Concurrent Engineering used to Implement Risk & Hazard Control

Gheorghe Florea
Societatea de Inginerie Sisteme – SIS S.A.
Bucharest, Romania
e-mail: gelu.florea@sis.ro

Luiza Ocheana
University “Politehnica” of Bucharest
Bucharest, Romania
e-mail: luiza.ocheana@sis.ro

Abstract — **In the current modern and industry-based society, automation is the key to success. The technology has changed over the last decades towards full control systems. Requirement specifications for Safety Instrumented Systems (SIS) form the core of Risk and Hazard (RH) assessment. SIS are the most flexible and effective tools for guarding the plants. Despite the debate pro and against the integrated approach of Basic Process Control System (BPCS) and SIS, more than a safety system is needed to keep the process running even with diminished functionalities instead of shutdown the plant. Our new 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 RH control implemented as a superior hierarchical level of decision and intervention. Concurrent Engineering (CE) applied to process control is the approach that can help the designers to achieve this level and efficiently use the proposed system architecture. Basically, a remote Process Help Center will host not only the copy of the process control system but the strategy and algorithms (RH control) to accomplish the safety task and to keep the process running. The CE and simulation are basic approaches to build the functionalities of new systems.**

Keywords – SIS; Redundancy; Remote intervention; Simulation; Diagnostics; Hierarchical decision; Concurrent engineering; Risk and hazard assessment.

I. INTRODUCTION

Process control and optimization represent the current way for safer and more efficient industrial plants, while risk management represents the starting point for new control algorithms and strategies. There is a stringent need for enhancing plant operations at production management level, because plants often operate near criticality, meaning in conditions far from the ideal ones from the point of view of control and stability. Continuous process industries are usually very complex and difficult to model and keep under control. While plant personnel feel there is a tremendous need for better and more versatile simulation and modeling tools, no product on the market offers the features necessary for dealing with the uncertain nature of complex plants [1].

Safety is an important issue nowadays that receives an increasing amount of focus lately. The reasons are, unfortunately, the numerous accidents that occurred in industrial plants, which compel the industry to take a better 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 “Application of Safety Instrumented Systems for the Process Industry” includes all elements from sensors to final elements, including inputs, outputs, power supply, logic solvers and user interfaces [2].

Applying these standards we obtain reliable facilities, but still we do not solve the problem of continuity of the production process - the main goal in the economic competition. This paper presents a way to solve the problem of maintaining the continuity of the process by introducing a level of control for risk and hazard situations.

In this paper, we present the challenge of Safety and Security systems (Section II), the introduction of Risk and Hazard control as a new level of decision (Section III), simulation as the key for Risk and Hazard control (Section IV), technologies to be used (Section V), results and conclusions (Sections VI and VII).

II. SAFETY AND SECURITY (SS) – THE CHALLENGE

In order to obtain the required level of safety and security, we must take into account four important phases: analyze the needed level of SS for the plant, design, implementation and maintenance.

Stand-alone safety systems have been the traditional method of choice, meaning separate design and operation requirements for Basic Process Control Systems (BPCS) and Safety Instrumented Systems (SIS) [3]. Separate systems were developed for process control and safety with proprietary operator interfaces, engineering workstations, configuration tools, data and event historians, asset management, and network communications. This approach affects the costs of infrastructure acquisition, plant systems 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 [4]. Until recently, users had little choice other than to use completely different systems for control and safety. “A war of words is raging in the process control industry over the “integration” of safety and control systems. It’s a debate that has been ongoing for years, but the recent introduction of new integrated systems by several process controls vendors has lately added fuel to the fire” [5].

Today, integrating safety and control has become a cost effective choice for manufacturers that could not justify a separate SIS in the past. As a process manufacturer, you need to perform rigorous Risk and Hazard (RH) analysis based on IEC 61511 or ANSI/ISA-84.00.01 safety standards to decide

Copyright (c) IARIA, 2011. ISBN: 978-1-61208-168-7

on the right level of protection required for your plants. You may do that by selecting a SIS that provides close integration with the software tools of your BPCS while still providing the required degree of separation. Figure 1 illustrates the three options.

