# Architecture framework for control strategies under risk and hazard conditions – CONTROL STRATEG

*Gheorghe Florea*[1], *Radu Dobrescu*[2],*

[1]Societatea de Inginerie Sisteme SIS SA, Bucharest, Romania
[2]Politechnica University, Bucharest, Romania
*Corresponding Author: gelu.florea@sis.ro

*Abstract* - The main motivation and the driving force behind the Control Strateg strategy is the need to respond to the main drawbacks related to the efficient control and risk management of safety-critical applications through the use of advanced data processing and intelligent control techniques that will enable the development of integrated generic and reliable control solutions. The aim of the Control Strateg project is to develop an integrated platform that will offer the much needed support for the decision making process at an organizational level regarding the safe operation of industrial plants and achievement of strategic objectives. The proposed system will tackle some of the most important problems related to the safe management of such applications, namely the early identification of potentially harmful situations and the optimization of the controlled process behavior, both under nominal operating conditions and in the presence of failures and malfunctions that have a negative influence on the system stability and dynamic performances.

***Keywords*** - fault detection, safety shut-down strategies, risk and hazard conditions, data warehouse, integrated platform

## I. Introduction

We live in a modern industry based society where automation undoubtedly is the key for success. The technology has been changing over the last decades toward full control systems and the requirement specifications for Safety Instrumented Systems (SIS) goes to more than a safety system, working together to have the ability to maintain the process running even with less functionalities instead of shut down. The integration of the Fault Detection and Diagnosis, Risk Analysis, Risk and Hazard Control, Reconfigurable Control strategies and System Optimization components within the same safety, security and control application is the main distinctive feature of the Control Strateg strategy.

The field of automatic control for the safe operation of industrial plants, while rather conservative for a long period of time, has been undergoing significant developments during the last two decades as a result of the increasing control demands of safety-critical complex applications. Therefore, it becomes obvious that the classical control solutions are no longer sufficient in the context of a modern industrial society, and that process control and automation technology are definitely the key factors for success.

For this reason, more complex control applications have been developed in order to tackle the various problems related to the efficient risk management of safety-critical plants, namely system optimization, early fault detection and diagnosis, system reconfiguration or restructuring, on-line risk assessment and analysis, prevention of potentially hazardous situations, energy efficiency.

Global requirements of control application in time and with critical environments should lead to the integration of computing, communication and storage capabilities within entities in the physical word [1]. As a result, significant effort has been made for the development of new integrated systems that will respond to all these problems, thus offering powerful support tools for the total risk management of complex industrial installations. There are, however, certain aspects that should be further addressed in order to ensure that such a solution provides the accurate answers to the above mentioned problems in an efficient manner, within the rather restrictive constraints given in real-time control applications.

More complex control applications have been developed in order to tackle the various problems related to the efficient risk management of safety-critical plants but these subjects have been treated rather disparately and the lack of an integrated control solution is becoming a major drawback for any organization that operates in this field.

The most important problem is the fact that there is a very large volume of data involved in the decision making process stored in disparate collections that are used for very specific purposes and serve the needs of different types of users and little effort is being made towards the integration of the separate data streams into a single coherent database; this could then be manipulated more easily and become the building block for a strong knowledge base that will ensure the continuous optimization of the proposed solutions.

During the last decades, the industry has been investing heavily both in Automation Control Systems (ACS) and in Management Information Systems (MIS), like Manufacturing Execution Systems (MES), Enterprise Resource Planning (ERP) or Supply Chain Management

(SCM). The information systems that are used for monitoring and management of industrial plants are usually hierarchically structured in order to deal with the large collection of functional components. However, when it comes to risk analysis and hazard prevention, the monitored process information is far from being used efficiently. Moreover, complex software systems tend to be unpredictable and this is not acceptable in safety-critical application such as chemical and petro-chemical plants or power production plants.

When it comes to risk analysis and hazard prevention, the monitored process information is far from being used efficiently. Majority of the available solutions rely heavily on hardware redundancy, while analytical redundancy [2], plays a least important role. There is a stringent need for more precise and versatile modeling and simulation tools for continuous processes [3].

