. We present a university network topology, derive the network security and the availability with the main impact on the communication among DTCs and their LMS systems with remote laboratories.

It is worth noting that our virtualized cloud is designed to extend not only among several DTCs, but our final goal in REMLABNET project is to build the LMS communication bridge between two countries Slovak and Czech republic. The first and at present the active part of the cloud is located in TU in Trnava, Slovak republic, and the second, standby DTC is in Zlin, Czech republic that will be gradually transferred partially to Zlin, as the project will continue. In future we want to build our DTCs in active-active mode exclusively.

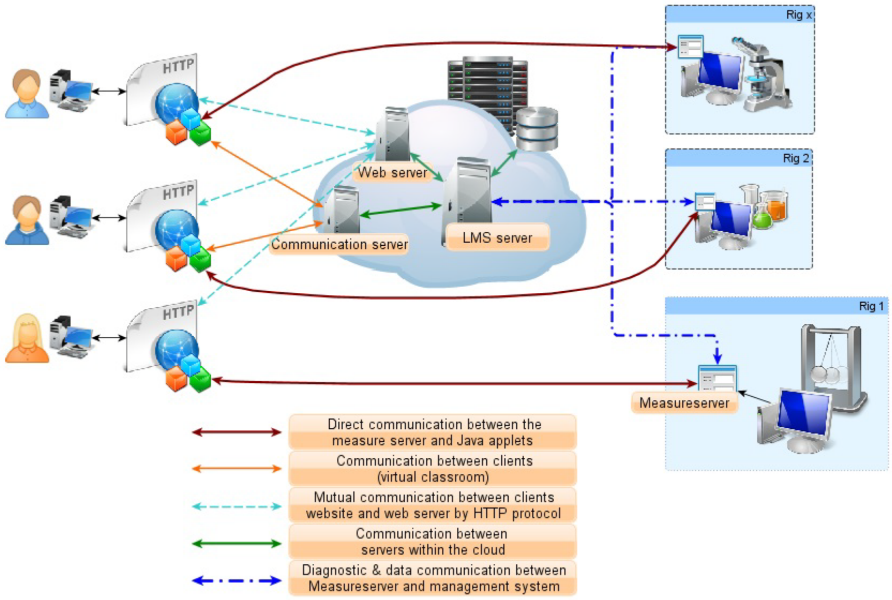

Rig x
Rig 2
Rig 1
HTTP
HTTP
HTTP
Web server
Communication server
LMS server
Measureserver
Direct communication between the measure server and Java applets
Communication between clients (virtual classroom)
Mutual communication between clients website and web server by HTTP protocol
Communication between servers within the cloud
Diagnostic & data communication between Measureserver and management system

Figure 1 Communication scheme of the designed Laboratory Management System – REMLABNET

1.1 Modern datacentres, cloud virtualized services and LMS

The last decade has seen the rise of the DTC computing in practically every application domain. The move to DTC has been powered by two separate trends. In parallel, functionality and data usually associated with personal computing has moved into the DTC; users continuously interact with remote sites while using local computers, whether to run intrinsically online applications such as email, chat, or to manipulate data traditionally stored locally, such as documents, spreadsheets, videos and photos. In effect, modern architectures are converging towards cloud computing, a paradigm where all user activity is funneled into large DTC via high-speed networks. Simply speaking, cloud computing is a set of computers, services or infrastructure. Delivering services is reducing every day work of users (clients), service providers, but also IT specialists. Cloud allows to offer more access services, reduces infrastructure delivery time from weeks to hours and reimbursement for really provided sources and services only [06].

Let us give some typical services provided in modern cloud computing DTC:

- Infrastructure as a service (IaaS),
- Platform as a service (PaaS),
- Software as a service (SaaS),
- Storage as a service (STaaS) ,
- Security as a service (SECaaS),
- Data as a service (DaaS),
- Business process as a service (BPaaS),
- Test environment as a service (TEaaS),
- Desktop as a service (DaaS),
- API as a service (APIaaS),

and, in the context of the present work - Rig as a service (RaaS), by means of the whole computer oriented experiment, or its part, will be provided for the interested clients and virtual simulations as a service (SIaaS).

A critical implication of the DTC computing model is that the user of the online service expects the same performance of the application as that, running on the desktop computer, immediately responsive as a desktop application. User expects the service to store data reliably and always and immediately available. For service providers, delivering on this expectation, it is an engineering task of immense proportions. DTC are composed of thousands of failure-prone components and exhibit a bewildering array of failure models. Each level of the SW and HW stack has its own litany of error models, ranging from simple to byzantine – hung machines, blown fans, corrupted disks, bad network cards, overloaded routers and switches, bugs in SW, rogue malware, partitioned networks - this list is endless. When faults occur, enterprises have to react extremely quickly to prevent service down-time.

Existing reliable communication protocols are reactive, and have an associated cost and latency of reaction. In many cases, they react too slowly to the packet loss. And often, they over-react – flooding the system with recovery traffic that potentially causes further data loss, as well as throttling back excessively on sending speeds to avoid more loss. Protocols such as TCP/IP were designed for congested public networks and do not work well in the high-speed networks deployed within and between DTCs.

The goal of our present work is a new and acute topic of providing a new service for the clients - completely functioning remote experiment as a service - Rig as a service (RaaS), forming a new service for the cloud computing systems for the first time. It is schematically depicted in Figure 1, where several accessible rigs are depicted, simultaneously providing corresponding virtual simulations as a service (SIaaS). Both services are accompanied by the scheduling and diagnostic systems built in the cloud system. The last part of the paper deals with the security of remote laboratories in cloud in general and these both new services in particular.

2 TRNAVA UNIVERSITY NETWORK AND REMLABNET

Let us show first the general scheme of communication among individual DTCs on example of DTCs in Trnava University. Trnava University has three locally separated DTCs, connected via fiber optic connection. Network connectivity is designed on the Cisco technology with security from the same company. Let us touch first the problem about general topology, connectivity and all special features of the communication system among DTCs.

2.1 *Transmition lines aggregation (TRUNKING)*

If we want to speak about the communication among individual DTCs, we must first show, how is network balanced. Cisco technology enables the setup of the network for excessive data transfer. Our project requires a good and stable network backbone, with the conservation of the required security level. One interesting part of the networking and communication setup is aggregation in form of trunking. The task of the aggregation of the transmission lines is to provide availability with divided communication network among more physical transmission lines. If one line exhibits failure, communication is continued on other lines. Aggregation is formulated in the standard IEEE 802.3ad, where there is described the compatibility of this solution with different network components from different producers as well.

In the aggregation (Figure 2) the logical MAC address is used that is assignment to more physical ports. This logical address is moved on the third layer, what is input Address Resolution Protocol (ARP). All ports who are in aggregation are in one interface Data Link Provider Interface (DLPI) ports of the router, which looks and behaves as one port and thus the Spanning Tree Protocol (STP) does not block it how a topology loop.

Aggregation must be supported on both sides of the communication channel what is ensured by the protocol Link Aggregation Control Protocol (LACP). Communication is started by the messages of the type “query”, where assigned for aggregation ports on both sides are. That is the way for creating a trunk with a sent message “start group”, where there are the identifying lines to ports. The collector compiles the communication from other ports and the distributor separates dataflow between ports in trunk or aggregation group.

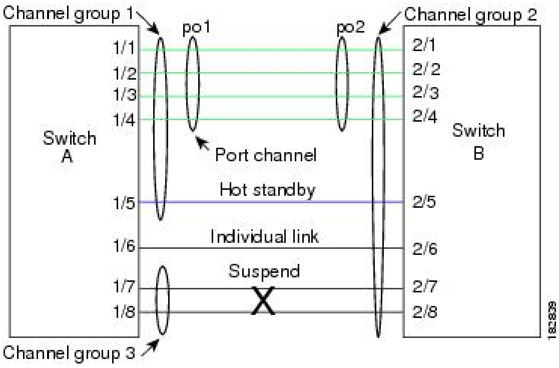


Figure 2 Scheme of transmition lines aggregation (TRUNKING) [07]

2.2 Data and WDM technology

Next part that we want to show for the support of the communication among individual DTCs is technology based on the multiplexing and demultiplexing transmition wavelength via fiber optic cable. [08]. In fiber-optic communications, wavelength division multiplexing (WDM) is a technology which multiplexes a number of optical carrier signals onto a single optical fiber by using different wavelengths of a laser radiation. This technique enables bidirectional communications over one strand of the fiber, as well as multiplication of its capacity. The WDM system uses a multiplexer at the transmitter side to combine the signals together and a demultiplexer at the receiver side to split them apart again. With the right type of fiber it is possible to have a device that does both simultaneously, and can function as an optical add-drop multiplexer.

2.2.1 Coarse WDM

Originally, the term "coarse wavelength division multiplexing" was fairly generic, and meant a number of different things. In general, these things shared the fact that the choice of channel spacings and frequency stability was such that erbium doped fiber amplifiers (EDFAs) could not be utilized. Prior to the relatively recent ITU standardization of the term, one common meaning for coarse WDM meant two (or possibly more) signals multiplexed onto a single fiber, where one signal was in the 1550 nm band, and the other in the 1310 nm band.

An interesting and relatively recent development relating coarse WDM is the creation of GBIC and small form factor pluggable (SFP) transceivers utilizing standardized CWDM wavelengths. GBIC and SFP optics allow for something very close to a seamless upgrade in even legacy systems that support SFP interfaces. Thus, a legacy switch system can be easily "converted" to allow wavelength multiplexed transport over a fiber simply by judicious choice of transceiver wavelengths, combined with an inexpensive passive optical multiplexing device.

2.2.2 Dense WDM

Dense wavelength division multiplexing (DWDM) refers originally to optical signals multiplexed within the 1550 nm band so as to leverage the capabilities (and cost) of erbium doped fiber amplifiers (EDFAs), which are effective for wavelengths between approximately 1525–1565 nm (C band), or 1570–1610 nm (L band). EDFAs were originally developed to replace SONET/SDH optical-electrical-optical (OEO) regenerators, which they had made them practically obsolete. EDFAs can amplify any optical signal in their operating range, regardless of the bit rate. In terms of multi-wavelength signals, so long as the EDFA has enough pump energy available , it can amplify as many optical signals as can be multiplexed into its amplification band (though signal densities are limited by choice of modulation format). EDFAs therefore allow a single-channel optical link to be upgraded in bit rate by replacing only equipment at both ends of the link, while retaining the existing EDFA or series of EDFAs through a long haul route. Furthermore, single-wavelength links using EDFAs can similarly be upgraded to WDM links at reasonable cost. The EDFA's cost is thus leveraged across as many channels as can be multiplexed into the 1550 nm band.

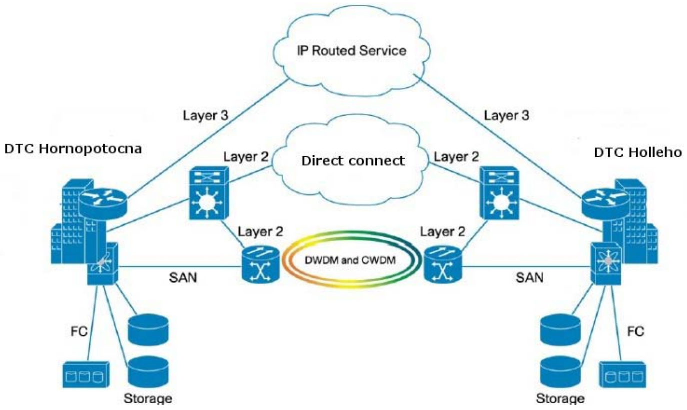


Figure 3 DWDM between DTCs in Trnava university

Let us show, how is Trnava university using DWDM technology (Figure 3). This communication is set up between two datacenters. The first is situated in Hornopotočná street (the rectorate of the university), the second is in Holleho street (Albertinum center). Among this two individual DTCs is DWDM connected via

Small Factor Pluggable (SFP) installed in Cisco Catalist 4507. DWDM using four wavelengths. Two of them are used for the standard communication between DTCs, one is used for phone lines and last one is used for Storage area network (SAN) connection between DTCs. SAN connection is very important, because this allows a higher functionality in virtualization or cloud computing. This higher functionality is in the first place migration of the VMs between ESX servers and datastores in the DTCs. If we look for our LMS on Figure 1, this part is not visible, but constitutes an important part of the whole communication system. Communication between DTCs should be very reliable, forming a backbone of the virtualized cloud and thus LMS. All three communication types of the LMS are in Figure 1.

3 SECURITY IN CLOUD COMPUTING AND NETWORK

Firstly, it is proper to show schematically the main topology of the Trnava University network. We can start from Figure 4, where is the topology of the Trnava University network. University network is designed with respect to the organization structure of the university. Structure of the network consists of two main parts. The first part is the rectorate part, where is Internet service provider (ISP) connected, DMZ core switch in redundancy mode and firewall Cisco ASA. The second part of the network is designed for faculties´ communication. Every faculty of the university is equipped with identical component parts designed to cooperate with the rectorate core switch, distribution and access switches in facultaties´ buildings.

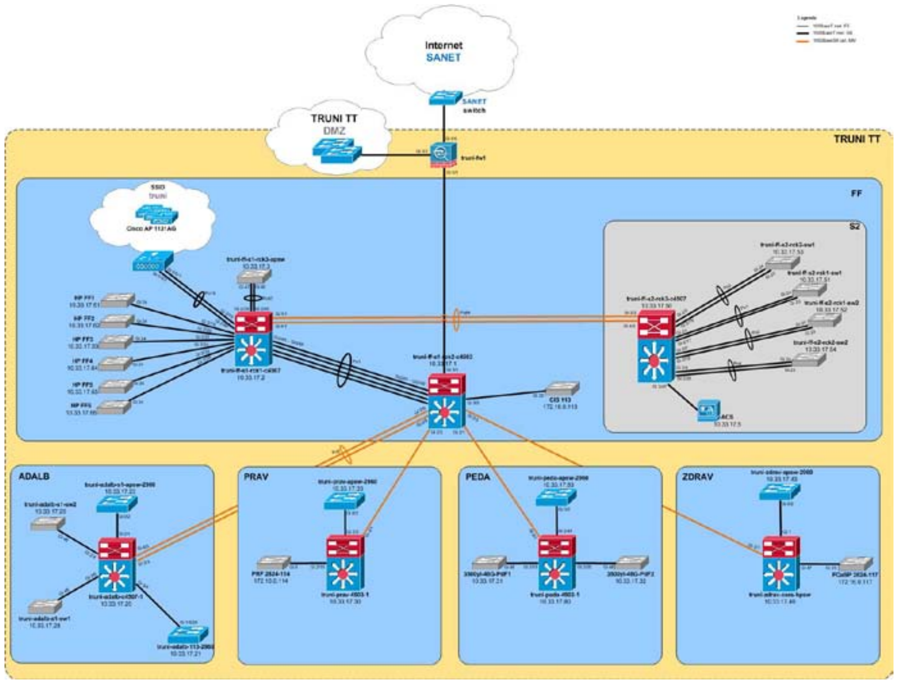


Figure 4 Topology of the Trnava University data communication network

The security of the university network is secured by four layers system. The first layer is the security provided by university's firewall. Cisco ASA is a good firewall choice, which enables to adjust the main security policy, for example blocking input/output communication with server or ports by the primary network antivirus - TrendMicro. The second level of the security is the access list on the core switch, where route policy for all faculties and buildings is set. The third part of the security is Intrusion Detection System (IDS) system for detecting problems and port security on the network. The last part is the security policy on the distribution switches, where is set the policy for every building and faculty. This is the network security element. On top of this, the university is protected with antivirus in all Windows servers and users end nodes. All network is designed with VLAN modes for all faculties and primary applications. For example this VLAN is defined for every faculty:

- Sunray – for thin client,
- User – for all users and end nodes,
- Management – for management and monitoring on network,
- Phone – for telephone central,
- Wifi – for APs and clients in the building,
- Elab – for communication of the our experiments with servers in DTCs.

Approximately 90% of the university communication is in crypt mode. Every page, every communication between servers is protected for cybercrime. Connection to the network from outer word, from other providers is just in VPN mode authenticated to IDM system of the university.

4 CONCLUSIONS

In this contribution we tried to show the communication among DTCs of the Trnava University with all the progressive parts, including virtualized cloud with Laboratory Management System for remote laboratories. Our three DTCs are geographically distributed in Trnava town, connected via Fiber optic (FO) . All transmission lines is design to transfer at minimum 1Gbps on one wavelengths λ=1310 or 1550 nm. Between DTCs Hornopotočná a Hollého is used DWDM connection for the separate communication. Under separate communication we mean the connection where different wavelengths for different communication are used. This approach enabled for the connection of the SAN (storage array network) between a both DTCs that is substantial contribution for virtualization, bringing migration among servers or datastores in both DTCs, resulting in many assets, the savings in the first place.

A strong and good idea for the future is hidden in using DWDM technology for our remote labs. Our intention is to use one transmition wavelength for every remote laboratory, We plan this sort of connection between the Faculty of Education and the Rectorate, where is the storage array and main server platforms.

Looking at the primary part of our work, i.e remote laboratories, the resulting LMS can work faster and reliably, if we resort to the communication using new technologies and protocols. The communication must contain components of the security, simplicity, speed and reliability. Communication between DTCs is very complicated and requires long time and attention for the setup. The problem in fulfilling this part of the design is not limited by the know – how of the participating staff of the University, but it is in the costs of the component parts, requiring the illuminated management of the University, who support this project, which is the case in Trnava University.

5 REFERENCES

01. J. Garcia-Zubia, and G. Alves, eds., "Using Remote Labs in Education," Ed. University of Deusto, Miller, F. P., 2009.
and K. Azad, M. Auer, J. Harward, "Internet Accessible Remote Laboratories: Scalable E-Learning Tools for Engineering and Science Disciplines," Ed. IGI Global. USA. DOI: 10.4018/978-1-61350-186-3, ISBN: 9781613501863 , 2012.

02. M. Tawfik, D. Lowe, S. Murray, M. de la Villefromoy, M.Diponio, E. Sancristobal, M. José Albert, G. Díaz, M.Castro, "Grid Remote Laboratory Management System - Sahara Reaches Europe", in Proc. 10th REV conference, 2013, Sydney

03. V. J. Harward, J. A. del Alamo, S. R. Lerman, P. H. Bailey, J. Carpenter, K. DeLong, C. Felknor, J. Hardison, B. Harrison, I. Jabbour, P. D. Long, M. Tingting, L. Naamani, J. Northridge, M. Schulz, D. Talavera, C. Varadharajan, W. Shaomin, K. Yehia, R. Zbib, and D. Zych, "The iLab Shared Architecture: A Web Services Infrastructure to Build Communities of Internet Accessible Laboratories," Proceedings of the IEEE, vol. 96, pp. 931-950, 2008

04. https://en.wikipedia.org/wiki/Data_center

05. Submitted Project Grant Agency of the Czech Republic: INFORMATICS MEANS FOR GRID OF e-LABORATORIES – PROJECT REMLABNET , 2013

06. Beňo, P., & Kurtha, T. (2011). *Cloud computing, This is it!* Bratislava, Zutom 2012

07. http://cisco.sitecelerate.com/en/US/docs/switches/datacenter/sw/6_x/nx-os/interfaces/configuration/guide/if_portchannel.html

08. http://cdn.ttgtmedia.com/ITKE/uploads/blogs.dir/58/files/2009/01/etherchannel7.jpg

09. http://en.wikipedia.org/wiki/Wavelength-division_multiplexing

10. http://zolotech.com/sub/photonics/dwdm.php

Safety research of population protection according to population differentiation

Lenka Brehovská,
Lenka Brehovská, Libor Líbal, Zuzana Freitinger Skalická,

[1] University of South Bohemia in České Budějovice, Faculty of Health and Social Studies,
Department of radiology, toxicology and population protection, Czech republic
BrehovskaLenka@seznam.cz

Abstract. The third appeal of the Home Office of the Czech Republic, concentrated on the support of research, experimental development and innovation, came up for the period between 2013 – 2015. The Faculty of Health and Social Studies, the Department of Radiology, Toxicology and Population Protection, has taken part in the appeal with the research concentrated on population protection according to population differentiation. The aim of the project is to analyse the current status of the evacuation planning from the emergency zone planning according to the population differentiation and the population readiness for potential disruption of functionality of critical infrastructure, to suggest new methods of evacuation planning along with incorporating new aspects of health evacuation protection and design manuals for the population on the methods to handle emergencies with the disruption of critical infrastructure in the context of ethical issues

Keywords: research, population protection, analysis,

1 Introduction

To reduce threats in the Czech Republic, the Home Office proclaimed the Security Research Programme in the Czech Republic in the years 2010 - 2015, where into the 3rd public tender in research, experimental development and innovation project of the University of South Bohemia in České Budějovice was accepted, titled "Population Protection According to Population Differentiation", which is designed for 2013 - 2015.

The aim of the project is:

1. analysis of the current status of evacuation planning from the emergency planning zones of nuclear power plants Temelín and Dukovany, according to the differentiation of the population, and to prepare people for possible disruption in critical infrastructure
2. proposing a new methodology for evacuation planning along with integrating new aspects of medical support

3. designing manuals for the population for the procedure to handle emergencies with the disruption of critical infrastructure in the context of ethical issues.

The research project addresses 10 scientific and technical staff members and 4 other people as members of the project team. Team members are direct employees of the University of South Bohemia - Faculty of Health and Social Care (USB - FHCS) and the Czech Fire and Rescue Brigade (FRB CZ), which is the main co-operative institution.

1.1 Realisation of the reseach evacuation project

To determine the underlying data to process a certified methodology that will serve as the basis for the adjustment of legal measures related to the VHP nuclear facilities, there is a questionnaire survey.

To cover all spheres of life in the emergency planning zone (hereinafter "EPZ"), four types of questionnaires have been prepared for households, individually for physical persons, schools and educational facilities and social facilities.

Household questionnaires

Between November and December 2013, questionnaires were distributed to all local authorities in both EPZ‘s. The questionnaires are addressed to all households in both EPZ‘s. Distributed questionnaires are registered in the municipalities in the way that 13,750 questionnaires were distributed in the EPZ JETE and 39,102 questionnaires in the EPZ JEDU, making a total of 52,852 questionnaires.

Prallelly with this leaf form an electronic version of the questionnaire was prepared with a direct possibility of completing it on-line on the faculty website. This is a questionnaire for households in the EPZ‘s. The census of the questionnaires cast has not yet been completed, but the EPZ of Temelín nuclear power plant returned 902 questionnaires and the EPZ of Dukovany nuclear power plant has returned .... questionaires.

Questionnaires for physical persons

In the same period, April to November 2013, a questionnaire was prepared for physical persons. Because this survey aims to determine accurately the views and knowledge of the population by age groups, citizens were divided into 4 age groups.

To ensure the objectivity of the investigation and the statistical significance of the investigation, it was all based on the percentage representation of each of these groups of the population determined by the last census; in the same proportion the number of questionnaires was prepared for individual communities of both EPZ’s. The questionnaires were addressed to all municipalities of both EPZ’s and the survey was conducted by contact mode.

Every EPZ was addressed 500 questionnaires. Considering the mode of data assembling, 100% of questionnaires were returned.

Questionnaire for nurseries, primary and secondary schools and educational facilities

All nursery, primary and secondary schools and educational facilities were found in each EPZ. The questionnaire is focused on personal and material possibilities of each school. In the EPZ of Temelín nuclear plant there are 11 kindergartens, 12 primary and two secondary schools. There is also one educational facility. In the EPZ of Dukovany nuclear power plant there are about 70 kindergartens, 66 primary and 5 secondary schools and three educational facilities. In all schools, data for the questionnaires, a total of 16 questions, were obtained by contact mode with the exception of schools in the EPZ of Dukovany, where questionnaires were sent to each school with a covering letter asking for their completion.

Questionnaire for social facilities

The same procedure was followed with social facilities, data collection by contact mode in all facilities, which means that in the EPZ of Temelín nuclear power plant there are 2 social facilities and both questionnaires are available, and in the EPZ of Dukovany nuclear power plant there are 12 social facilities. Also, all completed questionnaires are available. The questionnaire contains 20 questions.

2 Realisation of the research awareness project

To determine the underlying data to process manuals for the population, there is a questionnaire survey. The author - designed questionnaire reflects the structure of selected questions focused on basic problems that people may encounter during power outages and their own self - protection during this incident. The questionnaire was presented to respondents in the emergency planning zone of a nuclear power plant and to respondents living outside the emergency planning zone of a nuclear power plant. The comparison of the knowledge of these two groups will be taken using parametric selective t-test. (Záškodný, 2011) The type of questions found in the questionnaire is based on various recommendations of international organizations and agencies, such as the CDC (Centres for Disease Control and Prevention in Atlanta), which deals with the readiness of the population issuing from biosafety during power outage. Federal organizations FEMA (Federal Emergency Management Agency) prepares the population in the form of analyses of previous power outage and creates a system for individual federal countries of the USA on how to prepare the population.

Centres for Disease Control and Prevention

The website of the Centre for Disease Control and Prevention, provides information on how to proceed in case of sudden power outage. The section is divided into parts (What You Need to Know When the Power Goes Out unexpectedly, 2009):

a) food safety: CDC advises when it is safe to consume foods placed in refrigerators and freezers and how to proceed with turning the power on again to ensure food safety.

b) safe water drinking: in this section advice is given on how to proceed in order to maintain the safety of water drinking. CDC also gives instructions for disinfecting contaminated or rainwater using chloramine, iodine, and carbon tetrachloride.
c) extreme heat and cold: here you are given advice on how to behave in case power outage occurs during periods of heat or cold to prevent damage to the organism.
d) first aid for contact with electricity

American Red Cross

One of the key organizations involved in crisis management is the American Red Cross. Its activities are great and involvement in handling emergencies is more than important. After flipping websites, we will find the issue of power outage. The American Red Cross has prepared a point checklist that all residents should follow in case of power outage. The checklist is divided into three parts (Power Outage Checklist, 2012):

a) how can I prepare for power outage
b) what should I do during a power outage
c) what should I do when starting up power again

Ministry of Agriculture Department of Food Safety and Inspection

The Ministry of Agriculture of the United States of America is very intensely involved in the issue of emergency preparedness with a focus on food security. The information they publish on their website is valuable material for the population and a manual how to preserve quality food during emergencies. All information is given in the 12 factual points (Emergency preperadness, 2012):

a) safe food handling
b) population endangerment
c) meat preparation
d) poultry preparation
e) preparation of egg dishes
f) seasonal food safety
g) other

Canadian government authorities

Like the USA, Canada as well, thanks to the experience of previous electricity black-outs, is trying to prepare the population against power outages. Canadian government has issued a publication entitled Your Emergency Preparedness Guide 72 Hours. This 36-page publication provides instructions to the population on how to proceed in case of selected 13 critical situations. Among the selected situations is power outage. There are instructions on how to proceed in preparation for power outage, how to secure your home and yourself, how to behave in case of power outage and restoration after power outage. The advice is similar to the one of the American Red Cross, but each territory of Canada regulates the recommendations according to its jurisdiction.

Within the statistical survey, a total of 400 questionnaires were distributed within emergency planning zones and also 400 questionnaires outside emergency planning zones, which directed the questions to determination of public awareness about electricity outages. Questions were divided into two groups. One group of questions was strictly informative (where people live, whether they own alternative sources of electrical energy, and what the influence or power outage is medically). The second group of questions was directed to the actual statistical survey. Of a total of 15 questions, six were informative and 9 subject to statistical survey.

For finding the information on the awareness, randomly selected people were surveyed in emergency planning zones of nuclear facilities Temelín and Dukovany and also outside the emergency planning zones. Addressed people were selected according to age differentiation in four major groups:

a) from 15 to 18 years of age
b) from 18 to 40 years of age
c) from 40 to 65 years of age
d) over 65 years of age

Both groups of respondents in each group were divided into men and women and specifically addressed in the relevant numbers corresponding to the age structure of the population of the Czech Republic.

Table 1. Numbers of addressed groups to age differentiation.

Age of the addressed	Number of women surveyed	Number of men surveyed
From 15 to 18 years of age	21	21
From 18 to 40 years of age	63	84
From 40 to 65 years of age	84	63
Over 65 years of age	42	22

Source: own survey

Groups of people were surveyed throughout the day in order to classify not only all age groups, but also other specific groups such as workers, the unemployed, parents on maternity leave and the like.

2 Conclusion

The results of the project, as it will, though it is currently impossible to predict, will contribute to improving the preparation of evacuation, incorporated in the external emergency plans and emergency plans of counties. Special attention in the project is paid to specific needs of individual age groups and sensitive approach to them while respecting ethical principles in the evacuation of the population. An important source of problems may also be loss - disruption – of some elements of critical infrastructure. It turns out that the majority of the population does not have enough knowledge of electricity outages. They do not know how to behave during power outage, how to secure thir home or how to ensure safe food and drink. In a situation such as long-term power outage, the population will need to be disciplined for the situation to be adequately managed with the smallest impact possible. One possibility is a ready citizen.

Evacuation, as the most effective measure to protect the life and health of citizens, must be prepared and implemented according to the latest knowledge and experience from the Czech Republic and the world, and that is the goal of the research project "Population Protection According to Population Diferentiation"

References

American red cross: Power outage safety [online]. 2014 [cit. 2014-02-25]. Dostupné z: http://www.redcross.org/prepare/disaster/power-outage

CENTERS FOR DISEASE CONTROL AND PREVENTION. *Emergency Preparedness and Response: What You Need to Know When the Power Goes Out Unexpectedly* [online]. 7. června 2013 [cit. 2014-02-25]. Dostupné z: http://emergency.cdc.gov/disasters/poweroutage/needtoknow.asp

Disaster survival Resources: Power outage [online]. 2009-20144 [cit. 2014-02-25]. Dostupné z: http://www.disaster-survival-resources.com/power-outage.html

European Commission: Humanitarian Aid & Civil Protection. EUROPEAN UNION. *European Commission: Humanitarian Aid & Civil Protection* [online]. 2014 [cit. 2014-02-25]. Dostupné z: http://ec.europa.eu/echo/policies/prevention_preparedness/dipecho_en.htm

Federal Emergency Management Agency: Plan, Prepare & Mitigate [online]. 2013 [cit. 2014-02-25]. Dostupné z: http://www.fema.gov/plan-prepare-mitigate

GOVERNMENT OF CANADA. Get Prepared: Your Emergency Preparedness Guide [online]. 9. prosince 2013 [cit. 2014-02-25]. Dostupné z: http://www.getprepared.gc.ca/index-eng.aspx

ZÁŠKODNÝ, Přemysl, Renata HAVRÁNKOVÁ, Jiří HAVRÁNEK a Vladimír VURM. *Základy statistiky (s aplikací na zdravotnictví).* Praha: CURRICULUM, 2011. ISBN 978-80-904948-2-4. Dostupné z: http://sites.google.com/site/csrggroup/Appendix: Springer-Author Discount

Checklist of Items to be Sent to Volume Editors

1. A final Word or RTF file
2. A final PDF file
3. A copyright form, signed by one author on behalf of all of the authors of the paper
4. A readme giving the name and email address of the corresponding author

Usability CAN Bus For Encrypted Communication InIntrusion And Hold-up Alarm Systems

Adam Hanáček, Martin Sysel,

Tomas Bata University in Zlín, Faculty of Applied Informatics, Nad Stráněmi 4511
760 05 Zlín, Czech Republic
{hanacek, adam}@fai.utb.cz

Abstract. The work deals with the possible solution of low sabotage protection in analog alarm systems and also problem with high cost of digital systems. The main part of the work is focused on the description of developed system, which applies bus named controller area network for encrypted transmission between a components in analogintrusion and hold-up alarm systems. There is possible to connect analog detectors, fire alarms, hold-up facilities, code keypads andacontrol and indicating equipment of analog alarm system to the developed system. The work also describes testing of the work, cost factors, and comparison with the currently used systems. Finally, the results are evaluated and there is also discussed the applicability of achieved knowledge.

Keywords: Intrusion and hold-up alarm system, microcontroller, detector, controller area network

1 Introduction

Current situation in the field of intrusion and hold-up alarm systems(I&HAS) shows an increasing ability of intrudersto overcomesecurity systems and gain access to the object. On the other side, security systems are currently very expensive for many subjects to protect their poverty. Therefore, it is important to reduce the threat of sabotage by improving security systems, which can not only prevent the loss of property, but it can also protect the people life and health. Further, it is also important to look for possible ways to reduce the costs of intrusion and hold-up alarm systems and thus improve availability of I&HAS also for less wealthy subjects.

Intrusion and hold-up alarm systems comply with standard CSN EN 50131, which specifies the terms alarm system for the detection of entry and alarm system for the detection of attack. [1]

It is possible to choose metallic or wirelesss communication between nodes and a control and indicating equipment(CIE) in the selection of security system. If is chosen metallic connection for object security, it is possible to select analog or digital communication. The advantage of analog communication in intrusion and hold-up alarm systems lies in low price of individual components, but the disadvantage lies in low protection against sabotage. In contrast with digital communication, the price of individual components is much more higher, but communication ensures higher protection against sabotage.

The work deals with the possible solution of mentioned problem by adding a microprocessor with bus named controller area network(CAN) to each component, that uses analog transmission. This enables data to be encrypted and transmitted by designed protocol for mentioned CAN bus.

1.1 Controller Area Network

The bus controller area network was basically designed for usage in automotive industry, but currently it is often implemented in development kits.

CAN bus is based on the CSMA/CR mechanism to prevent frame collisions during transmission messages on the bus. [4], [5]

The CAN network protocol has been defined with the following features and capabilities: [6]

- Message priority
- Multicast communication
- System-wide data format
- Error frame detection
- Detection of permanent failures in nodes and isolate faulty node

CAN is a high-integrity serial data communications bus for real-time applications and more cost effective than any other serial bus systems. Some another advantages are written below. [3]

- Data rates of transmission up to 1 Megabit per second
- Length of CAN BUS up to 1 kilometer.
- Is an international standard: ISO 11898

There are defined four types of messages in CAN protocol. [7]

- Data frame
- Remote frame
- Error frame
- Overload frame

At present, CAN is widely used in many other sectors of industry. It is atwo-wire differential serial communication protocol for real-time control and implements three layers of ISO/OSI reference model as physical layer, data link layer and application layer.

The thorough description of layers, message frames and communication speed is explained in [8], [9], [10].

1.2 Standard Connection of Alarm Circuits Used in Analog Security Systems

Figure 3 shows a standard connection of analog detectors to the control and indicating equipmentof intrusion and hold-up alarm systems. It is connection type NC (Normally Closed) with closed resistor.An alarm can be activated by switching off one of the contacts, which is connected to the circuit.

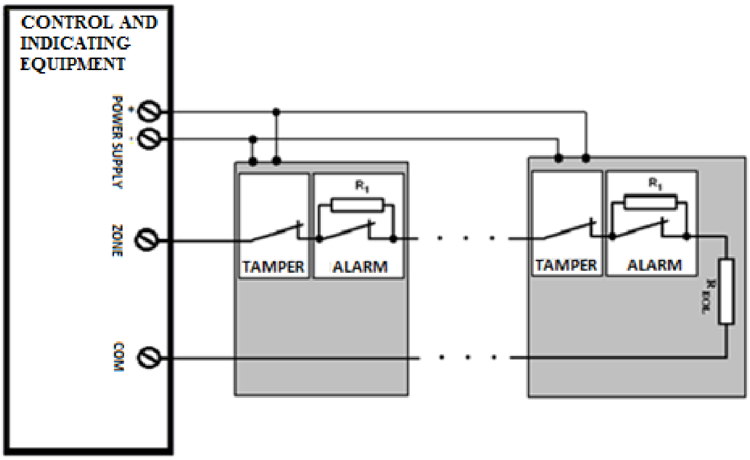


Fig. 1. Normally closed connection [2]

2Testing of Analog Intrusion and Hold-up Alarm Systems

As it was mentioned in the introduction, the system was designed for usage of standard analog security components with the exception of adding a processor with CAN bus to the control and indicating equipmentand to the each component. Then, the communication will be realized digitally and encrypted on the CAN bus by using created protocol. There is shown a method of connection of detector to the designed system in the figure 4.

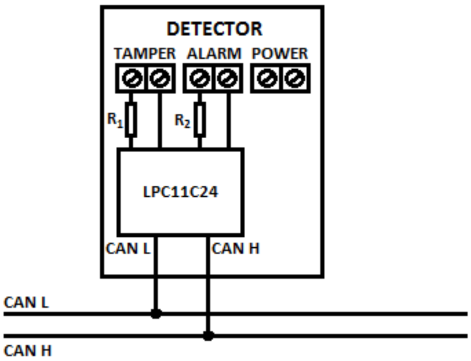


Fig. 2. Connection detector's in designed system

The processor has to be located inside the detector to eliminate the possibility of a sabotage. Contacts called "tamper" and "alarm" are connected by evaluating circuit to the processor LPC11C24, which is further connected to the CAN bus. In the case of switching off a contact, the alarm is transmitted to the processor LPC11C24, which send an alarm message to the CAN bus.

The figure 5 provides view of connection the CIE to the CAN bus.

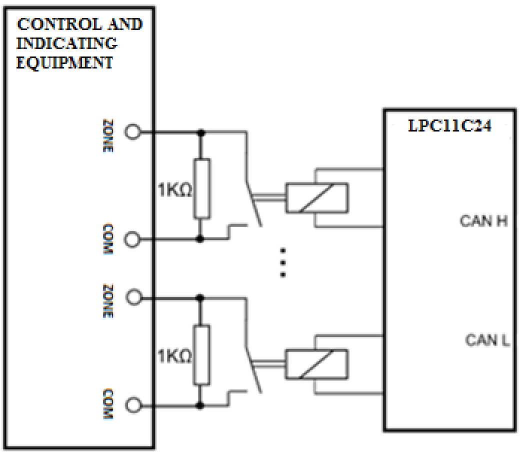


Fig. 3. Method of connection of the CIE to the bus

The circuits with closed resistor are connected to the CIE of intrusion and hold-up alarm system. Relay contacts are connected in parallel to the closed resistor. Switching relays is controlled by the processor LPC11C24, which is further attached to the CAN bus. The main purpose of the relay contacts lies in resistance change in the circuit connected to the CIE. This way it is possible to send an alarm message from CAN bus to the CIE. The processor LPC11C24, relays and circuits with closed resistor have to be placed inside the CIE of security system for the elimination of possible sabotage.

2.1 Transmission of Alarm Messages in the Designed System

In the figure 6 is depicted comprehensive view of the system.

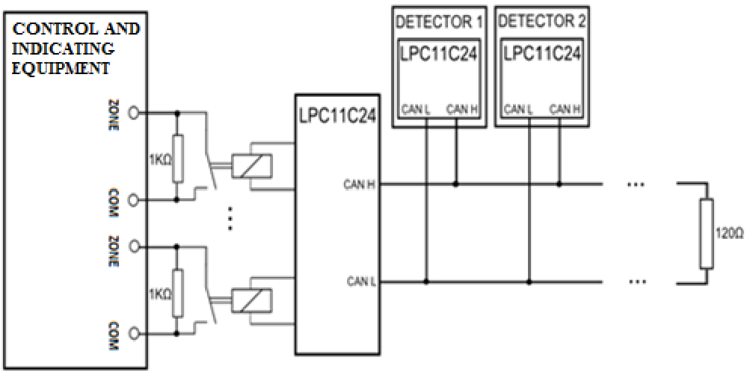


Fig. 4. Comprehensive view of the system

In the case of an intrusion of intruder into the protected object, an alarm message is sent to the processor LPC11C24, which is located inside the detector. The main purpose of mentioned processor lies in transmission of an alarm message to another processor LPC11C24, which is located inside of the control and indicating equipmentI&HAS.

Designed system was tested on development kits NXP – OM13036, 598 and EVAL NXP – OM13012-LPC11C24, LPCXPRESSO. The development kit NXP-OM13036, 598 – EVAL was designed for placement into the CIE and development kit NXP-OM13036 was designed for placement in the detector.

Used CAN bus was configured for speed 125kbit/s and a length of 400 m.

2.1 Communication Protocol

The main requirements on the designed protocol are security of data transmission, regular monitoring of all connected devices and possibility of system arming by the CAN bus.

Some basic information about the detector are stored in structure below.

```
typedefstruct {
    UINT8 ID;
    UINT8 Active;
    UINT8 Start_Key[24];
    UINT8 Key[24];
} Detector;
```

Each detector has its own ID for the network identification. There is also saved an information about the detector activation, encrypted key for start of the communication, and a key, from which are data encrypted during a communication.

"Start_Key" provides the basic encrypted key, which is used to start the communication in case of power failure or in case of data read failure caused by electromagnetic interference.

"Key" is used for detecting of currently used key. There is also possible to connect more than 50 detector to 1 CAN bus. Each detector changes its own encrypted key every 60 seconds.

2.2 The Main Features of the Proposed Protocol Incudes:

A) Regular monitoring of all connected devices every four seconds.

B) The detection of an alarm status and attempt to detector sabotage. If an alarm is activated, alarm message is processed by mentioned technique and further is alarm message saved to the flash memory including the information about the cause of the alarm.

C) A possibility of activation of multiple output devices already at each detector.

D) Exact identification of the place of an alarm. One of the main problem of analog systems lies in impossibility of exact identification of alarm place. If described system is used in practice, it is possible to locate the place of an alarm exactly by ID, which every detector uses for reporting to the bus.

E) Designed system can arm or disarm an intrusion and hold-up alarm system by code keyboard connected to the CAN bus.

F) Communication is encrypted by 3DES.

G) Protection against possible attack is minimalized by regular change of the encryption key every 60 seconds.

2.3 The Price Comparison

A price of each element in case of uses designed system is equal to price of analog detector increased by the processor LPC11C24 with CAN bus, which is added to each element. This can increase the price of each element by 8 €. Despite of mentioned necessity to add processor LPC11C24, the finally price of each element in case of used descripted system is approximately equal one-third the price of digital detector currently uses in I&HAS.

3Conclusion

This work illustrates the usage of CAN bus in analog intrusionand hold-up alarm systems. The designed system provides possible way, how to increase the protection against any sabotage and also shows, how to reduce the cost of digital communication in I&HAS.

The designed system combines the advantages of analog and digital communication in an intrusion and hold-up alarm systems.

Proposed system also provides an opportunity to choose from wide offer of analog detectors in comparison with limited selection of digital detectors.

The communication between components and a CIE of intrusion and hold up alarm system is digital and encrypted. Therefore, the created system provides better protection against sabotage than commonly used analog systems. One of the other benefits of described system lies in exact identification of the detector, which activated the alarm. Moreover the I&HAS system can be activated by the code keyboard connected to the CAN bus.

The described system is more expensive than commonly used analog intrusion and hold-up alarm systems, but less expensive than digital intrusion and hold-up alarm systems.

Acknowledgments. This work was supported by grant No. IGA/FAI/2014/020 from IGA (Internal Grant Agency) of Thomas Bata University in Zlin.

