Emerging Technologies- the base for the next goal of Process Control - Risk and Hazard Control

GHEORGHE FLOREA, LUIZA OCHEANA, DAN POPESCU, OANA ROHAT
Department of Control and Industrial Informatics
Politehnica University of Bucharest
Spl.Independenței 313, sector 6, 77206 Bucharest
ROMANIA
gelu.florea@sis.ro, luiza.ocheana@sis.ro,dan_popescu_2002@yahoo.com, oana.rohat@sis.ro

Abstract: - Over the last decades the requirement specifications for Safety Instrumented Systems (SIS) form the central network for the process risk and hazard assessment to be carried out. SIS are flexible and effective tools for guarding the process plants. Our approach is based on how a new hierarchical decision level can complete the mission regarding safety when the control room is not functional or cannot act properly in a hazard situation. Layers of protection should be used in order to reduce the risk to an acceptable level. The key is risk and hazard control implemented as a superior hierarchical level of decision and intervention. Emerging technologies used for engineering and implementing is the approach that can help the designers to apply the proposed system architecture. The simulation and concurrent engineering are basic approaches to accomplish the functionalities of new system architecture and the results of an R&D project (PH Center) show the feasibility. Based remotely from the site the Process Help Center host not only the copy of the process control system but the strategies and algorithms to accomplish the safety and security tasks, maintain the process operation, run the simulation and optimization.

Key-Words: - Safety instrumented systems, Simulation, Diagnostics, Hierarchical decision, Concurrent engineering, Risk and hazard assessment, Remote intervention

1 Introduction

Process control and optimization represent the current base for safer and more efficient industrial plants, while risk management represents the base for new control algorithms and strategies. There is a stringent need for the enhancement of process operations at plant production management level, because plants should often operate near criticality, meaning in conditions far from ideal ones from the point of view of control and stability. Continuous process industries are usually very complex and difficult to model and kept under control. There is a tremendous need for better and more versatile simulation and modeling tools but no product in the market offers the necessary capabilities to deal with the uncertain nature of complex plants including safety and security threats.

Safety is an important issue nowadays that received an increasing amount of focus lately. The reasons are, unfortunately, the numerous accidents occurred in industry plants which require the process industry to take a hard look at current practices like process design, process control, risk analysis and control, risk assessment. Worldwide engineering organizations have developed standards for the engineering of process safety. IEC released two standards IEC 61508 aimed at the suppliers of process safety equipment and IEC 61511 aimed at the end users of process safety equipment. ISA S84.01 includes all elements from sensors to final elements, including inputs, outputs, power supply, logic solvers and user interfaces.

In order to achieve the required level of safety and security, we should take into consideration four important phases: analyze the needed level of Safety Instrumented Systems (SIS) for the plant, design, implementation and maintenance.

Today, integrating safety and control has become a cost effective way for manufacturers that could not justify a separate SIS in the past [1]. Entire issue of safety has direct influence on the activity of the plant and therefore it must be integrated into the plant control system.

2 RH Control – the New Level of Decision

According to the IEC 61511/ISA 84 process safety standards, the process risk has to be reduced to a tolerable level as set by the process owner [2]. The solution is to use multiple layers of protection, including the basic process control system, alarms, operator intervention, mechanical relief system and a SIS.

The Basic Process Control System is the lowest layer of protection and is responsible for the operation of the plant in normal conditions. If BPCS fails or is incapable of maintaining control, then, the second layer, Operator Intervention (OI) attempts to solve the problem. If the operator also cannot maintain control within the requested limits, then the SIS Layer must attempt to bring the plant in a safe condition [3]. Our approach is based by 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

Fig.1.

Risk is defined as the combination of the probability and the severity of a hazardous event, meaning how often it can appear and how bad are the consequences when it does. The best way to reduce risk in a manufacturing plant is to design safer processes. Unfortunately, it is impossible to eliminate all risks, so a manufacturer must agree on a level of risk that is considered tolerable. After identifying the hazards, a hazard and risk analysis must be performed to evaluate each risk situation [4].

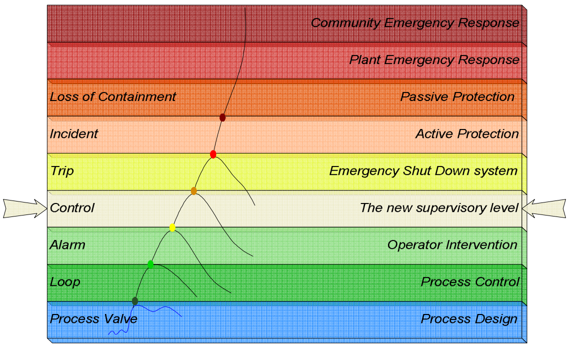

Fig.1. Layers of protection and impact on process.