Since industrial plants often operate near criticality points, in conditions that are far from ideal from the point of view of their controllability and stability, safety is an important aspect of nowadays process control applications; this is, unfortunately, a results of the numerous accidents that occur in industrial plants and that compel the industry to take a better look at current practices like process design, process control, risk analysis and management. Consequently, worldwide organizations have developed standards for the engineering of process safety.

Stand-alone safety systems are the traditional method but this means separate design and operation requirements for Basic Process Control Systems (BPCS) and Safety Instrumented Systems (SIS) [4].

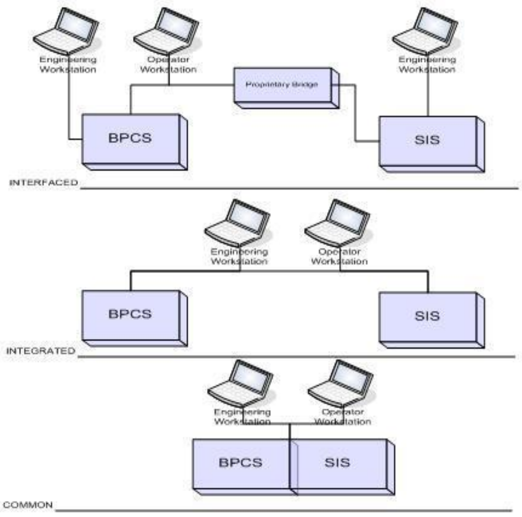


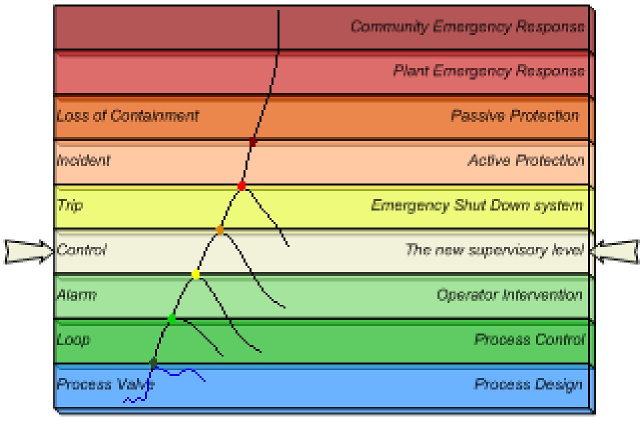
**Figure 1.** SIS and BPCS Integration Levels

Separate systems were developed for process control and for safe operation, but this is an approach that affects the cost of infrastructure acquisition, system integration, control and instrumentation hardware, wiring, project execution, installation and commissioning, as well as ongoing expenses such as training, spare parts procurement and logistics contracts. Integrating safety and control has become a cost effective way for manufactures that could not justify a separate SIS.

According to process safety standards, the process risk has to be reduced to a tolerable level as set by the process owner. The solution is to use multiple layers of protection, including Basic Process Control System (BPCS), alarms, operator intervention, mechanical relief system and a SIS. The BPCS is the lowest layer of protection; Operator Intervention (OI) attempts to solve the problem SIS Layer brings the plant in a safe condition. The author's approach [5] is based on the introduction of a new decision level – Risk and Hazard Control and a new state of the process-safety state. The layers of protection and also the impact over the process are illustrated in the picture below.

When it comes to the automatic control of industrial processes, a common practice consists of using a hierarchical structure with three levels, namely the executive one, the supervisory one and the decision making one. The executive Level is in charge of computing the corresponding commands based on the data acquired from the process and on the given set-points. The supervisory level offers the system operators the possibility to monitor the system status and to manage unexpected events. Finally, the decision level is in charge of determining the optimal functioning regime so that a number of quality criteria, like production quantity or energy efficiency, are maximized; this is performed through the computation of the corresponding set-points that are further sent to the executive level.

**Figure 2.** Layers of protection and impact of the process



Unfortunately, the majority of the control systems that are in use nowadays only take into consideration the optimization of the process behavior under nominal operating conditions. When the system functioning point is driven outside the boundaries of the admissible domain as a result of perturbations r of the occurrence of a fault, however, the generally accepted practice is to proceed to the system shut-down; this is a costly and inefficient procedure that could be avoided in a significant number of cases. It is needless to say that the provided solutions, limited as they are, only address a certain type of users, namely the system operators. Other applications are needed in order to support the decisions taken at higher levels in the management structure of the organization.