References

1. ČSN. *EN 50131-1 ed. 2.* Praha: Úřad pro technickou normalizaci, 2007, 40 s.
2. HANÁČEK, Adam. *Using Personal Computer as an Intruder Alarm System Control Unit.* Zlín, 2012. Diploma thesis. Tomas Bata University.
3. VOSS, Wilfried. *A Comprehensible Guide to Controller Area Network.* 2. vyd. Canada: Copperhill Media Corporation, 2005. ISBN 0976511606.
4. IBRAHIM, Dogan. *Controller Area Network Projects*. United Kingdom: Elektor International Media, 2011. ISBN 978-1-907920-04-2.
5. *Implementation of Controller Area Network (CAN) Bus*. Berlin: Springer Berlin Heidelberg, 2011. ISBN 978-3-642-18439-0.
6. *Understanding and Using the Controller Area Network Communication Protocol*. London: Springer Science Business Media, 2012. ISBN 978-1-4614-0313-5.
7. *Vehicle Test Data Visualization and Processing*. Prague, 2011. Diploma thesis. CZECH TECHNICAL UNIVERSITY IN PRAGUE.
8. SPURNÝ, František. *Controller Area Network*. Automatizace.1998, 41, 7, s. 397 - 400.
9. *Device for transmitting messages on CANbus*. Plzen, 2012. Diploma thesis. University of West Bohemia.
10. *Measurement system with CAN interface*. Plzen, 2013. Diploma thesis. University of West Bohemia.

On Different Approaches to Human Body Movement Analysis

Kateřina Sulovská
Department of Security Engineering
Tomas Bata University in Zlín, Faculty of Applied Informatics
Nám. T. G. Masaryka 5555, 760 01 Zlín, Czech Republic
{sulovska}@fai.utb.cz

Abstract. Biomechanics of human gait belongs to the biometric recognition systems for identification/recognition of people for various security applications. The method itself is not new, but its utilization in real world is still not in its maximum, especially due to a time-consuming processing and a demand for reliable algorithms. We focus on unique manifestation of gait patterns and their equability under different conditions of walk in our basic research. As the movement of each selected segment of human body is generating curves in space, the basic statistical methods cannot be utilized as they do not have predicative value due to incorrectness of used principles on curves analysis. Thus, we incorporated the functional analysis to obtain proper results.

Keywords: VICON, gait, functional analysis, biometrics, pattern recognition, ANOVA, statistics.

1 Introduction

Analysing the human gait is very time demanding area not only from the side of physicians, but from the overall scientific point of view. As the human gait is very variable between each point on the one human body, but said to be consistent and invariant between persons its correct analysis is necessary. When dealing with analysis of human gait for security purposes, the result of such analyses must be as precise as possible as utilization of incorrect biometrics (in our case gait patterns) may cause problems during and after implementation into praxis.

Until now, the most attention was dedicated to development of algorithms for automated gait recognition software. The studies of gait patterns changes were done mainly for the purposes of rehabilitation, proper treatment of injuries and health problems and monitoring the health states of patients after strokes, paralyses, surgeries, etc. Unfortunately, only few studies or theses dealt with changes of gait patterns during various conditions. Those studies include: changes in gait during menstrual cycle [1], between dressed and light clad participants [2], genders, age, race, acoustics of gait on different surfaces [3,4,5], changes during various speeds [6], influence of rehabilitation tools [7], diseases [8], rehabilitation after diseases [9], changes in elders [10], effect of shoes [11], behaviours during sports [12], effect of poor sight [13], therapy effects [14], and analyses like electromyography [15], comparison of tools [16], new equipment [17], variability for biometric purposes [18], and many other (e. g. testing robots, adapting algorithms to obtain higher functionality of software solutions).

These experiments more or less proved that the gait patterns are personally unique and therefore can be used as biometrics; although it is not yet clearhow useful gait can be for biometrics in larger scale. These studies can be divided into two main categories – sensor-based (especially medical researches) and video-based (most often silhouette or model based image testing). When talking about classical statistical analyses, the most frequently analyses employed are well-known parametric tests,TuckeyHSD test, correlation factor-coefficients, Euclidean distances, multivariate data analysis, Fourier transformations and ANOVA. These statistical tests are used in majority of the researches providing acceptable results. A different approach contains statistical evaluation by functional analysis as functional data are often multivariate in a different sense. The basic philosophy of functional data analysis is to consider each function a single entity. Body movement sets of functions (curves in datasets) are periodic and functional analysis can serve us with smooth functions, their interactions, highlighted various characteristics, exploration of overall variability in functional data, comparison of data sets with respect to certain types of variations and explanation of variations in an outcome or variable [19]. The functional analysis can therefore answer better the requirements for proper gait data analysis.

This paper introduces compendium of different approaches to gait analysis based on curves (functions) gained from a 3D motion capture systems with markers on chosen body parts and participants passing the “catwalk” (corridor). The Methods section also describes some requirements for measuring on such system to avoid unnecessary problems with processing the data statistically.

2 Methods

2.1 Participants and Data Acquisition

The minimal amount of participants for security and other purpose analyses are 10, ideal number is 25+. However, this number is not very sufficient from the statistical side of view. The problem with higher amount of people in dataset is a time demandingness of processing acquired data. If we talk about analyses for security purposes, participants should have no serious pathology, injury or any posttraumatic history in their musculoskeletal system prior to the measurement. On the other hand, when measuring clinical trials for condition or health analyses, it is good to have a template gait (or body segment) functions that are from a healthy people to have contrast to the one with issues.

Apart from amount of participants in our trials, it is also necessary to calculate with number of double-steps in one trial. The minimal number is, according to [21], 10 cycles of single double-steps. To obtain this amount, the minimum trials to go is 10, but our recommendation is to do at least 20 trials, as some of the markers’ functions can be missing and/or with errors, and it is not possible to expect which ones and when will do so during the single experiment. We must also bear in mind that the possibility of inapplicability of some participants occurs, even though this error rate is very low.

Another parameter that must be taken into account is the shape of monitored area/corridor and the cameras disposition in the space. Cameras should be disposed equallyto the movement recorded to be able to depict all of markers continually as they move in the space. Fig. 1 shows some of the ideal camera set-up.

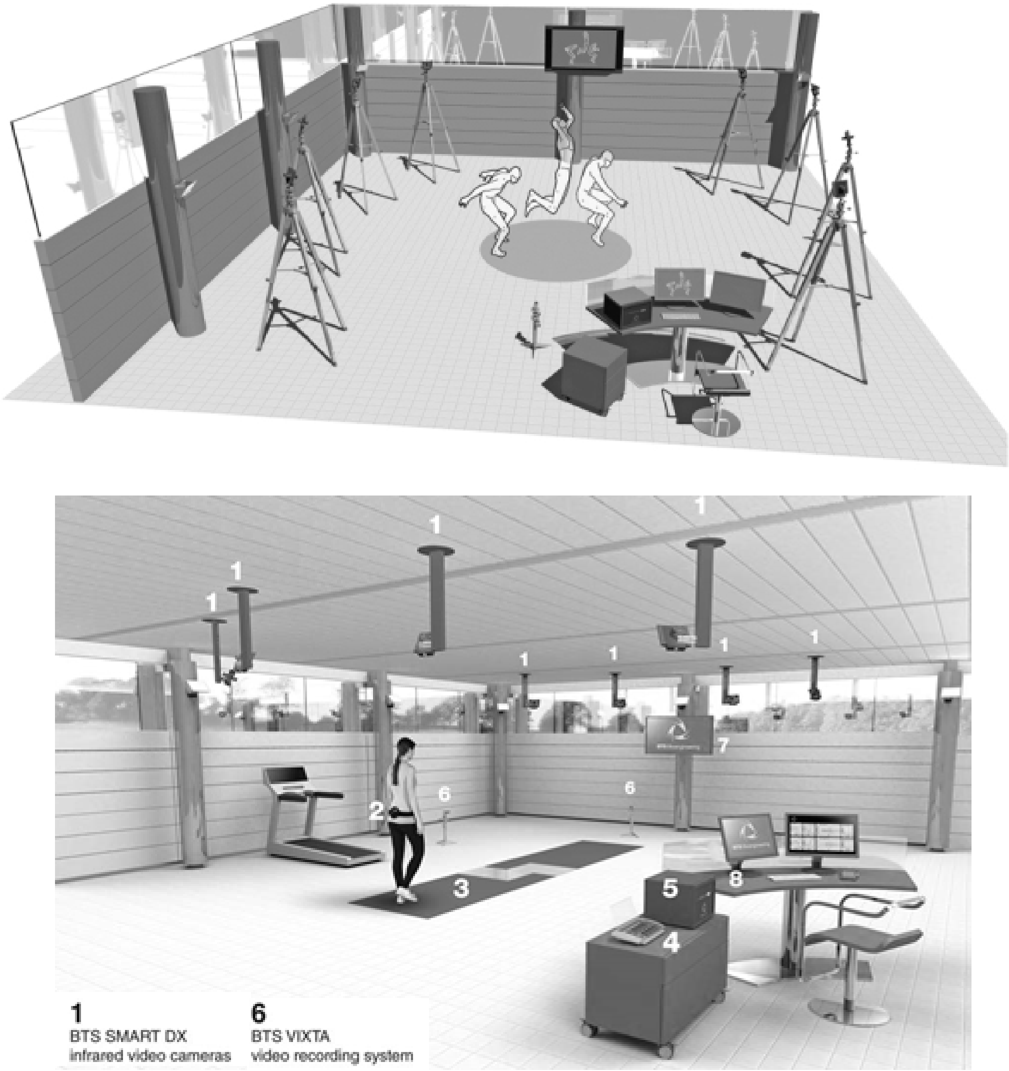


Fig. 1. Examples of ideal indoor camera set-up [31]

The most utilized systems for 3D motion capture are BTS SMART, VICON, and QUALISYS. The movement is captured by 2 - 16 cameras with infrared filters detecting passive markers placed on human body in the area. For the self-analysis in security, a double-step (one stride cycle length) is usually chosen, although in some cases two or three cycles are captured. The height of cameras is between 1.2 – 2.5 m depending on the focused markers, and the frequency should be minimally120 fps.

The commonly used models includes more than 35 markers (ø 3- 25 mm depending on our research intentions) placed on anatomically significant places (based on walk analysis protocols: Davis, Helen Hayes, Newington, Lamb, Cast, Foot Model), position of markers used for this part of research can be seen in Fig. 2. Those parts, respectively their widths/lengths together with the basic anthropometric data are defined before the beginning of experiments for accurate calculations.

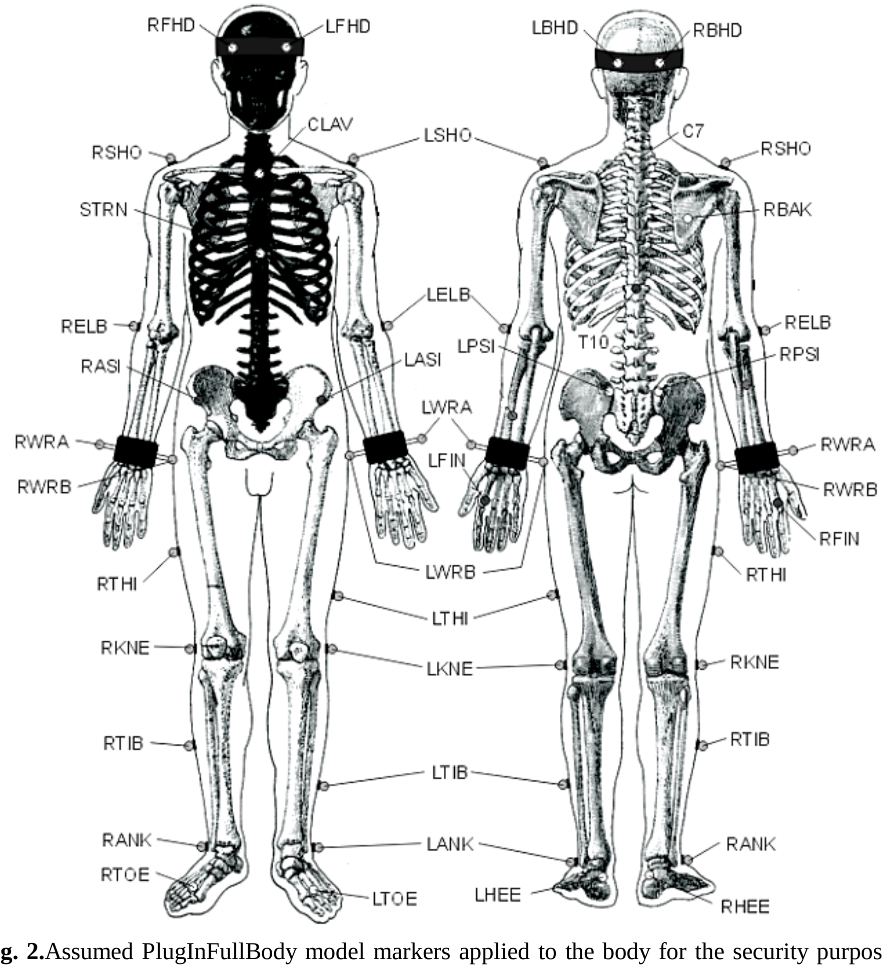


Fig. 2. Assumed PlugInFullBody model markers applied to the body for the security purposes measurements [20]

2.2 Data Analysis

Recordings of pass-troughs are rendered, smoothed, filtered, calculated and if required normalized by the software usually enclosed to the system. The initial contact and swing phase of stride cycle is detected where it is possible according to the force plates, or they can be found in the exported spreadsheets through heel markers surface contacts in other cases. All measured data can be converted into *.CSV and similarformats to be used for further calculations/testing in the MS Excel, statistical software (STATISTICA, R, SAS/STAT, etc.),Matlab or others.

2.3 Functional Analysis [19]

This chapter will briefly introduce some basic approaches to functional analysis, which is highly suitable for gait pattern analysis.

The record of the function x_i might consist of $n_i$pairs (t_{ij}, y_{ij}), $j = 1,\dots,n_{i,}$ and takes place separately or independently for each record i.

The sampling rate or resolution of the raw data shows us what is possible in the way of the functional data analysis. This can be displayed by the curvature of a function, which is usually measured by the size of second derivative. The higher the curvature, the better estimation of the function. The sufficient sampling rate for gait data is c. 20 values per cycle. Unfortunately, too high rate may cause serious problems.

$$|D^2x(t)| \text{ or } [D^2x(t)]^2 \tag{1}$$

The first step in functional analysis is the smoothing and interpolation of the data. If the data are assumed to be errorless, the process is called interpolation, but in our case we suppose some observational errors that need removing, so the conversion from discrete data to functions may involve smoothing to function x_i witch values $x_i(t)$ computable for any desired argument value t. This can be done by roughness penalty smoothing method or by using smoothing splines.

One of the next steps is displaying the result of analysis, where different displays of data bring different features of interest and information. One of the possibilities is also to plot pairs of derivatives to get the relationship between derivatives: the exponential function

$$f(t) = C_1 + C_2e^{\alpha t} \tag{2}$$

satisfies the differential equation

$$Df = -\alpha(f - C_1) \tag{3}$$

and the sinusoid

$$f(t) = C_1 + C_2 \sin\,[\omega(t - \tau)] \tag{4}$$

with phase constant τ satisfies

$$D^2f = -\omega^2(f - C_1) \tag{5}$$

Plotting the 1st and 2ndderivative against the function value explores the possibility of demonstrating a linear relationship corresponding to one of these differential equations. Plotting the higher derivative against lower is more informative due to departures from linearity and exposure of effects that are cannot be easily seen in original function.

The classical summary statistics for univariate data applies equally for functional data. The mean function with values

$$\bar{x}(t) = N^{-1} \sum_{i=1}^{N} x_i\,(t) \qquad (6)$$

is the average of the functions point-wise across replications. The variance function *var* is then

$$var_X(t) = (N-1)^{-1} \sum_{i=1}^{N} [x_i(t) - \bar{x}(t)]^2 \qquad (7)$$

and the standard deviation function is

$$\sqrt{var_x(t)} \qquad (8)$$

The covariance function summarizes the dependence of records across different argument values, and is computed for all t_1 and t_2

$$cov_x(t_1, t_2) = (N-1)^{-1} \sum_{i=1}^{N} \{x_i(t_1) - \bar{x}(t_1)\}\{x_i(t_2) - \bar{x}(t_2)\} \qquad (9)$$

The associated correlation function is

$$corr_x(t_1 - t_2) = \frac{cov_x(t_1,t_2)}{\sqrt{var_x(t_1) var_x(t_2)}} \qquad (10)$$

If we had pairs of observed function (x_i, y_i) their reciprocal dependency can be quantified by the cross-covariance function

$$cov_{X,Y}(t_1, t_2) = (N-1)^{-1} \sum_{i=1}^{N} \{x_i(t_1) - \bar{x}(t_1)\}\,\{y_i(t_2) - \bar{y}(t_2)\} \qquad (11)$$

or the cross-correlation function

$$corr_{X,Y}(t_1, t_2) = \frac{cov_{X,Y}(t_1,t_2)}{\sqrt{var_X(t_1) var_Y(t_2)}} \qquad (12)$$

The Fourier basis system for periodic data is provided by the Fourier series

$$\hat{x}(t) = c_0 + c_1 sin\omega t + c_2 cos\omega t + c_3 sin\omega t + c_4 cos\omega t + \cdots \qquad (13)$$

defined by the basis $\emptyset_1(t) = 1$, $\emptyset_{2r-1}(t) = sinr\omega t$ and $\emptyset_{2r}(t) = cosr\omega t$, where ω determines $2\pi/\omega$.

Functional linear models investigate the way in which variability in observed data can be accounted for by other known observed variables. They can be all placed within the framework of the general linear model

$$y = \boldsymbol{Z}\beta + \epsilon \qquad (14)$$

where y is typically a vector of observations, β is a parameter vector, **Z** is a matrix defining a linear transformation from parameter to observation space, and ε is an error vector with mean zero.

The principal component analysis for functional data started with combining a weight vector β with a data vector x to calculate the inner product

$$\beta' x = \sum_j \beta_j x_j \qquad (15)$$

When β and x are functions *β(s)* and *x(s)*, summations over *j* are replaced by integrations over *s* to define the inner product

$$\int \beta x = \int \beta(s) x(s) ds \qquad (16)$$

Using (16) the principal component scores corresponding to weight β are now

$$f_i = \int \beta x_i = \int \beta(s) x_i(s) ds \qquad (17)$$

by choosing the ξ_1(s), following equation is maximized

$$N^{-1} \sum_i f_{i1}^2 = N^{-1} \sum_i (\int \xi_1 x_i)^2 \qquad (18)$$

subject to the continuous analogue of the unit sum of squares constraint

$$\int \xi_1(s)^2\, ds = 1. \qquad (19)$$

3 Results and Discussion

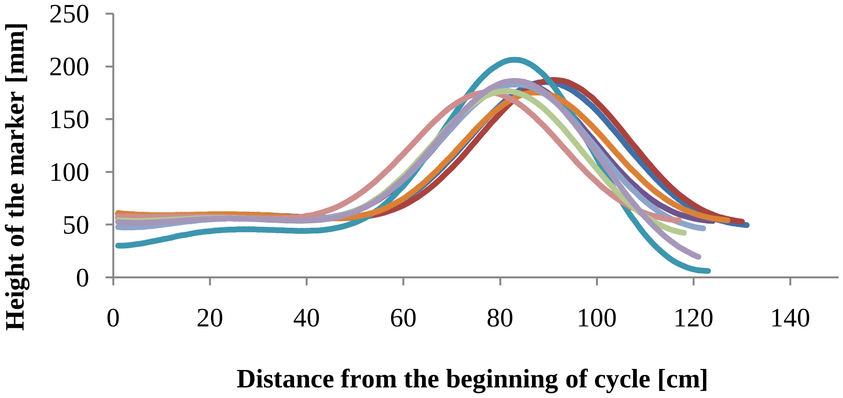


Fig. 3. Correct trajectories of left ankleof one person during normal gait cycle[author]

In our preliminary research [32], we discuss the differences and resemblance of 11 people (5 women, 6 men; all healthy) during eight various conditions. We used classical statistical methods that are used across the literature. Results were according to our expectations, though it was shown that the gait differs from the average in extreme conditions (too slow and fast walking, first three passages after workout) and the markers can be interchanged (even between men and women) or shifted in a way that may be in some cases positions of marker above or below.

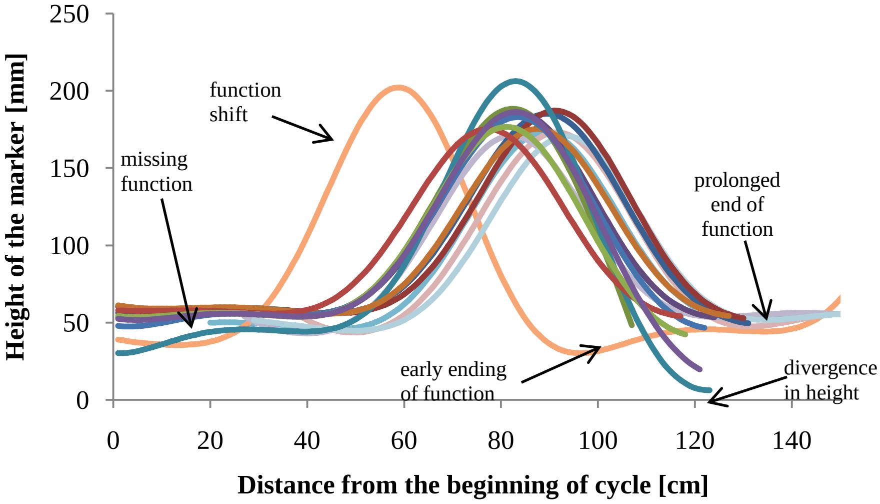


Fig. 4. Trajectories of left ankle with errors and missing parts of functions of one person during normal gait cycle [author]

However, some issues during data processing occur and therefore we were unable to use the rest of our data (another 10 people), as they contain serious errors (Fig. 4-5) or missing marker functions, or missing bigger parts of marker functions in cycles (e.g. the marker C7 is in 98 % of cases ill-structured; in some participants, there are only two functions of toe marker in men 1 and normal gait as the marker heights are shifted to the level of hips). This happened even though we were very precise during marker placing and 3D data acquisition. These errors occur not only in dataset with distances, but also in datasets with angular and time data. Most of these errors are impossible to be fixed manually. What is more, the most unexpected issue is that the errors occur in full body parts movements where all other markers are correct, not only in partial movements where we occasionally expected them. All of these functions were exempted from the testing dataset available for further analysing. Nevertheless, some errors in functions also arise due to extreme walking conditions and are therefore in such cases retained in datasets.

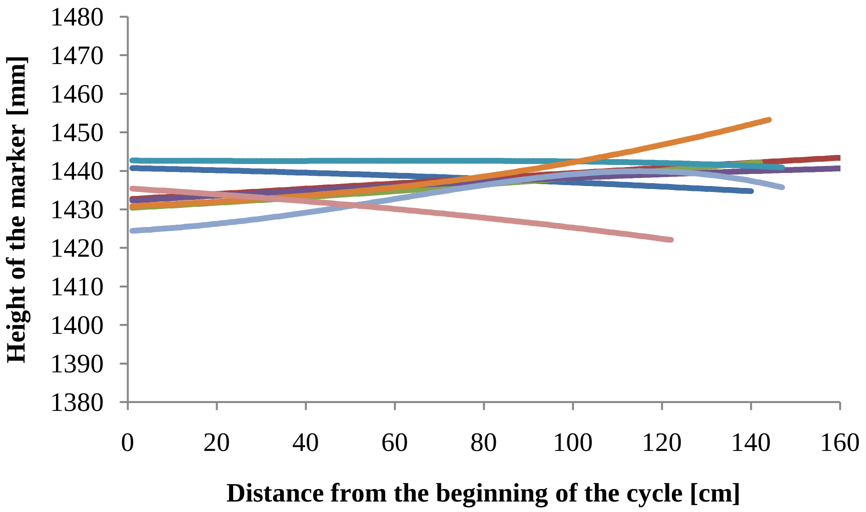


Fig. 5. Trajectories of C7with ill-structured functionsof one person during normal gaitcycle [author]

Some of these problems probably arose from a software failure of the VICON mocap software. However, most of the errors in functions are hardly explicable. Trials where a marker was unstuck (3 cases) or the person was not walking as planned (1 case) were removed. In two cases, data are entirely unavailable as the participants did not hit the force plates and the software solution was unable to build up the model. Therefore, we would like to make proposal for consequent measurement:

- each person undergo at least 30 trials (including hitting the force plates) to each 7 correct trials,
- the corridor (space) should be approx. 8 meters long,
- markers for people that sweat a lot must be fixed by highly sticky tapes (probably assembling ones),

- an extra marker stacked in the middle of a forehead and both earlobes (for security purposes recognition),
- processing data in mocap software immediately after the daily measurement to get the necessary feedback and if possible re-measure needed number of trials.

4 Conclusion

The possible utilization of the gait analysis and recognition is great. The gait analysis has its place in many parts of our lives beginning with the biomechanics and ending with the field of virtual reality. The time saved by tests made in the 3D environment is invaluable asthe 3D gait analysis can save time and money expended on redundant surgeries, prevent from injuries in many sports, including people as well as animals.

The contribution of gait as a biometrics may be after obtaining data set of the gait patterns big enough invaluable.However, after big data collection of gait patterns, it could be said whether the successful gait recognition for security purposes in great extent is possible or not. So far the variability of the gait appears to be big enough, but further testing with a greater amount of people under different conditions is necessary.

The future may contain the biometric recognition based on the gait analysis, where ill, injured or endangered persons will be detected automatically by a remote surveillance; and violators, ambushers, terrorists and other suspects will be detected before they will have an opportunity to harm or damage protected interests. Such future could have, on the other hand, some disadvantages – mistaken identity, falsely accused people, lack of freedom in some way, protests against such surveillance, and many more. It will be necessary to consider all the pros and cons[25], public opinions and overall morale of the population in the country. We must always bear in mind that no system is perfect and everything is exploitable, even though it was originally intended for a good thing.

Our further research focuses on gait patterns analyses by means of functional analysistogether with mixed models to obtain accurate results that will be used not only as another resource for assessment of applicability/inapplicability of gait as a biometrics, but will be also used in further security projects at our university dealing with marker-free video recognition. The data will not be chosen by whole body part complex movement, but will be selected separately to derive as much correct functions as possible for accurate functional analysis. Results of these analyses will be published to make available knowledge arising from direct application of these analyses to broad public dealing with gait patterns recognition and to show their awaited benefits.

Acknowledgments. This work was supported by the Internal Grant Agency at Tomas Bata University in Zlín, project No. IGA/FAI/2014/001, by the European Regional Development Fund under the Project CEBIA-Tech No. CZ.1.05/2.1.00/03.0089. KS. would like to thank 21 volunteers for their participation in experimental measurements in laboratory. Authors KS.and MA. thank Mr. Jan Jadrný and prof. Jan Poul from the University Hospital Brno, Children’s Medical Centre, Gait Lab for providing the VICON MoCap system and helping with the experimental part of the research in terms of data acquisition.

References

1. Clark, R. A., Bartold, S., and Bryant, A. L.:Tibial acceleration variability during consecutive gait cycles is influenced by the menstrual cycle. Clinical Biomechanics, Volume 25, Issue 6, Pages 557 – 562 (2010).
2. Théveniau, N., Boisgontier, M. P., Varieras, S. and Olivier, I.: The effects of clothes on independent walking in toddlers. Gait & Posture, Volume 39, Issue 1, January 2014, Pages 659-661 (2014).
3. Abadi, F. H., Muhamad, T. A. and Salamuddin, N.: Energy Expenditure through Walking: Meta Analysis on Gender and Age.Procedia Social and Behavioral Sciences 7(C) 512 – 521 (2010).
4. Alpert, D. T. and Allen, M.: Acoustic Gait Recognition on a Staircase. World Automation Congress (2010)
5. Boyer, K. A., Beaupre, G. S. and Andriacchi, P.: Gender differences exist in the hip joint moments of healthy older walkers. Journal of Biomechanics 41, 3360 – 3365 (2008).
6. Liu, Y., Lu, K., Yan, S., Sun, M., Lester, D.K. and Zhang, K.: Gait phase varies over velocities.Gait & Posture, Volume 39, Issue 2, February 2014, Pages 756-760 (2014).
7. Magagnin, V., Bo, I., Turiel, M., Fornari, M., Caiani, E.G. and Porta, A.: Effect of robot-driven gait orthosis treadmill training on the autonomic response in rehabilitation-responsive stroke and cervical spondylotic myelopathy patients. Gait & Posture, Volume 32, Issue 2, June 2010, Pages 199-204 (2010).
8. Lemos, R., Pereira, A., Dias, J. and Geada, M.: Impact of foot reconstruction surgery on the daily life of patients with cerebrovascular accident sequelae. Revista Española de CirugíaOrtopédica y Traumatología (English Edition), Volume 56, Issue 2, March–April 2012, Pages 98-103 (2012).
9. Rosenbaum, D., Macri, F., Lupselo, F.S. and Preis, O.C.: Gait and function as tools for the assessment of francture repair-The role of movement analysis for the assessment of fracture healing. Injury, Volume 45, Supplement 2, June 2014, Pages S39-S43 (2014).
10. Dibble, L.E., Nicholson, D.E., Shultz, B., MacWilliams, B.A., Marcus, R.L. and Moncur, C.: Sensory cueing effects on maximal speed gait initiation in persons with Parkinson's disease and healthy elders. Gait & Posture, Volume 19, Issue 3, June 2004, Pages 215-225 (2004).
11. Doi, T., Yamaguchi, R., Asai, T., Komatsu, M., Makiura, D., Shimamura, M., Hirata, S., Ando, H., and Kurosaka, M., “The effects of shoe fit on gait in community-dwelling older adults”, Gait & Posture 32, 274 – 278 (2010).
12. Wasik, J.: Kinematic analysis of the side kick in Taekwon-do.Acta of Bioengineering and Biomechanics, Vol. 13, No. 4 (2011).
13. Helbostad, J. L., Vereijken, B., Hesseberg, K. and Sletvold, O.: Altered vision destabilizes gait in older persons. Gait & Posture 30, 233 – 238 (2009).
14. Guner, S. and Inanici, F.: Yoga therapy and ambulatory multriple sclerosis Assessment of gait analysis parameters, fatigue and balance. Journal of Bodywork and Movement Therapies, In Press, Corrected Proof, Available online 16 April 2014 (2014).
15. Chang, W.-N., Schuyler Lipton, J., Tsirikos, A.I. and Miller, F.: Kinesiological surface electromyography in normal children: Range of normal activity and pattern analysis.

Journal of Electromyography and Kinesiology, Volume 17, Issue 4, August 2007, Pages 437-445 (2007).

16. Benedetti, M.G., Merlo, A. and Leardini, A.: Inter-laboratory consistency of gait analysis measurements. Gait & Posture, Volume 38, Issue 4, September 2013, Pages 934-939 (2013).
17. Carse, B., Meadows, B., Bowers, R. and Rowe, P.: Affordable clinical gait analysis: An assessment of the marker tracking accuracy of a new low-cost optical 3D motion analysis system. Physiotherapy, Volume 99, Issue 4, December 2013, Pages 347-351 (2013).
18. Collins, T.D., Ghoussayni, S.N., Ewins, D.J. and Kent, J.A.: A six degrees-of-freedom marker set for gait analysis: Repeatability and comparison with a modified Helen Hayes set. Gait & Posture, Volume 30, Issue 2, August 2009, Pages 173-180 (2009).
19. Ramsay, J. O., Silverman, B. W.: Functional Data Analysis. 2nd ed., Springer Science+Business Media, Inc., New York, 2005, 431 pgs., ISBN 978-0387-40080-8(2005).
20. VICON: Vicon’s plug-in-gait marker placement. [Online]. Available: http://www.idmil.org/mocap/Plug-in-Gait+Marker+Placement.pdf
21. Dolná, Z.:Analýza variability parametrovchôdze a možnostijejvyužitia v biometrike. Dissertation Thesis, Technical University Košice (2010), in Slovak language.
22. Šimšík, D., Porada, V., et al.:Analýzapohybučlovekapriidentifikáciiosôb v kriminalistike.Edíciavedeckejaodbornejliteratúry, StrojnickáfakultaTU v Košiciach, Košice, ISBN 978-80-553-0023-8, (2008), in Slovak language.
23. Majerník, J. and Šimšík, D.: Marker-free Analysis of Human Gait.Lékař a technika, Vol. 37, No 1, 23 – 27 (2007).
24. Zhang, R., Vogler, Ch. and Metaxas, D.: Human gait recognition at sagittal plane. Image and Vision Computing, Volume 25, Issue 3, March 2007, Pages 321-330 (2007).
25. Silveira J Jr., J. C. S., Musse, R. S. and Jung, C. R.: Crowd Analysis Using Computer Vision Techniques. IEEE Signal Processing Magazine, ISSN 1053-5888 (2010).
26. Ikizler, N.: Understanding Human Motion: Recognition and Retrieval of Human Activities. Dissertation Thesis, Bilkent University (2008).
27. Murray, M.: Gait as a total pattern of movement. Amer. J. Phys. Med., vol. 46, no. 1, pp. 290–332, (1967).
28. Whittle,M.W.: Clinical gait analysis: A review. Human Movement, Sci., vol. 15, pp. 369–387, Jun. 1996, (1996).
29. Hooker, G.: Functional Data Analysis: A Short Course. International Workshop on Statistical Modeling, Glasgow Unversity, July 4, 2010 (2010).
30. Friedman, J.: Functional data analysis. Course, MACCS, Maquarie University, November 2010, online, available: http://curiousjason.com/talks/Analysis_of_arm_movement_data_part_3.pdf
31. BTS Bioengineering. BTS SMART DX &BTSGAITLABProductBrochures. Available: http://www.btsbioengineering.com/
32. Sulovská, K., Bělašková, S., and Adámek, M.: Gait Patterns for Crime Fighting: Statistical Evaluation. In Burgess, Douglas; Owen, Gari; Zamboni, Roberto; Proceedings of SPIE Vol. 8901, Optics and Photonics for Counterterrorism, Crime Fighting and Defence IX; and Optical Materials and Biomaterials in Security and Defence Systems Technology X. Bellingham : SPIE - International Society for Optical Engineering, 2013, s. \'89010G-1\'-\'89010G-7\'. ISSN 0277-786X. ISBN 978-081949770-3 (2013).

Intelligent Video Surveillance System Evaluation Dataset Proposal Methodology

Jiri Sevcik

Tomas Bata University in Zlin, Faculty of Applied Informatics, Department of Security Engineering, Nad Stráněmi 4511, 760 05 Zlín, Czech Republic
jsevcik@fai.utb.cz;

Abstract. There are several approaches how to evaluated effectiveness of Intelligent Video Surveillance System. General Intelligent Video analytics Algorithms evaluation techniques review is contained in the first part of this research paper. Moreover, brief analysis of recent methods and unique evaluation dataset proposal methodology are provided. Finally, detailed procedure of developing dataset annotation is described and applied.

Keywords: Intelligent Video Surveillance System, Evaluation, Algorithms, Annotation techniques, Methodology;

1 Introduction

Intelligent Video Surveillance Systems (IVSS) are dynamically evolving field, probably for their global usefulness within the wide range of real-world applications. Manufacture, traffic regulation or security belongs among typical segments where IVSS are utilized. All of these applications are based on recent possibilities of video analytics functions. Evaluation of semantic factors readable from the scene, an identification and classification of objects, measurement of their particular parameters, are the most often utilized preferences of high quality IVSS [1].

The level of IVSS quality could be evaluated through several specific methods, the most used is mapping [2]. This technique is in principle comparison evaluating between real semantic factor of the particular scene and the information generated by video-analytics algorithm. Several groups of evaluating video sequences were designed in order to increase effectiveness of video analytics algorithms. Moreover, there are relatively great amount of conditions, which should be taken into account by the designer of the system. Probably, one of the most important factors is the photogrammetric calibration of the sensing element, which is in this case surveillance camera. Calibration is defined by its intrinsic and extrinsic parameter. Intrinsic is described as determination of sensing element parameters (focal length, resolution, and frame rate) [3]. On the other hand, the extrinsic calibration disserts on appropriate selection of parameters related to camera position and orientation within the coordinates [4].

The unique evaluation dataset is proposed within the paper and IVSS evaluation dataset methodology is designed. Firstly, the evaluation technique used is described in detail. In next chapter the annotation design process is explained. The methodology is then proposed as a solution of the problem formulated.

2 Algorithm effectiveness evaluation procedure

Standardized process of IVSS evaluation, which is utilized in the biggest percentage of evaluation methodologies, is based on relation of evaluation video databases annotations on information generated by Video Content Analysis (VCA) and Video Event Understanding (VEU) algorithms. On the basis of established metrics is possible to evaluate IVSS´s intelligent functionality layer. Visualization of this process is illustrated in Fig. 1.

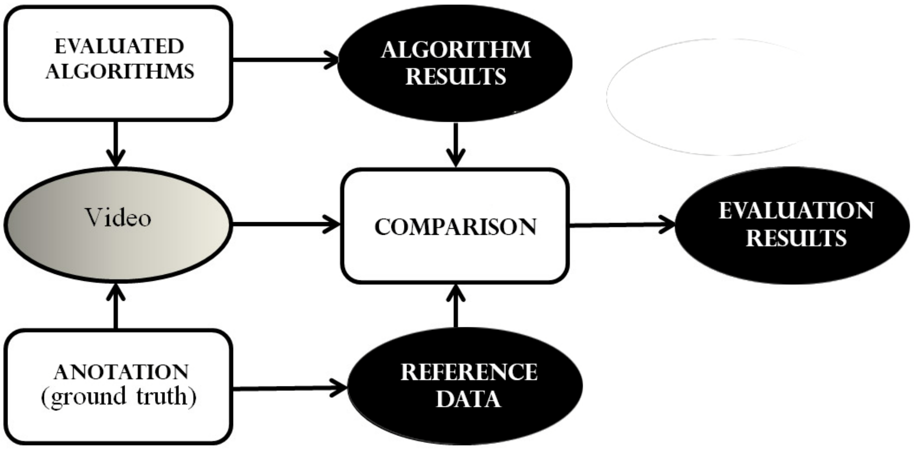


Figure 1: IVSS evaluation procedure

2.1 Annotation tools

Real parameters descriptions of particular video-sequences are provided through evaluation video-database annotation. The annotation design process should be detailed as much as possible what makes it relatively difficult and time consuming. Description of the object in the scene, its marking through bordering frames is also one of the key goals of annotation. Moreover, adequate parameters have to be assigned to particular objects (velocity, color, position etc.). Description of events which are happening in the scene is necessary for the purposes of VEU evaluation. There are several annotation development methods:

- Manual acquisition (the most used method recently): The annotation is developed by the observer with utilization of adequate tools. This approach is not fully objective, because the annotation created by two observers never produces the same result.
- Semi-automatic acquisition: Basic annotation is realized through standardized analytics algorithms and results are then repressed by human corrector. The final annotation is then developed on the basis on corrected one.
- Detectors and meters utilization: annotation data gathering is realized through detectors and meters. Common is utilization of position detectors, distance detectors or infrared barriers. This approach is very complex, however it is impossible to make data gathering process full automatic. That is why it is necessary to combine it with other techniques mentioned above.
- Video data synthesis: Evaluation video databases are created by utilization of image synthesis or by augmentative reality technology. The annotation is generated continuously within the video sequence acquisition process and it strictly corresponds with real parameters of object located in the scene. Nonetheless, recently it is unusable in real testing [5].

3 Evaluation video sequence design

Detailed documentation of evaluation video sequence design procedure realization. Main contribution is represented in recommended procedure of evaluation video sequence design. Dataset instrument Video Image Annotation Tool was utilized for annotation acquisition.

Corridor was chosen as a representative scene for evaluation video sequence application. The length of corridor is approximately 10 meters, width 4,5 meters and 3,5 meters high.

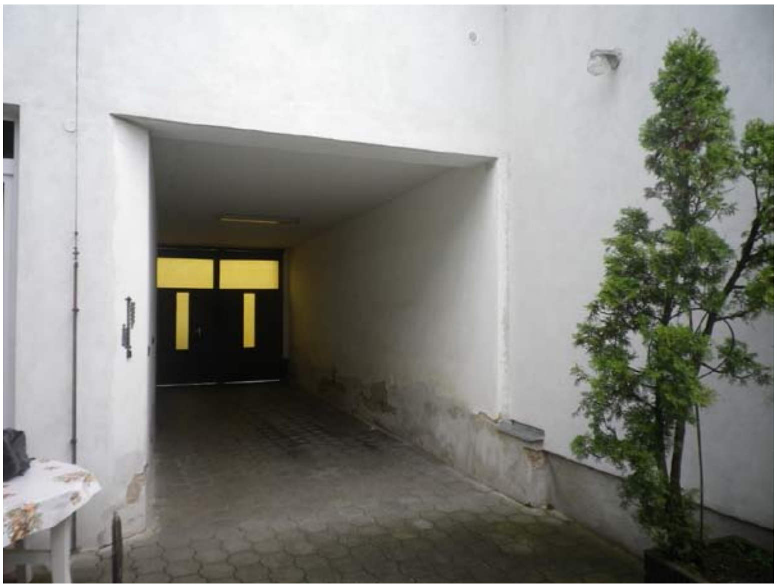


Figure 2: Corridor scene

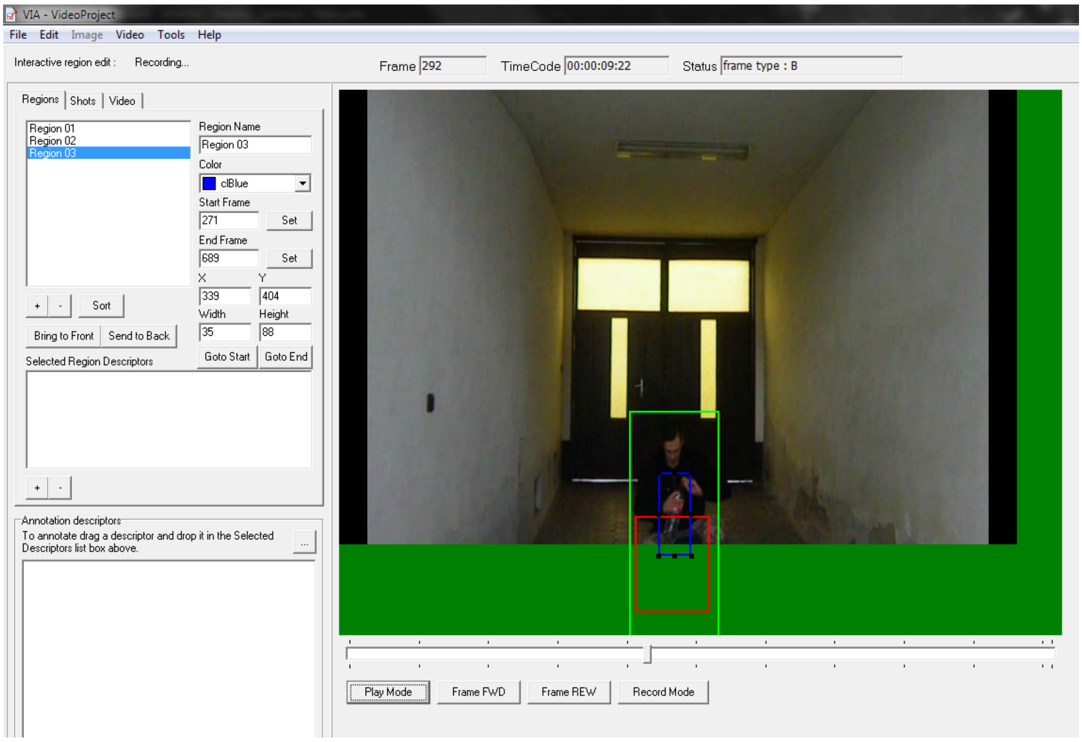
Following action were used as a content of evaluation video sequences:

- individual person crosscut,
- run through the scene,
- run and jump within the scene,
- walk and do up shoelace,
- walk and backpack searching,
- walk and jacket take off,
- walk and telephoning.