BPCS, along with process alarms and facilities for manual intervention, provide the first level of protection and reduce the risk in a manufacturing facility. Additional protection measures are needed when a BPCS does not reduce the risk to a tolerable level. They include SIS along with hardware interlocks, relief valves, and containment dikes but the process must be stopped. The start-up of the process means a lot of time and money.

To implement additional risk and hazard control is the next goal of Process Control. The technical approach tries to provide reusability in the broadest sense using functional blocks. Object technology can be one of the cornerstones of this approach [5]. Reusability can be achieved for any stage in the 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 adapted or modified to fit new requirements with little effort. Function block based development and integration middleware concepts provide the basis for reusability. RH Control will incorporate components for process control, risk analysis, optimization, etc.

The customized components will be integrated in a global architecture using a real-time integration. This software, based on function block specification, will incorporate extensions to make possible its use in real-time applications. This facilitates the easy reuse of components and even the reuse of the global application architecture because run-time components can be easily changed without affecting other components behavior.

2.1 Advantages

The benefits of this approach can be classified into two categories:

- From the user’s point of view: the implementation addresses the problems related to the global management of the plant while taking into account the interrelation of the strategic objectives, such as production, quality, maintenance, safety, efficiency and continuity, as well as problems closer to the process control layer.
- From the systems integrator’s point of view: the development of an open software architecture based on OPC and function block specification, will allow the construction of distributed intelligent control systems on top of the existing control systems being used in the industrial plants with back-up functions.

2.2 System architecture

Better automation is a key aspect for improving industrial competitiveness. Intelligent automation at management levels - in particular - can play a major role regarding this aspect. RH Control aim is to help in this improvement by building a new architecture (Fig.2) and a distributed and generic software system that addresses decision support for near critical situation management in continuous process industries. In particular, assistance, in terms of diagnosis and solutions, is provided to the plant and/or to the staff when situations suitable to be corrected, prevented or enhanced are detected.

The focus is on new algorithms and strategies for the integration of different software components as well as on the system architecture itself. These software components include core modules, user interface modules and problem solving modules.

RH Control follows the conceptual structure of most distributed control systems that is a hierarchical and multilayered structure, similar to a pyramid (Fig.2). The complexity of the control mechanism increases in higher layers. All the basic functionalities of the system are grouped into problem solving components that work in a cooperative way to find a solution to the plant problems or to optimize the plant objectives.

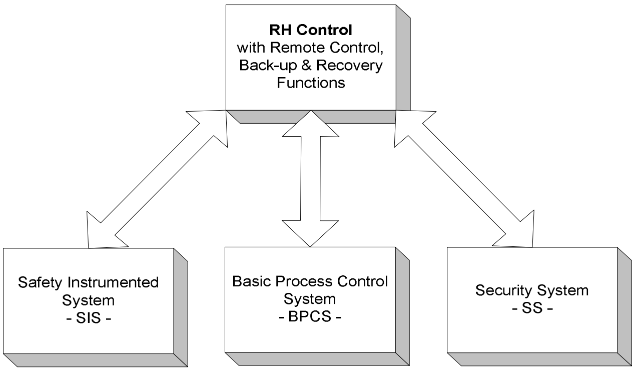

Fig.2. System architecture.

The solutions include the following functionalities at the different control layers:

- Strategies: Management of global objectives of the plant and their interrelation (management of maintenance operations, incident prevention, risk and hazard control, assessment of production costs in real time, loop tuning optimization, quality deviation detection and alarm management)
- Tactics: Assistance through the problem lifespan, including process failure prevention, risk detection and diagnosis, plant-wide analysis, corrective actions, actions or recommendations for reestablishing effective control.
- Operations: Tasks such as filtering and validation of plant data, variable estimation, alarms analysis and optimization, intelligent alerting based on intuitive technologies and trend forecasting.

The software architecture will be Service Oriented Architecture - SOA based approach [6]. It is common that the infrastructure and the environment of applications are very important security-related issues in the system and it gets even more important, if a SOA-based on Web Services has been chosen as application-architecture. For this reason asymmetric cryptography will be used, meaning a pair of two keys: public key and private key.

3 Emerging Technologies

Future applications of simulation technology applied to process control will be driven by advancing capabilities of simulators. Much of this advancing capability is the direct benefactor of advancing computing technology applied to activities with high return on investment in areas such as concurrent engineering, process fault detection, self testing capabilities for hardware and internet retrievable simulation models and tools.