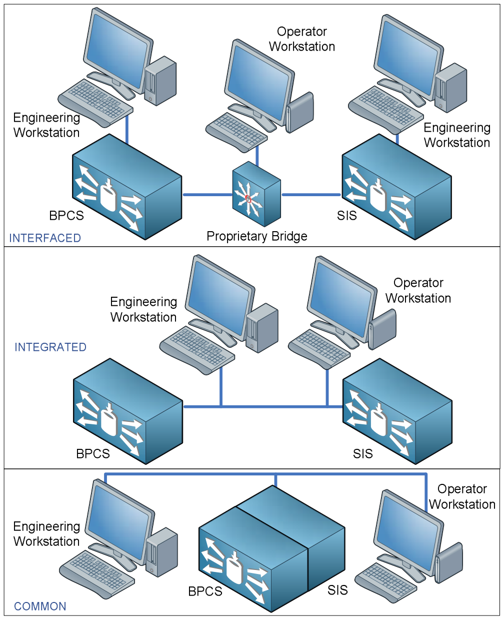


Figure 1 – SIS and BPCS Integration Levels

In the traditional sense, process safety refers to additional components that protect personnel and plant from injury, death and economic loss. However, many end users now recognize that the deployment of intelligent integrated safety solutions can directly improve process and personnel safety.

The entire issue of safety has direct influence upon the activity of the plant and therefore it must be integrated into the control system.

III. RH Control – the new level of decision

According to process safety standards, the process risk has to be reduced to a tolerable level as set by the process owner [6]. The solution is to use multiple layers of protection, including the BPCS, alarms, Operator Intervention (OI), mechanical relief system and a SIS.

The BPCS 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, 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 [7]. If SIS also fails in restoring normal operation, then the hazard is imminent.

Risk is defined as the combination of the probability and the severity of a hazardous event, meaning how often it can appear and how severe 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 RH analysis must be performed to evaluate each risk situation.

The layers of protection and also the impact over the process are illustrated in Figure 2. On the left side, the layers of protection are listed; on the right side, the corresponding actions on the process are listed.

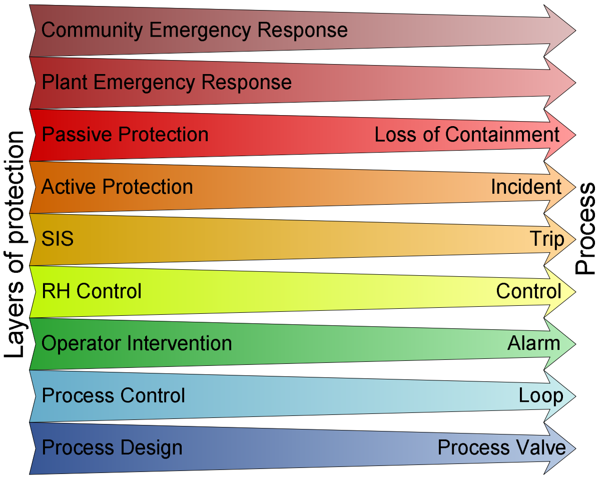


Figure 2 - Layers of protection and impact on process

Risk assessment procedure (detailed in Figure 3) is the first process in the risk management methodology to determine the extent of the potential threat and the risk associated with a system [8]. The procedure includes 5 important steps: (1) identify all possible hazard situations and (2) risks, (3) evaluation of the existing tools and strategies, (4) implementation of new ones if needed, and (5) the continuous monitor and evaluation of the behavior of the process.

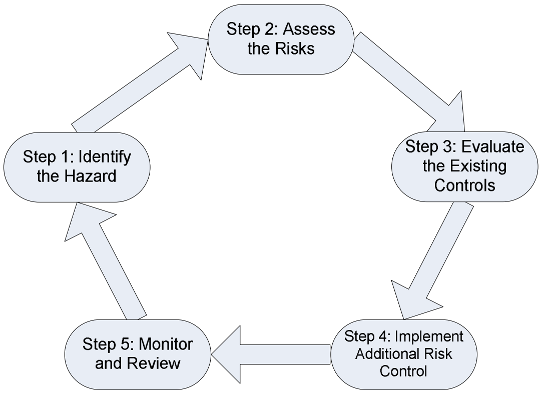

Step 2: Assess the Risks
Step 1: Identify the Hazard
Step 3: Evaluate the Existing Controls
Step 5: Monitor and Review
Step 4: Implement Additional Risk Control

Figure 3 - Risk assessment procedure

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. Unfortunately, all the additional protection measures mentioned above can only help to safely shut down the plant.

We have proposed designed and implement a new level of decision: RH Control (Figure 4) to keep the plant running.