All of activities are shot under various conditions:

- day light,
- artificial light.

The axis of movement and camera axis are parallels within all shot actions.



Interactive region edit : Recording...

Frame 292

TimeCode 00:00:09:22

Status frame type : B

Region Name: Region 03

Color: clBlue

Start Frame: 271

End Frame: 689

X: 339

Y: 404

Width: 35

Height: 88

Selected Region Descriptors

Annotation descriptors

To annotate drag a descriptor and drop it in the Selected Descriptors list box above.

Figure 3: Three objects marked within the VIA tool

Annotation of images and video sequences in MPEG format is supported by VIA tool. Final project is exportable in two formats:

- ANP – its primary format of VIA tool, which contains video and register of all changes in parameters of objects,
- XML – it is possible to record only changes in objects parameters without the video. This format is appropriate for consequent application of evaluation metrics for video sequences from other tools, which also supporting it.

4 Dataset documentation

Table 1: Evaluation video sequences description table

Dataset information	
Identifications	
Author:	Lukas Gajdusek
Institute:	Faculty of applied informatics, Tomas Bata University in Zlín
Country:	Czech Republic
Year of publication:	2014
Descriptive document:	Appendix 1, extended version
Primal objectives	
Main objectives:	Video sequence design procedure verification.
	Modelling of particular situations within corridor.
	Dataset developing guideline design.
Examples of video sequences:	
Context	
Type of scene:	Singular
Lighting conditions:	Day light and Artificial light.
Type of background:	Static scene background.
Number of persons:	One person in the scene.
Number of videos:	Completely 14 videos
Number of simulated actions:	7 different actions
Ground Truth (annotation)	
Available in	AMP and XML format.

4 Conclusion

There are many aspects which have influential magnitude on IVSS quality. One of the most recent problems is the most sophisticated level, the intelligence of whole system. A lot of research papers have been solving the problem of the IVSS´s intelligence effectiveness, even the quality of whole systems. It is necessary to take this image functional level into account even before the installation of the IVSS and to consider all conditions and circumstances, which have noticeable influence of its functionality. The unique methodology related to preparation of IVSS evaluation dataset is designed in this paper. More detailed description of the process included the necessary appendixes will be provided in extended version.

References

1. ŠEVČÍK, Ing. Jiří. Metody testování funkčních vlastností vybraných kategorií prvků poplachových systémů. Zlín, 2013. Pojednání o disertační práci ke státní doktorské zkoušce. Univerzita Tomáše Bati, FAI.
2. Aleksandra Karimaa (2011). Efficient Video Surveillance: Performance Evaluation in Distributed Video Surveillance Systems, Video Surveillance, Prof. Weiyao Lin (Ed.), ISBN: 978-953-307-436-8, InTech, DOI: 10.5772/15259.
3. Du, F., Brady, M.,1993.Self Calibration of the Intrinsic Parameters of Cameras for Active Vision Systems. In: Proceedings of the Conference on Computer Vis and Pattern Recognition, IEEE Proceedings Computer Society. New York. pp. 477–482
4. Faugeras, O., 1995. Stratification of three-dimensional vision: projective, affine, and metric representations. Opt. Soc. America 12(3), 465–484
5. Kasturi, R.; Goldgof, D; Soundararajan, P.; Manohar, V; Garofolo, J.; Boonstra, M.; Korzhova, V.& Zhang, J. (2009). Framework for Performance Evaluation of Vace, Text and Vehicle Detection and Tracking in Video: Data, Metrics and Protocol, IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 31, No. 2, pp. 319 - 336, ISBN 0162-8828
6. VALOUCH, Jan. Integrated Alarm Systems. In Computer Applications for Software Engineering, Disaster Recovery, and Business Continuity. The 2012 Internationa Conference on Disaster Recovery and Business Continuity, Jeju Island, Korea. Proceedings. Series: http://www.springer.com/series/7899 Communications in Computer and Information Science, Vol. 340, 2012, XVIII. Berlin: Springer Berlin Heidelberg, 2012. Chapter, p. 369 - 379. ISBN 978-3-642-35267-9.
4. Ashani, Z., "Architectural Considerations for Video Content Analysis in Urban Surveillance," Advanced Video and Signal Based Surveillance, 2009. AVSS '09. Sixth IEEE International Conference on, vol., no., pp.289, 289, 2-4 Sept. 2009 doi: 10.1109/AVSS.2009.112.
5. EN 50 132-7. Alarm system - CCTV surveillance systems for use in security applications - Part 7: Application guidelines. B - 1000 Brussels: Management Centre: Avenue Marnix 17, 2011.W.-K. Chen, Linear Networks and Systems (Book style). Belmont, CA: Wadsworth, 1993, pp. 123–135.
6. Pavlidis, I.; Morellas, V.; Tsiamyrtzis, P.; Harp, S., "Urban surveillance systems: from the laboratory to the commercial world," Proceedings of the IEEE , vol.89, no.10, pp.1478,1497, Oct 2001
7. HROMADA, M., LUKAS L., Conceptual Design of the Resilience Evaluation System of the Critical Infrastructure Elements and Networks in Selected Areas in Czech Republic, The twelfth annual IEEE Conference on Technologies for Homeland Security (HST ’12), held

13-15 November 2012 in Greater Boston, Massachusetts. Pp. 353-358, ISBN 978-1-4673-2707-7

8. HROMADA, M., LUKAS L., The Status and Importance of Robustness in the Process of Critical Infrastructure Resilience Evaluation, The 13th annual IEEE Conference on Technologies for Homeland Security (HST ’13), held 12-14 November 2013 in Greater Boston, Massachusetts. Pp. 589-594, ISBN 978-1-4799-1533-0

Comparison of Corn and Corncob using as fungal culture medium

Jaruwan Chutrtong[1]

[1]Industrial Microbiology Department,
Suansunandha Rajabhat University,Bangkok 10300, Thailand
{Jaruwan Chutrtong, jaruwan.ch}@ssru.ac.th

Abstract. Corn or maize is the most widely grown grain crop. It is used as staple food and grown to feed for livestock. But corncob is the rest waste which require disposal. This research aims to compare pigment synthetic of *Neurospora* sp., when use corn, dry corncob and potato dextrose agar as culture medium. After fully grow up, extracted mycelium pigment with 95% ethyl alcohol and measure pigment absorbance by spectrophotometer at wavelength 450.5 nanometer. From the results, the best growth of *Neurospora* on dry corncob was sample which added water 90 % w/w. The best growth of Neurospora on corn was sample which added water 15 % w/w. When compare the intensity of mycelium pigment, the best medium for pigment synthetic of Neurospora. Absorbance of pigment extract from mycelium culture on corncob was 0.64(diluted 5X). As the absorbance of pigment extract from mycelium culture on corn and PDA were only 0.34(diluted 5X) and 0.35(diluted 2X).

Keywords: Comparison, corncob, fungal, medium

1 Introduction

Agricultural products produce many types of wastes in its daily operations. It is important that these wastes must be managed properly to protect community as well as the environment. Corn or maize is one of the most widely grown grain crop. It is very practical. It is used as staple food, major source of cooking oil and grown to feed for livestock. Starch from maize can be made into syrups plastics, fabrics, adhesives, and many other chemical products and also fermented and distilled to produce alcohol. So each year there is a lot of waste from corn, corncob. Useful of corncob has been studied by many researcher such as implemented to eliminate industrial pollution [1], produce xylooligosaccharide [2], produce activated carbons [4] and produce bio-oil [5] etc.. The results can produce value-added products from farm waste and transferring that knowledge to industry. Therefore, this research conducted to evaluate the useful of corncob by using as fungal culture medium for *Neurospora* sp., widely used organism as a model in genetics research.

2 Method

2.1 Prepared of corncob

The experiment used sweet corn (*Zea mays* convar. *saccharata* var. *rugosa*). Pull back the outer leaves of cob to expose the kernels. Strip off any of the silky threads. Cut off the ends of the cob, then wash. Place cob in unsalted boiling water. Covered the pan and return it to a boil. Cook corn for 3-5 minutes or until tender. Get all *kernels off* a *corn* on cob. Keep kernels in refrigerator. Cob was broken into chips and dried at 60 ^{o} C in hot air oven 48 hours.

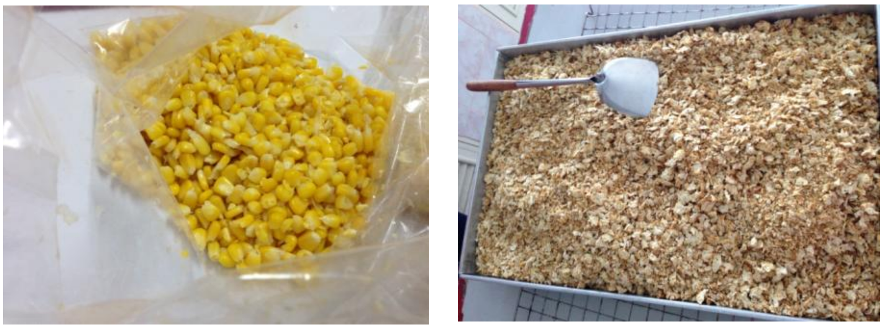


Fig. 1 (a) kernels of corn (b) dried corncob

2.2 Strain and media

The fungi *Neurospor*a sp. was obtained from industrial microbiology department, Suansunandha Rajabhat University. It was performed using potato dextrose agar (PDA).

2.3 Effect of moisture

The experiments were established using 500 ml laboratory glass bottle (Duran) containing prepared corncob with sterile water (w/w) at various ratios (35: 65, 40:60, 45:55, 50:50, 55:45, 60:40, 65:35, 70:30, 75:25, 80:20, 85:15, 90:10 and 95:5). Other set of bottle contained *corn kernels* with sterile water (w/w) at various ratios too. Inoculated *Neurospor*a sp. in those prepared bottle (triplicate). Observe growth rate of fungi.

2.4 Pigment synthetic

After fully grow up, mycelium from *Neurospor*a sp. on PDA, oven-dried chips corncob and corn kernels 2 gram was extracted pigment with 95% ethyl alcohol 10 ml. [3]. Measured pigment absorbance by spectrophotometer at wavelength 450.5 nanometer.

3 Result and discussion

3.1 effect of moisture on *Neurospora* sp. growth

After fully grow up, mycelium pigment was extracted with 95% ethyl alcohol from *Neurospor*a sp. on PDA, oven-dried chips corncob and *corn kernels*. Measured pigment absorbance by spectrophotometer at wavelength 450.5 nanometer.

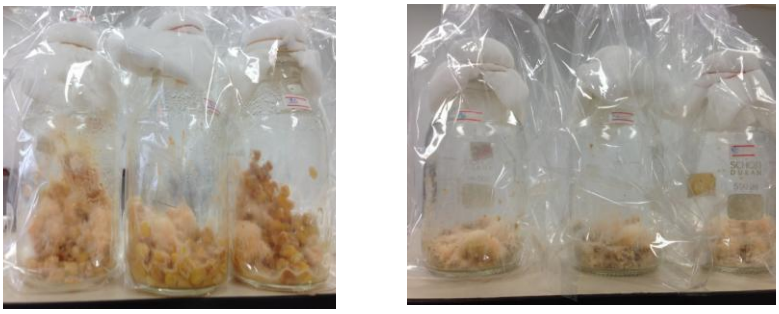


Fig. 2 (a) *Neurospor*a sp. culture on *kernels* (b) *Neurospor*a sp. culture on dried corncob

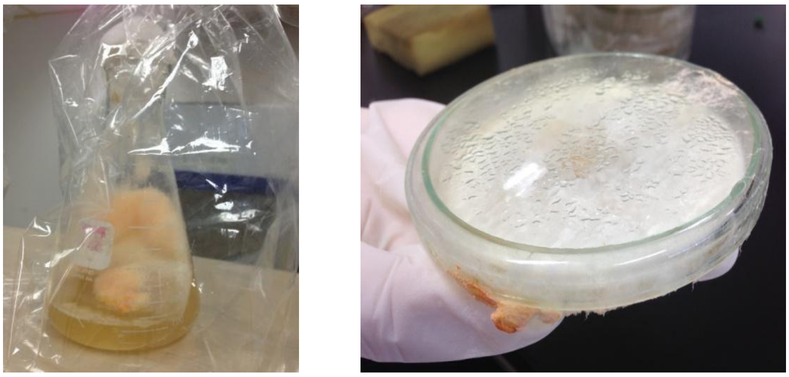


Fig. 3 (a) *Neurospor*a sp. culture on PDA (b) *Neurospor*a sp. colony on PDA plate

3.2 Pigment synthetic of *Neurospora* sp.

When compare the intensity of mycelium pigment, it was found that corncob is the best medium for pigment synthetic of *Neurospor*a. Absorbance of pigment extract from mycelium culture on corncob (which diluted 5X) was 0.64 at ratio of moisture 90% (w/w). The absorbance of mycelium pigment which extract from culture on *kernels* of corn at ratio of moisture 15% (diluted 5X) was only 0.34. While absorbance of mycelium pigment from culture on PDA (which diluted 2X) was 0.35.

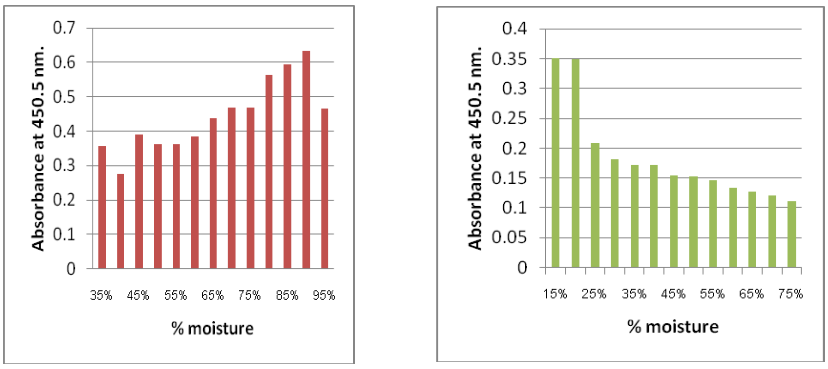


Fig. 4(a) absorbance of *Neurospor*a pigment culture on dried corncob

(b) absorbance of *Neurospor*a pigment culture on *kernels*

Benefits of corn to use as solid medium for culture fungus are available in *Neurospora*. It is unnecessary to add anymore nutrients. Mold can grow well and can produce more color than culture with corn and PDA, which is more expensive. So if more researches have been applied, corncob may be a value added material. It will be increase in value, without having to allow it to be waste which creates pollution problems to the environment.

Acknowledgments. The author would like to thank the Suan Sunandha Rajabhat University, Thailand, for providing fund, necessary equipment and laboratory area.

References

1. Chandran, B., Nigam, P., Robinson, T.: Removal of dyes from an artificial textile dye effluent by two agricultural waste residues, Corn cob and barley husk. Environment International, 28, 29--33(2002)
2. Garrote, G., Dom, H., Parajó, J. C.: Autohydrolysis of corncob: study of non-isothermal operation for xylooligosaccharide production. J. of Food Engineering, 52, 211--218(2002)
3. Stamets, P.: Mycelium Running: How Mushrooms Can Help Save the World, pp. 54--64. California; Ten speed press (2005)
4. Tseng, R.L., Tseng, S.K.: Pore structure and adsorption performance of the KOH-activated carbons prepared from corncob. J. of Colloid and Interface Science, 287, 428-437(2005)
5. Worasuwannarak, N., Sonobe, T., Tanthapanichakoon, W.: Pyrolysis behaviors of rice straw, rice husk, and corncob by TG-MS technique. J. of Analytical and Applied Pyrolysis, 78, 265-271. (2007)

The Use of Simulation in Education of Security Technologies, Systems and Management

Petr Svoboda and Jiri Sevcik,

Faculty of Applied Informatics, Tomas Bata University in Zlín, Nad Stráněmi 4511, 760 05 Zlín, Czech Republic
psvoboda@fai.utb.cz, jsevcik@fai.utb.cz

Abstract. This article presents a research focused on the needs of the security officers and on their knowledge, based both on the content of security technologies, systems and management studies also taught at Tomas Bata University in Zlín and the European training standards in security industry. In the first part of this paper, the research of the knowledge of unfamiliar people and students of Security technologies, systems and management is presented. In the second part the simulators for improving the knowledge are proposed.

Keywords: European Training Standard, Private security industry, Private security training manual, Security officers, Training simulation.

1 Introduction

A private security industry (PSI) is a rapidly growing industry not only in the Czech Republic. The increasing importance of PSI leads to the need of professionalization and the educational process improvement. Nowadays, the knowledge is improved especially thanks to universities with educational programs focused on the PSI.

This paper describes the content of standards reflecting needs of private security officers' knowledge and the ways, how to improve the educational process using training simulators.

2 Knowledge Test

The knowledge test used in this research originates from the test to gain competence certifications of "detective" due to Czech system. A test subjects were unfamiliar people and students of Tomas Bata University in Zlin who finished 1, 6 and 9 semesters. The test consisted of 150 questions and the participants had 180 minutes, however, the average time was 37 minutes. To pass the test, the 100 points had to be gained.

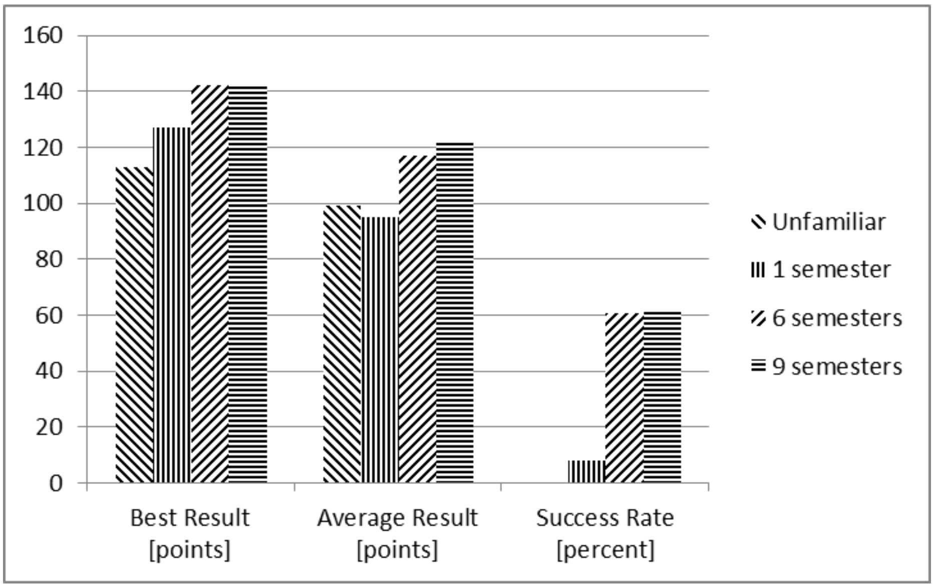


Fig. 1. The graph shows results of each testing group. In the first part, best results from the testing groups can be found. The second part shows the average result and the last the success rate of participants in test. As can be seen, there are big differences between participants of each group. Reasonably, the unfamiliar participants' to PSI success rate is the lowest, but even the success rate of 9 semester student is only about 60 percent (61.9%).

Moreover, the research showed the most problematic group of questions – legislative questions, occupational health and safety and first aid.

3 Education Process Optimization

In this part of the paper, the research focused on the European training standards (ETS) in security industry is described. ETS is divided into 14 chapters. These chapters are focused on the different parts of the PSI principles and are summarized below.

Private Security Industry

This chapter of ETS is focused on the basic definitions of private security industry (PSI) and private security services (PSS). It also contains a basic sectionalization of PSI to the sectors and services and their best practices. An introduction to the issue of guarding services, including the basic duties as well as the evaluation methods of security risk management, security analysis and audit are presented in this chapter. Moreover, the chapter deals with the issue of private detectives and the issue of basic law regulations and standards.

Private Security Officer

In the second chapter of the ETS, the profile of security officer is mentioned in relation to his duties, abilities and equipment.

Equipment

This chapter deals with private security officers' equipment, object documentation and its electronic systems. The personal equipment contains not only uniforms and radio, but even handcuffs, pistol, pocket spray "Mace", alarm button and baton.

Safety Procedures

Safety procedures are presented in the book as the methods and means of preclusion the undesirable situation and are divided into 6 chapters as can be seen in Table 1.

Table 1. Chapters of safety procedures.

Chapters	
Security Guard	Access Control Activities
Occupational Health and Safety procedures	Duties of Security Guard Leader
Firefighting Procedures	Observation

Emergency Procedures

Emergency procedures are described as a complex of activities, which should be done by security guard to prevent, detect or minimize loss caused by accidents including first aid and the content of communication with fire department operator.

Private Security Industry Legislation

This part of ETS, the legislation of PSI is described, especially the privileges of private security officers.

Firefighting procedures

The impact of a fire, the process of burning, the most common occasions of fire, the ways of fire spreading, the kinds of fire-distinguisher and its utilization, all these problems are discussed in the seventh chapter of ETS.

Occupational Health and Safety

This chapter deals with basic knowledge of occupational health and safety field, the company occupational health and safety management, proceedings during Occupational Health and Safety breach, the suitable legislation and governance supervision.

First Aid

In this chapter, the security guard is learning the basics of the first aid, the most common types of injuries, bleeding, fractures, etc. Students becomes familiar with measures and countermeasures of communication with afflicted by injury.

Customer care and quality of service

Customer care and quality of service chapter describes the principles of customer care in relation to the safety. The aim of this chapter is to:

- Establish the principles of customer care,
- describe ways to help customer professionally and friendly,
- describe principles of ISO 9000,
- summarize rules of quality and OHS,
- describe responsibility for the quality of services.

Communication

Communication, both verbal and nonverbal, is one of the basic skills characterizing each human and is crucial for security guards. Using this skill, he can not only professionally talk to customer, but also prevent potential problems or resolve conflicts.

Job relations

This part of ETS is focused on the optimization human activities, such as time-management and solving traumatic and stressful situations.

Work regulations

This chapter deals with labor legislation, security guards' and their employers' duties, collective agreement, internal regulations of the company and work order.

"Basic training" project

This chapter is focused on the training methods of ETS and training evaluation

3.2 Optimization the Educational Process

In this chapter, the appropriate simulators or simulator types for each part of ETS are proposed to improve the educational process. The simulator types are proposed if the market with simulators of this type is wide enough. The concrete simulator is proposed if it is unique or if it let us to learn more chapters of ETS to safe costs. The simulator types and concrete simulators are described below, in Table 2, moreover, the concrete simulators are described below the Table 2.

Table 2. Appropriate types of simulators.

Chapters	Appropriate Types of Simulators
Private Security Industry	Educational simulators
Private Security Officer	Communicational simulators
Equipment	Projection screen simulators
Safety Procedures	VBS3 [1]
Emergency Procedures	VBSWorlds [2]
Private Security Industry Legislation	Educational Simulator
Firefighting procedures	Firefighting simulator, VBSWorlds [2]
Occupational Health and Safety	Live simulation
First Aid	Live simulation (Casualty Simulation Kit)
Customer Care and Quality of Service	VCAT [3]
Communication	VCAT [3]
Job Relations	Educational Simulator
Work Regulations	Educational Simulator
“Basic Training” Project	N/A (test)

VBS 3

“*The VBS virtual environment offers realistic physics, comes with an extensive content library for creating models and populating scenarios, and has the capability for expanding existing terrains and developing geospecific terrains. VBS3 is well suited for learning how to think, communicate and make sound decisions. As a tool for tactical scenario training and mission rehearsal, VBS3 allows trainees to practice* *field tactics many times over without expending live ammunition, without costly travel time, and without risk of injury to soldiers or damage to expensive equipment.*" [1] This simulator is suitable especially for learning safety procedures thanks to its variability and the possibility of communication in a group.

VBSWorlds

"*VBSWorlds is a revolutionary 3D learning engine based on the powerful Thinking Worlds technology that will allow you to create more motivating, immersive virtual training scenarios."* [2] It allows to make new scenarios focused on the learning emergency procedures and firefighting.

Alelo VCAT (Virtual Cultural Awareness Trainer)

"*Powered by industry-leading technology and experts with unmatched diversity in educational, cultural and experiential backgrounds, Alelo combines understanding of your unique goals with the efficacy of a role-playing learning environment."* [3] However, this simulator is focused on the learning communications especially in army, it could be helpful even in everyday life.

References

1. Bohemia Interactive Simulations, http://bisimulations.com/
2. Caspian Learning, http://www.caspianlearning.co.uk/products-2/vbsworlds
3. Alelo, http://www.alelo.com/
4. FLEISCHMANN, M., *Zkoušky odborné způsobilosti osob k vykonávání živností ostraha majetku a osob a služby soukromých detektivů*. In. The diploma thesis at Tomas Bata University, 2014.
5. HROMADA, M.,Využitie modelovania v problematike ochrany kritickej infraštruktúry/The modeling use in area of Critical Infrastructure protection, In: Security Magazín, Číslo 96, 2010, ISBN – 1210-8723
6. LUKÁŠ, L., HROMADA, M. *Simulation and Modelling in Critical Infrastructure Protection*, In: INTERNATIONAL JOURNAL of MATHEMATICS AND COMPUTERS IN SIMULATION, , Issue 1, Volume 5, p. 386-394, 2011, ISSN: 1998-0159, dostupné tiež z WWW: http://www.naun.org/journals/mcs/
7. PETZ, I., NECAS, P., KELEMEN, M., ANDRASSY, V., HROMADA, M., SOUSEK, R., *Constructive simulation entities behaviour modelin in realm of blended simulation.* In. Brno, ICMT ,2011, 1211-1214, 4 s, ISBN 978-80-7231-787-5

Performance of Hybrid Mobile Application UI Frameworks

Radek Vala, Roman Jasek

Tomas Bata University in Zlin, Faculty of Applied Informatics, nám. T.G.Masaryka 5555,
CZECH REPUBLIC
{vala, jasek}@fai.utb.cz

Abstract. The choice of right hybrid mobile application UI framework is not elementary these days, because there is lot of possibilities and on the other hand there are no comparative studies, which can help to solve this problem. This paper is focused on HTML5, CSS a JavaScript Hybrid Mobile Application UI frameworks and comparative tests of these frameworks are conducted. The comparison focuses on both the subjective (documentation quality, learning speed, implementation simplicity) and objective parameters, influencing performance of the final application (size of source codes, complexity of DOM structure or scripts optimization).

Keywords: hybrid mobile application, performance test, mobile UI frameworks

1 Introduction

With the increasing use of mobile phones, mobile applications market is rapidly growing. Developers are facing the problem how to produce the mobile application in the shortest time and with minimal costs. To meet these objectives, developers are finding the easiest way to solve the “cross-platformity” in the development process. A lower-cost alternative to native development seems to be a hybrid mobile application approach. Using this approach the need to have different development teams for each mobile platform is eliminated. Moreover the time of the development process could be reduced. Therefore this approach becomes in recent years very popular, but it is not possible to mark it as the only correct. Conversely, if there is not selected ideal hybrid mobile applications development framework (FW), the developers are likely to face a number of issues. The selection of appropriate FW is difficult due to the number of new products appearing on the scene and due to the fact, that there is no comparative study, which could help with the decision.

This paper focuses on the most commonly used hybrid mobile application UI FWs and provides the comparison which should bring relevant data, which are necessary for the right selection.

2 Related Work

Although the hybrid mobile application development is a very interesting area in recent years, there is lack of complex comparative study in this field. The situation is very similar to general mobile development area few year ago and the existing body of knowledge is highly pragmatic, with lots of guidelines and many pieces of sample code as examples. [1]

It is probably due the fact, that the research in this field is highly relevant only in short term and for specific FW development version or in context of specific mobile platform version.

Currently, there is possible to find research papers focusing on the basic comparison of native and hybrid development [2] [3] or the challenges of hybrid approach [4][5][6] and lot of the overall statements are well known within the community of developers. However, the specific comparison of the most used hybrid FWs could be a very important information for a huge number of developers which are focusing in non-native mobile application development. The developers are currently honing their knowledge from different on-line sources, such as professional forums, developer groups or other projects which brings comparative information. On-line professional discussion forums with answer quality voting such as StackOverflow, can be considered as a relevant source of information [7], but only in form of partial question/answers. More condensed information can be found on web portals http://mobile-frameworks-comparison-chart.com/ or http://propertycross.com/. However, these sources do not offer any complex FWs feature comparison resulting in some conclusions. It is basically an overview of FW features, or database of example implementations without any performance testing.

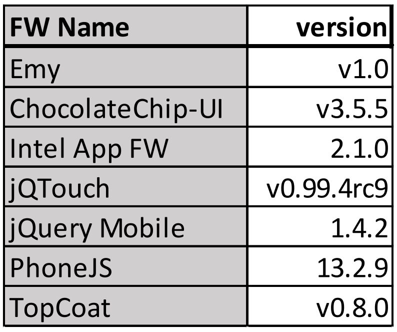
3 Candidates of Comparative Tests

For the comparison, following hybrid mobile application UI FW were selected. In the tested group there are both open-source and commercial software tools. Selected FWs are listed below:

1) Intel App Framework [http://app-framework-software.intel.com/]
2) Emy [http://www.emy-library.org/]
3) ChocolateChip-UI [http://chocolatechip-ui.com/]
4) jQTouch [http://jqtjs.com/]
5) jQuery Mobile [http://jquerymobile.com/]
6) PhoneJS [http://phonejs.devexpress.com/]
7) TopCoat [http://topcoat.io/]

All research data were taken in May 2014 and the latest FWs release were used. Table 1 provides the version numbers.

Table 1. Version numbers of tested FWs.



FW Name	version
Emy	v1.0
ChocolateChip-UI	v3.5.5
Intel App FW	2.1.0
jQTouch	v0.99.4rc9
jQuery Mobile	1.4.2
PhoneJS	13.2.9
TopCoat	v0.8.0

4 Weighted Multi Criteria Matrix Comparisonof Frameworks' Features

To obtain comparative results of FWs, following FWs' features were evaluated as important criteria using weighted multi criteria matrix.

4.1 Suitability for Mobile Applications Development (MA)

The criteria of suitability for mobile applications development is subjectively rated from 1 to 5, where 1 means the least appropriate and 5 means the most suitable. In this criterion following parameters are considered: FW contains common GUI objects for mobile platform, layout is responsive and the primary target is the mobile platform. The universal desktop/mobile UI FWs are less suitable because usually offers worse user experience. The DOM structure of HTML elements is usually more complicated and performance issues can be observed.

4.2 Suitability for Desktop Applications Development (DA)

The criterion of suitability for desktop applications development is subjectively rated from 1 to 5, where 1 means the least appropriate and 5 means the most suitable. Desktop development suitable FWs should contain especially common desktop GUI objects (user input dialogs, information dialogs, buttons etc.). In other hand, there should be available also the mobile version of these components. However, this universality can cause performance and user experience issues especially in mobile applications. From the mobile development point of view, there is no need to provide desktop browser support.

4.3 Actuality (A)

Actuality is one of the most important selection criteria of development tools in general. Within this criterion, the frequency of updates per month and date of last commit were evaluated. The frequency usually reflects the usability of the FW in future, when new versions of mobile platforms are issued and some fixes of FW core are needed. These parameters were gathered from the Git accounts [8] in case of open-source projects. According the two parameters above, the FWs were ordered and rated as follows: 7 points – the best and 1 point the worst result. In case of commercial project PhoneJS, average value was chosen, because of lack of public information.

4.4 License (L)

The license policy may be also one of the important feature, which indicates, if there is the possibility of a commercial use without restrictions or it is necessary to buy a commercial license. The rating is as follows: The FW is possible to use without restrictions – 3 points; there is dual license for commercial or non-commercial use – 2 points; only commercial license available – 1 point.

4.5 Documentation (D)

Availability and quality of documentation is directly influencing the learning curve of the new technology. The rating is subjective and based on empirical knowledge and experiences gathered from practical use of tested FWs. The worst evaluation is 1 point and the best is 5 points.

4.6 Size (S)

This factor means the minimal size of FW's source code, which is necessary to import to the project of mobile application. For the evaluation purpose, 6 size classes were set as follows: < 100 kB – 6 points, > 100 kB – 5 points, > 200 kB – 4 points, > 500 kB – 3 points, > 1 MB – 2 points, > 2 MB – 1 point.

4.7 Native look (NL)

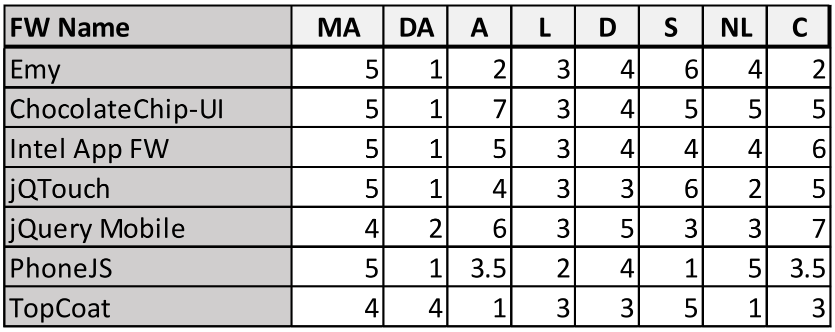
The support of native look for different platform is desired property, but it is not a standard. The native looking applications provide better user experience, because the user is familiar with provided GUI patterns and overall look of the GUI objects. The rating is as follows: Support of the newest versions of at least 3 main mobile platforms (Android, iOS, Windows Phone) – 4 points; support of oldest versions of at least 3 main mobile platforms (Android, iOS, Windows Phone) – 3 points; Basic color themes for different mobile platforms – 2 points; universal look – 1 point.

4.8 Community (C)

Especially in case of open-source products, the size and quality of community around the project is very important factor which indicates future development of the whole project. The information about the community size was taken from Git accounts. Especially these parameters were evaluated: number of contributors with at least 50 commits and number of issued opened and closed in last 30 days. The FWs were ordered and rated as follows: 7 points – the best and 1 point the worst result. In case of commercial project PhoneJS, average value was chosen, because of lack of public information.

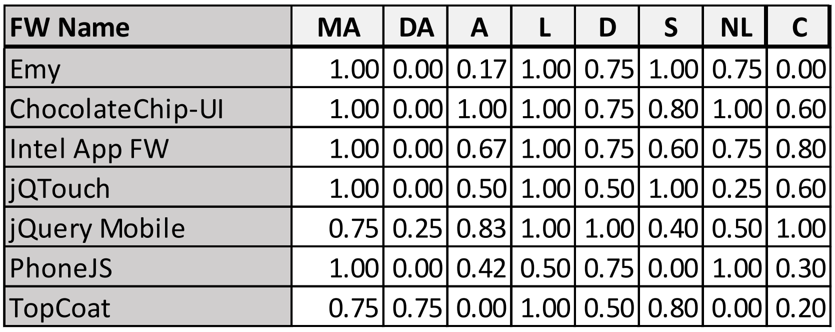
From all of the criteria listed above, the criteria matrix shown in table 2 was created and the normalized version is available in table 3.

Table 2. Criteria matrix for FWs comparison



FW Name	MA	DA	A	L	D	S	NL	C
Emy	5	1	2	3	4	6	4	2
ChocolateChip-UI	5	1	7	3	4	5	5	5
Intel App FW	5	1	5	3	4	4	4	6
jQTouch	5	1	4	3	3	6	2	5
jQuery Mobile	4	2	6	3	5	3	3	7
PhoneJS	5	1	3.5	2	4	1	5	3.5
TopCoat	4	4	1	3	3	5	1	3

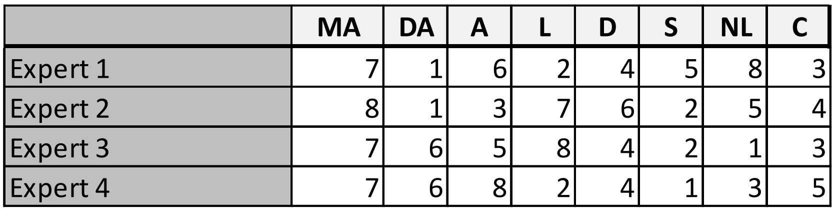
Table 3. Normalized criteria matrix



FW Name	MA	DA	A	L	D	S	NL	C
Emy	1.00	0.00	0.17	1.00	0.75	1.00	0.75	0.00
ChocolateChip-UI	1.00	0.00	1.00	1.00	0.75	0.80	1.00	0.60
Intel App FW	1.00	0.00	0.67	1.00	0.75	0.60	0.75	0.80
jQTouch	1.00	0.00	0.50	1.00	0.50	1.00	0.25	0.60
jQuery Mobile	0.75	0.25	0.83	1.00	1.00	0.40	0.50	1.00
PhoneJS	1.00	0.00	0.42	0.50	0.75	0.00	1.00	0.30
TopCoat	0.75	0.75	0.00	1.00	0.50	0.80	0.00	0.20

In context of the mobile application development process with use of some development framework, not all criteria are the same importance. The importance of the criteria differs in each specific project and it is possible to change its weights according subjective preferences. In the case of this research, 4 experts from mobile development area were addresed to compile the expert-reated weights to obtain the ordinal ranking. There is p criteria and q experts. The criteria are ordered by assigning the rating p, $p - 1$, …, 1. The most important criterion is rated by number p, and the less important by number 1. Table 4 shows the resulting expert criteria ratings.

Table 4. Expert criteria rating.



	MA	DA	A	L	D	S	NL	C
Expert 1	7	1	6	2	4	5	8	3
Expert 2	8	1	3	7	6	2	5	4
Expert 3	7	6	5	8	4	2	1	3
Expert 4	7	6	8	2	4	1	3	5

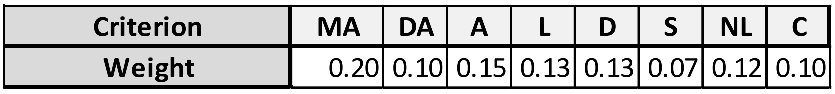
When a_{ij} be the i-th criterion rating of j-th epert, then the weight of i-th criterion by j-th expert is calculated using (1). The weight of i-th criterion is calculated using (2).

$$w_{ij} = \frac{a_{ij}}{\sum_{i=1}^{p} a_{ij}} = \frac{a_{ij}}{\frac{p(p+1)}{2}} \tag{1}$$

$$w_i = \frac{\sum_{j=1}^{q} v_{ij}}{q} = \frac{\sum_{i=1}^{p} a_{ij}}{\frac{p(p+1)q}{2}} \tag{2}$$

Final results of (2) – expert-rated weights are shown in table 5. As can be seen from the results, the most imporant criteria are the suitability for mobile application development (MA), then the native look (NL) and the size (S).

Table 5. Weights for criteria matrix.



Criterion	MA	DA	A	L	D	S	NL	C
Weight	0.20	0.10	0.15	0.13	0.13	0.07	0.12	0.10

Advantage of this evaluation is the possibility of changing the proposed weights (table 5) to cover own subjective priorities, which could differ in different projects.

According to the result of weighted multi criteria matrix (table 6 or figure 1), the most successful candidate FW is Chocolate-Chip UI and the less successful one is TopCoat. Although PhoneJSis very interesting FW, it has two areas, which were highly penalized. The first one is the license – only commercial use is possible and the second one, more problematic in most of use cases, is the size. PhoneJS contains an iOS theme CSS file which has 1112 kilobytes (due the inserted graphics). But this amount of kilobytes could cause performance issue by initial run of the application.

Table 6. Comparison of hybrid mobile application UI FWs

FW Name	points	percent
ChocolateChip-UI	0.82	100%
jQuery Mobile	0.75	92%
Intel App FW	0.74	91%
jQTouch	0.63	78%
Emy	0.61	75%
PhoneJS	0.57	70%
TopCoat	0.49	61%

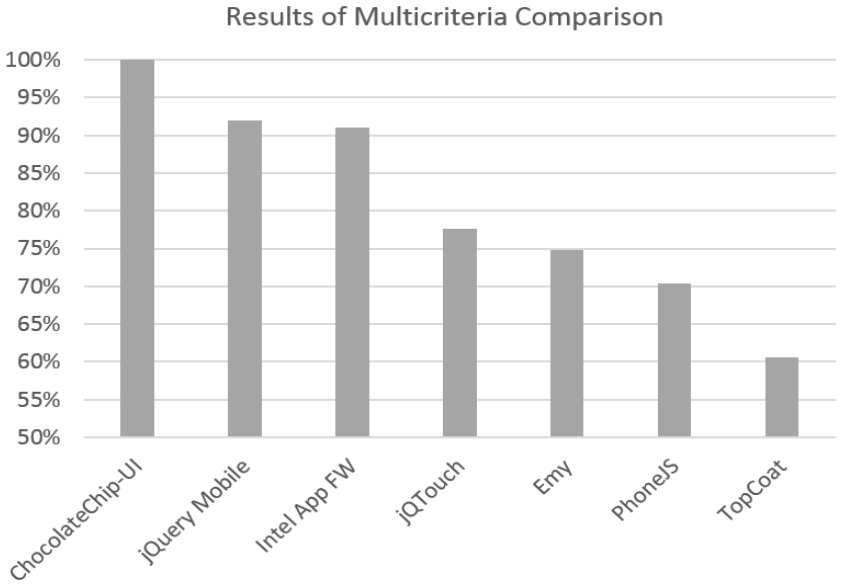


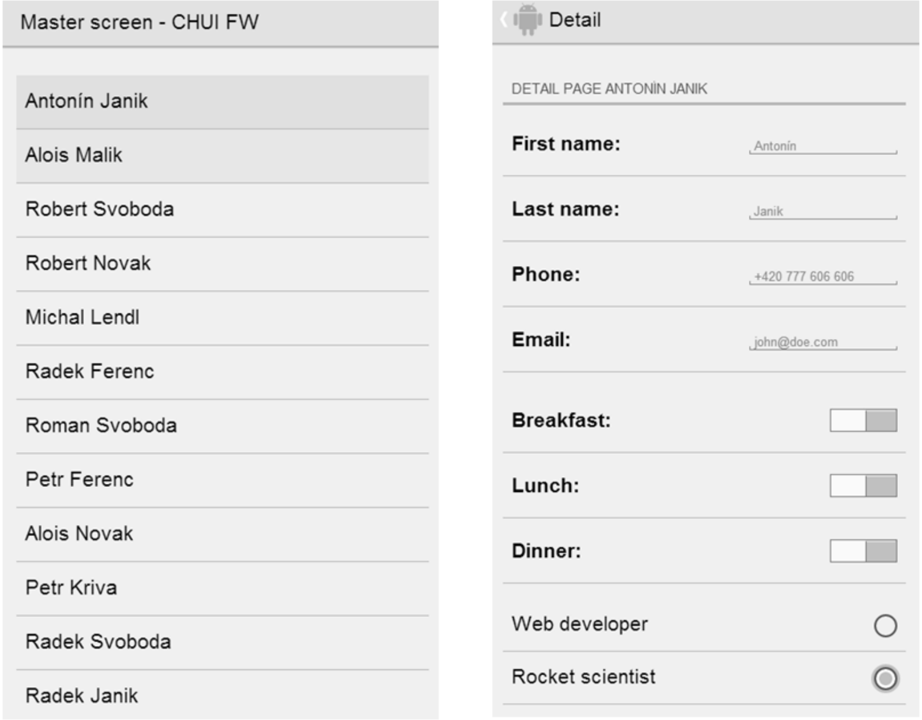
Fig. 1. Results of hybrid mobile UI FWs criteria matrix comparison

5 Hybrid Mobile Testing Application

For performance testing purpose, simple hybrid mobile application were implemented using each of selected FWs.