Simulation technology. Simulation technologies are not something new but till our days the research, contributions and experiments was more theoretical. The evolution of computing, of hardware performances, of software capabilities are the fundamentals to implement simulation in real time. Some of these advancements are:

- *Advanced networking*. Advances in network technology are making possible to link computers together to share data at increasing speeds, enables multiple computers to work in parallel to simulate more complex systems and to connect the simulator and controller. Three types of network interfacing applicable to simulation can be use:
  - o Bus adapter and shared memory
  - o Data broadcast network
  - o Internet
- *Intelligent I/O*. Applied Dynamics International developed and uses an intelligent input/output processor card to predict outputs and update the value more frequently than the update rate from the simulator increasing speed for the next prediction
- *Very High Speed Simulation*. This approach is based on development of digital hardware-in-the-loop simulations that permit simulation frame-times below 10 microseconds.

There are many approaches to be used to achieve good results and in time, the most important we will describe briefly.

- *Integration algorithms*. Integration algorithms are used to solve a function in time, given the differential equation for the variable of interest. Runge-Kuta is probably the best known integration algorithm. A newer algorithm, named after its developers R. Bulirsch and J. Stoer is gaining popularity and may replace Runge-Kuta.
- *Discrete-Event Simulation*. Two types of discrete-event simulation tools are available; the state transition diagram editor and user/resource queuing tools.

State-transition diagram editors allow the user to model a process by what state the process is in and by events that cause a transition from one state to another [7]. The use of state-transition diagrams allows the behavior of a process to be dependent on the state. A process simulator with a state-transition-diagram editor allows different dynamics to be assigned to different operational states of the same process. Fig.3 shows the classical states: start-up, nominal and shut-down. We will add risk and hazard state to keep process under control.

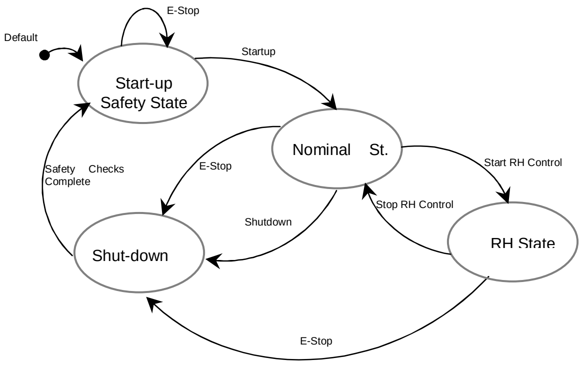

Fig. 3. Operational states.

User/resource analyzes tools queuing systems that can be characterized by a collection of resources and tasks using these resources [8]. The modeling tools allow resources to service tasks in many priorities such as first-come-first-served, infinite servers, last-come-first-served, processor-sharing. System parameters such as response times, utilization rates, queue populations and throughput rates can be assessed. Probability distributions and tasks attributes such as creating, terminating and delaying can be changed. This will be used further to implement the appropriate DCS or PLC and SCADA strategies to run on the site system or remote.

- *System Identification*. The data handling and computing capability available today enables not only standard on-line identification techniques but also sophisticating empirical model development methods that in the past were to difficult to be done by hand. Tools are available with today’s simulators to help gather perturbation data from the process and develop empirical that sometimes are with much fidelity than classical models. Even the theory of system identification has been around for a long time, only recently these theoretical tools become practicable because of the large amount of data processing required.

Concurrent Engineering

An activity that requires a high degree of effort by a design company, but not without rewarding return on investment is concurrent engineering. This design paradigm is based upon the principle that the process and the associated control strategy are design in parallel before the process is built. Trade-off analysis is performed before conflicting criteria of the two designs. Even the HAZOP study was performed to establish the functions, algorithms and strategies for SIS from the beginning, the concurrent engineering must perform the total approach of the hole process. The evolution of Software Engineering methodology, from waterfall to spiral, from spiral to agile, indicates that high concurrency, iterative development and short cycles are key factors for effective Software Engineering [9]. Using concurrent engineering not only to establish the general architecture of the integrated system but to software engineering also it is recommended. In the mean time dynamic process simulators must be combined with traditional static simulators in order to asses transient behavior and controllability of the process.