## II. Materials and Methods

The proposed approach is a hybrid one, combining elements of the classical Fault Tolerant Control Systems (FTCS) with certain techniques that are characteristic to Artificial Intelligence (AI) in order to obtain a reliable and generic risk management application to be used in a wide range of industrial plants.

The proposed system responds to the needs of plant monitoring, control and management and will represent a powerful support tool for taking the best decisions in critical situations, under severe time constraints. Moreover, the architecture that will be adopted for the integrated system, control strategies and algorithms that will be implemented, will guarantee the successful coherent integration of a large volume of data from various disparate sources and the efficient manipulation of this data, which are the most important requirements from the point of view of the successful implementation.

The technical approach will be based on reusability in the broadest sense using functional blocks. Object technology can be one of the cornerstones of this approach. Reusability can be achieved for any stage in the system life cycle: from requirements and design to commissioning and maintenance. The approach is based on the availability of design template and reusable component implementation with few design compromises. These implementations are flexible enough to be adopted or modified to fit new requirements with little effort. Function block based development and integration middleware concepts provide the basis for reusability. Risk and Hazard Control will incorporate components for process control, safety and security, risk analysis, optimization.

The system will make use of advanced processing techniques for a large amount of data that will be acquired from various sources and that is relevant for the accurate description of the process status at all time and also of intelligent control techniques in order to perform on-line risk assessment based on fault diagnosis and statistical analysis, on the one hand, and also to establish the optimal control strategies in view of maximizing the production potential hazards and unnecessary plant shut-downs during impaired operation, on the other hand.

The Control Strateg strategy will offer solutions to most of the problems related to the efficient supervisory control of safety-critical applications, like chemical and petro-chemical plants, energy production plants, utilities storage and distribution, while also establishing a strong knowledge base for further developments in the field for the constant improvement of the proposed solutions.