The application uses typical list view and detail pattern, because it is one of the most used mobile application structure. Moreover, the list view component, allows performance testing of application with very rich and complex DOM structure. The data for the list view component are loaded from the JSON file [9].

In the detail page, there are used the most common form fields, such as labels, text fields, switch fields, radio buttons and buttons. If the detail page is loaded, the form field values are prefilled using the data from the JSON object. Most of the UI FWs are creating some type of form field using DOM Element transformation with JavaScript. Especially switch fields and radio buttons are often generated using this way. Therefore this types of fields are included in testing application to address potential performance issues in different approaches.



Master screen - CHUI FW

Antonín Janik
Alois Malik
Robert Svoboda
Robert Novak
Michal Lendl
Radek Ferenc
Roman Svoboda
Petr Ferenc
Alois Novak
Petr Kriva
Radek Svoboda
Radek Janik

Detail

DETAIL PAGE ANTONIN JANIK

First name: Antonín
Last name: Janik
Phone: +420 777 606 606
Email: john@doe.com
Breakfast:
Lunch:
Dinner:
Web developer ○
Rocket scientist ●

Fig. 2. List view and detail view screen with form components.

6 Performance Testing

The performance testing of selected FWs is focused into the most critical areas such as loading time, scrolling smoothness and page transition smoothness.

The tested applications were run on the Samsung Galaxy Note 10.1 (GT-N8010), with Android version 4.1.2 (in factory settings), within a mobile Chrome browser application (version 35.0.1916.138). The measurements were realized using the Chrome Remote Debugging [10] and Chrome Developer Tools [11].

6.1 Loading time

The loading time of an application could be one of the key factor of application success. According to Compuware research, the median time of user expectation of mobile application load time is about 2 seconds. If this time is exceeded, there is the risk, that some of the users turn the application off.

Loading time measurement methodology.
The time of mobile application load were measured using Chrome Developer Tools Timeline and the goal was to capture the time of DOM Load Event [12] occurrence. Average value of 10 measurement were taken. Between each measurement, the cache memory of the browser were cleared and garbage collector were run.

The second approach was the time measurement of different browser activities, such as Loading, Scripting, Rendering, Painting, Other and Idle.

Loading time results.
In the pictures below are shown the results from the DOM Load measurement (Fig. 3) and particular loading activities times (Fig. 4). As can be seen from this results, the document can be loaded in half the time of particular loading activities. This is thanks to asynchronous loading of external resources, such as Cascading Style Sheets, Java Scripts or Fonts. The overall load time is most influenced by the Scripting time.

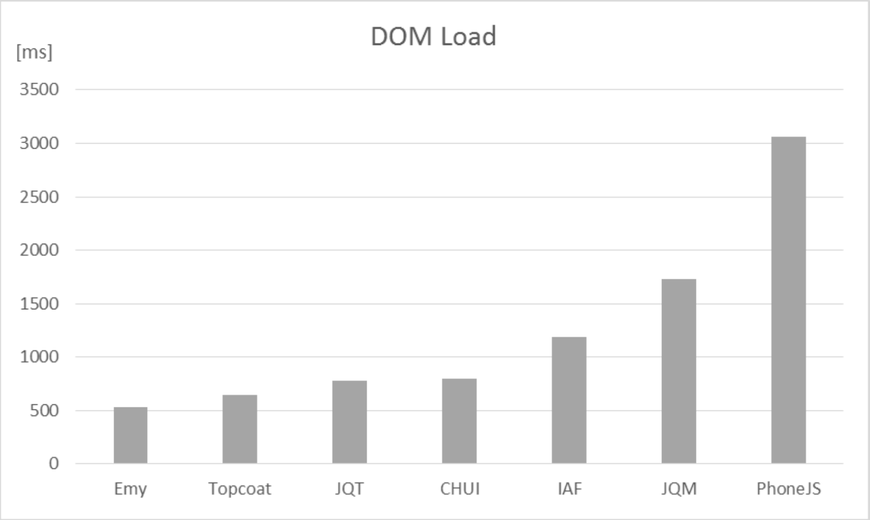


Fig. 3. DOM Load comparison

According the results in Fig. 3, all tested FWs loads within less than 2 seconds (except PhoneJS), therefore it can be stated, that from the application loading time point of view these FWs are suitable for real use. However, it is desirable to have the load time less than one second, because in real scenario, the application could be more complex and other external resources could be loaded.

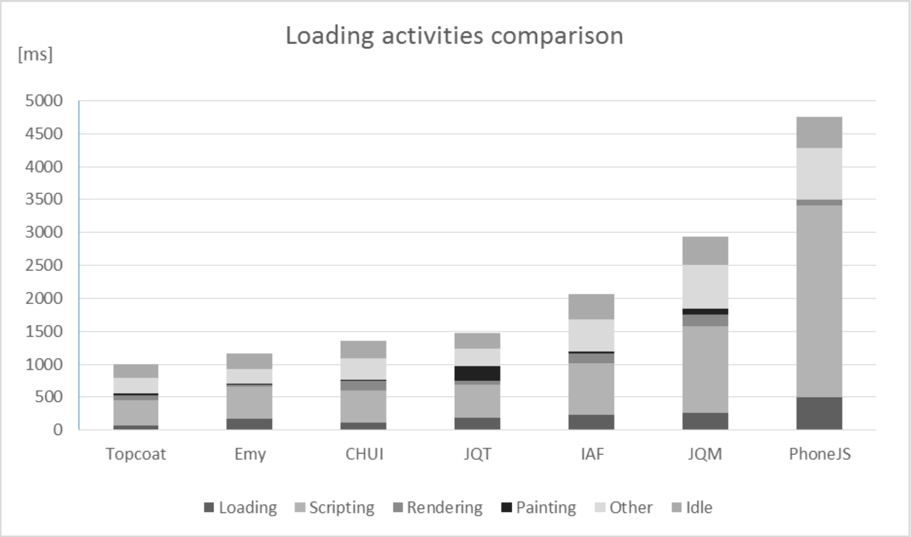


Fig. 4. Loading activities comparison

6.2 Scrolling Smoothness

The user experience is not build only during the application lunch, but especially by using the application. Because of limited screen dimensions one of the most often application task is content scrolling. The scrolling should be smooth and the feel should be if possible the same like in case of native application. Especially this area should suffer from the non-fluency, which can be caused by the memory-intensive manipulation with complex DOM structure. If the value of frames per second (FPS) is less than 30 FPS, users are starting to recognize animation plucking.

Scrolling Smoothness Measurement Methodology.
Scrolling smoothness was measured using Chrome Developer Tools FPS meter and continuous page repaint tool. [13] The tested page with 100 items (list-item elements within HTML element ul) were continuously scrolled to obtain the average FPS, minimal FPS and maximal FPS. If the minimal FPS is considerably lower than 30 FPS, users are able to recognize occasionally worst user experience. If there is FPS less than 15, scrolling is obviously not fluent. The maximal FPS of today’s browsers is 60 FPS.

Scrolling Smoothness Results.
The most important value from the results in Fig. 7 is the Avg FPS (average FPS). If this value is higher or slightly lower than 30 FPS, the scrolling can be considered as fluent, like in native application. It is necessary to consider also the Min FPS (minimal FPS), because if this value is significantly lower than 30 FPS (under 20 – 15 FPS), it can cause recognizable tearing in particular moment of the animation.

As can be seen from Fig. 5, the most successful FW in scrolling test was TopCoat, where nor average neither minimal FPS was under 60 FPS. It is thank to very simple DOM structure and only CSS formatting with no Java Script transformations. Also very good performance meets ChocolateChip UI FW, Intel App FW and PhoneJS. JQuery Mobile's result is not very satisfactory with 100 items in the list and framework Emy and especially jQTouch was very slow. In real world it is recommended to preserve the item number count under 30 in list views to maintain the smooth user experience. [14]

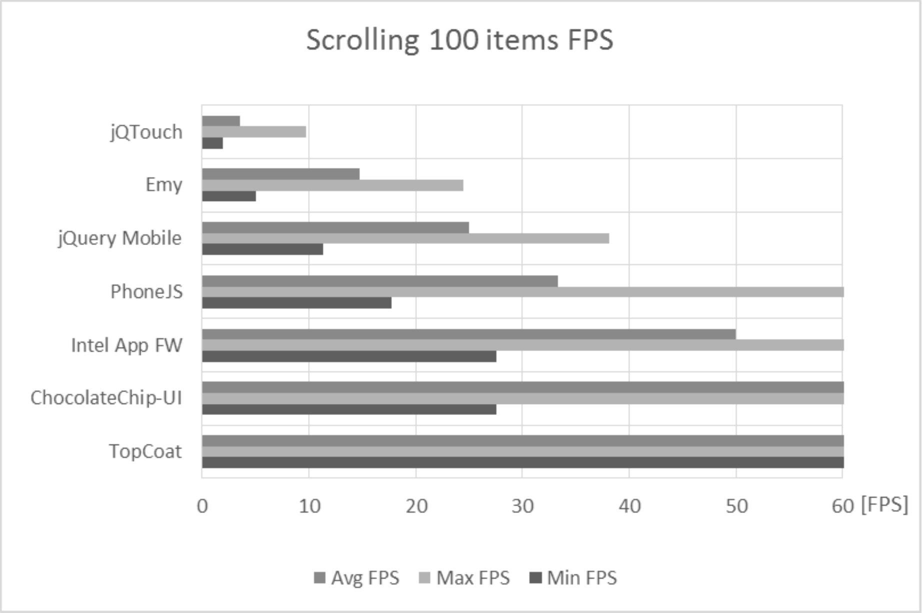


Fig. 5. Scolling 100 items FPS results.

6.3 Page Transition Smoothness

User's orientation within mobile application is ensured using proper page transitions. This transitions improve user's idea of mobile screen context. Therefore transitions are highly used among mobile applications on different platforms. Also hybrid mobile application should use this transitions, but there can be often the performance issue caused by complex DOM structure of manipulated content. Choppy transitions are affecting the user experience in a very negative way.

Page Transition Smoothness Measurement Methodology.
FPS of transitions between list view screen to detail screen of the application and back was continuously measured using Chrome Developer Tools FPS meter and continuous page repaint tool.

Page Transition Smoothness Results.
The results of page transition test are relatively satisfactory, taking into account the complex DOM structure (100 items in the list). According to test results in the Fig. 6, only FWs Emy, jQuery Mobile and jQTouch have significant problems with transition animations. But it has to be stated, that the minimal FPS which is under 30 FPS in case of all tested frameworks could be causing little worse user-experience than in case of native applications.

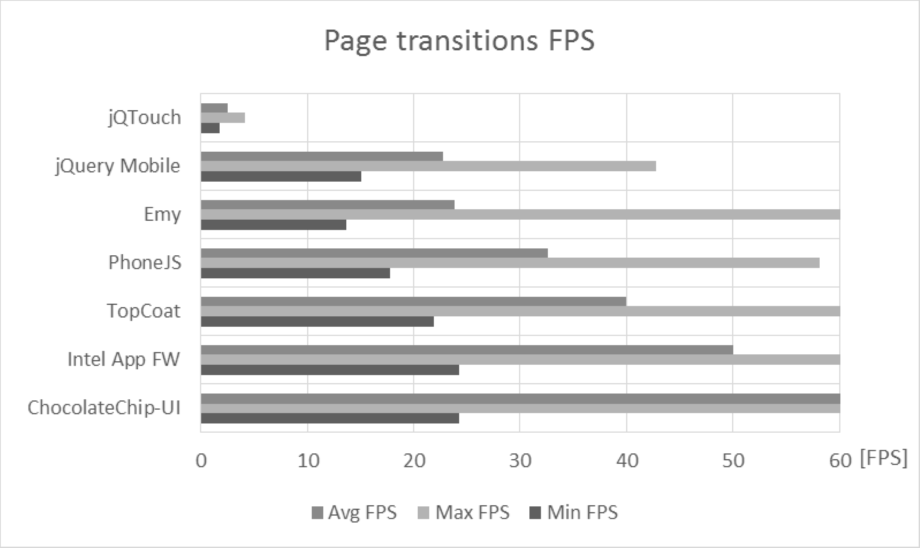


Fig. 6. Page transitions master – detail FPS.

7 Conclusion

Mobile application programming is one of the most developing area in IT world today. Developers are trying to lower their time and money cost per line of code and the cross-platform development is the promising way. In recent years few hybrid mobile application frameworks appeared on the scene and the offer of this type of developer tools is nowadays varied. It leads to the problem of proper choice, because there are no published comparative studies within these FWs.

This paper aims to create a comparative study focused in performance and other selected criteria within 7 widely used hybrid mobile application development FWs.

The selected candidates are firstly compared using these criteria: Suitability for mobile applications development, suitability for desktop applications development, actuality, license, documentation, size, native look and community. Criteria were evaluated using weighted multi criteria matrix in 4. Weightedmulti criteria matrix comparison of frameworks ‘features.

From the performance point of view, the most exposed area such as application load time, scrolling performance and page transition performance were measured and evaluated in 6. Performance testing. The results showed, that performance issues are very common by using hybrid mobile FWs, and are connected especially with slow scripting and rendering and manipulating a complex DOM structure. There is a direct correlation between FW's simplicity (simple DOM, CSS, no JavaScript) and performance. The simplerthe FW is, the fasterit is, but in this case, there is a lack of tools and widgets often used by developers. The correct choice should be a compromise between power and feature richness. The most successful candidates in this point of view, were Chocolate Chip UI and Intel App Framework.

Acknowledgment

The research work was performed to financial support by the European Regional Development Fund under the Project CEBIA-Tech No. CZ.1.05/2.1.00/03.0089.

References

1. Tony Wasserman. "Software Engineering Issues for Mobile Application Development" *FoSER2010* (2010).
   Available at: http://works.bepress.com/tony_wasserman/4.
2. CHARLAND, SuyeshaArianit KURTI. Cross-Platform Mobile Development: Challenges and Opportunities. [online]. 2011-05-01, issue 5, s. 219 [cit. 2014-05-20]. DOI: 10.1145/1941487.1941504. Available at: http://link.springer.com/10.1007/978-3-319-01466-1_21.
3. *Techniques for Surviving the Mobile Data Explosion* [online]. Hoboken, NJ: John Wiley, 2014-03-17, vol. 54, issue 5 [cit. 2014-05-20]. ISSN 00010782. Dostupné z: http://doi.wiley.com/10.1002/9781118834404.ch10.
4. Sin, D.; Lawson, E.; Kannoorpatti, K., "Mobile Web Apps - The Non-programmer's Alternative to Native Applications," *Human System Interactions (HSI), 2012 5th International Conference on* , vol., no., pp.8,15, 6-8 June 2012
   doi: 10.1109/HSI.2012.11.
5. Ng Moon Hui; Liu Ban Chieng; Wen Yin Ting; Mohamed, H.H.; RafieHjMohd Arshad, M., "Cross-platform mobile applications for android and iOS," *Wireless and Mobile Networking Conference (WMNC), 2013 6th Joint IFIP* , vol., no., pp.1,4, 23-25 April 2013
   doi: 10.1109/WMNC.2013.6548969.
6. AMATYA, SuyeshaArianit KURTI. Cross-Platform Mobile Development: Challenges and Opportunities. [online]. s. 219 [cit. 2014-05-20]. DOI: 10.1007/978-3-319-01466-1_21. Dostupné z: http://link.springer.com/10.1007/978-3-319-01466-1_21.
7. Nasehi, S.M.; Sillito, J.; Maurer, F.; Burns, C., "What makes a good code example?: A study of programming Q&A in StackOverflow," *Software Maintenance (ICSM), 2012 28th IEEE International Conference on* , vol., no., pp.25,34, 23-28 Sept. 2012
   doi: 10.1109/ICSM.2012.6405249.

8. GitHub - Build software better, together (2014). Retrieved May 14, 2014, from https://github.com.
9. Introducing JSON (2014). Retrieved May 16, 2014, from http://json.org/.
10. Remote Debugging on Android with Chrome (2014). Retrieved May 16, 2014, from https://developer.chrome.com/devtools/docs/remote-debugging.
11. Chrome Overview (2014). Retrieved May 16, 2014, from https://developer.chrome.com/devtools/index.
12. DOMContentLoaded (2014). Retrieved May 17, 2014, from https://developer.mozilla.org/en-US/docs/Web/Reference/Events/DOMContentLoaded.
13. Chrome Rendering Settings (2014). Retrieved May 17, 2014, from https://developer.chrome.com/devtools/docs/rendering-settings.
14. Secrets of aGoodJQueryMobilePageArchitecture (2014). Retrieved May 17, 2014, from http://www.gajotres.net/secrets-of-a-good-jquery-mobile-page-architecture/.

Stress Intensity Factors In Two Bonded Elastic Layers Containing Crack Perpendicular on the Interface with Different Elastic Properties

Mahdi Keikhaie1, Nasser Keikhaie2, Reza Keikhaie3, M.M. Kaykha3
1Department of Mechanical Engineering, Sharif University of Technology, Azadi Ave., 14588-89694 Tehran, Iran.
2Department of Mechanical Engineering, University of Sistan and Baluchestan, 98135-987 Zahedan, Iran.
3Department of Mechanical Engineering, University of Zabol, 98615-538 Zabol, Iran.
mm.kaykha@gmail.com

Abstract. Thin bonded films have many applications (i.e. in information storage and processing systems, and etc.). In many cases, thin bonded films are in a state of residual tension, which can lead to film cracking and crack extension in one layer often accompanies failure in whole systems. In this paper, we analyze a channel crack advanced throughout thickness of an elastic thin film bonded to a dissimilar semi-infinite substrate material via finite element method (FEM). In order to simplify modeling, the problem is idealized as plane strain and a two-dimensional model of a film bonded to an elastic substrate is proposed for simulating channel crack in thin elastic film. Film modeled by common 4-node and substrate by infinite 4-node meshes. The stress intensity factor (SIF) for cracked thin film has obtained as a function of elastic mismatch between the substrate and the film. The results indicate that in elastic mismatch state, SIF is more than match state. On the other hands, mismatch state is more sensitive to crack than match state. And SIF has also increased by increasing Young's modulus and Poisson ratio of film.

Keywords: Thin film, Channeling crack, Infinite element, Stress intensity factor

1 Introduction

This Many modern materials and material systems are layered. The potential applications of fracture mechanics of layered materials ranges over a broad spectrum of problem areas; included are: protective coating, multilayer capacitors, thin film/substrate systems for electronic packages, layered structural composites of many varieties, reaction product layers, and adhesive joints [1]. Many applications in microelectronics (e.g., interconnects and electronic packaging) often involve integrated structures with dissimilar materials. Stresses are introduced during the processes of fabrication, reliability testing, and operation. The stress field concentrates at the junctions of dissimilar materials, at the corners, or, if there exists a crack, at the crack tip [2]. In all of these applications, the films are very thin, with thicknesses measured in nanometers or micrometers, and they are bonded to comparatively thick substrates, with thicknesses typically measured in millimeters or centimeters.

Many cracking patterns in film-substrate systems have been observed and analyzed (Evans et. al. [3]; Hutchinson and Sue [1]). A crack nucleates from a flaw either in the film or at the edge, and propagates both towards to interface and laterally through the film. Depending on the material, the crack may stop at the interface (Fig. 1a), penetrate into the substrate (Fig. 1b), or bifurcate onto the interface (Fig. 1c) [4].

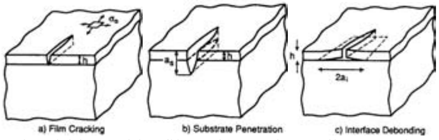


Fig 1. (a) A channeling crack within a thin film. (b) A channeling crack penetrating substrate. (c) A channeling crack with interface debonding [4]

Irwin [5] claims that the stress field in the vicinity of a crack tip can adequately be defined by a single parameter proportional to the SIF. When the intensity of the local tensile stresses at the crack tip attains a critical value, a previously stationary or slow-moving crack propagates rapidly. This critical value defines the “fracture toughness” and it is a constant for a particular material. If the size of the hugest flaw in a particular structure is known, minimum toughness standards can be established for the materials in this structure. In the application of most of the current fracture criteria, the SIF and the crack opening displacement are the mostly used quantities [6].

The objective of this study is investigating sensitivity of two bonded elastic layers to a single crack perpendicular to the interface between film and substrate. In this paper also has considered different elastic ratio of film and substrate. Because there are similar works in the literature (The problem of a crack perpendicular to the interfaces may be found in [7-11]), the main emphasis here is on using infinite meshes to simulating substrate (to be close to real problems) and also presenting results in different form, i.e. plotting SIF versus elastic properties instead of Dundurs’ parameters [12], to have better understanding.

1. Analytical Methods Background

In this section, we first give an overview of the fracture mechanics modes and then previous analytical works of SIF on both homogeneous and layered systems.

Three linearly independent cracking modes are used in fracture mechanics. These load types are categorized as Mode I, II, or III as shown in the figure. Mode I, shown to the left, is an opening (tensile) mode where the crack surfaces move directly apart. Mode II is a sliding (in-plane shear) mode where the crack surfaces slide over one another in a direction perpendicular to the leading edge of the crack. Mode III is a tearing (antiplane shear) mode where the crack surfaces move relative to one another and parallel to the leading edge of the crack. Mode I is the most common and important load type encountered in engineering design [13].

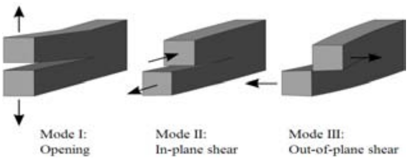


Fig. 2. Mode I, Mode II, and Mode III crack loading [13]

*1.1.*SIF in Single Edge Notched Tension Specimen:

The SIF equation for a single edge notch and homogeneous properties in an infinite specimen is [14],

$$K = \sigma ZY\sqrt{a} \tag{1}$$

Where,

$$ZY = \frac{\sqrt{\pi}(1+2(\frac{a}{w}))}{(1-(\frac{a}{w}))^{\frac{1}{2}}} \times V \tag{2}$$

Where,

$$V = 1.12078 - 3.68220(\frac{a}{w}) + 11.95434(\frac{a}{w})^2 - 25.85210(\frac{a}{w})^3 + 33.09762(\frac{a}{w})^4 - 22.4422(\frac{a}{w})^5 + 6.17836(\frac{a}{w})^6 \tag{3}$$

Range of applicability of this equation: The defect depth, a, should be less than the specimen width, w, [14]. For different a/w ratio it has plotted in Fig. 3.

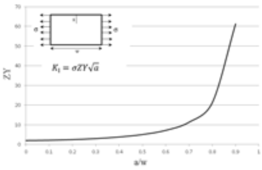


Fig. 3. Plot of ZY (nondimensionalized SIF) vs the variation of *a/w* for plane strain condition

1.2. SIF for Two Bonded Layer by Fully Cracked Film

Fig. 4 shows a crack channeling through a pre-tensioned film on a semi-infinite substrate. The crack is confined by the film/substrate interface in the direction perpendicular to the interface.

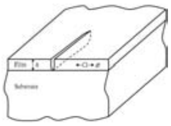


Fig. 4. Steady-state crack channeling across the film for the fully cracked film

For the fully cracked film problem, with its crack tip at the interface (Fig. 4), the KI is as the following form [15],

$$K_I = \sigma f_{(\alpha,\beta)}(\pi h)^s \tag{4}$$

Where f(α,β) is a non-dimensionalized SIF and a function of Dundurs' (His work shows that for any problem of a composite body made of two isotropic, elastic materials with prescribed tractions, the material dependence of the problem is reduced from three dimensionless parameters to the two "Dundurs parameters" α and β) parameters. For plane strain problems α and β are given by [12];

$$\alpha = \frac{\bar{E}_f - \bar{E}_s}{\bar{E}_f + \bar{E}_s} \quad (5)$$

$$\beta = \frac{1}{4}\frac{\bar{E}_f(1-\nu_f)(1-2\nu_s) - \bar{E}_s(1-\nu_s)(1-2\nu_f)}{\bar{E}_f(1-\nu_f)(1-2\nu_s) + \bar{E}_s(1-\nu_s)(1-2\nu_f)} \quad (6)$$

Where $\bar{E} = E/1-\nu^2$, Furthermore, the compilation by Suga et al. [16] indicates that for most practical material combinations, values of a typically lie between β= 0 and β= α/4. The stress singularity exponent, s in Eq. 7, is a function of α and β, too, and satisfies the following equation derived by Zak and Williams [17];

$$\cos(s\pi) - 2\frac{\alpha-\beta}{1-\beta}(1-s)^2 + \frac{\alpha-\beta^2}{1-\beta^2} = 0 \quad (7)$$

Values of s as a function of α for β= 0 and β= a/4 are plotted in Fig. 5.

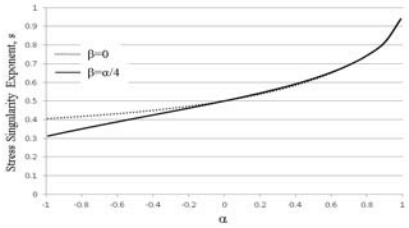


Fig. 5. Plot of crack tip singularity exponent, *s*, vs α for *β = 0* and *β = α/4*.

2. Finite Element Simulation

Consider a composite consisting of an infinite layer of width h and a half space (Fig. 6). The half space can be assumed to approximate a semi-infinite substrate with average material constants as well as a homogeneous substrate. The layer is perfectly bonded to the half space (i.e. the bonding agent is neglected). There is a transverse crack in the layer. The film is subject to a uniform tensile stress σ and the substrate is stress-free (Fig. 6).

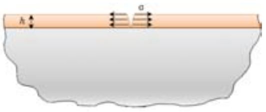


Fig. 6. Fully cracked film under tensile stress

Fig. 7 shows the geometry and the boundary conditions of the plane-strain problem. The crack is represented by the line CD. The thickness of the film is h. The substrate has an infinite thickness. The model is fully fixed along AB. The vertical boundary EF is subjected to an initial tensile stress (σ = 1 Pa) and other boundaries are traction free. At equilibrium, the film and the substrate deform so that the tractions along the crack faces vanish and the crack opens. For each set of material properties of the film and the substrate, solutions were sought with various values of Ef/Es and νf/νs in order to obtain the asymptotic solution for an isolated single crack with a semi-infinite substrate.

The finite element meshes are generated as follows. First divide the whole domain into two regions, as indicated in Fig. 8. In the upper region, the one with the crack, a uniform mesh (number: 101*11) is generated with the plane strain solid continuum four-node bilinear quadrilateral elements (CPE4R). In the lower region, semi-infinite substrate, the mesh (number: 101*1) is generated with the plane strain solid continuum infinite four-node linear quadrilateral elements (CINPE4). The meshes of the regions are compatible in their intersection, and also alignment of the crack with the elements is convenient for the computation of the opening displacement.

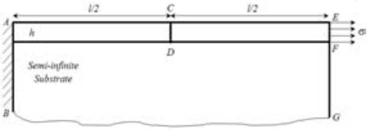


Fig. 7. The FEM model of the plane-strain problem: geometry and boundary conditions.

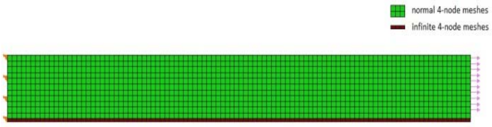


Fig. 8. The FEM model of the plane-strain problem:assigning mesh to the film and the semi-infinite substrate

3. Results and Discussion

For the two-dimensional analysis, the two type of SIF (KI and KII) are related to the energy release rate, G, as follow [18],

$$G = \frac{1}{\bar{E}}(K_I^2 + K_{II}^2) \quad (8)$$

In the previous studies of cracking in thin films (e.g., [1]), a unifying dimensionless number Z has been defined such that the energy release rate for a crack is,

$$G = Z\frac{\sigma_0^2 h}{\bar{E}} \quad (9)$$

where $\bar{E}$ is the plane-strain modulus of the film. The number Z is a dimensionless driving force, depending on the cracking pattern. Huang et. al. [2], modeled dimensionless energy release rate of channeling cracks by XFEM and obtained that energy release rate has increased by increasing α.

For the channeling crack in the present study, the first type of SIF (KI) of a two bonded elastic layers was calculated using finite element method. Different Poisson's ratios, νf/νs, of 0.5, 0.9, 1, 2, 3, 4, 5 and the elastic modulus ratios, Ef/Es, of 0.1, 0.2, 0.3 … 8, 9, 10 were choosing for calculation, because all different materials can be located in this range.

The variation of the SIF for different elastic ratios is presented in Fig. 9, 10. It can be seen, the change of the KI value for different modulus ratios decreases by decreasing Poisson's rations. In the case of no elastic mismatch (α=β=0), the stress singularity reduces to the square root singularity of a crack tip in a homogeneous elastic material, i.e. s= 0.5 (Eq. 7), and KI has the minimum values (Fig. 9). When the substrate is stiffer than the film (α < 0), the singularity is weaker, i.e. s < 0.5, and KI values are lower. When the substrate is more compliant than the film (α > 0), the singularity is stronger, i.e. s > 0.5, and KI values are higher. For an extremely compliant substrate (α → 1), the singularity exponent approaches 1(s → 1) and KI has the maximum value. All the results can be tabulated in Table 1.

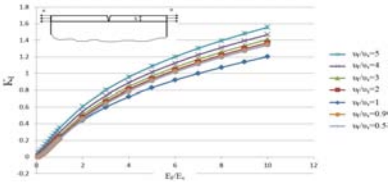


Fig. 9. Variation of KI with different Poisson's ratios, νf/νs, and Young's modulus ratios.

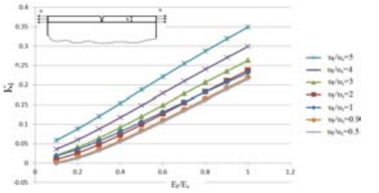


Fig. 10. Variation of KI with different Poisson's ratios, νf/νs, and Young's modulus ratios, Ef/Es, of 0.1-1 for detail.

Table 1. Summary of the results

Property		Dundurs' parameters		S (Eq. 7)	SIF	Non-dimentional energy release rate [2]	Status
E_s ↑	E_f -	α ↓	β -	s ↓	K_I ↓	ω_I ↓	good
ν_s ↑	ν_f -	α ↓	β -	s ↓	K_I ↓	ω_I ↓	good
E_f ↑	E_s -	α ↑	β -	s ↑	K_I ↑	ω_I ↑	bad
ν_f ↑	ν_s -	α ↑	β -	s ↑	K_I ↑	ω_I ↑	bad

4. Conclusion

The infinite elements, for an elastic fracture mechanic problem, have been used to characterize the cracking of thin films bonded to thick substrate materials. The SIF has been extracted from the simulations. The SIF of the plane-strain problem depends on the elastic mismatch between the film and the substrate. The result demonstrates that the infinite elements can be applied to model problems with different elastic properties of films and substrates. SIF for channeling crack has obtained as a function of elastic mismatch ratio between the substrate and the film. Results show that KI has the minimum value in Ef/Es=0.1 and νf/νs=0.5 condition and it has the maximum value in Ef/Es=10 and νf/νs=5. In general view KI has the minimum value when νf=νs. Because of there is no results in this form, qualitative comparisons with the available previous studies (i.e. Non-dimentional energy release rate [2]) show good general agreements.

References

1. Smith, T.F., Waterman, M.S.: Identification of Common Molecular Subsequences. J. Mol. Biol. 147, 195--197 (1981)
2. Hutchinson J.W, Suo Z, Mixed Mode Cracking in Layered Materials, Adv. Appl. Mech., 29, 63-191 (1992).
3. Huang R, Prevost J.H, Huang Z.Y, Suo Z, Channel-cracking of thin films with the extended finite element method, Eng. Fract. Mech., 70, 2513-26 (2003).
4. Evans A.G, Drory M.D, Hu M.S, The cracking and decohesion of thin films, J. Mater. Res. Soci., 3, 1043-49 (1988).
5. Ye T, Suo Z, Evans A.G, Thin Film Cracking and the Roles of Substrate and Interface, J. Solid Struct., 29, 2639-48 (1992).
6. IRWIN G.R, Structural Mechanics (Edited by J. N. Goodier and N. J. Hoff), Pergamon Press: Oxford, 1960.
7. Gecit M.R, Fracture of A Surface Layer Bonded to A Half Space, Int. J. Eng. Sci., 17, 287-95 (1979).
8. Cook T.S, Erdogan F, Stresses in bonded materials with a crack perpendicular to the interface, Int. J. Eng. Sci., 10, 677-97 (1972).
9. Erdogan F, Biricikoglu V, Two bonded half planes with a crack going through the interface, Int. J. Eng. Sci., 11, 745-66 (1973).
10. Bogy D.B, The plane elastostatic solution for a symmetrically loaded crack in a strip composite, Int. J. Eng. Sci., 11, 985-96 (1973).
11. Gupta G.D, A layered composite with a broken laminate, Int. J. Solid Struct., 9, 1141-54 (1973).
12. Arin K, A note on the fracture of laminated composites, Lett. Appl. Eng. Sci., 3, 81-5 (1975).
13. Dundurs J, Edge-bonded dissimilar orthogonal elastic wedges, J. Appl. Mech., 36, 650-52 (1969).

Safety requirements for the organization

Vladislav Stefka[1]

[1]Facultyof Applied Informatics, Tomas Bata University in Zlín, NadStráněmi 4511, 760 05
Zlín, Czech Republic, stefka@fai.utb.cz

Abstract. The essence of security planning in the commercial security industry is to create a scientifically substantiated program activity systems apparatuses commercial security industry in order to achieve the objectives

Keywords: Safety planning, Technical requirements, Internal control system

1 Introduction

The starting point for the organization's overall security policy (strategy) organization. The overall security policy of the organization is the most general expression of the fundamental principles of the principles and means to ensure the security of the organization. The overall security policy is the starting point for information security policy of the organization. The term information security organization understand all safety measures to protect the information regardless of the method of processing and storage (regardless of whether the information is stored on paper, electronically, or otherwise). Information Security Policy of the organization is the basis for the formulation of security policy in the IS organization.

The goal of IS security policy is to ensure the safety of operation of information systems used in the organization with regard to the security of information entering the system, contained therein and extending it. So to prevent, eliminate, minimize, or otherwise overcome the threats and risks, which may be an information system for the organization realistically rendering, without organization suffered significant damage. The content of IS security policy is very similar to the overall security policy organization, IS security policy must address the following issues:

- Aim IS securitypolicy,
- Descriptionoftheinformation system and evaluate its importance for the functioningoftheorganization,
- Thelegislativebasis,
- Definecategoriesofimportanceofinformation,
- Definethepossiblethreats and risks to IS,
- Theprinciplesofpersonnelpolicyforthe IS,
- Principlesoforganizational and administrative (regime) measuresapplicable to IS,
- Technical and operational IS security,
- Databackuppolicies,

- Definesecurityservicesthatmeetthe IS,
- Addressthe IS recovery in thecaseofaccidents,
- Determinemethodologyforcrisis and emergencysituations, etc.

Comprehensive security solutions organization presents design:

- Comprehensivesafety expert information security organization (or complexexpertise IS) in terms of whichwillbemade,
- Anoverallanalysisof IS (analysis bases, resources and environment, a descriptionof IS, etc.),
- Risk Analysis,
- Formulationofalternativesolutions,
- Definingthe IS securitypolicy,
- Project IS security and itsimplementation.

One of the basic criteria of IS is that the system must satisfy the conditions laid down by generally applicable laws and regulations, technical standards and generally recognized standards - if any. Blending European and domestic space is evident in the editing existing state legislations of the European Union, but unfortunately do not always change for the better. However, we will address those areas of computer technology and information technology. For the analysis of IS security and risk analysis are available today, such as:

- TCSEC - the so-called Orange Book (Orange Book) 18 - defined criteria provide a uniform set of basic requirements and evaluation classes to determine the effectiveness of security controls built into automaticdataprocessingsystems,
- ITSEC - thereis a defined term evaluation of the course. Defining 7 classes depending on the level of guarantees and ten other classes. According to the results, the evaluatorshallissue a certificate,
- CRAMM (CCTA) comesfrom the UK and is a method of risk analysis. The method distinguishes two basic activities - risk analysis and risk management,

  Thepurposeof security analysis is to propose IS IS security function while respecting organizational options (especially financial). The most important part of this analysis is theanalysisofrisks.

2During the safety planning

Safety planning is done on a partial safety analysis, one based on partial safety forecasting, safety concepts and their synthesis in ensuring the overall safety concept of corporate security. In the overall project meet the security interests and objectives of the company are based on the development of sub-goals. Framework concept of sub-objectives based on the criteria:

- Places a hazard risks - buildings, plants, various fields of activity - commodity, rooms, spaces,
- Time probability of risks - operating time objects (buildings, equipment, ..), day or night time, time of year, etc,
- Process hazard risks - filling each functional sites of ongoing activities, ongoing technological processes, etc,
- Organization danger risk - the structure, responsibilities border, formal or informal groups, etc.

Principles of safety planning:

- Completeness and linking security measures - either individual measures envisaged in draft form optimization, or project must build on each other and must also be linked to each other,
- The adequacy of security measures - we realize just such security measures that are appropriate both in terms of security objectives and in terms of the permissible boundaries of self-help and self-defense within the limits of a real emergency. Security measures must be in compliance with the safety objectives,
- Action by security measures - planning and execution of safety measures must be qualified to implement and capable of risks and damage, and the risks and damages must be able to minimize it. We require these security measures achieve the desired state in meeting safety objectives and must assume the risk of situations which could be different safety measures more difficult or completely impossible,
- Practical security measures - security is not a business goal, but a means to the successful implementation of complex business objectives respective companies,
- Comprehensive security measures - Safety measures must be designed to counter the overall threat to security in the respective company. Thus it is not just concentrate on the elimination or reduction of risk of each risk or harm, but to protect the security must be considered as a complex,
- Alternative approach to security planning - Safety planning should be made in several variants. Criteria for the creation of variants can be ease when security interests, the relationship between physical protection, technological protection.

The complexity of the security measures - Safety measures must be designed to counter the overall threat to security in the respective company. Thus it is not just concentrate on the elimination or reduction of risk of each risk or harm, but to protect the security must be considered as a complex.

- Alternative approach to security planning - Safety planning should be made in several variants. Criteria for the creation of variants can be ease when security interests, the relationship between physical protection, technological protection and the internal protection, etc. For each variant is necessary to determine the pros and cons and what level of risk the individual variants admit. The sponsor will decide which option is selected, no option may not admit excessive risks. Comfort protection of security interests is reflected in the cost of implementing security measures for their implementation.

Safety requirements

- Safety requirements provide guidance on the establishment of internal security management in an enterprise, regardless of its size, type of activities, character, etc. Safety requirements are designed for businesses and entrepreneurs subject to the supervision of the state professional supervision within the meaning of § 3 of Act No. 174 / 1968 Coll. , As amended.

3Terms and terminology

Audit - a safety audit is a management tool comprising a systematic, documented, periodic and objective, expert assessment and evaluation of the safety management system in place in the monitored area. This area includes risk prevention system operational incidents and accidents, environmental protection, including legislative background. The aim is to verify the function of the safety management system in the company. This takes the form of the outer (external) or intrinsic (internal), or self-audit. The output document is the final report of the audit findings and conclusions.

- External audit - carried out by an independent professional organization or body,
- Internal audit - performed by professionals or specialized departments of their own business (safety management).

Work safety - protection of life and health of persons, property and the environment from the adverse effects of work processes and all other activities which are not directly related to work processes, but ultimately this may cause danger.

Department - are all places where employees are, or where you are going to do their job. They are also places where the premises with the knowledge of the employer and subject to the direct or indirect supervision.

Regulations - legal and other regulations to ensure the safety and health at work. These transcripts of radio:

- Regulations on the protection of life and health,
- Regulations hygienic and anti-epidemic,
- Transcripts of safety of technical equipment and technical standards
- Traffic regulations,
- Regulations on fire protection,
- Regulations on handling flammables, explosives, weapons, radioactive substances, toxins and other substances that are harmful to health.

Under regulations to ensure the safety and health at work are considered as the rules for safety and health at work issued by central authorities or employers in consultation with the relevant authorities.

Internal control - planned, organized, systematic control activities, tailored and implemented to ensure compliance with the requirements and regulations - in all activities at all levels and stages of the business. Internal checks are done every senior employee in the workplace, for which it is responsible.

Security policy - written an aspiration senior management to ensure the security, to make commitments in the field of security and visibility of these activities both inside and outside the company.

Near miss - a real event that occurred in which could be dangerous to life and health, property (or simultaneously), but only a coincidence to avoid this effect.

Safety management - is an effective, self-regulating system, providing integrated security management in an enterprise that implements management (business management) on the basis of security policy, the involvement of all employees.

Riskmanagement - management system (reducing) risk, which includes the activities to identify, quantify and eliminate the risk or reduce risks to an acceptable level.

Education - education which includes initial, periodic and special training:

- Induction training - training of staff upon taking up employment before their mandate a particular job, the relevant safety regulations and rules of safe behavior in the workplace and in full working process, ie training of legal and other regulations to ensure BOZ at work (in § 273 of the Labour Code No. 262/2006 Coll.), the legislation relating to environmental protection and accident prevention,
- Periodic training - is periodic training on the dates set by the regulations, or employer,
- Special training - training and practical work-out specialists in special activities performed by them.

4Principles of internal security management company

Implementation of the system - the need to establish an effective and efficient system of health and safety, the environment and property incurred at the time the decision to manage human resources efficiently and implement such a documented set of management and control components which allow both efficient use and the possible exclusion of failure, regardless of how they are involved in economic activity. To control the same principles apply as for the management of economic activities. Safety management must be taken as an organic part of the management of all business activities and should be understood as an economic, ethical and humane approach part of entrepreneurs to address all activities. Is referred to as continuous activity, and therefore controlled, provision and required by senior management of the company.

5Conclusion

Among the sub-steps of the safety plan also includes security policy, which is another very important activity. Many companies, however, until now no such concept have developed. It is not necessary to wait until the first incident, but security policy should be applied preventively. However, this is an excellent resource on which you build an entire system of security. The essence of planning is also creating several options for learning the direction of where to draw the planning. For the organization, this means surround yourself with a good team led by a qualified security manager.