C. Other emerging technologies

- Controller Testing. Using simulators to test control systems is an increasing trend in almost every industry. Simulator-based control system testing removes control software development from the project critical path. A test using simulators can be more comprehensive than a test using actual process because the normal safety or process operational limits are not a concern, so the virtual test can transcend those limits, if necessary, to perform a more robust test. The networking options enable interfacing a simulator to a control system at a higher level in the system architecture than in the past when individual wiring terminations were required.
- *On-line Diagnostics*. Modern simulators offer the ability to detect faults in operating plants. A well tuned model of the plant runs in parallel with the plant, on-site or remote, comparing the model’s outputs with the real outputs. As shown in
- Fig.44 a difference between the two indicates a fault. Advanced fault-detection algorithms will lead the RH control or supervisory engineers to provide the appropriate action.
- *Asset management*. The new approach of asset management taken in to consideration not only process assets but instrumentation and process control system is the first step to more safety of the plant. Probably the evolution from compressors and drums to sensors and valves will continue incorporating the operator, may be the most important “asset” from the safety and security of the process point of view.
- *Internet Applications*. This amazing technology (NEOXITE [10]) offer today the capability to interconnect the on-site system with a

remote control center (PH Center) and to perform simulation, on-line identification, RH strategies, on-line tests and training, back-up and restoration. Based remote from the site the Process Help center will host not only the copy of the process control system but the strategies and algorithms to accomplish the safety task and to maintain the process running even in hazard and risk conditions.

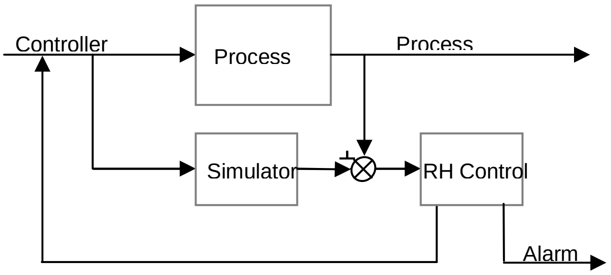

Fig.4. Online diagnostic.

4. Results

The totally new approach in process control systems engineering, based on new process control algorithms, scalable and modular architectures and platforms, risk and hazard control, is independent of the industry sector. The capability of the systems to perform the four states, having four different strategies and the capability to change the state accordingly with the functional parameters can be taken in consideration by concurrent-engineering. The correlation factor between different applications will influence the future decisions. This way, the time needed for solving a problem will be minimized, as well as the time that a plant needs to be shut down because of instrumentation process control strategy.

Some of the expected results are the integrated exploitation of a collection of heterogeneous technologies for the prevention of anomalous situations related to the safety of an industrial complex and the suitability of function blocks and OPC based development for integrated control systems construction.

From the user’s point of view, the accomplishment is that RH Control will allow the integration of the preventive and corrective aspects of safety, which were dealt, until this moment, in a separate way. Another advantage of great importance arises able to take into account automatically the constraints posed by the current plant situation and the ongoing maintenance operations.

The results achieved so far within the R&D project “Help Center and platform for remote diagnosis and remote intervention for the management of plants in hazardous situations – PH Center” will be used in order to develop and implement the hierarchical superior level for safety and security problems. The work carried out in the project establish the base for a new architecture of process control taken into consideration the risk and hazard situation correlated with capability to be remote from site (Fig.5).

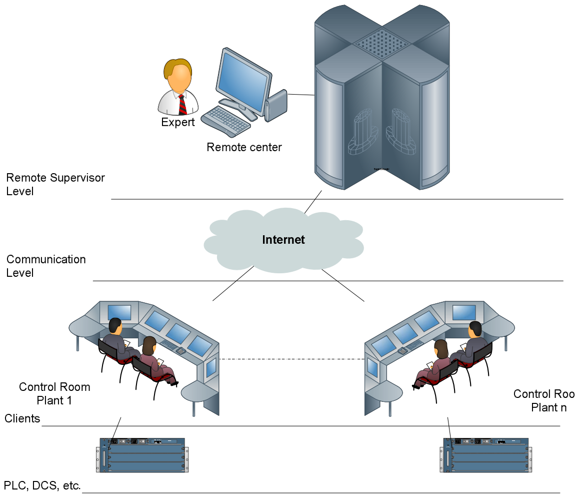

Fig.5. PH Center architecture.

In the main time the results achieved underlay the feasibility. This statement is based on two reasons:

- The two demonstrators have been designed according to real plant requirements with a large involvement of the site staff. At present, both applications installed are under operation after a period of user validation and evaluation.
- The three generic products constructed within the project are truly reusable and exploitable components.

As stated by many relevant projects, safety and security can be better managed through IT technologies and can increase systems autonomy and performances. This project demonstrates that advanced control technology can be modularized, deployed and integrated with legacy control systems, progressing effectively toward complete automatic operation.