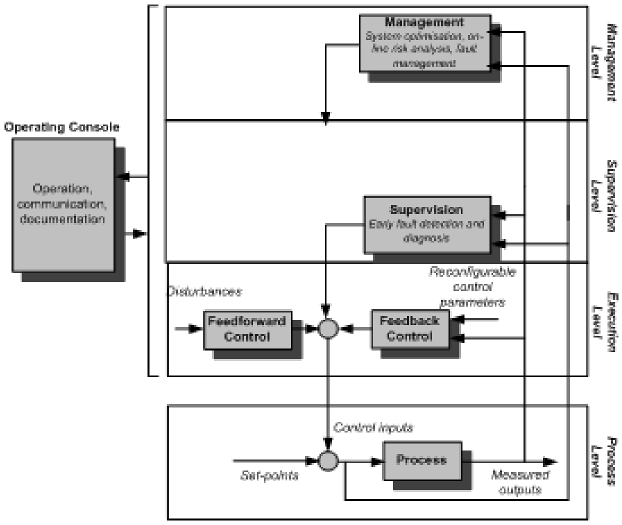


**Figure 3A.** Classical Control System Architecture

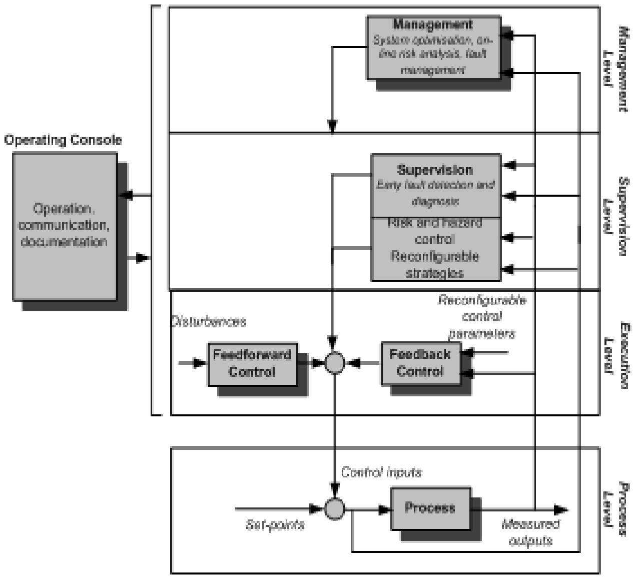


**Figure 3B.** Control Strateg System Architecture

In comparison to the classical approach, the Control Strateg strategy proposes a solution that will determine the optimal control strategies for a wide variety of industrial applications, both under nominal operating conditions and in the presence of system faults, perturbations or modeling uncertainties that can affect the behavior of a plant in such manner that not only the dynamic performances are degraded, but also the system stability is loss. The basic idea is to make use of all the available data from the plant in order to establish the need for system reconfiguration or restructuring in order to accommodate the detected faults and to determine the best strategies that will guarantee the closed-loop stability and the graceful performance degradation, while avoiding the plant shut-down whenever this is possible.

Figures above illustrate the main differences between the majority of the control systems that are in use nowadays for the management of industrial plants and the solution proposed by the Control Strateg strategy.

The first important aspect that differentiates the two approaches is the utilization of the available data describing the process behavior, both instantaneously and in time. More precisely, the Control Strateg system will provide an efficient way of integrating a large volume of data from rather disparate sources in order to obtain an accurate and complete description of the process status at all times. For this purpose, three main types of data will be considered, namely real-time, statistical and modeling data.

Real-time data is acquired on-line from the various components of a classical system, like sensors or controllers, and it usually consists of the measured process outputs and the computed control inputs. This data can be used for early fault detection and diagnosis and for system optimization under nominal operating conditions.

Statistical data refers to data collected over longer periods of time and stored in view of its processing. In the case of the Control Strateg strategy, statistical data will be used for the accurate assessment of the risk level associated to the occurrence of an unexpected event.

Modeling data is computed on-line in order to overcome the drawbacks generated by the lack of information relevant to the description of the process behavior and to support the decision making process regarding the control strategy that should be implemented in a critical situation. Therefore, process modeling will play an active role in the control of industrial plants, as opposed to just supporting the design procedure, which is the case in most applications available nowadays.

Given the diversity and the large volume of the data that will be integrated within the Control Strateg system, it is essential to ensure that there is a reliable solution to the acquisition and correlation of information from various streams. The approach proposed through this project is based on the principles of the OPC UA (Unified Architecture), which is the most recent OLE for Process Control (OPC) specification from the OPC Foundation and differs significantly from the previous specifications by providing a patch to a cross-platform Service Oriented Architecture (SOA) [6] based on different logical levels for process control, while enhancing security and providing an information model [7].

The advantages of the OPC UA approach consist of its multi-platform implementation capabilities, its scalability, its multi-threaded and also single-threaded operation, security based on new standards, configurable time-outs for each service and the ability to incorporate big datagram's.

The most important aspect, however, is the architecture of the OPC information model, which is referred to as a Full Mesh Network based on nodes that can include any kind of meta information, from attributes for read access (DA – Data Access, HDA – Historical Data Access) to methods that can be called commands and triggered events that can be transmitted (AE – Alarms and Events).

The OPC UA can be used for a wide range of applications dedicated to the different levels of control, from the field and process control levels, to the plant and even the enterprise level. This makes it the ideal solution for developing and implementing the integrated system proposed by the Control Strateg strategy, which focuses on the efficient processing of all available data about the process behavior in order to address some of the most important issues related to overall risk and hazard control of industrial applications. Moreover, OPC UA not only offers solutions for data communication and integration, but also for the development of reliable control strategies and for their application with the use of the corresponding generic algorithms in order to ensure the safe operation of the controlled plant.

As illustrated in Figure 2B, there are several system components that will be developed in order to achieve the proposed goals of the project and to ensure that the Control Strateg system respond to all the control requirements of safety-critical applications.

The first one of these functions is early Fault Detection and Diagnosis (FDD). Model-based Fault Detection is a two-step procedure. First, a residual is generated based on the information available from the process (known command inputs and measured outputs). The residual is a linear or non-linear function of the system inputs and outputs. The computed value is further compared with a threshold in order to establish whether a fault has occurred or not. It is essential for the correct performance of the system that the threshold is chosen appropriately because if its value is too low there is a high false alarm probability whereas if its value is too high certain faults can remain undetected.