References

1. Grasseová Monika, Bohumil Brecht: Effective decision making: analyzing decision-making, implementation and evaluation. . 1st edition Edik Brno 2013, ISBN 978-80-7454-312-8
2. Kerzner, Harold C.: Using the Project managemant Model: Strategic Planning for Project Management. Second edition 2005 ISBN 978-0-471-69161-7
3. Yeates, Donald and James Cadle: Business analysis 2nd edition London, Britisch Computer Society 2010 ISBN 978-190-6124-618.
4. Pile M. et al. : Critical Infrastructure Protection in the Czech energy sector in 2014 1st edition ISBN 978-80-7385-144-6
5. National Counsil Safety: Safety Management Systems 2014, available from: http:/www.nsc.org./safety _ work /

A comparison of PSO and BFO applications for the PID controller synthesis in time-delay systems

Ilir Juniku[1], Petraq Marango[2]

[1] Department of Electrical Engineering, Polytechnic University of Tirana,
Tirana, Albania, ijuniku@hotmail.com

[2] Department of Electrical Engineering, Polytechnic University of Tirana,
Tirana, Albania, marango@fie.upt.al

Abstract. Time delay systems are very common in industry. Their study has been in the focus of worldwide research, taking into consideration the problems associated with their difficult control. PID controllers have found wide application in the control of time delay processes. The classical approaches for obtaining the K_p, K_i and K_d parameters of these controllers usually result in overshoot, and significant rising and settling times. In this paper we have proposed the application of PSO and BFO intelligent algorithms for obtaining the optimal parameters of a PID controller, applied in the control of a high order process with time delay. The performance of the proposed control system with PSO and BFO algorithms is analyzed through time response characteristics. A comparison of the proposed approaches, with the cases where integral performance indexes are used to determine the PID parameters, is also introduced. From the obtained results, we conclude that, when applied to time delay processes, the intelligent algorithms achieve better control performance than classical methods.

Keywords: Integral performance index (IAE, ISE, ITAE, ITSE), PID controller, PSO algorithm, BFO algorithm.

1 Introduction

Delays are usually present in control systems as computing or processing delays or as delays in information acquiring. Time delays are common in industrial processes which are characterized by energy and materials' transport, such as chemical, biological, information, and also measuring, and computing processes. Time delays introduce problems in process control due to decrease of robustness and performance deterioration, which bring the systems close to instability. To achieve the control of such processes, PID controllers have found wide application. Given that approximately 95% of the control schemes in practice are built on PID controllers, finding the right parameters that improve at maximum the control performance, poses a challenge in itself. Their popularity is related to the fact that they are simple to understand and to operate by operators, and are effective and robust in control.

There exist many methods for the calculation of the PID optimal parameters, in order to obtain a specific characteristic of process time response. To check the effectiveness of various methods for PID controllers, the comparison is usually made by analyzing the transient characteristics of the system.

The characteristics obtained by tuning the PID parameters, often do not meet the control performance criteria defined by the designer. For this reason, latest research is focused on optimization methods based on intelligent algorithms, which result very efficient in solving difficult optimization problems.

Algorithms, inspired by characteristics and organized behaviors of organisms and microorganisms in nature, have recently achieved an increasing interest. Among the algorithms that have been inspired by nature, the most common are particle swarm optimization (PSO) and bacterial foraging optimization (BFO) algorithms. These two optimization methods are the main focus of this work and our proposal is to apply them in finding the optimal PID parameters, in a high order control system with time delay.

Integral of absolute error (IAE), integral of squared error (ISE), integral of time multiplied absolute error (ITAE) and integral of time multiplied squared error (ITSE) integral performance criterions are proposed as optimization functions in our case. These performance indexes will be used to obtain the coefficients of PID controller, and the process transient responses will be analyzed and compared with the methods of obtaining PID coefficients from PSO and BFO algorithms.

The structure of the article is as follows. Section 2 presents the proposed control schemes for the high-order process with time delay, transient response measures and also the integral performance indexes used as optimization (cost) functions to find the coefficients of PID controllers. In section 3, PSO and BFO algorithms are treated, and their application in finding the coefficients of PID controllers. The process that will be considered for various simulations with classical methods (IAE, ISE, ITAE, ITSE) and intelligent methods (PSO and BFO) is presented in section 4. Conclusions obtained from simulations are presented in section 5. Algorithms and computational simulations are performed in MATLAB R2013b environment.

2 Optimization Functions

2.1 Control Scheme

The proposed control scheme for finding the optimal coefficients of PID controller is illustrated in Fig. 1.

Signals presented in the control scheme are:

R(s)-reference signal. In this case the reference signal is a step unit function.

Y(s)-output signal of the system

U(s)-control signal

E(s)-error signal. Derived from *E(s)=R(s)-Y(s)*

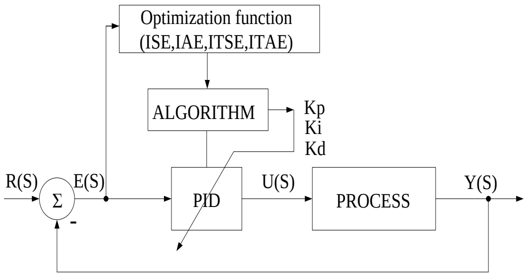


Fig. 1. Proposed control scheme for the process.

Proposed PID controller is in its parallel form, provided by the algorithm:

$$u(t)= K_p e(t)+ K_i \int_0^t e(\tau)d\tau +K_d \frac{d}{dt} e(t) \tag{1}$$

where

u(t)-control signal in time domain

K_p -proportional coefficient, a tuning parameter

K_i -integral coefficient, a tuning parameter

K_d -derivative coefficient, a tuning parameter

e(t) -error signal in time domain

In Fig. 2 is presented the typical PID controller structure in its parallel form. The process that will be studied is a single input-single output (SISO) third order system with time delay, which depicts many processes in industry.

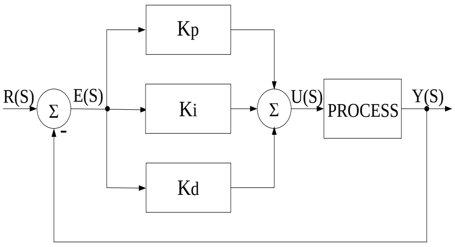


Fig. 2. Structure of PID controller.

The mathematical model of delay e^{-Ls} according to [1] can be approximated by a rational transfer function of the form:

$$G_i(s)=\frac{1}{\left(1+\frac{Ls}{i}\right)^i},\ i=1,2,\ldots \tag{2}$$

which is an *i*-th order truncation of expression

$$e^{-Ls} = \lim_{i\to\infty} \frac{1}{(1+Ls/i)^i} \tag{3}$$

2.2 Transient Response Measures

Analysis for the process transient response in time domain is done through performance quantities [2] like:
-Rising time t_r: time required for the output of the system to reach 90% of its final value $h(\infty)$.
-Settling time t_s: time after which the output remains within ±2% of the final value $h(\infty)$.
-Peak value h_{max}: peak value of the transient response $h(t)$ of the process.
-Peak time t_{peak}: time required for the transient response $h(t)$ to reach the peak value h_{max}.
-Overshoot M_r $(\%)$: output value exceeding final, steady-value of the process, expressed in percentage.
Rising and settling times are measures of response speed of the system. Overshoot, peak value, and peak time are related measures to the quality of response.

2.3 Integral Performance Criteria

In classical control methods, the performance of the entire control system can be estimated quantitatively using a single parameter that is the integral quality criterion J. This performance index is useful in treating optimization of parameters and obtaining optimal control designs. According to [3], a system is considered as an optimal control system when the system parameters are tuned to achieve an integral criterion ekstremum, which is usually a minimum value. So, integral criterion should always be a positive number or equal to zero $J \geq 0$. The best achievable control system is the system that minimizes this criterion. The general form of the integral performance criterion is:

$$J = \int_0^T f(e(t),r(t),y(t),t)dt \tag{4}$$

where f is a function of error, input, ouput signals and time. The most common integral criterions are:

- Integral of squared error $ISE = \int_0^T e^2(t)dt$ (5)

where T is a finite time, chosen arbitrarily, in order for the integral to approach the final stabilized value of the system. Generally T is chosen as equal to t_s-settling time.

-Integral of absolute error $IAE = \int_0^T |e(t)|dt$ (6)

-Integral of time multiplied absolute error $ITAE = \int_0^T t|e(t)|dt$ (7)

-Integral of time multiplied squared error $ITSE = \int_0^T te^2(t)dt$ (8)

3 Intelligent Algorithms

3.1 PSO Algorithm

PSO is created by Eberhart and Kennedy in 1995 [4], [5]. The method is suitable for solving nonlinear problems. This algorithm is inspired by natural behavior of animals, such as organized behavior of birds in flock for finding food [6], [7]. PSO algorithm operates using a population (called swarm) of a potential candidate solution (called particles). These particles move around a search space according to a specific routine (law). Movements of particles are guided by their best known position in the search space and also the best known position by the whole flock. When better positions are detected, these positions guide the further movement of the particles. The process is repeated until a satisfactory solution is reached. In this optimization method, a set of particles are placed in a d-dimensional space with a random specified speed and position. The initial position of the particle is taken as the best position in the beginning and then particle speed is reassessed based on the experience of other particles of the flock (population).

From [8], PSO algorithm elements are:

-the i-th particle in the population represented by:

$$x_i = (x_{i1}, x_{i2}, x_{i3}, \ldots x_{id}) \tag{9}$$

in the d-dimensional space

-previous best positions of the i-th particle are represented by:

$$P_{opt} = (P_{opt_{i,1}}, P_{opt_{i,2}}, P_{opt_{i,3}}, \ldots P_{opt_{i,d}}) \tag{10}$$

-the index of the best particle in the swarm is $G_{opt,d}$

-the speed of the i-th particle is represented by $V_i = (v_{i1}, v_{i2}, v_{i3}, \ldots v_{id})$ (11)

-reassessed speed and distance from $P_{opti,d}$ in $G_{opti,d}$ is given by the law:

$$\begin{aligned} V_{i,m}^{t+1} &= W \cdot V_{i,m}^{t} + C_1 \cdot rand() \left(P_{opt_{i,m}} - X_{i,m}^{t}\right) + C_2 \cdot rand() \left(G_{opt_m} - X_{i,m}^{t}\right) - X_{i,m}^{(t+1)} \\ &= X_{i,m}^{(t)} + V_{i,m}^{(t+1)} \end{aligned} \tag{12}$$

for $i=1,2,3,\ldots n$; $m=1,2,3,\ldots d$

where m number of particles in swarm, d dimension index, t iteration index, $V_{i,m}^{(t)}$ the particle speed in iteration i, W weighting factor of inertia, C_1, C_2 acceleration constants, $rand()$ random number between 0 and 1, $X_{i,d}^{(t)}$ actual position of the i-th particle in iteration, P_{opti} best previous position of the i-th particle, G_{opt} the best particle among all particles of the population.

The flowchart of PSO algorithm is illustrated in Fig. 3.

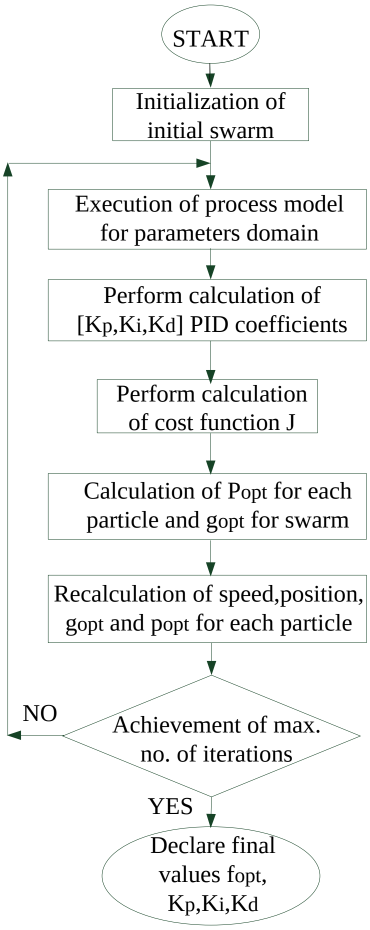

START
Initialization of initial swarm
Execution of process model for parameters domain
Perform calculation of [Kp,Ki,Kd] PID coefficients
Perform calculation of cost function J
Calculation of Popt for each particle and gopt for swarm
Recalculation of speed,position, gopt and popt for each particle
NO
Achievement of max. no. of iterations
YES
Declare final values fopt, Kp,Ki,Kd

Fig. 3. Flowchart of PSO algorithm.

3.2 BFO Algorithm

BFO is based on research conducted by K.M. Pasino [9], [10], related to development and behavior of E.coli bacteria. In this optimization method there are four typical behaviors that imitate nature [11]:

1) **Chemotaxis** This process resembles the movement of a bacterium (E.coli) through swimming and displacement via flagella. Biologically an E.Coli can move in two different ways. It can swim for a period of time in the same direction, or it can move alternatively between two modes of movements throughout lifetime. To represent a shift we use a casual direction with a given unit size by $\theta(j)$. This presentation is used to determine the movement direction after a displacement. In particular: $\theta^i(j+1,k,l)=\theta^i(j,k,l)+C(i)\cdot\theta(j)$. where $\theta^i(j,k,l)$ represents the i-th bacterium in the j-th chemotaxis, the k-th

reproduction, the *l*-th elimination and dispersal step *C(i)* is the size of the step taken in a random direction specified by the unit size *θ(j)*.

2) **Swarming** E.coli bacteria organize themselves into well-structured colonies with high environmental adaptability using a complex communication mechanism. To create the colonies, bacteria produce signals which are attractive to each other. Analytical presentation of this process is:

$$J_{cc} = (\theta, P(j,k,l)) = J^{i}_{cc}(\theta, \theta^{i}(j,k,l)) = \sum[D_{attractant} \cdot e^{(-W_{attractant} \cdot \sum(\theta_m - \theta^{i}_{m})^{2}}] + \\ + \sum[H_{repellant} \cdot e^{(-W_{repellant} \cdot \sum(\theta_m - \theta^{i}_{m})^{2}}] \tag{13}$$

where $J_{cc}(\theta,P(j,k,l))$ is the value of the optimization function (to be minimized) to represent a cost function that depends on time. *S* is the total number of bacteria; *P* is the number of parameters to be optimized, which are present in each bacteria and $D_{attractant}$, $W_{attractant}$, $H_{repellant}$, $W_{repellant}$, are different coefficients that should be chosen carefully.

3) **Reproduction** Less healthy bacteria die and each healthier bacteria split into two daughter bacteria, each located in the same position.

4) **Elimination and Dispersal** In the local environment, it is possible that the bacteria life of a population can change gradually (e.g. through the consumption of nutrients) or abruptly from other influences. It may happen that in a zone all the bacteria die, or a group is dispersed in a new environment. They can destroy the progress of chemotactic effect, but they can also help the effect, if dispersal occurs in areas with good food sources. From a broader perspective, elimination and dispersal are part of the motion behavior of the population for long distances.

Flowchart of BFO algorithm [12] is illustrated in Fig. 4.

4 Simulation Results

In this study we have taken a third order process with time delay, which has a characteristic with many oscillations.

$$G(s)= \frac{1}{0.31s^{3} + 1.75s^{2} + 3s} e^{-3s} \tag{14}$$

As shown in section 2.1, the delay in time will appear in a rational function form:

$$G_{delay,1}(s) = e^{-3s} = \frac{1}{3s+1} \tag{15}$$

The transfer function to be considered during the simulations is:

$$G(s)= \frac{1}{0.93s^{4} + 5.56s^{3} + 10.75s^{2} + 3s} \tag{16}$$

In PSO and BFO algorithms that realize the minimization of the integral performance indexes in cost function form, the PID parameters are used as input values and as output is used the optimization value of the PID controller model (17).

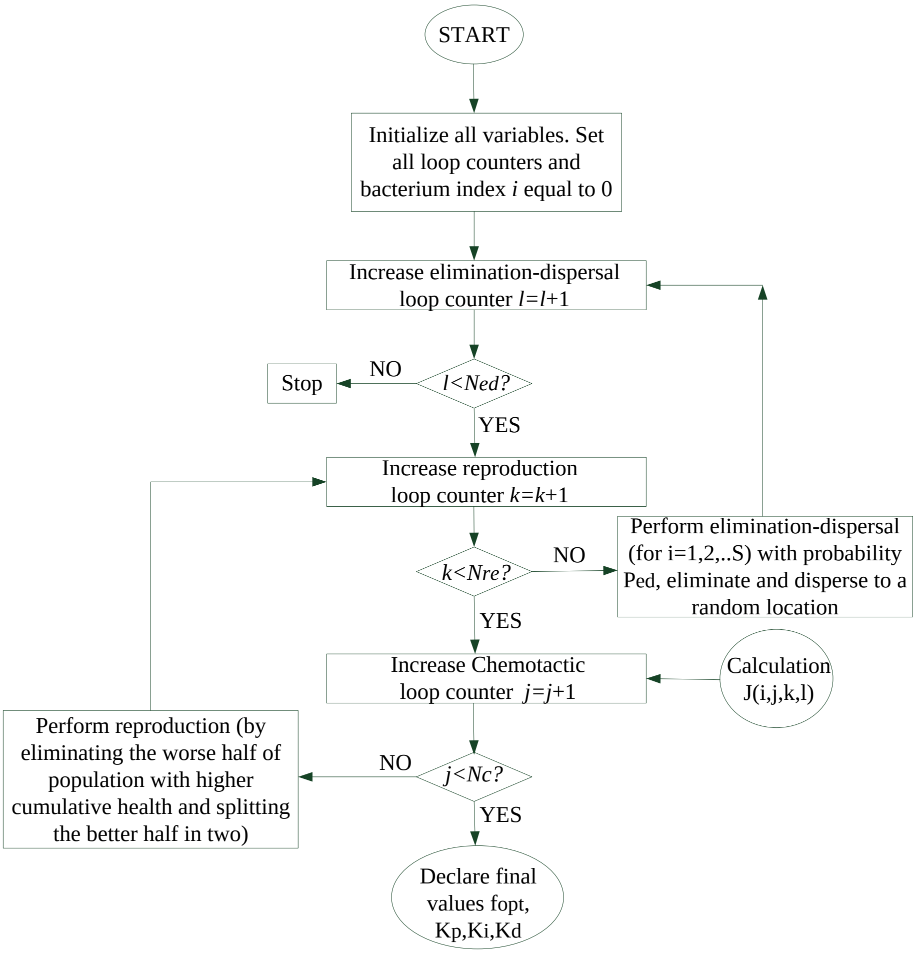

START
Initialize all variables. Set all loop counters and bacterium index *i* equal to 0
Increase elimination-dispersal loop counter *l*=*l*+1
l<*Ned?*
NO
Stop
YES
Increase reproduction loop counter *k*=*k*+1
k<*Nre?*
NO
Perform elimination-dispersal (for i=1,2,..S) with probability Ped, eliminate and disperse to a random location
YES
Increase Chemotactic loop counter *j*=*j*+1
Calculation J(i,j,k,l)
j<*Nc?*
NO
Perform reproduction (by eliminating the worse half of population with higher cumulative health and splitting the better half in two)
YES
Declare final values fopt, Kp,Ki,Kd

Fig. 4. Flowchart of BFO algorithm.

$$Function\ [J]=integral\ criteria\ (K_d,K_p,K_i) \tag{17}$$

In the proposed control scheme (Fig. 1), it is intended to tune the three coefficients of PID controller, in order to obtain the best output results, or otherwise said, is intended to optimize the PID coefficients to achieve optimal results. Integral criterions used as cost functions, evaluate the performance of various combinations of PID coefficients in a 3-dimensional search domain. Each point in this 3-dimensional search domain for the proposed algorithm, represents a certain combination of *[Kp, Ki, Kd]* coefficients, for which a certain transient response of the system is achieved.

4.1 Classical Approach

Using IAE, ISE, ITAE, ITSE integral criterions, treated in Section 2.3, in Fig. 5 are obtained the transient responses of our process. Executing the algorithms [13], we obtain the corresponding coefficients of PID controller for the four performance criterions. PID controller coefficients, obtained by the classical algorithms are shown in Table 1.

Table 1. PID controllers obtained by classical algorithms.

Performance Index	Coefficients of PID controllers		
	K_p	K_i	K_d
ISE	3.042	0.001987	22.1
IAE	2.328	3.997e-15	1.582
ITSE	3.505	2.753e-05	14.69
ITAE	8.596	1.518	13.26

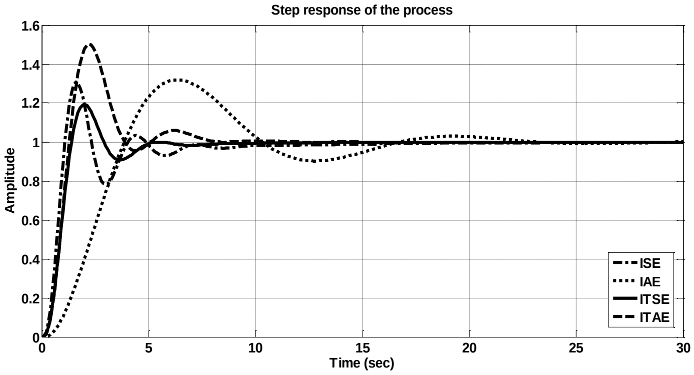


Fig. 5. Transient responses for classical algorithms.

4.2 Intelligent PSO and BFO algorithms approach

In order to find the PID controllers coefficients by the intelligent algorithms PSO and BFO, in this study we have used the 3-dimensional search domain where the K_p, K_i, K_d values are the three dimensions of domain. In both algorithms, the four integral criterions of time domain, treated in Section 2.3, were chosen as optimization functions. The algorithms were executed in Matlab R2013b environment where as cost functions were used:

- ISE: *J=e'*e*dt*
- IAE : *J=sum(abs(e)*dt)*
- ITSE: *J=(t.*e'*dt)*e;*
- ITAE: *J=sum(t'.*abs(e)*dt)*

The number of computing iterations that the algorithms will perform, is based on the calculations duration and complexity of the optimizing problem. The initial constants for the computing PSO algorithm were taken $W=0.3$, $C_1= C_2=1.5$.At the end of PSO algorithm execution, at Matlab prompt are displayed the *[Kp, Ki, Kd]* items of search domain, which is the final point of global optimum noted as g_{opt}, that corresponds to the minimum value of cost function, noted as f_{opt}.

Coefficients of PID controllers, obtained by intelligent PSO algorithm are shown in Table 2. In Table 2 are also shown the best (minimum) values of cost functions (integral criterions).

Table 2. PID controllers obtained by PSO algorithms

Algorithm	**Coefficients of PID controllers**			f_{opt}
	K_p	K_i	K_d	
PSO-ISE	0.8587	0.3290	18.7447	0.7002
PSO-IAE	3.4373	0.3114	14.1379	1.6575
PSO-ITSE	3.6658	0.1784	9.2223	0.6179
PSO-ITAE	5.2616	0.3611	11.2419	5.1510

The constants used for the initialization of the computing program in BFO algorithm are taken $D_{attractant}=0.01$, $W_{attractant}=0.01$, $H_{repellant}=0.01$, $W_{repellant}=0.01$. Table 3 presents the values of PID controller coefficients obtained by BFO algorithm, and the corresponding minimum values of cost functions.

Table 3. PID controllers obtained by BFO algorithms

Algorithm	**Coefficients of PID controllers**			f_{opt}
	K_p	K_i	K_d	
BFO-ISE	1.5823	1.5187	17.8117	0.7865
BFO-IAE	8.1119	0.4878	8.7152	1.9695
BFO-ITSE	4.3073	0.8238	6.7563	1.7230
BFO-ITAE	5.7679	0.7655	7.2006	4.2287

Tables 4,5,6 present the transient response measures for the three cases.

Table 4. Characteristics of transient responses for classical approach

Characteristics	**Classical approach**			
	IAE	**ISE**	**ITSE**	**ITAE**
Rising time t_r	25.29	6.59	8.60	7.84
Settling time t_s	210.13	95.95	48.77	75.08
Overshoot $M_r (\%)$	31.82	30.82	19.31	50.27
Peak value h_{peak}	1.32	1.31	1.19	1.50
Peak time t_{peak}	64	17	21	23

Table 5. Characteristics for transient responses for PSO approach

Characteristics	PSO approach			
	IAE	ISE	ITSE	ITAE
Rising time t_r	0.83	0.72	1.09	0.89
Settling time t_s	21.39	102.42	17.45	12.17
Overshoot $M_r(\%)$	22.2	20.52	18.22	30.27
Peak value h_{peak}	1.22	1.21	1.18	1.30
Peak time t_{peak}	1.97	1.67	2.59	2.3

Table 6. Characteristics for transient responses for BFO approach

Characteristics	BFO approach			
	IAE	ISE	ITSE	ITAE
Rising time t_r	0.73	0.91	1.19	1.07
Settling time t_s	100.68	9.26	7.62	10.87
Overshoot $M_r(\%)$	24.04	53.12	38.7	46.18
Peak value h_{peak}	1.24	1.53	1.39	1.46
Peak time t_{peak}	1.75	2.59	3.44	3.06

Fig. 6 presents the process transient responses obtained by PSO algorithm for various optimization functions.

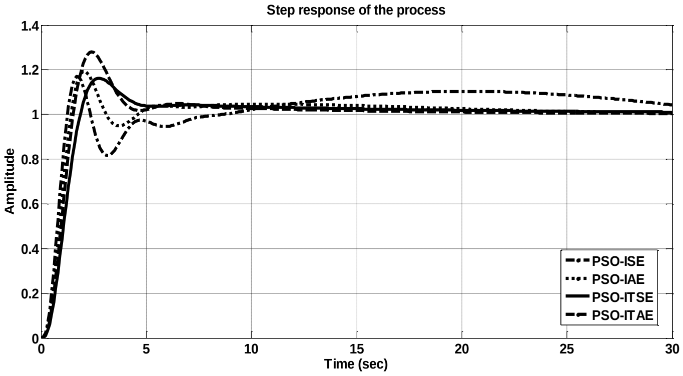


Fig. 6. Transient responses for PSO algorithms.

Fig.7. presents the process transient responses obtained by BFO algorithm, for various optimization functions.

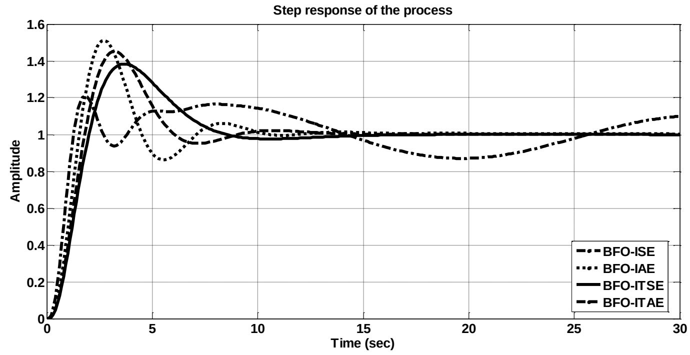


Fig. 7. Transient responses for BFO algorithms.

Fig. 8. presents the best transient responses of process obtained by ITSE, PSO-ITSE, BFO-ITSE algorithms.

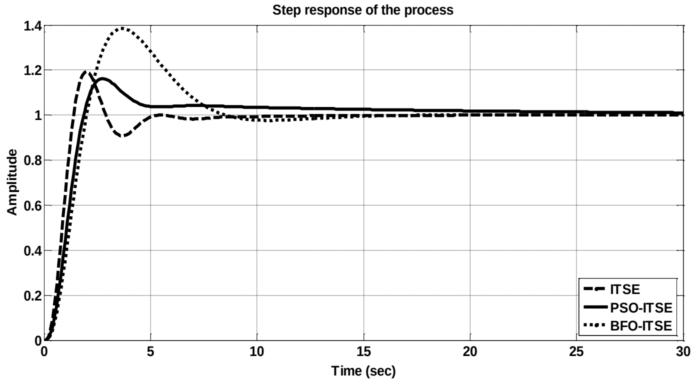


Fig. 8. Best transient responses for the process.

5 Conclusions

Based on the performed simulations, we arrive at the conclusion that methods based on PSO and BFO intelligent algorithms are quite efficient in achieving a very good control of processes with time delay. Specifically, the resulting rise time t_r and settling time t_s are reduced further, resulting in control systems that have a faster response to changes at the system's input. From Tables 4, 5, 6, we conclude that ITSE integral criterion, used as a cost function to find the optimal values of K_p, K_i, K_d coefficients of PID controller is the best function that can be used for the methods discussed above. Comparing the results from the application of intelligent algorithms, we concluded that the PSO algorithm is more efficient and provides a better tuning of the process. It provides the best value (minimum value) of the cost function f_{opt} . PSO algorithm has simpler computing architecture than BFO algorithm, resulting in a faster algorithm in computing time.

References

1. Normey-Rico, J.E., Camacho, E.F.: Control of Dead Time Processes, pp.22, Springer, New York (2007).
2. Marango, P.: Bazat e Automatikes (in albanian), pp.128, SHBLU, Tirana (2011).
3. Dorf, R.C., Bishop, R.H.: Modern Control Systems, 12th ed., pp. 330-332, Prentice Hall (2010).
4. Kennedy, J. and Eberhart, R. C.: Particle swarm optimization. In: Proc. IEEE int'l conf. on neural networks Vol. IV, pp. 1942-1948. IEEE service center, Piscataway, NJ, (1995).
5. Eberhart, R., Kennedy J.: A New Optimizer Using Particle Swarm Theory. In: Proc of 6th International Symposium on Micro Machine and Human Science, pp.39-43, Nagoya, Japan (1995).
6. Eberhart, R. C. and Shi, Y.: Particle swarm optimization: developments, applications and resources. In: Proc. congress on evolutionary computation 2001, pp.81-86, IEEE service center, Piscataway, NJ., Seoul, Korea, (2001).
7. Bai, Q.: Analysis of particle swarm optimization algorithm. In: CIS Journal of Computer and Information Science Vol. 3, No 1, February 2010, pp.180-184, (2010).
8. Haupt, R.L., Haupt, S.E.: Practical Genetic Algorithms, 2nd ed., pp. 189-190, Wiley (2004).
9. Liu, Y., Passino, K.M.: Biomimicry of Social Foraging Bacteria for Distributed Optimization: Models, Principles, and Emergent Behaviors. In: Journal of Optimization Theory and Applications (2002).
10. Das, S., Biswas, A., Dasgupta, S., and Abraham, A.: Bacterial Foraging Optimization Algorithm: Theoretical Foundations, Analysis, and Applications. In: A. Abraham, A.E. Hassanien, P. Siarry, A. Engelbrecht (Eds.), Foundations of Computational Intelligence, Studies in Computational Intelligence, vol. 3, Springer, Berlin, Heidelberg, 2009, pp. 23–55, (2009).
11. Passino, K.M.: Bacterial Foraging Optimization. In: International Journal of Swarm Intelligence Research, 1(1), pp.1-16, January-March 2010 (2010).
12. Dasgupta, S., Das, S., Abraham, A.: Adaptive Computational Chemotaxis in Bacterial Foraging Optimization: An Analysis. In: IEEE Transactions on evolutionary computation, vol. 13, no. 4 (2009).
13. Cao, Y.: Learning PID Tuning III: Performance Index Optimization, http://www.mathworks.com/matlabcentral/fileexchange/18674-learning-pid-tuning-iii-performance-index-optimization.

An efficient VM load balancer for Cloud

Ansuyia Makroo[1], Deepak Dahiya[1]

[1]Dept. of CSE & ICT, Jaypee University Of Information Technology, Waknaghat, HP, India
{komal.mahajan, deepak.dahiya}@juit.ac.in

Abstract. Cloud computing is filling the gap as a fifth utility service by building higher capabilities of IT infrastructure. This also lends the cloud for research as one of the focus areas. Cloud researchers lack the opportunity to work with real cloud test beds. The cloud simulation tools available in academia and research have limitations like dependency on programming for simulation setup; for further deployment of new load balancing algorithms, the understanding of underlying simulator architecture is required. Further non availability of a single snapshot of multiple simulation exercise and non availability of database support is not another disadvantage. This paper addresses these issues to a great extent by introducing a cloud simulation tool with enhanced features like algorithm editor, multiple simulation comparator and database support. The proposed features provide an abstraction to the simulator application. This allows researchers to focus on better analysis of the behavior of applications rather than understanding the implications and working of the underlying architecture.

Keywords: Virtual Machine (VM), Load balancing, CloudAnalyst, Data center, Virtualization, Cloud Computing, Spatial distribution

1 Introduction:

In this era of evolving infrastructure-less computing, the user community started exploring options of moving from traditional infrastructure investment to outsourcing infrastructure deployment based on the utility model. Alongside, the research community started realizing the need of the hour to move from the much hyped utility computing models to the more realistic cloud. The IT service sector realized that the major investments of any new startup were involved in purchase and maintenance of physical infrastructure and manpower resources, so they saw an opportunity in the philosophies of infrastructure-less and utility computing thus resulting in the evolution of a new computing paradigm termed as cloud computing. Thus, Cloud computing can be defined as follows:

"Cloud computing is the delivery of computing as a service rather than a product, whereby shared resources, software, and information are provided to computers and other devices as a utility (like the electricity grid) over a network (typically the Internet) [2]. "

"Cloud computing is defined as "a type of parallel and distributed system consisting of a collection of inter-connected and virtualized computers that are dynamically provisioned and presented as one or more unified computing resources based on service-level agreements established through negotiation between the service provider and consumers [3]".

Sun Microsystems (now acquired by Oracle) [4*] "takes an inclusive view that there are many different types of clouds like public cloud, private cloud, and hybrid cloud. Many different applications can be built by using these clouds."*

As per Forbes [1], Cloud-enabling technologies revenue will reach as high as $22.6 Billion by 2016. So, considering the growing importance of cloud, new ways to improve the cloud services is an area of concern and research focus.

Cloud computing is a layered model [13]. The generalized layered architecture of the cloud is shown in Figure 1. Cloud computing environment has four major layers viz. Physical Layer, Virtualization Layer, Platform Layer, Application Layer. The bottom most layer is the Physical layer that consists of rack of physical devices (processing, storage etc.) called as Servers. Above this layer is the Virtualization Layer. The Virtualization layer abstracts the underlying layer by virtually partitioning the physical devices in the underlying layer into virtual resources that can used to deploy the user requests. On the top of this layer is the Platform layer. This layer consists of operating system and application framework on which user applications can be deployed. This layer maps the user requests on the underlying Virtualization layer which are in turn physically deployed on the actual Physical layer. Above this layer i.e. at the highest level is the Application layer on which actual user's applications are present which are actually deployed on the underlying layers. Since the actual deployment of user requests is to be done on the VMs in the Virtualization layer. So there needs to be some mechanism to schedule the user's requests on the VMs. For this VM load balancing algorithms are used . In this paper, the authors have proposed an algorithm for VM load balancing called as Stateful Throttled VM load balancing algorithm that is an improvement over already existing Throttled VM Load balancing algorithm [5,11].

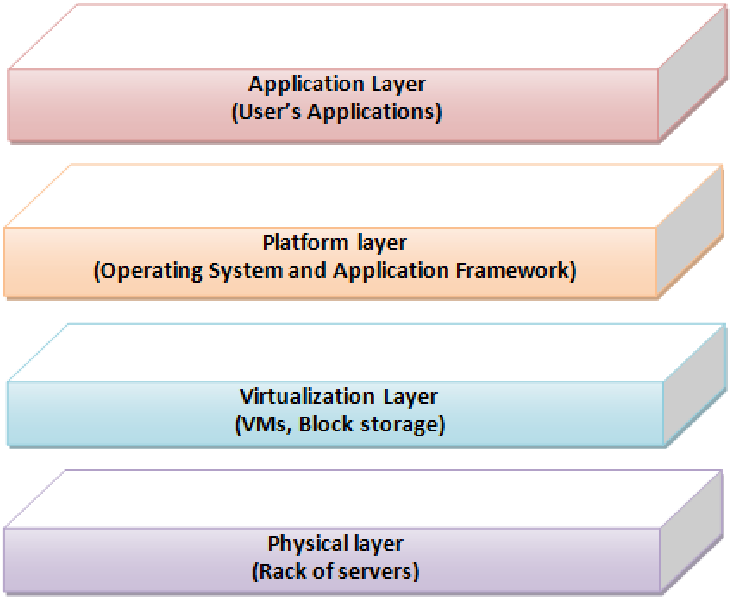


Fig. 1. Layered architecture of cloud

1.1 Motivation and Problem Definition

The growing popularity of cloud, its utility model will soon make it a Fifth utility service [15] which will add it to the list of other four popular utility services viz.: electricity, telephone, water and gas. Considering the immense popularity of the above four services, we can visualize, how popular the cloud computing model is going to be and how it is going to revolutionize the way people use computing resources. One of the biggest obstacle to the growth of cloud computing is performance unpredictability [15]. Multiple VMs share the same CPUs and main memory. A very important task in the cloud is to properly schedule the user's tasks on the VM in such a way that

VMs are efficiently utilized. Also, the response time and processing time needs to improve to provide better services and to satisfy the Service Level Objectives (SLOs) [16].

This leads us to the following problem definition i.e.

To develop Stateful Throttled VM load balancing algorithm for the cloud and to do a comparative analysis of the proposed algorithm with the existing algorithms.

This problem definition leads us to the following broad objectives that are summarized below:

- To setup the simulator i.e. CloudAnalyst.
- To identify the appropriate data sets and formulate corresponding test cases.
- To implement the algorithm on CloudAnalyst and analyze its performance
- Comparison of the proposed algorithm with the existing algorithms on identified parameters

The rest of the paper is organized as follows: Section 1 introduces of the proposed work. Section 2 includes a related study on available cloud simulators and the VM Load Balancing algorithms. Section 3 gives a detailed description of the proposed algorithm (i.e. Stateful Throttled VM Load Balancing algorithm). Section 4 describes the Mathematical model for Stateful Throttled VM load balancing algorithm. Section 5 describes the experimental setup and the simulation and parameter configuration. Section 6 includes the comparative analysis of Throttled VM Load Balancer and Stateful Throttled VM Load Balancer. Finally, Section 7 and 8 summarize the conclusion; limitations and the future scope of work respectively.

2 Related Study

Load balancing [25] is a process of dividing and distributing large processing jobs among different processing units to enhance the overall performance of the system. The task of load balancing is to improve both resource utilization and job response time by avoiding overloading or under loading of any specific node in a distributed system environment, thereby achieving the SLOs [34]. Virtualization is the enabling technology for cloud resource sharing [35]. A key component in private/hybrid clouds is the virtual infrastructure management and load balancing [32]. A physical node in a cloud is virtually divided into a number of Virtual Machines.[33] The task of VM Load balancing algorithms in the cloud based infrastructure is to allocate the VMs to incoming service requests/jobs in an efficient way such that it gives better response time and data center processing time for the user's jobs by maximum utilization of underlying resources in an optimum manner [31].

Load balancing algorithms, can be categorized into static and dynamic load balancing   algorithm [36]. A static load balancing algorithm does not maintain the state of the previous behavior of a node while distributing the load. A dynamic load balancing algorithm maintains and checks the previous state of a node while distributing the load.

The Figure 2 gives the overview of generalized architecture of the cloud [16]. The Data Center Controller [11] uses a VM Load Balancer to determine which VM should be assigned the next Cloudlet [11]. Cloudlet is an instance of request received from a Userbase for process. The VM load balancer plays a very important role in the overall response time and processing time of the cloud.

Fig. 2. Generalized architecture of a Cloud [16]

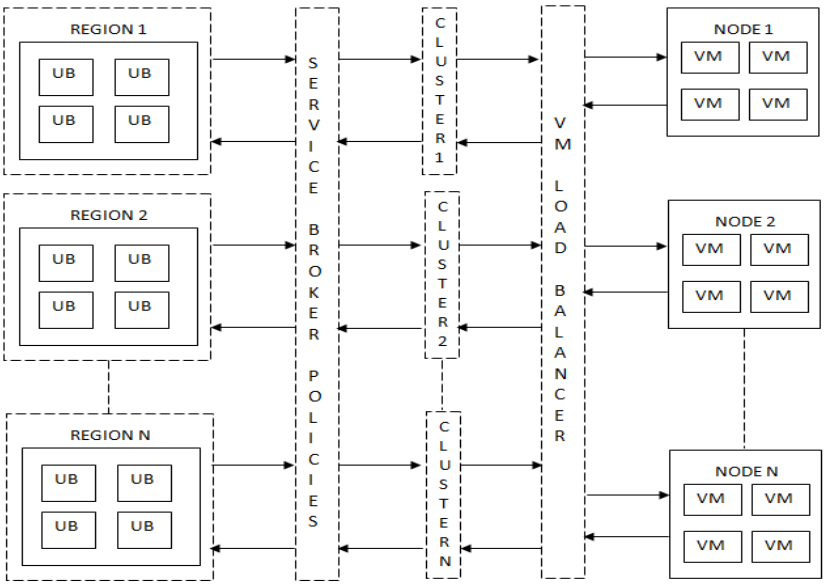


Fig. 2. Generalized architecture of a Cloud [16]

The various available VM Load Balancing algorithms are summarized in the Table 1:

Table 1: Available VM load balancing algorithms

Round Robin VM load balancing Algorithm[5, 11, 26]	It allocates the VMs to the incoming requests in a round robin fashion without considering the current load on each VM. It does not take into account the previous load state of a node at the time of allocating jobs.
Weighted Round-Robin Algorithm[27]	It a form of Round Robin VM load balancing Algorithm in which each VM is assigned a specific weight. The number of requests assigned to a VM depend on its weight. It works in the same manner as Round Robin VM load balancing Algorithm if all the VMs have equal weights.
Round Robin with Server Affinity[16]	It is a form of Round Robin Algorithm which saves the state of previous allocation of the request from a given Userbase and the next time a request is received from the same Userbase, the same VM can be allocated to it without using Round Robin algorithm.
Min-Min[28]	Min-Min algorithm finds the minimum completion time for all the unassigned jobs. It then selects the job with least minimum completion time and assigns it to the node that produces the minimum completion time for the jobs. The ready time of the node is updated. This process continues till all the unassigned jobs are allocated nodes. One of the major drawback of this algorithm

	is that it may lead to starvation of some jobs.
Max-Min[29]	Max-Min is similar to Min-Min algorithm. However in this algorithm, the node with minimum completion time for all jobs is assigned the job with the overall maximum completion time. The ready time of the node is updated. This process is repeated until all the unassigned tasks are assigned. The idea of this algorithm is to reduce the wait time of the large jobs. ⍰.
Active Monitoring Load Balancer[5,11]	This loads balancer allocates the VMs to the tasks in such a way that evens out the active tasks on each VM at any given time.
Honeybee Foraging Algorithm[30]	This load balancing technique is based on behavior of honey bee foraging strategy. This algorithm not only balances the load, but also takes into consideration the priorities of tasks that have been removed from heavily loaded Virtual Machines.
A Fuzzy-based load balancing[31]	The FLC-based algorithm is used to correctly evaluate the load status of a host in heterogeneous computing system. It can also efficiently determine the suitable host for migrating jobs.
Throttled Load Balancer [5,11]	This algorithm ensures only a pre-defined number of Internet Cloudlets are allocated to a single VM at any given time. If more request groups are present than the number of available VM's at a data center, some of the requests will have to be queued until the next VM becomes available.

Researchers interested in analyzing the performance of their applications or in testing their scheduling algorithms on cloud do not have the opportunity to work with real cloud test beds because of the huge expenditure involved in the set up of the same. So, to carry out research in the area of cloud computing, the researchers can work with the available cloud simulation tools to test their applications and algorithms.

Cloud computing is related to grid computing as both the computing technologies are based on large scale distributed resources [2]. To carry out research in the area of grid computing, various popular simulators are available viz. Gridsim [9], Simgrid [12, 18], OptorSim [19] and GangSim [20].