4 Conclusion

In the past SIS were strictly separate from the BPCS, mainly to segregate the safety and control functions and to have higher availability and reliability. Lately, there have been many launches of new "integrated" control systems that have both BPCS and SIS systems in the same package. But still, in the view of the standards bodies (like IEC and ISA), these two systems have to be separate, as the safety systems have to be dedicated to only the safety critical parts of the plant and the garden-variety DCS cannot be said to be robust, fail-safe and sure to operate the safety critical instruments at all times.

Hazard identification, risk assessment and control are on-going processes which involve a critical sequence of information gathering and the application of a decision-making process. These assist in discovering what could possibly cause a major accident (hazard identification), how likely it is that a major accident would occur and the potential consequences (risk assessment) and what options there are for preventing and mitigating a major accident (control measures).

In the following picture (Fig.6) we present the architecture of one on-going project: adding to the PH Center the control system from LPG terminal, Midia, Navodari (Romania).

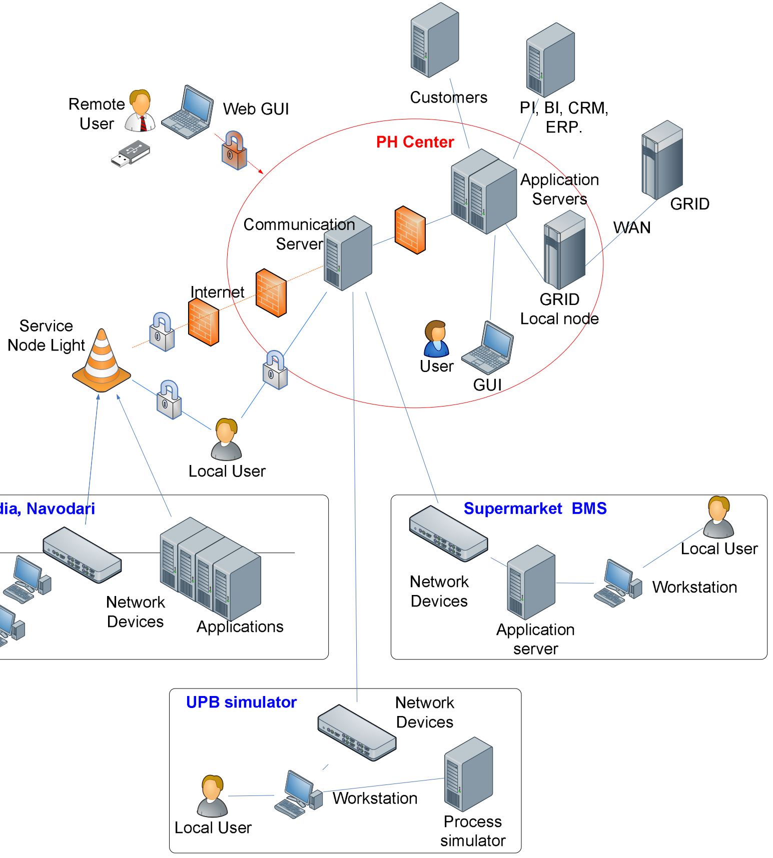

Fig. 1 – PH Center application

ACKNOWLEDGEMENTS
This work was supported in part by the Romanian Ministry of Education and Research under grant PN2 12-100/2008 by DocInvest Project ID 76813.

References:

[1] Asish Ghosh, Dave Woll. Business Issues Driving Safety System Integration. 2006. ARC Advisory Group

[2] David Hatch, Todd Stauffer. Operators on alert. Alarm standards, protection layers, HMI keys to keep plants safe. 2009. InTech.

[3] Merry Spooner, Trevor MacDougall. Safety Instrumented Systems: can they be integrated but separate?

[4] Gary Stoneburner, Alice Goguen, Alexis Feringa (2002). Risk Management Guide for Information Technology Systems. Recommendations of the National Institute for Standards and Technology. U.S.A.

[5] Guttman, Michael and Jason R. Matthews (1995). The Object Revolution. Wiley. New York.

[6] Stefan-Helmut Leitner, Wolfgang Mahnke. OPC UA – Service –oriented Architecture for Industrial Applications. ABB Corporate Research Center. Ladenburg, Germany

[7] Harel D(1987) State charts: A Visual Formalism for Complex Systems In: Science of Computer Programming vol.8

[8] Cassandras C(1993) Discrete Events Systems: Modeling and Performing Analysis In: Asken Associates Inc., Boston

[9] Jacky Estubier , Sergio Garcia Concurent Engineering support in Software Engineering, 2006.

[10] Project Consortium (2004). NEOXITE – Next Generation Open Control System Internet Ready