If a fault is detected, then Fault Diagnosis has to be performed in order to establish its location (Fault Isolation) and magnitude (Fault Identification/Estimation). The Fault Isolation consists of generating a residual set describing the possible fault scenarios and of comparing the given residuals with the elements of the set. The minimal distance between the computed residual from the fault detection module and the elements of the set in terms of vector norm indicates the faulty component or components (sensors, actuators, components of the physical plant). The Fault Estimation/Identification consists of identifying the post-fault process model.

A modern approach to Fault Diagnosis, however, makes use of artificial intelligence techniques, like fuzzy logics, artificial neural networks, genetic algorithms or various combinations of these techniques in order to perform pattern recognition for particular faults or system states [8] that are difficult to map using the more classical modeling procedures, including also nonlinear systems or processes that are highly affected by disturbances.

The Control Strateg strategy will take into consideration both the model-based and the knowledge-based approaches to FDD in order to obtain a high-performing and efficient technical diagnosis module that will be able to work within the rather restrictive real-time constraints imposed by the nature of safety-critical applications and to cover the detection, isolation and estimation of a wide range of faulty or otherwise undesired system states that could occur during the plant operation. Through the diagnosis of system faults that were not initially anticipated in the process design phase, the degree of reliability of the controlled application will increase; this approach relies heavily on analytical redundancy and less on hardware redundancy, which makes it more cost effective.

Nowadays, a reliable FDD module is becoming a must in every risk management application as it represents the building block for the control strategies that are meant to guarantee the safe operation of the plant in risk and hazard situations. For this reason, it is important to understand the relation between FDD and Risk Analysis (RA), which is the next phase in achieving the objectives of the strategy.

While a hazard is not a fault, it can be caused by the occurrence of one or more faults concurred with certain environment conditions, influencing the stability and safe operation of the plant and, ultimately, endangering the environment and the population safety if left unattended for. Depending on the influence of the fault on the system safety and reliability, there are several hazard classes and the corresponding supervisory actions taken for the fault management can vary from shut-down if there is an imminent danger for the process or the environment to reconfiguration, maintenance and instantaneous repair [9,10].

The hazard risk assessment is performed based on the information received from the FDD module and also using statistical analysis of the available data; the procedure is less generic than the FDD one, since a-priori information related to the specific behavior of the plant in certain risk scenarios has to be incorporated within the analysis. The nature of the RA problem and the large volume of data involved are the main factors that impose the integration of knowledge-based techniques with the classical approaches in order to develop generic and reliable tools for the accurate assessment of hazard risk for a wide enough range of industrial applications.

After the FDD and the RA, the final stage of the reliable risk and hazard control approach proposed by the Control Strateg strategy is the System Optimization (SO). This generally refers to the development and implementation of the appropriate control strategies and of the corresponding algorithms that guarantee the system stability and the best dynamic performances of the process by report to several criteria.

While SO is already a component of most control systems already in use in the industry, it is only used for improving the plant performances under nominal operating conditions. The problems, in this case, are the definition of the quality criterion or criteria that need to be maximized, the identification of the optimization model based on historic data acquired from the physical plant and the computation of the corresponding parameters that ensure the maximization of the chosen criterion or criteria for that particular model. These parameters represent the set-points that are further sent to the control elements at the executive level in order to drive the system behavior as close as possible to the optimal functioning point.

However, when the system is under the influence of a fault or disturbing signal that affects its stability and dynamic behavior, the generally accepted practice is to proceed to the plant shut-down. Safe shut-down strategies have already been established for safety-critical industrial plants. Therefore, the Control Strateg strategy does not propose new methods for performing this action, but takes into consideration the integration of the already existing solutions to this problem within the risk and hazard management platform that will be developed.

Another major difference between the Control Strateg system and the classical applications is the fact that, when the risk level is acceptable, new solutions are sought for the accommodation of the fault or otherwise the management of the undesired event that has led to the degraded plant performance or that has affected the system stability. The objective is to find new control parameters or even new control structures that will stabilize the plant and will ensure graceful performance degradation when possible, thus avoiding unnecessary and costly plant shut-downs.