Although, grid simulators can simulate a large scale distributed environment. However, unlike grid computing, cloud computing uses virtualization technologies at various levels for resource sharing and dynamic resource pooling to provide various services viz. IaaS, PaaS, SaaS [21]. Moreover, cloud is based on the pay per use i.e. utility model [15]. So, grid simulators cannot simulate a virtualized cloud environment based on utility model and thus cloud simulators were proposed. Some popular cloud simulators are CloudSim[6,7,8], CloudAnalyst[5,11], GreenCloud[22], NetworkCloudSim[23].The CloudSim[6] toolkit supports modeling and creation of one or more virtual machines (VMs) on a simulated node of a Data Center, jobs, and their mapping to suitable VMs. It also allows simulation of multiple Data Centers to enable a study on federation and associated policies for migration of VMs for reliability and automatic scaling of applications. CloudAnalyst [5, 11] is built directly on top of CloudSim [6] toolkit, leveraging the features of the original framework and extending some of the capabilities of CloudSim. GreenCloud [22] provides a simulation environment for energy-aware cloud computing data centers. GreenCloud is designed to capture details of the energy consumed by distributed environments. NetworkCloudSim [23] supports modeling of real Cloud data centers and generalized applications such as HPC, e-commerce and workflows. Out of all the above simulators, CloudAnalyst is the most suitable to analyze the proposed VM load balancing algorithm in different scenarios as CloudAnalyst provides users with the capability to modify and test their algorithms with the help of user friendly GUI (Graphical User Interface). This motivated the authors have used CloudAnalyst for testing and comparison of the VM load balancing algorithm.

3 Proposed Algorithm: Stateful Throttled VM load balancing Algorithm

The Throttled VM load balancing algorithm maintains a threshold value for all VMs which is the maximum number of cloudlets that can be assigned to a given VM. The VM can be in one of the two states i.e. busy or available. A VM is available if the number of cloudlets allocated to it is less than its threshold value, otherwise it is busy. When a VM is busy, no more cloudlets can be allocated to it. If at a given instance, all the VMs are busy, requests need to be queued until one of the VM becomes available. One of the major drawbacks of the Throttled VM load balancing algorithm is that it does not save the state of allocation of given Userbase to a particular VM due to which the algorithm needs to re-run every time a request is received.

This limitation is overcome in the proposed algorithm i.e. Stateful Throttled VM load balancing algorithm as whenever a cloudlet is received from a Userbase, state information of the current allocation to the Userbase is stored for future reference So the next time a cloudlet is received from the same Userbase the entire algorithm for load allocation need not be re-run as the state information for the Userbase can be used to assign the appropriate VM.

The Stateful Throttled VM load balancing algorithm, is based on the principle of locality of reference. That is, at a given point of time, cloudlet generation is concentrated mainly to the same Userbase. So if a request comes from the same Userbase there is no need to run the Throttled VM load balancing algorithm every time to allocate a VM . Instead, the same previously allocated VM can be allocated to the Userbase by using the stored state information. This saves a lot of time. This algorithm has two edge cases. One is when a Userbase generates the first cloudlet for the cloud. In this case there is no entry for the Userbase in the hashmap, so the Throttled VM load balancing algorithm need to be run and the state information is saved for future reference. This entry can be used to determine the VM to be allocated for consequent request from the same Userbase. Secondly, when the allocated VM attains the threshold value, the Throttled VM needs to run again as the current VM is busy. In this case, the state information for the current Userbase needs to be updated.

The algorithm utilizes two the tables to store the state information:

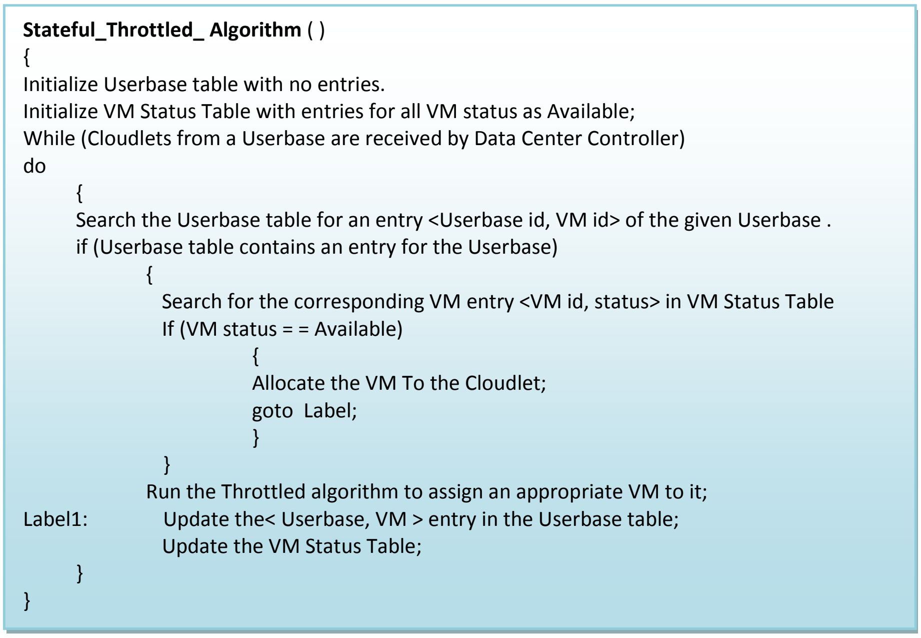
- **Userbase Table**: Userbase table consists of two entries <*Userbase Id, VM id*>. The algorithm will be able to benefit from the Userbase table only if the searching based on Userbase Id can be done is minimum possible time. The ideal data structure that can be used to implement a Userbase Table in this scenario is a hashmap which stores the key value pairs

<Userbase Id, VM id> such that the VM id corresponding to the key Userbase id can be retrieved and updated in the constant time.

- **VM Status Table**: VM state table stores the current status of the VM i.e. Busy or available. As explained above, a VM is available if the number of Cloudlets assigned to it are less than the threshold value otherwise it is busy. To implement the VM state table, the. ideal data structure that can be used is hashmap which stores the key value pairs *<VM id, Status>*. The VM status table will be able to retrieve and update the status of a VM in constant time.
- The working of the Stateful Throttled VM load balancing Algorithm is given below:

Whenever a cloudlet arrives at the datacenter controller, the datacenter controller uses the Userbase table to find the entry of the Userbase. An entry does not exist for a given Userbase only if sends the first cloudlet to the Datacenter. If the entry *<Userbase Id, VM id>* exists in the Userbase table, then it uses this state information entry to allocate the VM. However this VM can be allocated only if the current status of the VM is available. So to check the VM status the data center controller checks the VM Status Table for *<VM id, Status>* of the corresponding VM. If the status of the VM is available , the it can allocate the corresponding VM. In this scenario, a constant time is required to allocate a VM since searching of Userbase table and VM Status Table entry requires a constant time. However, there are two other cases. Firstly, when a Userbase entry does not exist in the Userbase Table. Secondly, when a Userbase entry exists in the Userbase Table however the VM Status Table shows the VM is busy. This is when the VM attains the threshold value. In both the above cases, the Throttled VM load balancing algorithm need to be run to allocate an appropriate VM to the Userbase Cloudlet. Also, the state information *<Userbase Id, VM id>* in the Userbase table and the VM status information *<VM id, Status>* in the Userbase table need to be updated.

The proposed algorithm i.e. Stateful Throttled VM load balancer and the related flowchart are given in Figure 3 and 4 respectively.



```
Stateful_Throttled_ Algorithm ( )
{
Initialize Userbase table with no entries.
Initialize VM Status Table with entries for all VM status as Available;
While (Cloudlets from a Userbase are received by Data Center Controller)
do
      {
      Search the Userbase table for an entry <Userbase id, VM id> of the given Userbase .
      if (Userbase table contains an entry for the Userbase)
               {
                 Search for the corresponding VM entry <VM id, status> in VM Status Table
                 If (VM status = = Available)
                            {
                            Allocate the VM To the Cloudlet;
                            goto  Label;
                            }
                 }
               Run the Throttled algorithm to assign an appropriate VM to it;
Label1:          Update the< Userbase, VM > entry in the Userbase table;
                 Update the VM Status Table;
      }
}
```

Fig. 3. Stateful Throttled VM Load Balancing Algorithm

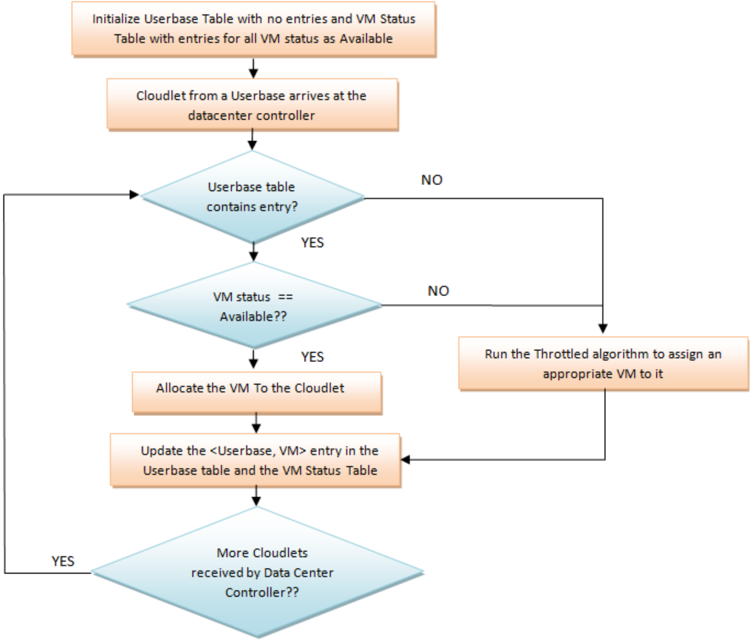

Initialize Userbase Table with no entries and VM Status Table with entries for all VM status as Available
Cloudlet from a Userbase arrives at the datacenter controller
Userbase table contains entry?
NO
YES
VM status == Available??
NO
YES
Allocate the VM To the Cloudlet
Run the Throttled algorithm to assign an appropriate VM to it
Update the <Userbase, VM> entry in the Userbase table and the VM Status Table
YES
More Cloudlets received by Data Center Controller??

Fig. 4. Flowchart for Stateful Throttled VM Load Balancing Algorithm

The following sections demonstrate that the Stateful Throttled VM Load Balancing algorithm is an improvement over the already existing Throttled VM load balancer.

4 Mathematical Model for Stateful Throttled VM Load Balancing Algorithm

The proposed algorithm also lends itself to a linear programming model [37] formulation to minimize the objective of overall operational cost i.e. average response time and overall average datacenter processing time and other identified constraints such as VM image size, VM memory, VM bandwidth, Data center (Architecture, OS, Data center, VMM, Number of Machines, Memory per Machine, Storage per machine, Available BW per Machine, Available BW per Machine, Number of processors per machine, Processor speed , VM policy), User Grouping Factor, Request Grouping Factor, Executable Instruction Length etc.

In general, the minimizing objective for the any model formulated as an LP model is

$$\text{Minimize } Z=c_1x_1+c_2x_2+\ldots\ldots\ldots\ldots\ldots\ldots+c_nx_n \qquad (1)$$

subject to constraints

$$a_{11}x_1+a_{12}x_2+\ldots\ldots\ldots\ldots\ldots\ldots a_{1n}x_n >= b_1 \qquad (2)$$

$$a_{21}x_1+a_{22}x_2+\ldots\ldots\ldots\ldots\ldots\ldots a_{2n}x_n >= b_2$$

$$:$$

$$:$$

$$a_{m1}x_1+a_{m2}x_2+\ldots\ldots\ldots\ldots\ldots\ldots a_{mn}x_n >= b_m$$

where

$$x_i \ \ldots\ldots\ x_n>=0 \ \& \ b_i>=0$$

Now, if c_1, c_2.............c_n be the cost associated with response time, processing time etc.

So, the objective of minimizing cost can be formulated as

$$\text{Minimize } Z= c_1x_1+c_2x_2+\ldots\ldots\ldots\ldots\ldots\ldots c_nx_n \qquad (3)$$

Now let $x_1,x_2,\dots\dots\dots\dots x_n$ be the variables associated with response time (R), processing time (P), CPU (C), Userbase request and other constraints specified in table 1 respectively.

So then the variables will take the polynomial form,

$$
\begin{gathered}
a_{11}x_1+a_{12}x_2+\dots\dots\dots\dots a_{1n}x_n \qquad (4)\\
a_{21}x_1+a_{22}x_2+\dots\dots\dots\dots a_{2n}x_n\\
:\\
:\\
a_{m1}x_1+a_{m2}x_2+\dots\dots\dots\dots a_{mn}x_n
\end{gathered}
$$

Since the objective is to minimize the overall operational cost in terms of response and processing time, CPU time and optimize Userbase request, the problem is formulated as

$$
\begin{gathered}
a_{11}x_1+a_{12}x_2+\dots\dots\dots\dots a_{1n}x_n <= R_1 \text{ (minimize response time)} \qquad (5)\\
a_{21}x_1+a_{22}x_2+\dots\dots\dots\dots a_{2n}x_n <=R_2 \text{ (minimize data center processing time)}\\
:\\
:\\
a_{(m-1)1}x_1+a_{(m-1)2}x_2+\dots\dots\dots\dots a_{(m-1)n}x_n <=R_{m-1} \text{ (minimize Waiting time)}\\
a_{m1}x_1+a_{m2}x_2+\dots\dots\dots\dots a_{mn}x_n >= R_m \text{ (maximize CPU utilization)}
\end{gathered}
$$

Since the problem definition is not in the standard form, so problem could not be formulated as a dual problem with a maximization objective due to non adherence to Von Neuman duality principle [37]. Since duality cannot be addressed for the above scenario, the authors proposed approach address the non- standard constraints individually by introducing a constraint specific solution i.e.

To minimize the response time, we use a hashmap entry (i.e. slack variable) h_1.

This hashmap entry is also responsible for minimizing the processing time h_2.

Add infrastructure slack variable h_{n-1}

Maximize CPU utilization by allocating more cloudlets by adding surplus variable $-h_n$.

Thus, LP model formulated is,

$$\text{Maximize } Z=-c_1x_1-c_2x_2+\dots\dots\dots\dots-c_nx_n \qquad (6)$$

subject to constraints:

$$a_{11}x_1+a_{12}x_2+\dots\dots\dots\dots a_{1n}x_n + h_1= R_1$$

$$a_{21}x_1+a_{22}x_2+\dots\dots\dots\dots a_{2n}x_n + h_2=R_2$$

$$:$$

$$:$$

$$a_{(m-1)1}x_1+a_{(m-1)2}x_2+\dots\dots\dots\dots a_{(m-1)n}x_n +h_{m-1}=R_{m-1}$$

$$a_{m1}x_1+a_{m2}x_2+\dots\dots\dots\dots a_{mn}x_n - h_m= R_m$$

Thus the mathematical model can be summarized as:

$$\sum_{j=1}^{n} a_{ij}x_j \pm h_i = R_i \quad \text{where } i = 1 \text{ to } m \qquad (7)$$

The above LP model in general can be solved by Simplex method [R] to identify the optimum value of Z (operational cost). Alternatively, from the above mathematical model, the optimum values of $x_1,x_2,\dots\dots\dots\dots x_n$ can be obtained that is incurred for the operational cost constraints.

The soundness of this mathematical model is experimentally verified in section 5.

4.1 Analysis of Stateful Throttled VM Load Balancing Algorithm

As discussed in previous sections, the Throttled Algorithm does not save the state of the previous allocation of a VM to a request from given Userbase, while the same state is saved in the proposed algorithm.

The Stateful Throttled VM load balancer maintains two data structures, which are as listed below.

Userbase Table: It stores the entry for the last VM allocated to a request from a given Userbase

VM State Table: It stores the allocation status (i.e. Busy/Available) of each VM.

Assumptions:

The authors have considered homogeneous VMs with same threshold values

Each node in the cloud has a total of m VMs

To initialize the Stateful Throttled Algorithm, state of all VMs is set to available in the Userbase Table which takes O (m) time. This time has not been included since the complexity of the VM allocation to a Cloudlet received from a Userbase at VM load balancer is being calculated.

Now when a request arrives at the Stateful Throttled VM load balancer from a given Userbase, first of all it hashes the Userbase id in the hash map. If corresponding entry is present in the hash map, then it checks the VM stateliest for the status of the VM. If the VM status is available, it is allotted to the request from the Userbase. Otherwise, the VM Load balancer allocates a new VM using Throttled VM load balancing algorithm and updates the entry of that VM in hashmap. Clearly the whole process of hashing user to VM takes O (1) time and checking whether the VM is available or busy, takes O(1) time.

In the worst case, the only dependency is allocating a new VM using Throttled Load balancing algorithm. So essentially the order of new Stateful Throttled is O (Throttled) i.e. O (m).

The best case is when an entry is present in the hashmap and that the VM is available. In this case time taken is O (1). To conclude, the worst case time complexity of the algorithm to allot a VM to a request from a given Userbase is O (m) and best case is O (1), where m is the number of virtual machines in each node of the Cloud.

4.2 Calculating the effective VM allocation time to a request from a given Userbase

Mathematical Assumptions:

Time taken for searching an entry of a Userbase in Userbase hashmap= t1

Time taken for checking the status of a VM in VM state list= t2

Time taken for processing request using Throttled VM Load balancing algorithm= t3

Let, ‘p’ (0<=p<=1) be the probability of finding an entry for the requesting Userbase in the Userbase hashmap and ‘k’ (0<=k<=1) be the probability of finding the corresponding VM status as available in VM state list.

Allocation time for a request whose entry is present in the Userbase hashmap and the corresponding VM is available= t1+t2 ...(1)

Probability of request to find an entry in the Userbase hashmap and the corresponding VM is available = p*k ... (2)

Allocation time for a request whose entry is present in the Userbase hashmap and the corresponding VM is busy= t1+t2+t3 ... (3)

Probability of request to find an entry is present in the Userbase hashmap and the corresponding VM is busy= p*(1-k) ...(4)

Allocation time for a request whose entry is not present in the Userbase hashmap = t1+t3 ...(5)

Probability of not finding an entry for a request in the Userbase hashmap = 1-p ... (6)

From equations 1, 2, 3, 4, 5 and 6, effective allocation time can be calculated as

Effective allocation time = (t1+t2)*(p*k) + (t1+t3)*(1-p) + (t1+t2+t3)*(p)*(1-k) … (7)

Equation 7 can be simplified as

Effective allocation time = t1+p*t2+ (1-p*k)* t3

In the ideal case,

p =1

k =1

Effective allocation time in the ideal case= t1+ t2

In this case, the throttled algorithm is not executed. Hence, effective allocation time is reduced which leads to decrease in the overall response and processing time.

5 Experimental Setup

To analyze and compare the proposed algorithm, the authors have used the popular social networking site Facebook, whose contents can be deployed on the cloud considering the large size of Facebook user's data. This data also provides a platform to test the efficiency of the proposed algorithm. To carry out simulations and analysis of the proposed algorithm the environment setup and the approach adopted is in line with the one adopted by CloudAnalyst [11]. CloudAnalyst is used as a simulator to compare with the existing algorithm that involves simulating of the Facebook data. As dated on Mar 31, 2012 the approximate distribution of the Facebook [10, 17] user base across the globe is given in the Table 1.

5.1 Simulation and Parameter Configuration

Considering the resource and budget constraints, the research work uses a subset of the data given in Table 1 for simulation. We further define six user bases representing the above 6 regions with the following parameters as shown in Table 2. Table 3 gives the data center and VM configuration used for simulation.

For all practical purposes, the following reasonable assumptions are made:

- Each user base is contained within a single time zone.
- Most of the users use the application after work for about 1 hour.
- 0.05% of the registered users will be online during the peak time simultaneously and only one tenth of that number during the off-peak hours.
- Each user makes a new request every 5 minutes when online.

Table 2. Userbase parameter list across the regions of the globe

Region	Region	Users	Userbase	Peak hrs. (GMT)	Online users during peak hrs.	Online users during off peak hrs.
North America	0	173 million	**UB1**	13:00-15:00	86,500	8,650
South America	1	113 million	**UB2**	15:00-17:00	56,500	5,650
Europe	2	233 million	**UB3**	20:00-22:00	97,500	9,750
Asia	3	195 million	**UB4**	01:00-03:00	116,500	11,650
Africa	4	40 million	**UB5**	21:00-23:00	20,000	1,200
Oceania	5	13 million	**UB6**	09:00-11:00	6,500	650

Table 3. The Data center and VM configuration used for simulation

Parameters	Value used
VM image size	10,000
VM memory	512 MB
VM Bandwidth	1000
Data center – Architecture	X86
Data center – OS	Linux
Data center – VMM	Xen
Data center – Number of Machines	5

Data center – Memory per Machine	*1,024 Mb*
Data center – Storage per machine	*100,000 Mb*
Data center – Available BW per Machine	*10,000*
Data center – Number of processors per machine	*3*
Data center – Processor speed	*100 MIPS*
Data center – VM Policy	*Time Shared*
User Grouping Factor	*1,000*
Request Grouping Factor	*100*
Executable Instruction Length	*250*

6 Comparative Analysis: Throttled VM Load Balancer and Stateful Throttled VM Load Balancer

The two algorithms i.e. Throttled VM Load Balancer and Stateful Throttled VM Load Balancer have been compared based on the scenario given in Table 4. In Scenario 1, we have assumed that we have deployed a web application on a single data center with 100 VMs in Region 0 (North America). In the next scenario we have spatially [24] distributed 100 VMs into 2 data centers such that each data center has 50 VM each. The spatial distribution of 100VMs is done in each scenario till 10 data centers. The VMs have been assumed to have 1024 Mb of memory each and are running on physical processors capable of speed of 100 MIPS

The simulation results that have been used for comparison are based on the following parameters:

- Overall Average Response Time (in ms)
- Overall Average Response Time (in ms)

The comparative graphs that depict the table for Overall Average Response Time (in ms) & Overall Average data center processing time (in ms) are Figure 5 & Figure 6 respectively.

Table 4. Overall comparative results

Scenario	**Overall Average Response Time (in ms)**		**Overall Average Data center Processing time (in ms)**	
	Throttled VM load balancing algorithm	**Stateful Throttled VM load balancing algorithm**	**Throttled VM load balancing algorithm**	**Stateful Throttled VM load balancing algorithm**
1 Data center (DC) with 100 VMs	*1,693.08*	*1,946.13*	*1378.13*	*1,768.80*
2 Data centers with 50 VMs each	*955.26*	*852.90*	*735.36*	*699.06*
3 Data centers with 35,35,30 VMs	*749.17*	*655.23*	*581.44*	*487.22*
4 Data centers with 25 VMs each	*663.92*	*543.67*	*497.23*	*394.11*
5 Data centers with 20 VMs each	*602.20*	*467.67*	*436.35*	*310.54*
6 Data centers with(4 DCs with 15 VMs each and 2 DCs with 20)	*564.67*	*450.78*	*399.14*	*290.65*
7 Data centers with (4 DCs with 15 VMs each and 2 DCs with	*542.23*	*400.79*	*377.22*	*280.20*

10 VM each & 1 DCs with 20 VMs)				
8 Data centers with (6 DCs with20 VMs each and 2 DCs with 20 VMs each)	*527.98*	*390.12*	*363.11*	*273.33*
9 Data centers with(8 DCs with 10VMs and 1 DCs with20 VMs each)	*514.70*	*381.55*	*350.00*	*263.98*
10 Data centers with 10 VMs each	*500.25*	*378.05*	*335.70*	*252.09*

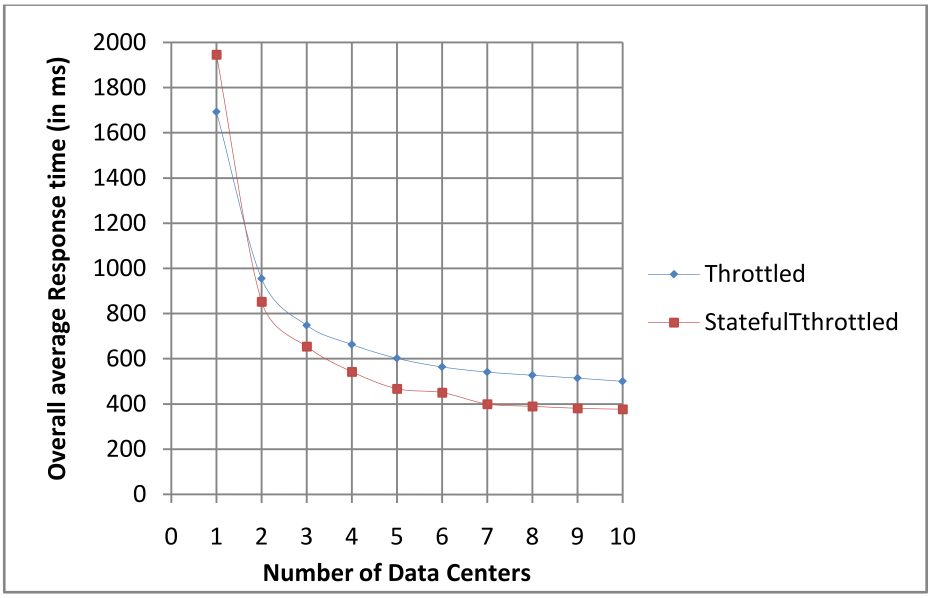


Fig. 5. Graph depicting a comparative analysis of the overall average response time

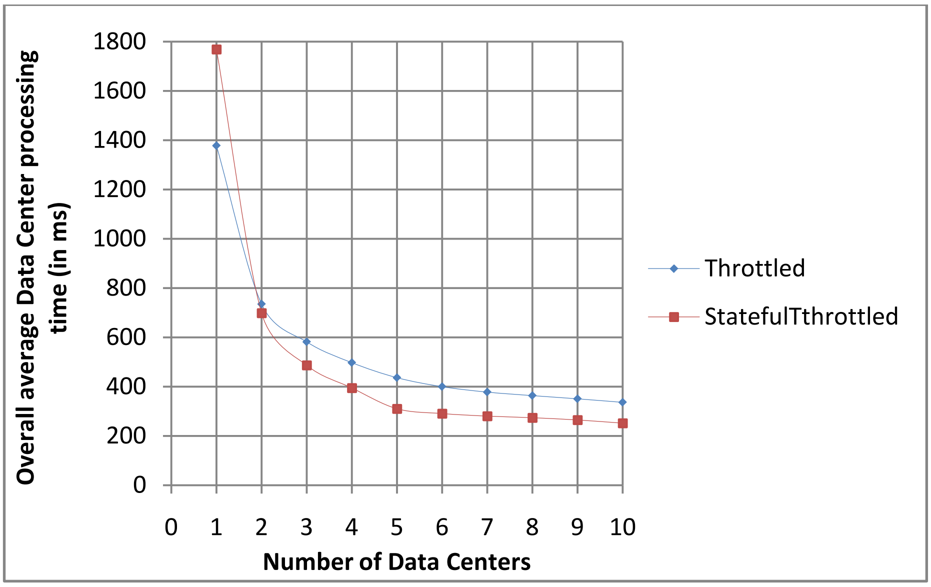


Fig. 6. Graph depicting a comparative analysis of the overall average data center processing time

The comparative analysis summarized in Table 4 and Figures 5 & 6 is given below:

On spatially distributing the VM into multiple data centers, a remarkable decrease in Overall Average Response Time and Overall Average Data center processing time is noticed for both the algorithms.

In case of single data center, the Throttled VM load balancing algorithm gives better Overall Average Response Time and Overall Average Data center processing time than Stateful Throttled VM load balancing algorithm.

On spatial distribution of VMs in multiple data centers, Stateful Throttled gives better Overall Average Response Time and Overall Average Data center processing time than Throttled VM load balancing algorithm.

To conclude, the proposed VM load balancing algorithm i.e. Stateful Throttled VM load balancing algorithm gives better results than Throttled VM load balancing algorithm in terms of experimental and mathematical analysis carried out i.e.

- Spatially distributed data centers
- Best case complexity of algorithm

7 Conclusion

In this era of evolving infrastructure-less computing, the user community started exploring options of moving from traditional infrastructure investment to outsourcing infrastructure deployment based on the utility model. One of the biggest obstacle to the growth of cloud computing is performance unpredictability [15]. A very important task in the cloud is to properly schedule the user's tasks on the VM in such a way that VMs are efficiently utilized. Also, the response time and data center processing time needs to improve to provide better services and to satisfy the Service Level Objectives (SLOs) to the users considering the growing number of cloud providers and ever increasing competition in the cloud. The research work develops an efficient VM load balancing algorithm for the cloud and carried out a comparative analysis of the proposed algorithm with the existing algorithms. Intermediate deliverables included studying the existing VM load balancing algorithms, proposing an efficient algorithm for VM load balancing, mathematical model formulation, implementing the algorithm on CloudAnalyst, and comparing the proposed algorithm with the existing algorithms on identified parameters. The major contribution of the proposed work in the field of cloud computing is that the authors have introduced VM load balancing algorithm i.e. Stateful Throttled VM load balancing algorithm gives better results than Throttled VM load balancing algorithm in case of spatially distributed data centers. The salient features of the proposed algorithm are better Overall Average Response Time and Overall Average Data center processing time in case of spatially distributed datacenters in cloud.

8 Limitations and Future Scope of the Work

The research work carried out in this paper has been tested on a simulator. The results might differ in case of real cloud environment. The results obtained using simulator serve as a basis for the comparison and analysis of the proposed work. The authors plan to test the proposed algorithm on a private cloud environment set up using Eucalyptus. Secondly, homogeneous VMs have been assumed to test the proposed algorithm. The working of the proposed algorithm has not been studied in case of heterogeneous VMs. The authors plan to test the proposed work on heterogeneous VMs also. The authors have not taken into account the fault tolerance in the data center. However, in future they plan to incorporate fault tolerance mechanisms in the proposed VM load balancing algorithm.

References

1. http://www.forbes.com/sites/louiscolumbus/2013/09/20/451-research-cloud-enabling-technologies-revenue-will-reach-22-6b-by-2016/ as on Sep. 2013.
2. Foster, I; Yong Zhao ; Raicu, I. ; Lu, S. “Cloud Computing and Grid Computing 360-Degree Compared”, published in Grid Computing Environments Workshop, 2008. GCE '08 IEEE DOI 12-16 Nov. 2008.
3. R. Buyya, C. S. Yeo, and S. Venugopal, “Market-Oriented Cloud Computing: Vision, Hype, and Reality for Delivering IT Services as Computing Utilities”, Proceedings of the 10th IEEE International Conference on High Performance Computing and Communications (HPCC 2008, IEEE CS Press, Los Alamitos, CA, USA), Sept. 25-27, 2008, Dalian, China.
4. Sun Microsystems, Inc.”Introduction to Cloud Computing Architecture” Whitepaper, Ist Edition, June 2009.
5. Bhathiya Wickremasinghe, Rodrigo N. Calheiros, and Rajkumar Buyya “CloudAnalyst: A CloudSim-based Visual Modeller for Analysing Cloud Computing Environments and Applications” ; Technical Report, CLOUDS-TR-2009-12, Cloud Computing and Distributed Systems Laboratory, The University of Melbourne, Australia, Oct. 23, 2009.
6. R. Buyya, R. Ranjan, and R. N. Calheiros, “Modeling and Simulation of Scalable Cloud Computing Environments and the CloudSim Toolkit: Challenges and Opportunities,” Proc. of the 7th High Performance Computing and Simulation Conference (HPCS’ 09), IEEE Computer Society, June 2009.
7. http://www.dcs.ed.ac.uk/home/hase/simjava/ as on March 2012.
8. F. Howell and R. Macnab, “SimJava: a discrete event simulation library for Java,” Proc. of the 1st International Conference on Web based Modeling and Simulation, SCS, Jan. 2008.
9. R. Buyya, and M. Murshed, “GridSim: a toolkit for the modeling and simulation of distributed resource management and scheduling for Grid computing,” Concurrency and Computation : Practice and Experience, vol. 14, Nov. 2002, pp. 1175-1220.
10. http://www.facebook.com as on April 2012

11. Bhathiya Wickremasinghe “CloudAnalyst: A CloudSim-based Tool for Modeling and Analysis of Large Scale Cloud Computing Environments “MEDC Project Report.
12. Legrand, L. Marchal, and H. Casanova, "Scheduling distributed applications: the SimGrid simulation framework," Proc. of the 3rd IEEE/ACM International Symposium on Cluster computing and the Grid (CCGrid 07), May 2001, pp. 138-145.
13. Qi Zhang, Lu Cheng, Raouf Boutaba, Cloud computing: state-of-the-art and research challenges, Journal of Internet Services and Applications, Springer, May 2010, Volume 1, Issue 1, pp 7-18.
14. http://aws.amazon.com/ec2/ "Amazon Elastic Compute Cloud (Amazon EC2)," as on Sep. 2012
15. Michael Armbrust et al. “Above the Clouds: a Berkeley View of Cloud Computing” Technical Report, Electrical Engineering and Computer Sciences, University of California, Berkeley,Feb 10,2009.
16. Komal Mahajan, Ansuyia Makroo and Deepak Dahiya “Round Robin with Server Affinity: A VM Load Balancing Algorithm for Cloud Based Infrastructure” Journal of Information Processing Systems, Vol. 9, No.3, Sept, 2013, pp. 379-394
17. http://www.internetworldstats.com as on August 2013.
18. H. Casanova, “Simgrid: A toolkit for the simulation of application scheduling,” in Proceedings of First IEEE/ACM International Symposium on Cluster Computing and the Grid.
19. Bell W, Cameron D, Capozza L, Millar P, Stockinger K, Zini F. Simulation of dynamic Grid replication strategies in OptorSim. Proceedings of the Third International Workshop on Grid Computing (GRID), Baltimore, U.S.A. IEEE CS Press: Los Alamitos, CA, U.S.A., 18 November 2002; 46–57.
20. Dumitrescu CL, Foster I. GangSim: A simulator for grid scheduling studies. Proceedings of the IEEE International Symposium on Cluster Computing and the Grid, Cardiff, U.K., 2005; 1151–1158.
21. Lizhe Wang et al. “Cloud Computing: a Perspective Study” , in New Generation Computing, Springer, Volume 28, Issue 2, pp 137-146,April2010.
22. D. Kliazovich, P. Bouvry, and S. Khan, “Greencloud: a packet-level simulator of energy-aware cloud computing data centers,” The Journal of Supercomputing, 2010.[Online].Available:http://dx.doi.org/10.1007/s11227-010-0504-1.
23. Saurabh Kumar Garg and Rajkumar Buyya, “NetworkCloudSim: Modeling Parallel Applications in Cloud Simulations”, Fourth IEEE International Conference on Utility and Cloud Computing, 2011.
24. Klaithem Al Nuaimi et al. “A Survey of Load Balancing in Cloud Computing: Challenges and Algorithms”, IEEE Second Symposium on Network Cloud Computing and Applications,2012.
25. Lee, Rich, and Bingchiang Jeng. "Load-balancing tactics in cloud." Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC), 2011 International Conference on. IEEE, 2011.
26. Rimal, B.P.; Eunmi Choi; Lumb, I., "A Taxonomy and Survey of Cloud Computing Systems," INC, IMS and IDC, 2009. NCM '09. Fifth International Joint Conference on , vol., no., pp.44,51, 25-27 Aug. 2009.
27. Junjie Ni; Yuanqiang Huang; Zhongzhi Luan; Juncheng Zhang; Depei Qian, "Virtual machine mapping policy based on load balancing in private cloud environment," Cloud and Service Computing (CSC), 2011 International Conference on , vol., no., pp.292,295, 12-14 Dec. 2011.
28. Ritchie, Graham, and John Levine. "A fast, effective local search for scheduling independent jobs in heterogeneous computing environments." (2003).

29. Graham, Ronald L. "Bounds on multiprocessing timing anomalies." SIAM Journal on Applied Mathematics 17.2 (1969): 416-429

Evaluation of Effectiveness of Alarm Systems

Jan VALOUCH

Tomas Bata University in Zlin, Faculty of Applied Informatics,
Nad Stranĕmi 4511. 76005, Zlin, Czech Republic
valouch@fai.utb.cz.

Abstract. Designing of alarm systems represents a set of creative technical activities, which include system design, preparation of project documentation and installation of systems. The proposal of alarm systems is based on the system and technical requirements, which are intended series of branch technical standards. These standards, however, does not solve the problems of evaluating the effectiveness of alarm systems. The aim of this paper is the presentation of the proposal aggregated coefficients, as a basic starting point for evaluating the effectiveness of alarm systems.

Keywords: Alarm system, designing, evaluation, integration.

1 Introduction

The proposal alarm systems, which include the following applications:

- intruder and hold-up alarm system (I&HAS),
- closed circuit television used for security and surveillance (CCTV),
- access control system (ACS),
- social alarm system (SAS),

is based on the system and technical requirements, which are intended range of professional technical standards CSN EN 50 13x representing support the process of setting up alarm systems in corresponding quality and structure. However, the technical standards specified range does not address the issue of evaluating the effectiveness of alarm systems. However, the technical standards specified range does not address the issue of evaluating the effectiveness of alarm systems.

The term efficiency, which for example in terms of energy is the ratio of output and input power equipment (expressed in percentages) can be understood as the ability of the alarm system to ensure the security of protected interests. The effectiveness of alarm systems depends on their quality [1].

The aim of this paper is the presentation of the original proposal of aggregate factors, which represent the basic starting point for evaluating the effectiveness of alarm systems with the assumption of the possibility of evaluation of systems according to project documentation, as well as systems already installed.

Materials and Methods

The proposed solution to evaluation of the effectiveness alarm systems, including a proposal for the aggregate coefficients is based on the analysis:

- system and technical requirements, which are intended by series of sector technical standards CSN EN 50 13x, which represent support for the implementation of alarm systems in adequate quality and structure,
- scope of application of the various components of the alarm system in the protected object,
- method of integration when deployed multiple types of alarm applications.

2 Fields of evaluation the effectiveness of alarm system

The effectiveness of alarm systems is dependent on many factors. I propose to use the following area of evaluation:

- security requirements,
- technical characteristics,
- application of systems
- systems integration.

The proposal of parameters for evaluation of the effectiveness and proposal of aggregated coefficients are based on the following assumptions:

- security requirements (B parameters) will be specified based on the security levels according to standards (the extent to which the equipment meets / does not meet this requirement in accordance with the output of the safety assessment or customer requirements),
- technical characteristics (T parameters) will be determined by the requirements of relevant branch technical standards and is expected evaluation in terms of "how much resp. to what extent "the device meets,
- application of systems (A parameters) will be based on the draft security and will assess the degree of protection object (placement of individual components of alarm systems) in comparison with the scale of the object,
- systems integration (I parameter) will be evaluated in case of integration of multiple alarm systems. I parameter will depend on the technical execution of integration,
- effectiveness of alarm systems will be expressed by the coefficient of the effectiveness of protective capabilities of the alarm system K_{PS} respectively in case integration of multiple systems as the coefficient of effectiveness of protective capabilities of the integrated alarm system K_{IPS}.

For each of the above parameters will be proposed evaluation criteria. These criteria are described by coefficients.

3 The proposal of aggregated coefficients

The following text presents a proposal of aggregated coefficients for intruder and hold-up alarm systems. Due to the possibility of comparison of individual coefficients are coefficients always evaluated in a numerical scale [1-10].

3.1 Security coefficient

Security coefficient of intruder and hold-up alarm system is based on the classification of security levels in accordance with CSN EN 50131-1 [2], which are divided into 4 levels (low risk, low to medium risk, medium to high risk and high risk). Classification is based on assumed knowledge of a potential intruder in IHAS and its technical equipment. The table of coefficients is completed with the possibility where the system does not meet any security level. The output is a factor K_B, whose value is in the range [1-10].

Table 1. Security coefficient

No.	Security coefficient K_B	Evaluation [1-10]
1	Level of security 1 – low risk	2,5
2	Level of security 2 – low to medium risk	5
3	Level of security 3 – medium to high risk	7,5
4	Level of security 4 –high risk	10
5	System does not meet any level of security	0

3.2 Technical coefficients

Technical coefficients include the evaluation of system requirements IHAS and technical requirements for the individual used components. System requirements are based on CSN EN 50131-1 [2]. The technical requirements for each component are set out in other parts of series of branch standards 50131-x, for example:

- CSN EN 50131-2-2 Alarm systems - Intrusion and hold-up systems - Part 2-2: Intrusion detectors - Passive infrared detectors.
- CSN EN 50131-3 Alarm systems -Intrusion and hold-up alarm systems - Part 3: Control and indicating equipment.
- CSN EN 50131-4 Alarm systems - Intrusion and hold-up alarm systems - Part 4: Warning devices.

3.3 Evaluation of system requirements

The following table presents a content and evaluation of system requirements (coefficient K_S) as a part of the calculation of the technical coefficient K_T. System requirements in different areas (see table) are classified by technical standard CSN EN 50131-1[2] with regard to security level (with the exception of class environment). Coefficient expresses to what extent IHAS meets the requirements of the standard. Here is the assumption that if it was declared that IHAS meets a security level (1-4), then will be all the system requirements conform to specified security level and the coefficient of K_S should be equal to the 10. If this is not, it means that IHAS does not meet the declared security level. This does not mean that it will not effective at the place deployment. However, it will identify a serious error caused in process of setting up IHAS (tender documents, design, and selection of components, design documentation, installation, repairs or replacement of additional components).

Table 2. System coefficient

Acronym	System coefficient K_S	Evaluation
K_{S1}	Environmental class	[1-10]
K_{S2}	Fault detection	[1-10]
K_{S3}	Access level	[1-10]
K_{S4}	Requirements for authorization codes	[1-10]
K_{S5}	Avoidance of brought into a condition guarding (ARM)	[1-10]
K_{S6}	Overcoming conditions to disallowing to set the status of guarding	[1-10]
K_{S7}	Restoration	[1-10]
K_{S8}	Signal processing / intrusion emergency, sabotage and fault	[1-10]
K_{S9}	Indication	[1-10]
K_{S10}	Indication available in the state of surveillance	[1-10]
K_{S11}	Reporting requirements	[1-10]
K_{S12}	Operational criteria for alarm transmission systems	[1-10]
K_{S13}	Tamper detection	[1-10]
K_{S14}	Monitoring of substitution	[1-10]
K_{S15}	Maximum unavailability connection	[1-10]
K_{S16}	Intervals verification	[1-10]
K_{S17}	Security of signals and messages	[1-10]
K_{S18}	The generated signals or messages	[1-10]
K_{S19}	Memory capacity	[1-10]
K_{S20}	Event recording	[1-10]
K_{S21}	Minimum time of power supply, charging time	[1-10]

The resulting coefficient of system requirements K_S, represents the arithmetic average of the coefficients K_{S1} and to K_{SN}.

$$K_S = \frac{K_{S1} + K_{S2} \dots \dots \dots . K_{Sn}}{n} \tag{1}$$

3.4 Evaluation of technical requirements

Evaluation of technical requirements (resulting coefficient K_T) is based on an assessment of compliance with the requirements of each type of components used

IHAS (Control panel, PIR detectors, dual detectors, warning device, power supplies, security fog device etc.) according to product standards. For example, PIR detector is compared with the requirements of the relevant product standard CSN EN 50131-2-2, parameters of IHAS control panel are compared with the requirements of standard CSN EN 50131-2-3 etc.

Factors that are evaluated for passive infrared detectors in accordance with CSN EN 50131-2-2:

- event handling,
- generating signals and messages,
- requirements on the speed of passage and body posture targets,
- security against sabotage,
- electrical requirements,
- environmental testing,
- verification of the detection coverage.

The partial coefficient K_{TSn}. is determined by comparing the parameters PIR detector and requirements standards. Parameters other components IHAS are compared in a similar manner. The following table shows an example of the content and evaluation of the technical specifications of the components IHAS (coefficient K_{TS}) as a part of the calculation of the technical coefficient K_T.

Table 3. Coefficients of technical specifications (selected components)

No.	Coefficients of technical specifications K_{TS}	Standard	Evaluation
1	Passive infrared detectors	CSN EN 50131-2-2	[1-10]
2	Microwave detectors	CSN EN 50131-2-3	[1-10]
3	Control panels PBX	CSN EN 50131-3	[1-10]
4	Warning devices	CSN EN 50131-4	[1-10]
5	Combined PIR and MW detectors	CSN EN 50131-2-4	[1-10]
6	Combined PIR and US detectors	CSN EN 50131-2-5	[1-10]
7	Power supplies	CSN EN 50131-6	[1-10]
8	Equipment using radio frequency techniques	CSN EN 50131-5-3	[1-10]
9	Opening contacts (magnetic)	CSN EN 50131-2-6	[1-10]
10	Security fog device	CSN EN 50131-8	[1-10]
n	Other used components	Relevant standards	[1-10]

The resulting coefficient of technical specifications K_{TS}, represents the arithmetic average of the coefficients K_{TS1} and to K_{TSn}.

$$K_{TS} = \frac{K_{TS1} + K_{TS2} \dots\dots\dots . K_{TSn}}{\mathrm{n}} \tag{2}$$

3.5 Calculation of technical coefficients

The coefficient K_T is the arithmetic average of the coefficients K_S and K_{TS}. Coefficient takes values in the range [1-10].

$$K_T = \frac{K_S + K_{TS}}{2} \tag{3}$$

3.6 Applications coefficients

The value of the application coefficient is not dependent on the requirements of the standards. We evaluate the practical deployment of individual components in a specific object [6]. The assessment is based on the basic dividing of types of protection:

- protection of space,
- protection of the building envelope,
- perimeter protection,
- protection of items,
- protection of persons in distress.

The basic prerequisite for evaluation is to determine the scope of protection of each area (in percentage terms), calculated as the coefficient $\mathbf{K_{An}}$. We evaluate the ratio of the total area (or the number of building openings, perimeter length and number of significant items) to the number of deployed technical resources.

For example, we evaluate for protection of space (coefficient $\mathbf{K_{APR}}$) what percentage of the total area of the protected object is covered with motion detectors, i.e. the ratio between the sum of the areas which correspond to the sensing characteristics of the detectors to the total area of the protected object.

Within the protection of the building envelope (coefficient $\mathbf{K_{APL}}$) is evaluated the ratio between the number of building openings to number of all building openings in guarded object.

Coefficient of perimeter protection $\mathbf{K_{APE}}$ represents the ratio between the length of the secure perimeter of the protected object to the total length of the perimeter.

Coefficient of protection of items $\mathbf{K_{APRE}}$ represents the ratio between the number of secure items and the number of important (valuable) objects (paintings, sculptures, etc.) in the protected object.

Coefficient of protection of persons in distress $\mathbf{K_{AT}}$ is the ratio between the number of secure rooms in the building and the total number of rooms in the building.

Output coefficient $\mathbf{K_A}$ is the arithmetic average of the coefficients for each types of protection. Coefficient K_A takes values in the range [1-10].

$$K_A = \frac{\mathrm{K_{APR}} + K_{APL} + K_{APE} + K_{APRE} + K_{AT}}{5} \tag{4}$$

3.7 Integration coefficient

In the case of the integration of multiple types of alarm systems in a single object [3], it is necessary in the calculation of the resulting coefficient of the protective capabilities to include the integration factor $\mathbf{K_I}$. The integration coefficient is dependent on methods of integration of alarm applications [4], [5].

The following Table 4 presents an overview of the determined values of the coefficients of integration.

Table 4. Coefficients of integration

No.	Coefficients of integration K_I	Evaluation
	Hardware integration	
1	IN/OUT integration	4
2	IHAS (modular system) / as an integration element	9
3	IHAS as an integration element (including control of home automation)	6
4	Automation system as an integration element	0
5	Integration using function CCTV, ACCESS, SAS	4
	Software integration	
6	Software for user administration	1
7	Security software	4
8	Visualization software	6
9	Integration software of systems of buildings	8

4 Aggregated coefficients of effectiveness of protective capabilities of intruder and hold-up alarm system

Based on the above described coefficients:

- security coefficient K_B,
- technical coefficient K_T,
- application coefficient K_A,
- integration coefficient K_I,

will be calculated:

- coefficient of effectiveness of protective capabilities of the the intruder and hold-up alarm systems $\mathbf{K_{PS}}$, or
- coefficient of effectiveness of protective capabilities of the integrated alarm system $\mathbf{K_{IPS}}$ in case of integration multiple systems.

$$K_{PS} = \frac{\mathrm{K_B} + K_T + K_A}{3} \tag{5}$$

Values KPS1 to KPSN are calculated for individual types alarm systems in case of integration of multiple types (n) of alarm applications. The resulting coefficient of the protective capability of the integrated alarm system KIPS will be calculated using the following formula. The resulting value will be in the range [1-10].

$$K_{IPS} = \frac{\mathrm{K_{PS1}} + K_{PS2.\dots\dots\dots} + K_{PSn}}{\mathrm{n}} + \left[10 - \frac{\mathrm{K_{PS1}} + K_{PS2.\dots\dots\dots} + K_{PSn}}{\mathrm{n}}\right] * \frac{\mathrm{K_I}}{10} \tag{6}$$

Subsequently we compare the calculated coefficients with the efficiency requirements for alarm systems respectively integrated alarm systems. These requirements may be determined for example by the verbal valuation, as shown in the following table.

Table 5. Evaluation of the effectiveness of alarm systems

No.	K_{PS}	K_{IPS}	Evaluation of effectiveness of protective compatibilities
0	[0]	[0-1]	Inconvenient
1	[1-2]	[2-3]	Sufficient
2	[2-4]	[3-4]	Satisfactory
3	[4-6]	[5-6]	Good
4	[6-8]	[7-8]	Very good
5	[8-10]	[9-10]	Excellent

5 Conclusion

The paper presents an original draft of aggregate coefficients, such as the basic starting point for evaluating the effectiveness of alarm systems with the assumption of the possibility of evaluation systems according to project documentation, as well as evaluation systems already installed. The proposed solution is based on an analysis of:

- system and technical requirements, which are intended by series of sector technical standards CSN EN 50 13x, which represent support for the implementation of alarm systems in adequate quality and structure,
- scope of application of the various components of the alarm system in the protected object,
- method of integration when deployed multiple types of alarm applications.

With regard to the assessment of the proposed system or alarm system already installer, using partial coefficients:

- security coefficient K_B,
- technical coefficient K_T,
- application coefficient K_A,
- integration coefficient K_I.

is calculated coefficient of effectiveness of protective capabilities of the alarm systems, K_{PS}, respectively coefficient of effectiveness of protective capabilities of the integrated alarm system K_{IPS} in case of integration multiple systems.

Based on the assumption that the designer makes the proper selection of components depending on the security level and class environment, the value (coefficient of the protective capabilities) depends primarily on the application and integration coefficient, i.e., the range of use of system components in the protected object respectively proposed technical way of integration.

The paper presents an example of a method to calculate the coefficient effectiveness of protective capabilities of the intruder and hold-up alarm system (IHAS). Calculation of the same coefficient for other types of alarm applications (CCTV, ACS, SAS) will comply with the requirements the relevant technical standards series IEC 5013x, and comply with the technical objectives of the installation in terms of the type of protection that is provided.

References

1. UHLÁŘ, J. Technical protection of objects II. Jan. Electrical security systems. 1st edition Prague: Police Academy of the Czech Republic, 2005. 230 p. ISBN 80-7251-189-0. (in Czech).
2. CSN EN 50131-1 ed.2: 2007. Alarm systems- Intrusion and hold-up alarm systems Part 1: System requirements. (in Czech).
3. CSN CLC/TS 50398: 2009. Alarm systems- Combined and integrated alarm systems - General requirements. (in Czech).
4. VALOUCH, Jan. Integrated Alarm Systems. In *Computer Applications for Software Engineering, Disaster Recovery, and Business Continuity.* Series: Communications in Computer and Information Science, Vol. 340, 2012, XVIII. Berlin: Springer Berlin Heidelberg, 2012. Chapter, p. 369 -379. ISBN 978-3-642-35267-9.
5. VALOUCH, Jan. Integration Alarm Systems. In *IJDRBC International Journal of Disastery and Business Continuity.* Sandy Bay, Tasmania, Australia: Science & Engineering Research Support Society, November 2012. Vol. 3. p. 21-30. ISSN 2005-4289.
6. VALOUCH, Jan. *Projecting of Security Systems.* [skriptum]. Zlín: UTB, 2012. ISBN 978-80-7454-230-5. 152 p. (in Czech).
7. VALOUCH, Jan. Security Assessment of the Object in terms of Alarm system design. *In the Science for Population Protection.* Lázně Bohdaneč: Ministry of the Interior. Fire Rescue Service of the Czech Republic. Population Protection Institute. Vol. 4. p. 185 - 190. ISSN: 1803-568X.

Orthogonal Chaotic Sequence Generation for a Class of Stochastic Wireless Channels

Anamika Sarma[1], Kandarpa Kumar Sarma[2], and Nikos Mastorakis[3]

[1] Gauhati University anamika.sarma15@gmail.com
[2] Gauhati University kandarpaks@gmail.com
[3] Technical University of Sofia mastor@tu-sofia.bg

Abstract. Chaotic sequences may effectively be used for secure communication. In this paper, a spreading sequence based direct sequence/spread spectrum (DSSS) communication system is proposed. The proposed scheme uses orthogonal chaotic code as the spreading sequences. The performance of the system is analyzed and demonstrated in a single path as well as multipath situation by means of computer simulation with additive white Gaussian noise, Rayleigh fading and selective fading channel conditions. Experiments reveal that the proposed system significantly outperforms the Gold code DSSS-BPSK system. The performance of the system is measured in terms of Bit Error Rate (BER), Mutual Information and Computational time. Moreover, channel types are changed to MISO and MIMO and again, performance measures are evaluated.

Key–Words: Logistic map, Chaotic code, Orthogonal code, Gold code, DSSS, Rayleigh fading

1 Introduction

With increasing application of wireless and mobile communication, quality of service (QoS) has become a major issue. Several techniques have already been developed and work on a few more are on to increase level of QoS. Among the recently considered methods, logistic map based chaotic techniques have started to receive attention. This is because of the fact that these are suitable for non-linear dynamical situations [1],[2]. Chaotic techniques are required for generation of spreading sequences. In frequency domain, several communication methods use spreading techniques to expand the bandwidth of the system much more than it actually requires. These methods are called spread spectrum (SS) communication systems. These are used for a variety of reasons, such as the establishment of secure communications, increasing protection against interference etc. There are several SS communication schemes. One of them is to use SS system with direct sequence (DS) approach. In this technique, the transmitted binary data is 'directly' multiplied with orthogonal (or nearly orthogonal) spreading sequences [3]. The performance of the system can be increased significantly if the spreading code is made perfectly orthogonal. Orthogonal codes have zero cross-correlation property. Because of this property, these codes can mitigate interference between data streams. Nowadays, the most commonly used spreading sequences in DSSS communication systems are pseudo-noise (PN) sequences such as m and Gold sequences. It is evident that they have proper correlation properties. But, they can be reconstructed by linear regression method and hence, they are not preferable for secure communications [3]. Hence, it is suitable to replace these non-zero cross-correlation PN code with orthogonal codes. In this paper, a new DSSS communication scheme is proposed. Here, a logistic map based chaotic sequence is used as a spreading factor in a Rayleigh fading channel. In this paper, a chaotic sequence is generated using logistic map and the sequence is used for spreading. The chaotic code is made orthogonal to improve the performance of the system. Results show that the proposed system has a significant improvement in BER. The mutual information and computational time of the system is also analyzed. This paper is organized as follows. The generation of spreading sequences are described in Section 2. Section 3 explains the model of the proposed chaotic spreading DSSS system in detail. Then, in Section 4, a detailed discussion on the experimental results is given. Section 5 discusses the conclusion of the paper.

2 Spreading Sequence Generation

Here, we briefly discuss the fundamental concepts related to the spreading sequence generation.

2.1 m-Sequences and Gold Sequences

Conventional DSSS systems use the PN sequences such as m-sequences (maximum length sequences) and Gold sequences as spreading sequences. Most commonly, m sequences are bit sequences generated using maximal linear feedback shift registers. They are periodic and reproduce every binary sequence that can be represented by the shift registers. Gold sequences can be generated by linear combination of two m-sequences; but the condition is that they must have same degree. All pairs of m-sequences cannot be used to generate Gold codes. Those which can generate Gold codes are called preferred pairs [3]. Gold codes are non-orthogonal codes. They can be made orthogonal by padding zeros to the original Gold code and they are called orthogonal Gold codes [9]. Other sequences like Walsh sequences, Kasami sequences etc. can also be used as spreading sequences [4].

2.2 Design of Spreading Sequence With Chaotic Map

Logistic map is used to generate a chaotic sequence. The logistic map is a polynomial mapping of degree 2. It produces chaotic behavior from simple non-linear dynamical equation. Mathematically, a logistic map can be expressed as

$$x_{n+1} = r * x_n(1 - x_n) \tag{1}$$

Table 1. Simulation Parameters

Sl.No.	Item	Description
1	Data Block	1000 to 10000 bits
2	Modulation Types	BPSK
3	Access Type	DSSS
4	Chaotic Sequence length	1000 to 10000
5	Channel Types	AWGN, Rayleigh
6	Antenna Configurations	MISO, MIMO

where, $x(n)$ is a number between zero and one, and represents the ratio of existing population to the maximum possible population at year n. Hence, $x(0)$ represents the initial ratio of population to maximum population (at year 0). Further, r is a positive number, and represents a combined rate for reproduction and starvation.

At r approximately equal to 3.56995 chaos behavior is observed. From almost all initial conditions, we can no longer see any oscillations of finite period. There is a little variation in the initial population and it shows huge variation in results over a specific time. It is a specific characteristic of chaos [8]. Most values beyond 3.56995 exhibit chaotic behavior, but there are still certain isolated ranges of r that show non-chaotic behavior. These are called islands of stability. The development of the chaotic behavior of the logistic sequence as the parameter r varies from approximately 3.56995 to approximately 3.82843 is sometimes called the Pomeau-Manneville scenario [8].

2.3 Design of Orthogonal Chaotic Codes

A logistic map based chaotic sequence is made orthogonal with the help of complement of the code. Suppose, we take a random code as ”10110”. Distinctly, this code is not orthogonal. We take the 1’s complement of the code and it is given as ”01001”. Now, if we make a code merging these two codes, it will be ”1011001001” and this code can be said to be an orthogonal code.

In the same way the chaotic sequence is also made orthogonal. The chaotic sequence generated using equation (1) is converted to binary sequence. The complement of the binary chaotic sequence is calculated and with the help of the complement, the chaotic sequence is made orthogonal.

3 System Model for Chaotic Sequence Based DSSS Modulation

Fig.1 shows the block diagram of the chaotic sequence based BPSK modulation system in a Rayleigh fading channel.

At transmitter side, first the data is generated from a random source. A random source can produce a series of ones and zeros. Modulation scheme used to map the bits to symbols in this work is BPSK . The modulated data is

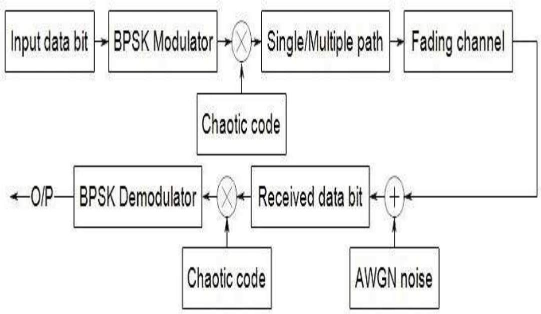


Fig. 1. System model for chaotic sequence based DSSS modulation

spreaded by a chaotic code in the transmitter side. Chaotic code is generated using logistic map and the code is made orthogonal as described in Section II. Thus a new chaotic sample is generated. Next, the signal is passed through a channel which has Rayleigh fading characteristics. AWGN noise to added to the signal. The final step of the communication system is the received signal. The received signal is first de-spreaded using a replica of the chaotic signal used at the transmitter side of the system. The received signal is demodulated using BPSK demodulator. Finally, BER is calculated between the transmitted and received bits. Performance measures are expressed in terms of BER, mutual information and computational time. The simulation parameters are given in Table 1.

A key aspect observed in this work is the use of logistic map based chaotic sequence generator which is a simple and efficient approach for obtaining spreading streams. The process logic of generating the logistic sequence is shown in Fig.2. Initially, we take r=3.56995, which is the value that generates chaotic behavior. We specify certain initial conditions and use the logistic map expression (1) to generate chaotic sequences. The sequence length depend upon the number of iterations completed by the generation process as shown in Figure 2. We have generated sequence lengths between 100 to 1000 for application in different fading situations.

4 Experimental Results

Numerical simulations for different cases of the proposed system are carried out in Matlab. BER performance of the simulation system using logistic map is presented in Fig.3 to compare with the theoretical performance curve for BPSK. The simulated results obtained using orthogonal chaotic code is compared with

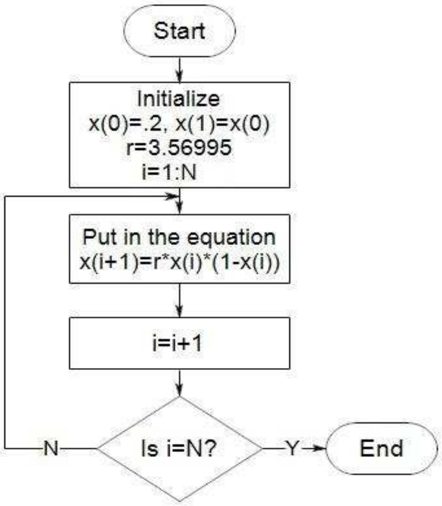


Fig. 2. Flow chart for generation of chaotic sequence

a non-orthogonal chaotic code based system. Fig.3 also shows the BER curves obtained using chaotic and Gold code in a Rayleigh fading channel.

The simulated result (Fig.3) shows that an orthogonal chaotic code can provide better performance compared to non-orthogonal codes. At BER value of 0.02, the chaotic code provides around 10 dB gain for a sequence of bits transmissions. Hence, it can be advantageous while using in wireless channels. The effectiveness of the chaotic coding is further analyzed using transmitted and recovered data sequences. The mutual information plot between these two sequences is shown in Fig.4. It reflects the closeness between the two relevant sequences.

Next,the channel type is changed to MISO and MIMO and BER is presented in Fig.5 and 6 using MISO and MIMO channel. The simulation results show that at BER value of 0.03,the orthogonal chaotic code provides around 10dB gain for a sequence of bits transmissions in MIMO channel. Hence, in these type of channels also, orthogonal chaotic codes can perform better compared to non-orthogonal chaotic codes and Gold codes. To measure the closeness between transmitted and received data sequences the mutual information for the systems is also plotted in Fig.7 and 8.

Next, performance measures are analysed in a multipath environment, which has Rayleigh fading characteristics. BER comparison between orthogonal chaotic code, non-orthogonal chaotic code and Gold code is presented in Fig.9. The

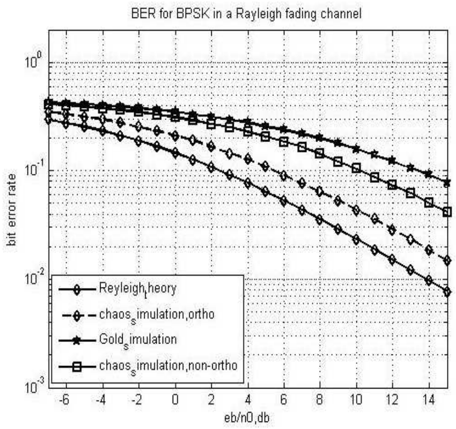


Fig. 3. BER comparison for different coding

Table 2. Comparative Results

Channel Type	Parameter at 10dB	Proposed code	Chaotic code	Gold code
AWGN	BER	.009	.02	.05
	Mutual information (bits/sec/Hz)	.9	.7	.8
	Computational time (sec)	1.10	1.22	2.28
Rayleigh	BER	.02	.04	.1
	Mutual information (bits/sec/Hz)	.7	.6	.7
	Computational time (sec)	1.22	2.23	2.13
MISO	BER	.04	.08	.1
	Mutual information (bits/sec/Hz)	.9	.8	.4
	Computational time (sec)	1.63	2.19	3.19
MIMO	BER	.02	.05	.12
	Mutual information (bits/sec/Hz)	.9	.7	.45
	Computational time (sec)	1.54	2.24	3.67

simulated results clearly indicate that orthogonal chaotic codes outperform non-orthogonal chaotic codes and Gold codes in any wireless channel. To figure out the effectiveness of chaotic sequence, mutual information is plotted in Fig.10.

The comparative results are summarized in Table 2.

Compared to conventional chaotic code, the proposed code provides a decrease of BER by 100 to 150% for AWGN, Rayleigh, MISO and MIMO cases. Computational time falls by atleast 34.3% and mutual information improves by minimum of 11.1%. This establishes the usefulness of the proposed approach.

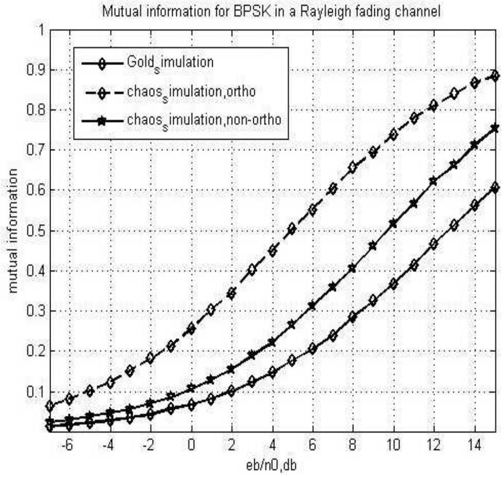


Fig. 4. Mutual information comparison for different coding

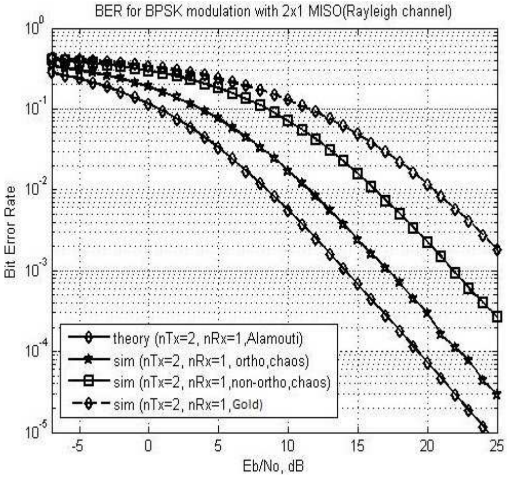


Fig. 5. BER comparison for MISO channel

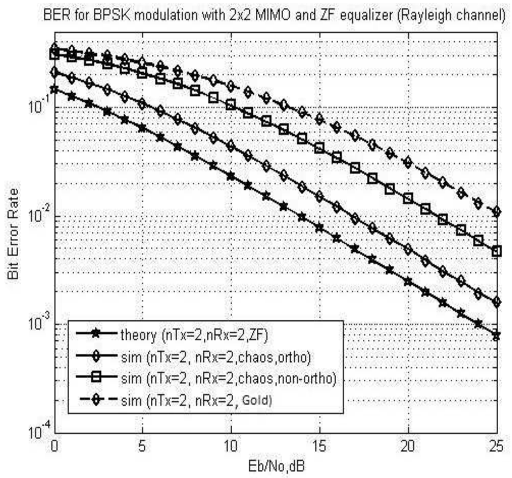


Fig. 6. BER comparison for MIMO channel

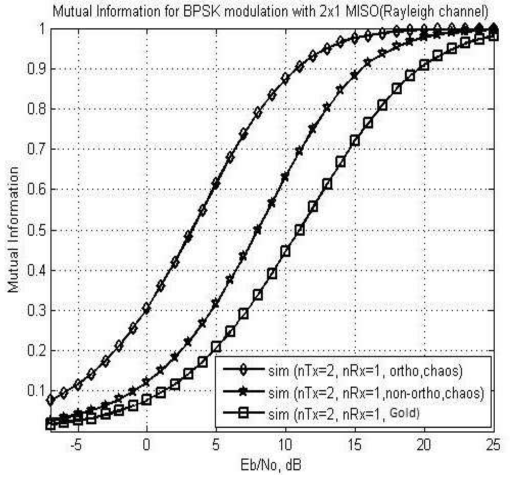


Fig. 7. Mutual information comparison for MISO channel

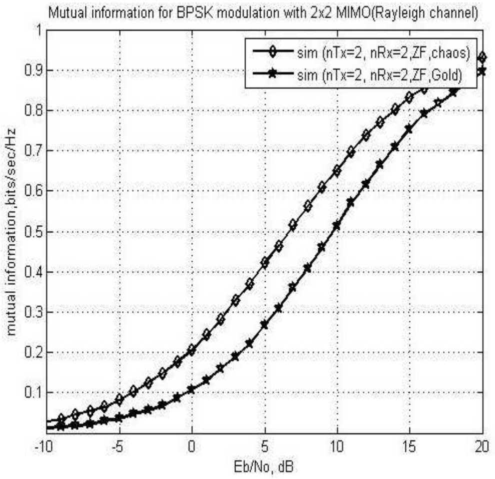


Fig. 8. Mutual information comparison for MIMO channel

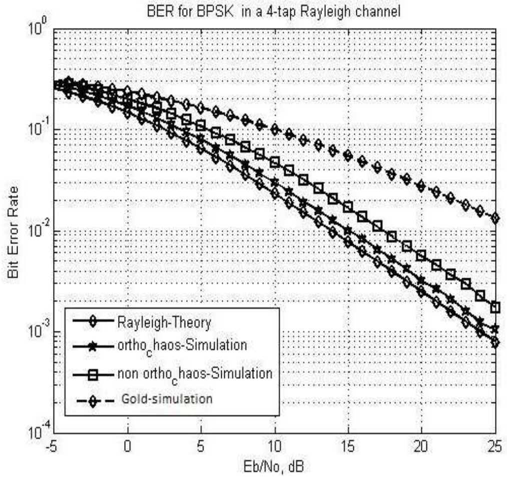


Fig. 9. BER comparison for different coding in multipath channel

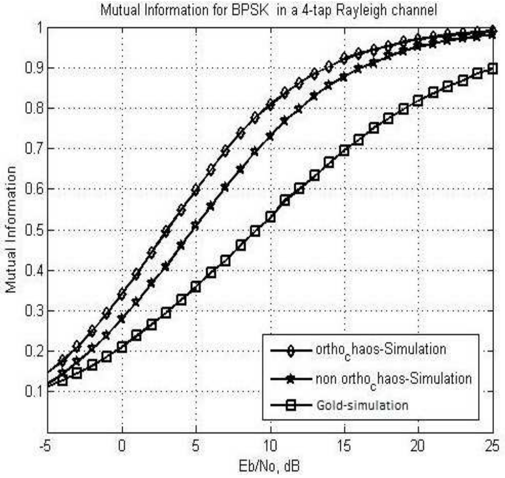


Fig. 10. Mutual Information comparison for different coding in multipath channel

Table 3. Percentage variation in performance parameters with proposed approach as compared to non-orthogonal chaotic code

Channel type	Parameter	% variation
AWGN	BER	fall of 122%
	Mutual information	rise in 22%
	Computational time	fall of 83%
Rayleigh	BER	fall of 100%
	Mutual information	rise in 14.2%
	Computational time	fall of 51.6%
MISO	BER	fall of 100%
	Mutual information	rise in 11.1%
	Computational time	fall of 34.3%
MIMO	BER	fall of 150%
	Mutual information	rise in 22%
	Computational time	fall of 45.5%

5 Conclusion

This paper has presented a chaos-based secure DSSS communication system, where a chaotic sequence is used as a spreading sequence instead of conventional PN sequences. The chaotic code is made orthogonal to mitigate interference and improve performnace. The performance measures of the proposed system are described and investigated by means of the theoretical analysis and numerical simulation. It can be seen from the obtained results, that the proposed system has significant improvement in performance measures compared to non-orthogonal chaotic codes as well Gold codes. Hence, it can fulfill the requirements of appropriate spreading sequences in DSSS communication systems. In future, the proposed system can be made dynamic to improve the performance of the system. A dynamic system can automatically adjust the length of the chaotic spreading sequence depending on fading situation. Hence, it is desirable to make the system dynamic.

References

[1] M. P. Kennedy, R. Rovatti, and G. Setti, Eds.: ”Chaotic Electronics in Telecommunications”, London, U.K.: CRC, vol 49, pp. 1495-1499, Oct. 2002.

[2] A. Abel and W. Schwarz, Chaos communicationsprinciples,schemes, and system analysis , Proc. IEEE, vol. 90, no. 5, pp. 691-710, 2002.

[3] A. P. Kurian, S. Puthusserypady, and S. M. Htut, ”Performance Enhancement of DS/CDMA System Using Chaotic Complex Spreading Sequence”, IEEE Transactions on wireless communications, vol. 4, no. 3, pp. 984-989, May, 2005.

[4] N. X. Quyen, V. V. Yem, and T. Hoang, ”A Chaos-Based Secure Direct-Sequence/Spread-Spectrum Communication System”, Hindawi Publishing Corporation, Abstract and Applied Analysis, Article ID 764341, 2013.

[5] C.K. Chen and C.L. Lin, ”Text Encryption using ECG Signals with Chaotic Logistic Map”, Industrial Electronics and Applications (ICIEA), Taichung, 5th IEEE Conference, pp. 1741 - 1746, June, 2010.

[6] L. D. Santamaria ” Secure communication using OFDM with chaotic modulation in the subcarriers” Vehicular Technology Conference, vol. 2, pp. 1022-1026, May-June, 2005.

[7] M.S.Chavan, R.H.Chile, S.R.Sawant ”Multipath Fading Channel Modeling and Performance Comparison of Wireless Channel Models” International Journal of Electronics and Communication Engineering, vol. 4, no. 2, pp. 189-203, 2011.

[8] $http://en.wikipedia.org/wiki/Logisticmap.$

[9] $www-mobile.ecs.soton.ac.uk/bjc97r/pnseq-1.1/node7.html.$

Task formation commander`s operation order for fire support

Martin Blaha, Karel Šilinger,

Department of Fire Support Control,
University of Defence, Kounicova 65,
662 10 Brno, Czech Republic
martin.blaha@unob.cz

Abstract. The Czech Republic, as a member of international organizations (NATO, EU, UNO), with respect to current global security environment, employs the units of the army both at its own state territory and outside the Czech Republic in multinational forces operations. The article focuses on task formation commander´s operation order (OPORD) for fire support of future Automated Command, Control, and Information system (C2I) in conditions of the Army of the Czech Republic. The issue of automated command, control, and information systems is of high importance in the solving of asymmetrical operations tasks today and in the upcoming future. Define the basic resources for creation of OPORD of NATO standards in Network Enabled Capabilities (NEC) conditions. The authors define group of OPORD for designing a new and by the Army of the Czech Republic required sophisticated Automated Fire Support Control System of Artillery meeting NATO standards in Network Enabled Capabilities (NEC) conditions. The article represents section of a huge defensive research project of Ministry of Defence of the Czech Republic and the Army of the Czech Republic solved by leading scientists of the University of Defence in Brno.

Keywords: fire support, artillery support, shooting schedule, list of targets, artillery, command and control automated system, shooting control, intensification, coordination of combat support.

1 Introduction

Fire support executed only by artillery, i. e. artillery support is the only and the main part of combat support at lower levels of commanding which can actively decrease combat potential of enemy in accord with requirements of task formation commander. Task formation commander is fully responsible for combat and therefore also for artillery support. This responsibility is expressed in task formation commander`s OPORD, which has to contain clear tasks for all subordinate subjects and therefore for subjects of artillery.

In case of using command and control automated system of artillery support (ASRPP-DEL) it is necessary that OPORD, more precisely its part E - fire support, contained data, which is indispensable for activity of ASRPP-DEL and which has not been told before. [5]

Issuing tasks is base for command and control. Tasks for artillery are usually issued in a form of order, command or signal. Commands make basis of communications for shooting control. Signals are coded commands with fixed content and defined subsequent activity used in every kind of activities. Regardless the form which task is issued in, its content has
to be complete, understandable and precise. Hierarchy of issuing tasks for units and subjects of artillery support is standard; i. e. tasks are issued only by superiors. Superior commanders of task formations issue their tasks in a system of command and control of artillery support by OPORDs and by some other orders and commands. Superior artillery commanders and leaders are usually at working post of a control shooting system and issue tasks by commands. In command and control automated system in necessary to formulate every activity in advance and to determinate authority for issuing orders and commands and for fulfilling them.

Content of this chapter is deduction, definition and explanation of data which the task formation (with units of artillery using ASRPP-DEL) by commander`s OPORD has to contain. In order to principle that all units of the system of artillery shooting control has to be ready at all times for change to secondary method of shooting control, data for manual shooting control are attached.

2 Main principles of writing OPORD

The main method of issuing tasks for subordinate units or subjects of artillery support is OPORD. This document has to be written in precise and exact way. The other types of orders then can be documents written as parts of OPORD which specify tasks of subordinate subjects in concrete situation. [12]

In present time OPORDs are based on experiences from the past and contain only data for sort of action which unit will do. Except that a lot of data is written only in graphic form. For ASRPP-DEL it is necessary to formulate OPORD containing precise orders for all tasks which artillery units and subjects can fulfill in every situation.

There should not be repeated present military publications in OPORD. For example every commander should know that artillery during fire cover of moving units destroys enemy artillery batteries, reconnaissance units, point of commanding and main objects of air defense and therefore it doesn`t have to be written in OPORD. It should be written there only in case, when commander decided to add any kind of target or to give any of targets higher priority.

3 GEOGRAPHICAL ZONE

In case that combat activity will take a place near to border of 6° geographical zone, task formation commander will have to determine if it will be needed to recalculate coordinates to neighbor geographical zone and if so, he have to decide if it will be the left or the right one. Chosen geographical zone will be known as the main one. This decision will depend on space which the task formation will be in. It can be generally said, that with using ASRPP-DEL it doesn`t matter which zone we choose, because the system is able to recalculate any coordinates in real time after creating needed mathematical apparatus. System, based on evaluation of combat structure, will automatically pick the zone in which it will find during combat activity more subjects of artillery units of the task formation. In case of manual shooting control, for time reasons it will be necessary to recalculate coordinates of combat units to the neighbor zone. In case of detection of enemy in neighbor zone this will allow to start firing without long recalculating coordinates to target zone in which combat units of artillery are situated. The decision which zone will be the main one is more important in case those subjects of combat structure and expected targets will lie in two neighbor zones. In this case the main zone will be the one with more expected targets.

Based on decision of recalculating coordinates, members of topographic and reconnaissance units will recalculate gathered coordinates of subjects of combat structure to main geographical zone and in order with "sketch of topographical-geodetic connection" they will mark them E_1, N_1. Subsequently they will calculate correction of direction for neighbor zone - $\Delta\alpha$. Rules for fulfilling the "sketch of topographical-geodetic connection" are written in chapter.

If the task formation will operate near to the border of two geographical zones, it will be necessary to give coordinate in whole shape PPV CC EEEEENNNNN, where PP marks 6 ° zone, V marks layer of the zone, CC marks 100km square in MGRS system and EEEEENNNNN stands for horizontal and vertical coordinate of the point.

In case it will not be necessary to recalculate coordinates to another geographical zone, it will be possible to work with shortened coordinates. It means that coordinate of subjects of combat structure will be given in five digit groups (EEEEE NNNNN). But ASRP-DEL will register coordinates of all given point in full shape. Mark of the zone and 100km square will be added in order of actual position of combat structure. If the coordinate will be given in tens or hundreds of meters, system will put instead of missing numbers zeros (for example: operator will write coordinates of a point in shape: 426847, combat structure is situated in 33rd zone, layer U and in 100km square marked VR, ASRPP-DEL will save the coordinates in shape 33U VR 4260084700)..

4 Determination of area

The Standard Among most important data written in OPORD belong areas of firing posts for firing units, areas of special attention and targets of special attention, borders of reconnaissance zones for reconnaissance units and minimum distance of shooting. This data is used for planning and positioning of units, executing maneuvers with units and planning of firing. So far this data has been given in graphic form and in text it has been determined by terrain subjects and objects. The purpose was only rough determination of area and therefore during subsequent preparation for combat, reconnaissance units exactly determined borders of areas and measured firing posts. This method is unsatisfied for automatic process of commanding. It also does not fit for shooting from firing posts with dispersedly placed cannons. An area has to be determined in a way so they can suit every tactical requirement and simultaneously chosen with such a precision which allows software to work with them.

Mentioned tactical requirements are for example sufficient area for required dispersing of combat units, sufficient areas for suitable artillery units and weapons, areas with natural camouflage for commander's post and waiting posts, good visibility to areas of predicted presence of enemy units, terrain allowing good connection within and out of the area, terrain allowing fast and hidden arrive and exit and so on. Therefore every area has to be set by right-angled coordinates of four or five points (2nd Areas of firing posts, 4th Front line of ally armies and borders of reconnaissance area, 5th Areas of special attention, 6th Areas of targets of special attention). It should be coordinates of terrain subjects which can be easily identified in terrain. In case of determination reconnaissance zone, coordinates has to be set at least in form of three front line points of our armies, which cannot be crossed by units of artillery reconnaissance. In scheme of OPORD are 4. Front line of our armies and border of reconnaissance zone 1st and 5th direction point determine left and right reconnaissance zone side and 2nd and 4th determine left and right side of observation post line.

This attitude will allow the possibility of automatic comparison of the weapon system, observation post or commanding post location with location of departure zone and in case of crossing this zone`s border, the system will automatically alert the operator. Except that, coordinates of left and right side of observations posts line will be used for determination of reconnaissance group`s cover angle.

Reconnaissance group should be kept because they have to prepare areas of firing posts for case of ASRPP-DEL malfunction. During activity areas preparation the reconnaissance groups will be able to use ASRPP-DEL in every way including automatic checking of departing firing posts in the area. [5]

The form, more precisely accuracy of points determining area`s coordinates will follow from ASRRP-DEL use. If the system will use the commander of task formation during order processing, it will be possible to write in complete coordinates in form PPV CC EEEEENNNNN. In case of ASRPP-DEL use there will be digital maps for disposition for determination of area`s edge points at contact screen by finding concrete point in a catalog of geodetic points coordinates or by some similar method. It will be possible to input vertical and horizontal coordinate with accuracy of one meter. If there will not be possible to work with needed map of ASRPP-DEL, it will be alright to quote only edge areas points with accuracy of one hundred meters without marking of zone and 100km square MGRS. The coordinates form will be EEENNN. This method is for areas determination sufficient.

Point coordinates giving (subject of combat structure, targets, edge points, areas or lines and so on) in complete form is appropriate for their unique identification especially in case when the combat activity will be made with use of ASRPP-DEL and in the bordering area of two 6° zones. This relatively long point location determination is chaotic and means time lost when using radio communication for transmitting data or during writing all data which cannot be always necessary. Therefore it is suitable to write coordinates in shortened form in accordance to allied publications.

Combat structure subject coordinates and targets is possible in accordance with AArtyP-1 and possibilities of used methods of determining coordinate to give in meters or tens of meters (form: EEEEENNNNN or EEEENNNN). The terrain subjects or objects location which are used for orientation in map is in accordance to STANAG 2014 given with marking 100km square and horizontal and vertical coordinate in kilometers or in case of need in hundreds of meters (form PVEENN or PVEEENNN).

5 Bearing of main direction of fire

Another major data which has to be part of task formation commander's order is bearing of main direction of fire for every firing post area. This data shouldn't be needed in future for standard cannon aiming into target course, but it will be necessary for cannon aiming by secondary method and therefore also for firing posts determination by reconnaissance units. Also it will make easier to orientate in area during machine departure and so on. It will be given in the same form as it has been so far, i.e. as direction course of main supported task formation rounded to hundreds of segments, miles marked α_{HS}.

6 Additional subjects determination

Regular part of task formation commander's OPORD is also an additional subject’s determination. In opposite to present practice we need to take into account adding not only firing, reconnaissance subjects, but also others like firing command, topographical-geodetic, logistic and meteorological support and so on. Possibilities of strengthening task formation by artillery support subjects are described in publications - Possibilities of strengthening task formation by artillery support subjects with use of artillery firing commanding support automatic system.

7 Basis for firing

The Data which is most important for artillery support realization and allows basic artillery role fulfilling are basis for firing. In task formation commander's OPORD are usually written basis for scheduled firing. It has to include all information which are necessary for effective artillery fire which contributes to meet task formation commander's requirements. Most of basis for artillery fire will be part of documents called "Fire schedule" and "Target list".

7.1 Fire schedule

Fire schedule will determine basis for tactical command of firing, especially choose of the unit which will lead the firing, time of fire, in case of need signals for start or end of fire and the document can also include other data - for example fire task, planned consumption etc. The first data of "Fire schedule" is unit kind determination for concrete task which will be possible to choose from formation task subjects.

From the artillery point of view there will be given if the task will be fulfilled by mortar or cannon weapon systems. Based on executor's determination and other needed input data, the system will process automatic choose of the unit. Choose of the unit will be processed with using ASRPP-DEL in accord to procedures created for automatic system.

Without using ASRPP-DEL the unit will be chosen by present rules. Decision about fire executor is basis for next planning of chosen fire unit. [6]

Planned ammunition consumption calculation for planned fire is made by present procedure. The standard of ammo consumption for the weapon system, shot, lighter, target (target area hectare), and fire length and fire task is needed. In present there is no standard for artillery ammo consumption in the Army of Czech Republic.

Determination of starting and ending times, more precisely length of firing is given by planning fire support results and it is written in order for firing. This number is used by ASRPP-DEL for weapon system fire mode determination. The form and content of "Fire schedule" is given by allied publication AArtyP-1(A) Artillery Procedures. It is wanted to keep the document content without changes in order to allow other army's commanders and our artillery commanders working on the field of international task formations to work with it without troubles. Although there is one exception.

For definite determination of starting and ending time of firing it is good to add a column named "Start/End". Therefore in the matter of time, every fire will be mentioned in the document twice. Once in a graphic form and once by letters expressing the start/end time of firing in astronomic time. Data start/end will be used by ASRPP-DEL to weapon systems number determination which will do the firing and the firing speed determination.

For the reasons of inserted data effective use by automatic system it is purposeful to input the firing time only by this method. If there will be in "Fire schedule" also a fire on request, there will be in a column "Fire on request" written a signal, on which the fire will be started and ended. Into the column "Notes" it is possible to write deflections from the standard suggested by system for determination of fire task and shoot and lighter kind for effective fire.