In other words, new control strategies need to be established on-line in order to allow the plant to keep running, even if certain performance degradation is accepted and sometimes unavoidable, while still maintaining the desired safety level. This phase can involve both analytical and physical redundancy and consists of solving an optimization problem where the quality criterion is usually defined so that it describes the closeness between the accommodated and the desired plant behavior. The RHC (Risk and Hazard Control) module is a new component of process control, involved when a hazard state can activate the emergency shut-down (ESD) system to stop the plant, having the goal to ensure the continuous operation. One of the most efficient ways to avoid the shut-down of the plant when key parameters are for from the nominal state is the reconfiguration. Reconfigurable set of sensors, of actuator, of interconnections can be used but Reconfigurable Control (RC) strategies and reconfigurable process can be more effective. All this tools will be analyzed and used in order to implement the most affordable and flexible solution.

The integration of the FDD, RA and SO components as described above within the same hazard and risk control application is the main distinctive feature of the Control Strateg strategy.

The project quantifiable or qualitative expected impacts are:

- ✓ Optimisation of large-scale plants operation under normal conditions from the point of view of productivity increase and operation costs decrease;

- ✓ Improvement of plants functioning under the influence of system faults, based on modelling uncertainties and external disturbances;
- ✓ Decrease of hazard occurrence risk as a result of permanent system monitoring, early failure detection and diagnosis, fault accommodation algorithms and hazard prevention procedures;
- ✓ Financial savings for the users due to the elimination of unnecessary plant shut- downs;
- ✓ Energy saving through the optimisation algorithms and the early detection of malfunctions;
- ✓ Support for the research and further developments in this field based on a strong knowledge base for professionals in the domain.

## III. Conclusions

The main expected result of our project is a commonly accepted system architecture that will guarantee that all the control requirements of safety-critical industrial applications are met through an integrated solution that will support the decision making process regarding hazard risk management for all types of users.

Further work will focus on:

- Coherent data collection for the complete and accurate description of the process dynamic behaviour.
- Generic fault detection and diagnosis strategies and algorithms.
- Generic risk assessment strategies for industrial plants.
- Experience-based learning strategies and techniques for the continuous optimisation of the control solution.
- Integrate with remote control system for the total risk management in industrial applications.

Any comments and suggestions are welcomed so that we can constantly improve this template to satisfy all authors' research needs.

## Acknowledgements

We are very grateful to experts for their appropriate and constructive suggestions to improve this template.

## REFERENCES

[1] P. Albertos, "Challenges in the Control of Cyber-Physical Systems", *Proceedings of the 18th International Conference on Control Systems and Computer Science*, Bucharest, 2011.

[2] Y. Zhang, J. Jiang, "Bibliographical Review on Reconfigurable Fault-Tolerant Control Systems", *Annual Reviews in Control*, Vol. 32, pp. 229-252, 2008.

[3] A. Gosh, D. Woll, "Business Issues Driving Safety System Integration", *ARC White Paper*, 2006.

[4] M. Spooner, T. MacDougall, "Safety Instrumented Systems. Can they be Integrated but Separate?", *ABB White Paper,* 2011.

[5] G. Florea, L. Ocheana, D. Popescu, O. Rohat, "Emerging Technologies – the base for the next goal of Process Control – Risk and Hazard Control", *Proceedings of REV2011* – 2011.

[6] S.H. Leitner, W. Mahnke, „OPC UA – Service Oriented Architecture for Industrial Applications", *Proceedings in Softwaretechnik* – Trends, 2006

[7] W. Mahnke, S.H. Leitner, „OPC Unified Architecture – The Future Standard for Communication and Information Modeling in Automation", *Proceedings ABB Review*, pp. 55-61, 2009

[8] J. Kacpprzyk, J. Korbicz, J. M. Koscielny, Z. Kowalczuk, W. Cholewa, "Fault Diagnosis – Models, Artificial Intelligent, Application", Springer Verlag, 2004

[9] A. Zolghadri, "The Challenge of Advanced Model-Based FDIR Techniques for Aerospace Systems: The 2011 Situation", *Proceeding in 4th European Conference for Aerospace Sciences*, 2011

[10] I. Hwang, S. Kim, Y. Kim, C. E. Seah, „A Survey of Fault Detection, Isolation and Reconfiguration Methods", *Proceedings in IEEE Transactions on Control Systems Technology*, Vol. 18, No. 3, pp. 636-653, 2010