7.2 Target list

Fire schedule Document Target list obtains information about target which is needed for fire element calculation and at the same time it is one of the most important resources of data for whole ASRPP-DEL. There are numbers of lines in the first column and it is possible to orientate by them in the table.

The second column gives numbers of targets. These are determined by rules described in "Numbering targets". There are coordinates of targets in 3^{rd} - 7^{th} column. Artillery observer will discover and input coordinates into the target list or if the fire is ordered by superior level, coordinates will be taken from it. Artillery observer inputs right-angled or polar target coordinates. If he inputs polar coordinates, he has to input right-angled coordinates of his own post. Superior estimates the target position by right-angled coordinates.

Every target has to be estimated by right-angled or polar coordinates. Right-angled coordinates will be input according to principles for determining the geographical zone and it will be done with toleration of ten or hundred meters (form: EEEEENNNNN or EEEENNNN). Target position can be set by polar coordinates only in case when we know the coordinates of post (coordinates of post are in the system) which the values where measured from. System will automatically recalculate polar coordinates into right-angled ones and if the coordinates of observation post which detected the target are known, it will calculate polar coordinates for this post.

Data will be used for calculation of distance and direction of fire, fired reparation and in case of fire to targets in dangerous distance from our units for calculating new aiming point. Steps for calculating a new aiming point is written in Fire requiring in ASRPP-DEL. There are data about target description - its sort, character, position and activity in the 9th - 12th column. This data is necessary for choose of the firing unit, estimating of firing task and the method of fire activity, determining of shot fly trajectory, shot kind and initiator and its adjustment according to scheme Effective fire.

There is target turn in the 13th column. Target turn is front target direction written in hundreds of panels and it is needed for determining of aiming points of NATO armies artillery units. Data will be given by subjects of artillery reconnaissance ACR in case of cooperation with other armies firing units.

The 14th and 15th columns include values of target width and depth, if need be there could be a value of round target radius in the 14th column. The value is used for determining needed number of weapon systems for fire, fan calculation and consumption of ammo for fire to given target. There is written accuracy of target coordinates determination on the last - 15th column. The accuracy is given by term "accurate" labeled "P" or "inaccurate" labeled "N".

Accurate coordinates are determined in accord with rules of fire with probable round error within 50 meters and are in accord with conditions of complete preparation. Inaccurate coordinates are determined with greater probable round error. This value is used for decision about method of determination subjects for effective fire. The value has to be input by subject which gives target coordinates.

8 Sources for marking the targets

Marking the targets is activity performed always after detection of the target. Process of marking the targets is set in ahead. In an OPORD it is necessary to set two first symbols of marking the target, i.e. letter which will be in front of number marking of every target which will be detected by reconnaissance group of task formation. This letters will be determined by task formation commander or on basis of superior's order. Entry is basis for creating numbers, which the targets (detected by task formation reconnaissance units) will be marked by. Except that he can also determine departure from standard procedure.

9 Marking of fire control system elements

The For marking of fire control system elements in sense of scheme - System of fire command and control and target marking according to Numbering targets it is important to establish names of task formations. It should contain number marks of regiments (brigades) which are parts of the task formation. Nevertheless it is possible, that task formation is made by bigger amount of units and none of them is the biggest one. If lack of clarity is likely to appear in task formation marking, it is vital that superior task formation's commander will establish marking of subordinate task formations in his order. [7]

10 Target priority

For planning and choice of targets automation it is necessary to establish priorities of targets for single periods, tasks or fazes of combat activity. Strengthened task formation commander will establish by this method which enemy objects are most important for the success of mission. Based on this decision, official responsible for combat support can decide about elimination of targets detected in real time without necessity of approving by task formation commander. Also ASRPP-DEL suggests target elimination order in accord to priority established by OPORD.

11 Ammunition replenishment

Commander has to set a value of ammo stock which will lead to requirement for ammunition replenishment from logistic units OPORD. The amount depends on logistic capabilities to react immediately to required amount of ammunition. The faster logistic reaction will be the smaller amount of ammo can be set by the commander.

12 Conclusion

It is necessary to write a great number of facts in task formation commander's OPORD, which has never been there so far or which has been written in a different form. It is obvious that these facts will not be usually written in main parts of OPORD, but in its annexes, i.e. annex E - Fire support, in firing schedule and in target list.

All basics for fire command and control have to have the form which will allow printing and using the documents without ASRPP-DEL support. [5]

The system also has to allow an access to documents and information to all subjects of command, coordination and fire support control which would obtain them regularly by normal way or they need it for their activity. The system of creating OPORDs allows changing of OPORD parts according to actual needs.

Therefore there are conditions for automatic fire command and control even in case of cooperation with superior task formation commander.

For effective work of artillery units near to the meeting line of two geographical zones it is needed for ASRPP-DEL to create mathematic apparatus allowing automatic recalculation of coordinates from one geographical zone to another.

For calculation of ammo consumption for fire to expected sort of targets it is necessary to set norms of ammo consumption for weapon systems which are in ACR.

References

[1] *Military Strategy of The Czech Republic*. Praha: MO CR, 2008.

[2] *Long-Time Scheme of Ministry of Defence*. Praha: MO CR, 2008.

[3] *NATO Capabilities/Statements - 2018*. Brusel, 2007.

[4] *Doctrine of the Army of the Czech Republic*. Praha: MO CR, 2005.

[5] BLAHA, M., SOBARŇA, M. Some develop aspects of perspective Fire Support Control System in Czech Army conditions. In *The 6th WSEAS International Conference on Dynamical Systems and Control*. Sousse (Tunisia): University of Sfax, 2010, pp. 179 - 183.

[6] BLAHA, M., SOBARŇA, M. Principles of the Army of the Czech Republic Reconnaissance and Fire Units Combat using. In *The 15th International Conference „The Knowledge-Based Organization"*. Sibiu (Romania): Nicolae Balcescu Land Forces Academy, 2009, pp. 17-25.

[7] POTUŽÁK, L. *Control and Realization of Fire Support - The Cooperation of Artillery and Units of Artillery Reconnaissance during Fire Support of Forces*. Partial task - Specific research of FEM. Brno: University of Defence, 2006.

[8] *AD-6.1 Doctrine of Communication and Information systems*. Praha: MO CR, 2003.

[9] *AAP-6 NATO Glossary of Terms and Definitions* (english and french). 2009.

[10] BLAHA, M., BRABCOVÁ, K. Decision-Making by Effective C2I system. In *The 7th International Conference on Information Warfare and Security*. Seattle (USA): Academic Publishing Limited, 2012, pp. 44-51. ISBN 978-1-908272-29-4

[11] BLAHA, M., BRABCOVÁ, K. Communication environment in the perspective Automated Artillery Fire Support Control System. In *The 10th WSEAS International Conference on APPLIED INFORMATICS AND COMMUNICATIONS (AIC '10).* Taipei, 2010. pp. 236-240. ISBN 978-960-474-216-5.

[12] BLAHA, Martin. Communication as a basic for future Artillery Fire Support Control System. In: *The European Conference of COMMUNICATIONS (ECCOM'10)*. Tenerife: WSEAS Press, 2010, p. 140-142. ISBN 978-960-474-250-9.

[13] BLAHA, Martin; POTUŽÁK, Ladislav. Decisions in the perspective Automated Artillery Fire Support. In: *Recent Researches in Applied Informatics & Remote Sensing*. Penang: Wseas Press, 2011, p. 87-91. ISBN 978-1-61804-039-8.

CloudAnalyzer: A cloud based deployment framework for Service broker and VM load balancing policies

Komal Mahajan[1], Deepak Dahiya[1]

[1]Dept. of CSE & ICT, Jaypee University Of Information Technology, Waknaghat, HP, India
{komal.mahajan, deepak.dahiya}@juit.ac.in

Abstract. Cloud computing is filling the gap as a fifth utility service by building higher capabilities of IT infrastructure. This also lends the cloud for research as one of the focus areas. Cloud researchers lack the opportunity to work with real cloud test beds. The cloud simulation tools available in academia and research have limitations like dependency on programming for simulation setup; for further deployment of new load balancing algorithms, the understanding of underlying simulator architecture is required. Further non availability of a single snapshot of multiple simulation exercise and non availability of database support is not another disadvantage. This paper addresses these issues to a great extent by introducing a cloud simulation tool with enhanced features like algorithm editor, multiple simulation comparator and database support. The proposed features provide an abstraction to the simulator application. This allows researchers to focus on better analysis of the behavior of applications rather than understanding the implications and working of the underlying architecture.

1 Introduction:

In the last few years, distributed applications have opened up various avenues for the advancement of cloud technologies. Cloud technologies provide us a platform for various infrastructure services portraying thus itself as a very attractive option for industry, startups and academia. The growing popularity of cloud and the increasing competition has also made cloud an emerging area of research focus. However, the cloud researchers in industry and academia lack access to real cloud test beds[21]. Thus, the most feasible option available is to simulate the powerful cloud infrastructure so that cloud researchers can use the simulators to analyze and predict the behavior of their applications and algorithms which can later be deployed on real cloud test beds. However at present only a limited number of cloud simulators [18] are present. Further, to deploy new service broker [7] and VM load balancing algorithms [7,10] a researcher has to understand the underlying details of the simulators which leads to non productive effort. Also, the simulators available do not have a database support as a result of which the powerful query based analysis of the results is not available. So the goal of this paper is to propose a cloud simulation tool with enhanced features like algorithm editor, multiple simulation comparator and database support that addresses the limitations highlighted above to a great extent. The proposed features provide an abstraction to the simulator application. This allows researchers to focus on better analysis of the behavior of applications rather than understanding the implications and working of the underlying architecture.

The rest of the paper is organized as follows: Section 1provides an introduction to the proposed work. Section 2 includes the motivation & problem definition, section 3 includes the related study on available cloud simulators. Sections 4 and 5 provide an exhaustive description of the proposed research work i.e. CloudAnalyzer and architectural design of CloudAnalyzer respectively. In addition, sections 6 and 7 includes the detailed design and Implementation of CloudAnalyzer. Section 8 summarizes the observations using the evaluation criteria for CloudAnalyzer. Section 9 uses a case study to demonstrate the successful testing and implementation of the CloudAnalyzer tool. Finally, Section 10 summarize the conclusion and limitations respectively.

2 Motivation & Problem Definition

There are several popular toolkits [18] available that can be used to model a simulated cloud environment to study the behavior of researcher's applications and algorithms. In spite of these facts there is ample space available foe feature enhancement so that the focus is on the simulation parameters and not on the coding part.

A major problem most researchers face while working on load balancing[20] algorithms face is the complexity involved in understanding the underlying complexities of the simulator. Due to this, the focus of the researcher shifts from the generation of new ideas in the form of query at new level to understanding the core architectural design of the simulator at the physical level which unnecessary leads to reinventing the wheel of nonprofitable effort . So, there is need for a cloud simulation toolkit that abstracts the underlying architecture and design, With the above limitations overcome the researcher can focus on the design of new load balancing algorithms. Limitations of the existing simulator to provide a user the capability to run only a single simulation at a time leads to the comparison of algorithms and multiple simulations to be done manually by running one simulation at a time. Therefore, there is a need for a simulator which makes the task of comparing multiple simulations easier and reduce the manual and repetitive work.

Another problem in the available simulators is that one has to manually analyze the results of the queries to draw meaningful conclusions as they lack database support. So, there is a need for a simulator with database support. This database should store the simulations for powerful database query analysis.

The above scenario leads us to the following problem definition:

To simulate a cloud environment that provides easy deployment and allows comparison of innovative Service broker and VM load balancing policies that provide persistence storage for database query analysis.

The above problem definition leads to the following broad objectives that are summarized below:

- Investigate existing simulation techniques for studying cloud based infrastructure.
- Comparison of different cloud simulators
- Identify the shortcomings of each simulation technique.
- Explore different approaches that can be adopted to extend the existing simulators to make them more usable and flexible for the researchers.
- Design a new cloud simulation toolkit ie. CloudAnalyzer which uses the identified approaches that has flexible design and can be refined and extended.
- Identify test scenarios to test the simulation tool introduced in this paper.

- Test application using the CloudAnalyzer.

3 Related Study

The growing popularity of cloud computing in both research and academia has introduced cloud as one of the focus area of future research. However, researchers who want to analyze their applications performance on cloud or to test their scheduling algorithms on cloud do not have the opportunity to work with real cloud test beds because of the huge expenditure involved in the set up of the same[7]. So, to promote research in the area of cloud computing the best that can be done is to provide researchers with cloud simulation tools on which they can test their applications and algorithms [19].

Cloud computing is related to grid computing [22] as both the computing technologies are based on large scale distributed resources [1]. To promote research in the area of grid computing, various popular simulators are available viz. Gridsim [6], Simgrid [8, 11], OptorSim [12] and GangSim [13]. Although, grid simulators can simulate a large scale distributed environment. However, unlike grid computing, cloud computing uses virtualization technologies at various levels for resource sharing and dynamic resource pooling to provide various services viz. IaaS, PaaS, SaaS [14]. Moreover, cloud is based on the pay per use i.e. utility model [9]. So, grid simulators cannot simulate a virtualized cloud environment based on utility model. So, cloud simulators were proposed.

Some popular cloud simulators are CloudSim[3,4,5], CloudAnalyst[2,7], GreenCloud[15], NetworkCloudSim[16].The CloudSim[6] toolkit supports modeling and creation of one or more virtual machines (VMs) on a simulated node of a Data Center, jobs, and their mapping to suitable VMs. It also allows simulation of multiple Data Centers to enable a study on federation and associated policies for migration of VMs for reliability and automatic scaling of applications. CloudAnalyst [2, 7] is built directly on top of CloudSim [3] toolkit, leveraging the features of the original framework and extending some of the capabilities of CloudSim. GreenCloud [15] provides a simulation environment for energy-aware cloud computing data centers. GreenCloud is designed to capture details of the energy consumed by distributed environments. NetworkCloudSim [16] supports modeling of real Cloud data centers and generalized applications such as HPC, e-commerce and workflows.

Out of all the above simulators, CloudAnalyst is the most suitable to analyze Service broker and VM load balancing algorithm in different scenarios as CloudAnalyst provides users with the capability to modify and test their algorithms with the help of user friendly GUI (Graphical User Interface).

4 Proposed research work: CloudAnalyzer

The Figure 1 shows that the proposed simulator has functionalities built on top of the existing simulator CloudAnalyst [7] which inturn has built on top of CloudSim[4]. CloudAnalyst extended the capabilities of CloudSim by providing GUI which could provide ease of use to user [3]. CloudAnalyzer extends the functionality of CloudAnalyst by adding support for multithreading, algorithm editor and database. Algorithm editor abstracts the underlying architecture and design of the CloudAnalyzer from the user. This functionality is useful to the user as the user can add new and innovative load balancing algorithms on the simulator without understanding the underlying architecture. This way the user of this simulator can focus on the design aspects of his simulator rather than focusing on the underlying architecture leading to reduced effort and better algorithm design. Multithreading support added in CloudAnalyzer allows a user to run multiple simulations at a time which can help the user to compare multiple simulations with different parameters or algorithms. this reduces the manual comparisons which leads reduced effort. The database support in CloudAnalyzer allows the user to maintain a record of the simulations. Also, the query support in database can help in analyzing the simulations in a better way.

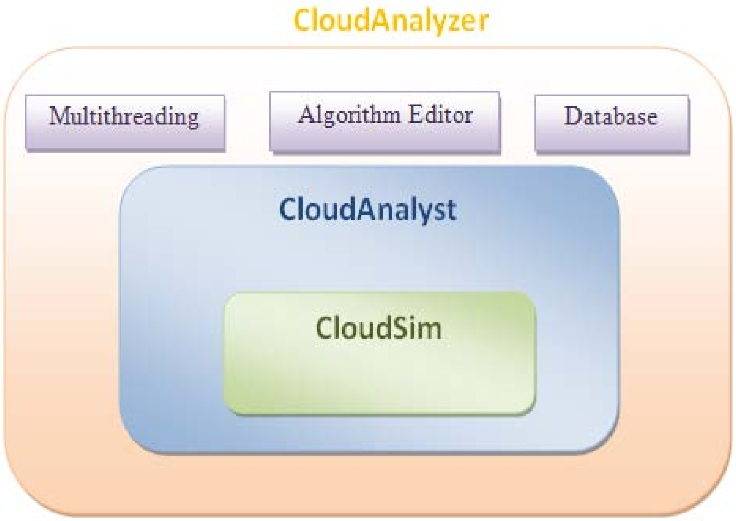


Fig. 1. CloudAnalyzer: An overview

5 CloudAnalyzer : Architecture Design goals

The proposed simulator supports the existing features of CloudAnalyst like Graphical output for more powerful analysis, Parameter Selection, Separation of simulation exercise from coding

The features of CloudAnalyzer that extend its capabilities over existing simulators are:

- Database support
  Proposed approach should support a database so that we can save our simulation in database and access them anytime.

- Query window
  The user is provided with a query window so that he can query the database to analyze various patterns.

- Algorithm editor

It provide user with a higher level of abstraction where user can deploy his innovative service broker and VM load balancing policy without having the insight of the underlying architecture.

- Graphical output for more powerful analysis
  It should provide a graphical output of the simulation results which enables the results to be analyzed more easily and more efficiently.

- Real time Monitoring
  Proposed approach should monitor the simulations in real time. The graphs generated should depict the real time scenario in the cloud environment.

- Multithreading support to run multiple simulations run over network
  Proposed approach should provide support for multithreading to run multiple simulations simultaneously which will allow us to compare the results of multiple simulations and draw useful conclusions from them.

- Separate simulation exercise from coding
  Separate the simulation exercise from a programming exercise and enable a modeler to concentrate on the simulation parameters rather than the technicalities of programming.

5.1 CloudAnalyzer: Use Case Diagram

The Figure 2 shows that a use case diagram of CloudAnalyzer which depicts the following:

- A user of CloudAnalyzer can manage the Nodes, Clusters and VM configuration in the cloud by selecting appropriate parameters for simulation configuration.
- A user of CloudAnalyzer can manage the load balancing and service broker policies for the simulation .

- The algorithm editor in the CloudAnalyzer allows a user to add new VM and service broker algorithms without understanding the underlying coding details.
- A modeler can also monitor the simulation in real time and can generate reports and graphs for various simulations.
- A user can configure multiple simulations based on different parameters/ VM and service broker algorithms for better comparison n real time.
- The user can store the parameters and the results of the simulation in the database
- The user can see the schema of the database and can query the database in the query window to analyze the results to derive meaningful conclusions.

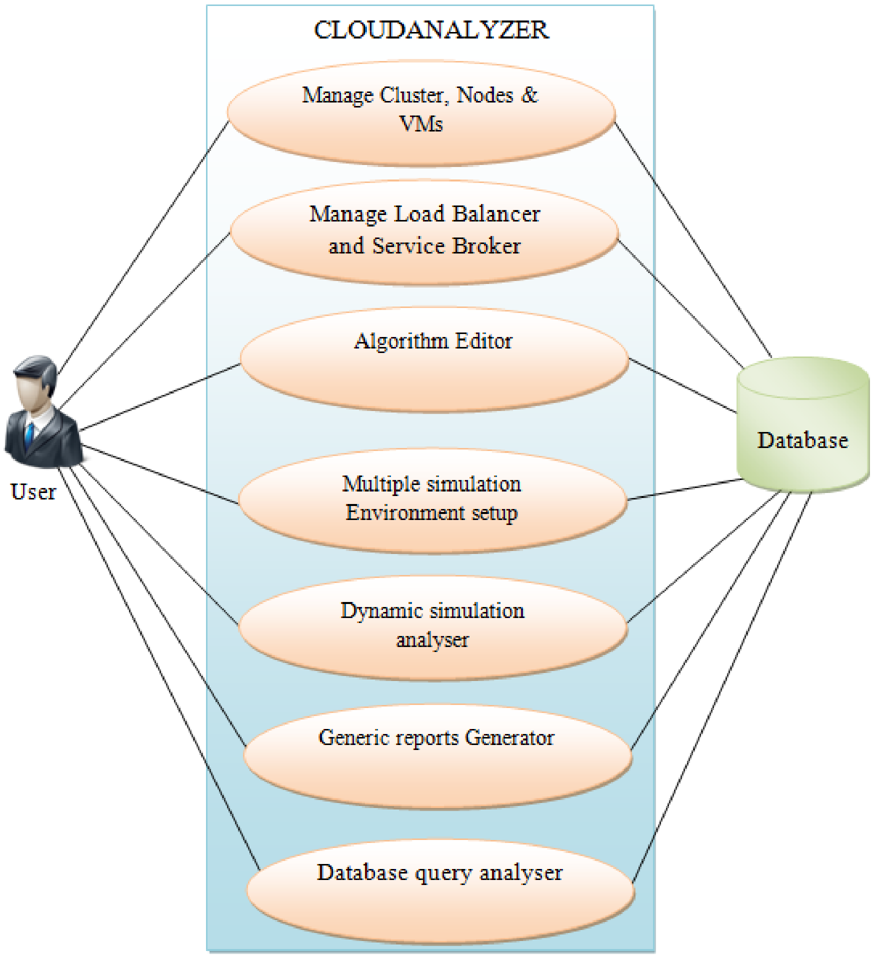

CLOUDANALYZER
Manage Cluster, Nodes & VMs
Manage Load Balancer and Service Broker
Algorithm Editor
Multiple simulation Environment setup
Dynamic simulation analyser
Generic reports Generator
Database query analyser
User
Database

Fig. 2. Figure 2: Use Case Diagram for CloudAnalyzer

5.2 CloudAnalyzer: Architectural design

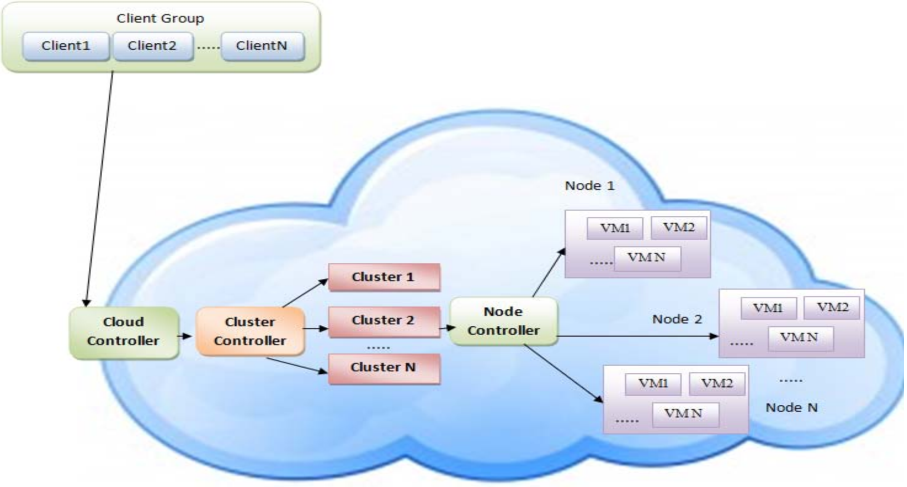


Fig. 3. Figure 3: Architectural design of CloudAnalyzer

CloudAnalyzer is extending the functionality of CloudAnalyst [7]. A Cloud consists of a number of physical machines called as Nodes. A group of nodes form a Cluster. Hence, a Cloud is composed of number of Clusters. Each node is virtually divided into a number of Virtual Machines(VMs) .A Client in a cloud gives of number requests to the cloud which are deployed on VMs. A unit of client request group is called as a Cloudlet. A group of a clients is called as Client Group. Cluster Controller manages a Cluster while the Node Controller manages the Nodes in a cloud. When a Cloudlet arrives at a cloud the first job of scheduling is of Cluster Controller that allocates an appropriate Cluster to the Cloud using Service Broker algorithms. The next job of scheduling to allocate an appropriate VM on a node from amongst the nodes in a cluster is done by Node Controller by using appropriate VM load balancing algorithms. All these components of a cloud are modeled in the CloudAnalyzer to fully implement the functionality of a cloud.

5.3 Cloudlet Processing: Effective time computation

The effective time taken for a processing of a cloudlet includes the following: Let,

t1=Network delay time
t2=Waiting time in queue at Service broker
t3=Delay at service broker to allot a cluster
t4=Waiting time in queue at VM load balancer
t5=Delay at VM load balancer to allot a VM
t6= execution time on the allotted VM

So, the effective time taken for a processing of a cloudlet= t1+t2+t3+t4+t5+

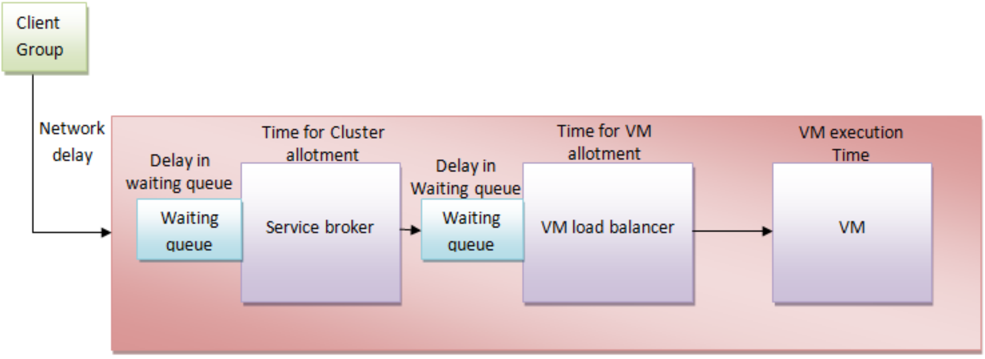


Fig. 4. Figure 4: Times for a processing of a cloudlet on a cloud

In the ideal case the waiting queue will be empty, so there will no waiting time in queue at Service broker and VM load balancer. i.e.t2=0 , t4=0.

So, the ideal case effective time taken for a job to process= t1 +t3 +t5+t6

6 CloudAnalyzer: Detailed Design

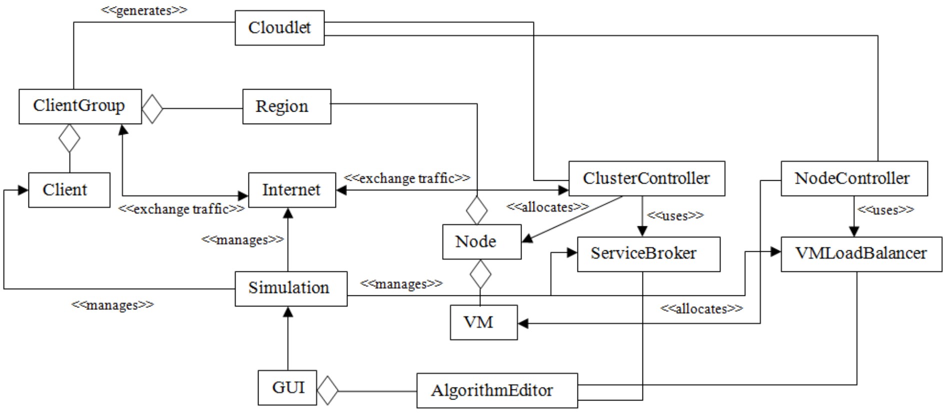
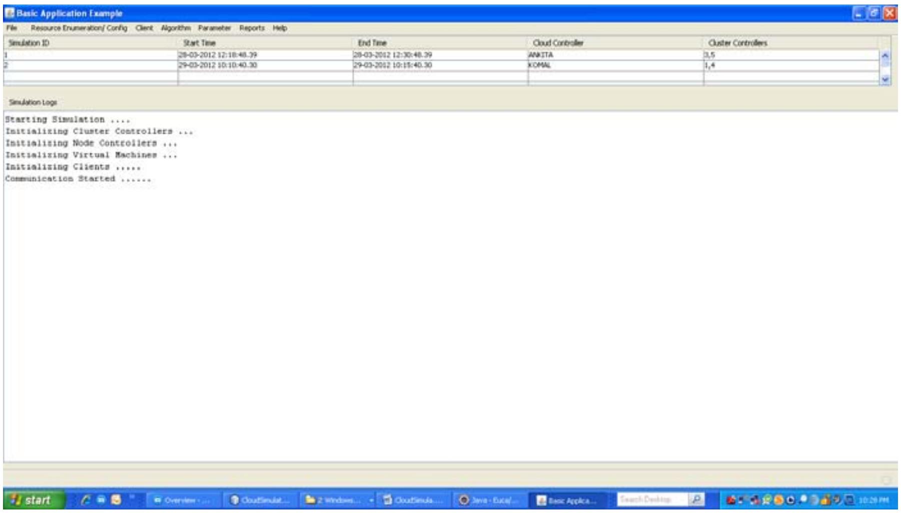


Fig. 5. Figure 5: Domain Class Model for CloudAnalyzer

The Figure 5 shows the Domain Class Model for CloudAnalyzer. The CloudAnalyzer has been built on top of CloudAnalyst using its features. The world is divided into 'Regions' that coincide with the 6 main continents in the World. Internet is an abstraction for the real world Internet, implementing only the features that are important to the simulation. ClientGroup groups a number of Clients in a given region who use the services of cloud. ClientGroup component is responsible for generating Cloudlet, which are a unit of request. These cloudlet traverse through internet and received by the ClusterController component. The ClusterController uses the ServiceBroker policies to allocate an appropriate cluster to the Cloudlet. The Cluster further consists of a number of nodes which are virtually divided into number of VMs. The NodeController uses VMLoadBalancer policies to allocate an appropriate VM to a Cloudlet. The GUI helps to define the simulation parameters and view the results graphically. The simulation components keeps a track of simulation parameters, creating and executing the simulation. It also uses multithreading to run multiple simulation together so that they can be analyzed in a better way. The Algorithm Editor allows a user to add new VM and service broker algorithms without understanding the underlying architecture by abstracting the architecture details. The simulation results are stored in a database so that we can retrieve and analyze them easily.

7 CloudAnalyzer: Implementation

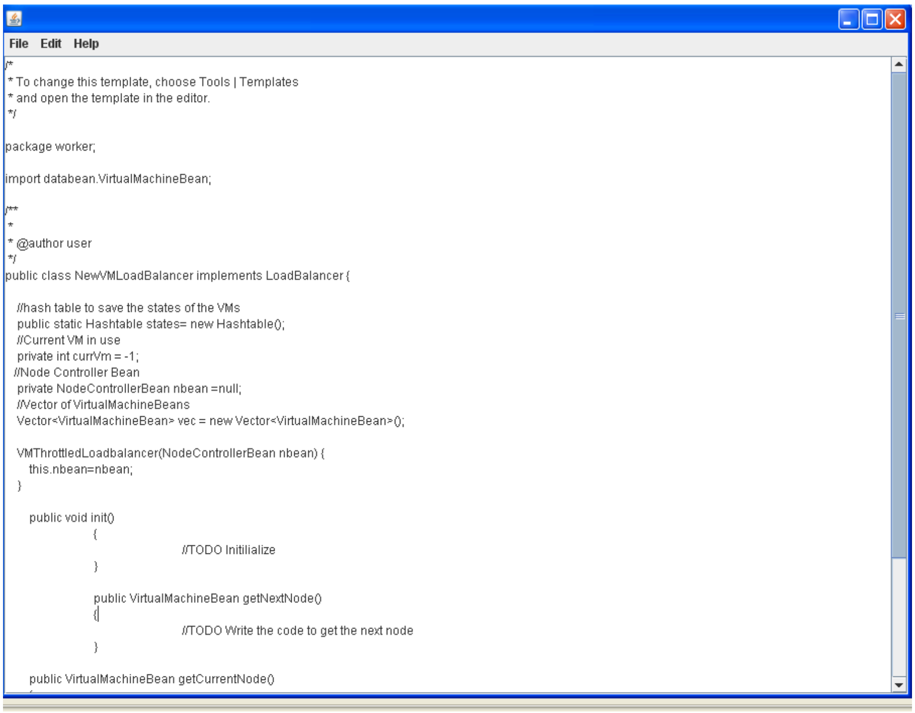
CloudAnalyzer is based on a component driven design that is subject to flexible extensions. the tools and technologies used for implementation comprised of Java (Java SE 1.6); Netbeans IDE 6.5, Java Swing (Java Foundation Classes for GUI); CloudAnalyst; CloudSim; SimJava and MySQl The implementation snapshots are depicted in Figure 6 and 7 respectively.



Simulation ID	Start Time	End Time	Cloud Controller	Cluster Controllers
1	28-03-2012 12:18:48.39	28-03-2012 12:30:48.39	ANKITA	3,5
2	29-03-2012 10:10:40.30	29-03-2012 10:15:40.30	KOMAL	1,4

```
Starting Simulation ....
Initializing Cluster Controllers ...
Initializing Node Controllers ...
Initializing Virtual Machines ...
Initializing Clients .....
Communication Started ......
```

Fig. 6. Figure 6: Main Screen of CloudAnalyzer



```
/*
 * To change this template, choose Tools | Templates
 * and open the template in the editor.
 */

package worker;

import databean.VirtualMachineBean;

/**
 *
 * @author user
 */
public class NewVMLoadBalancer implements LoadBalancer {

   //hash table to save the states of the VMs
   public static Hashtable states= new Hashtable();
   //Current VM in use
   private int currVm = -1;
  //Node Controller Bean
   private NodeControllerBean nbean =null;
   //Vector of VirtualMachineBeans
   Vector<VirtualMachineBean> vec = new Vector<VirtualMachineBean>();

   VMThrottledLoadbalancer(NodeControllerBean nbean) {
      this.nbean=nbean;
   }

      public void init()
                    {
                                        //TODO Initilialize
                    }

                    public VirtualMachineBean getNextNode()
                    {
                                        //TODO Write the code to get the next node
                    }

      public VirtualMachineBean getCurrentNode()
```

Fig. 7. Figure 7: Algorithm editor Screen of CloudAnalyzer

8 Observations : Evaluation Criteria for CloudAnalyzer

CloudAnalyzer helps to separate the simulation configuration exercise from coding exercise and makes it easy for a researcher and the practitioner to focus on analyzing the algorithm by providing a GUI. The graphical output in CloudAnalyzer helps in more analytical interpretation of the results and serves as a basis for comparative analysis The parameter configuration can be customized to test the behavior of different applications on cloud. the algorithm editor window abstracts the underlying architecture details so that the researcher can focus on analyzing the behavior of its innovative Service Broker or VM load balancing algorithms rather than understanding the architecture details of the simulator. The PDF report generator helps in generating a summarized results of a simulation. The database support helps in persistent storage of the results which helps in Query based analysis of the results for deriving meaningful results. The Real time Monitoring gives a real time picture of the simulation for better analysis of the simulation.

Table 1: Comparative Study of CloudAnalyzer and CloudAnalyst

Features	CloudAnalyzer	CloudAnalyst
GUI support	YES	YES
Graphical output	YES	YES
Parameter configuration	YES	YES
Multiple simulations	YES	NO
Algorithm editor	YES	NO
PDF report exporter	YES	YES
Database support	YES	NO
Real time monitoring	YES	NO
Query based analysis	YES	NO

9 Case study:

To test the behavior of a social networking site, facebook with users distributed globally [round robin] on a cloud using Round Robin with server affinity VM Load balancing algorithm for various scenarios of multiple data centers ranging from 1 to 15 [10].

The bar chart for Overall Average Response Time for multiple data centers ranging from 1 to 15 is shown in Figure 8.

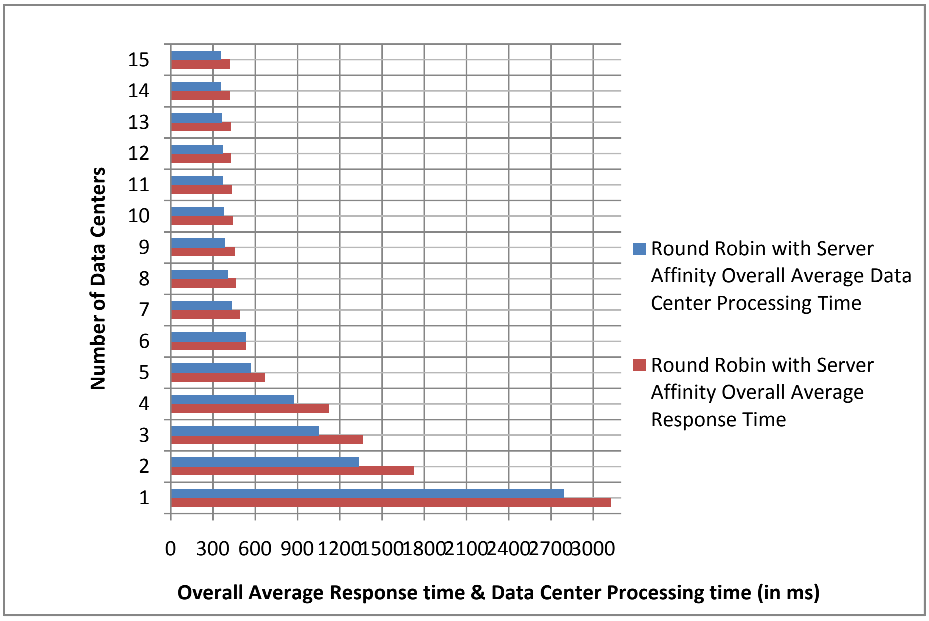


Fig. 8. Figure 8: Bar chart depicting the Overall Average Data Center Processing time and Overall average Data center response time for Round Robin with Server Affinity VM Load balancing algorithm

10 Conclusion and limitations

The Cloud environment has made it possible to address the deployment and hosting of applications more economically and more flexibly by using powerful infrastructure services. The work addressed in this paper proposes an enhanced simulation tool CloudAnalyzer for researchers. that will serve the purpose of studying the large scale applications on the cloud with different configuration parameters. This simulation tools provides enhanced features like multithreading support, algorithm editor window and database support which will help the researchers in the area of cloud particularly in VM load balancing and service broker policies to apply and test their innovative ideas more analytically without going into the details of the underlying implementation architecture. This allows researchers to focus on better analysis of the behavior of their applications rather than understanding the implications and working of the underlying architecture.

Delays & cost may differ from real time cloud environment depending on different cloud infrastructures. Simulation results only serve as a basis for comparison. Due to budget constraints, authors has tested the proposed application on a considerably low cost hardware. However, in future authors are planning to test the application on a more powerful hardware. Authors has not taken care of the security issues and fault tolerance mechanisms in a cloud base infrastructure.

References

1. Foster, I; Yong Zhao ; Raicu, I. ; Lu, S. “Cloud Computing and Grid Computing 360-Degree Compared”, published in Grid Computing Environments Workshop, 2008. GCE '08 IEEE DOI 12-16 Nov. 2008.
2. Sun Microsystems, Inc."Introduction to Cloud Computing Architecture” Whitepaper, Ist Edition, June 2009.
3. Bhathiya Wickremasinghe, Rodrigo N. Calheiros, and Rajkumar Buyya “CloudAnalyst: A CloudSim-based Visual Modeller for Analysing Cloud Computing Environments and Applications” ; Technical Report, CLOUDS-TR-2009-12, Cloud Computing and Distributed Systems Laboratory, The University of Melbourne, Australia, Oct. 23, 2009.
4. R. Buyya, R. Ranjan, and R. N. Calheiros, “Modeling and Simulation of Scalable Cloud Computing Environments and the CloudSim Toolkit: Challenges and Opportunities,” Proc. of the 7th High Performance Computing and Simulation Conference (HPCS’ 09), IEEE Computer Society, June 2009.
5. F. Howell and R. Macnab, “SimJava: a discrete event simulation library for Java,” Proc. of the 1st International Conference on Web based Modeling and Simulation, SCS, Jan. 2008.
6. R. Buyya, and M. Murshed, “GridSim: a toolkit for the modeling and simulation of distributed resource management and scheduling for Grid computing,” Concurrency and Computation : Practice and Experience, vol. 14, Nov. 2002, pp. 1175-1220.
7. Bhathiya Wickremasinghe “CloudAnalyst: A CloudSim-based Tool for Modeling and Analysis of Large Scale Cloud Computing Environments " MEDC Project Report.
8. A. Legrand, L. Marchal, and H. Casanova, "Scheduling distributed applications: the SimGrid simulation framework," Proc. of the 3rd IEEE/ACM International Symposium on Cluster computing and the Grid (CCGrid 07), May 2001, pp. 138-145.
9. Michael Armbrust et al. “Above the Clouds: a Berkeley View of Cloud Computing” Technical Report, Electrical Engineering and Computer Sciences, University of California, Berkeley,Feb 10,2009.
10. Komal Mahajan, Ansuyia Makroo and Deepak Dahiya “Round Robin with Server Affinity: A VM Load Balancing Algorithm for Cloud Based Infrastructure” Journal of Information Processing Systems, Vol. 9, No.3, Sept, 2013, pp. 379-394
11. H. Casanova, “Simgrid: A toolkit for the simulation of application scheduling,” in Proceedings of First IEEE/ACM International Symposium on Cluster Computing and the Grid.
12. Bell W, Cameron D, Capozza L, Millar P, Stockinger K, Zini F. Simulation of dynamic Grid replication strategies in OptorSim. Proceedings of the Third International Workshop

on Grid Computing (GRID), Baltimore, U.S.A. IEEE CS Press: Los Alamitos, CA, U.S.A., 18 November 2002; 46–57.

13. Dumitrescu CL, Foster I. GangSim: A simulator for grid scheduling studies. Proceedings of the IEEE International Symposium on Cluster Computing and the Grid, Cardiff, U.K., 2005; 1151–1158.
14. Lizhe Wang et al. “Cloud Computing: a Perspective Study” , in New Generation Computing, Springer, Volume 28, Issue 2, pp 137-146,April2010.
15. D. Kliazovich, P. Bouvry, and S. Khan, “Greencloud: a packet-level simulator of energy-aware cloud computing data centers,” The Journal of Supercomputing, 2010.[Online].Available:http://dx.doi.org/10.1007/s11227-010-0504-1.
16. Saurabh Kumar Garg and Rajkumar Buyya, “NetworkCloudSim: Modeling Parallel Applications in Cloud Simulations”, Fourth IEEE International Conference on Utility and Cloud Computing, 2011.
17. http://www.cloudbook.net/directories/research-clouds/research-project.php?id=100007 as on March'14.
18. G. Sakellari, G. Loukas, A survey of mathematical models, simulation approaches and testbeds used for research in cloud computing, Simulat. Modell. Pract. Theory (2013), http://dx.doi.org/10.1016/j.simpat.2013.04.002
19. Qi Zhang, Lu Cheng, Raouf Boutaba, Cloud computing: state-of-the-art and research challenges, Journal of Internet Services and Applications, Springer, May 2010, Volume 1, Issue 1, pp 7-18
20. Xu, Gaochao; Pang, Junjie; Fu, Xiaodong, "A load balancing model based on cloud partitioning for the public cloud," Tsinghua Science and Technology , vol.18, no.1, pp.34,39, Feb. 2013
21. R. Buyya, C. S. Yeo, and S. Venugopal. Marketoriented cloud computing: Vision, hype, and reality for delivering IT services as computing utilities. In Proceedings of the 10th IEEE International Conference on High Performance Computing and Communications, 2008.
22. Ian Foster, Yong Zhao, Ioan Raicu, Shiyong Lu, “Cloud Computing and Grid Computing 360-Degree Compared”, IEEE,Grid Computing Environments Workshop, GCE’08, Nov.’ 2008, pp. 1 - 10.

Authors Index