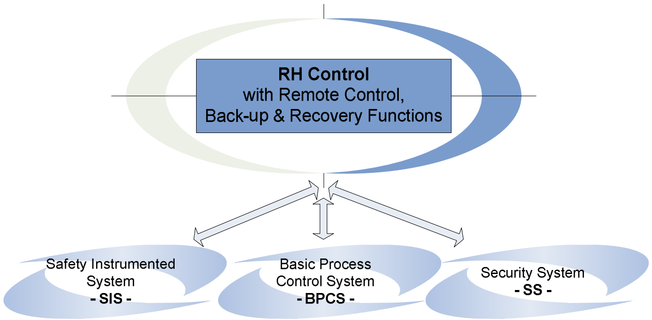

RH Control
with Remote Control,
Back-up & Recovery Functions
Safety Instrumented System - SIS -
Basic Process Control System - BPCS -
Security System - SS -

Figure 4 – System architecture

Better automation is a key aspect for improving industrial competitiveness [9]. Intelligent automation, at management levels in particular can play a major role regarding this aspect. The purpose of RH Control is to help with this improvement by building a new architecture and a distributed, generic decision support software system for near critical situation management in continuous process industries. In particular, assistance in terms of diagnosis and elaborating solutions is provided (directly to the plant's control system and/or to the staff) when certain situations are detected, i.e. situations suitable to be corrected, prevented or enhanced.

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, user interface 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. The complexity of the control mechanism increases for the 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 according to the plant objectives.

These applications include the following functionalities at different control layers:

- Strategies: Management of global objectives of the plant and their interrelation (management of maintenance operations, incident prevention, RH control, assessment of production costs in real time, loop tuning optimization, set-point 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 main challenges at the beginning of a system configuration are: software architecture and reusability.

A. *Reusability*

The technical approach tries to provide reusability in the broadest sense using functional blocks. Object oriented technology can be one of the cornerstones of this approach [10]. Reusability can be achieved for any stage in the life cycle: from defining 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 comply with the new requirements with little effort. The concepts of function block–based development and integration middleware 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 real-time integration. This software, based on function block standard, will incorporate extensions to make possible for its use in real-time applications. This facilitates the easy reuse of components and even of the global application architecture because run-time components can be easily changed without affecting the behavior of others.

B. *Software architecture*

The software architecture is based on the Service–oriented architecture concept (SOA) [11]. In most applications, the infrastructure and the environment are very important security-related issues and it gets even more important if a SOA-based on Web Services has been chosen.

For this purpose, asymmetric cryptography will be used, implying a pair of two keys: public key and private key.

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

- From the user's point of view: the implementation addresses 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 availability, 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 the OPC standard and function blocks, will allow the construction of distributed intelligent control systems on top of the existing ones, with back-up functions.

IV. Simulation - the key for an effective RH Control

Future applications of simulation technology applied to process control will be driven by the advancing simulator capabilities. Many of them are the direct result of computing technology applied to certain activities with high return on investment: concurrent engineering, process fault detection, self testing capabilities for hardware and internet retrievable simulation models and tools.

- Advanced networking

Advances in network technology are allowing for faster data sharing between computers, parallel processing for simulating more complex models and linking the simulator with the real process. Three types of network interfacing applicable to simulation can be used:

- Bus adapter and shared memory
- Data broadcast network
- Internet

- Intelligent I/O

Applied Dynamics International (ADI) 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 the development of digital hardware-in-the-loop simulations that allow simulation frame-times lower than 10 microseconds.

Simulation technology

There are many approaches to achieve good results in time. We will briefly present the most important of them.

- Integration algorithms

Integration algorithms are used to solve a function in the time domain, given the differential equation of the variable of interest. Runge-Kutta 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-Kutta [12].

- 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 the state the process is in and by the events that cause a transition from one state to another [13]. 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. Figure 5 shows the classical states: start-up, nominal and shut-down but the RH state is added in order to maintain the system under control.

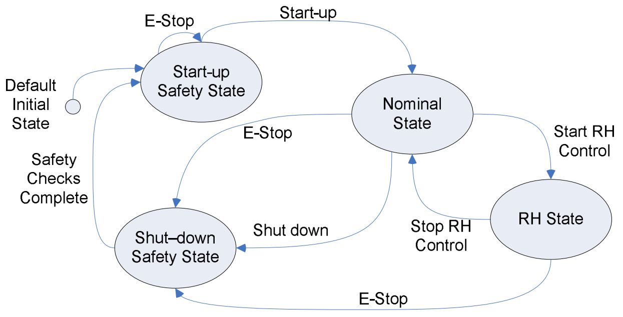


Figure 5 - Operational states

The user / resource analysis queuing system can be described as a collection of resources and the tasks using these resources [14]. The modeling tools allow resources to be allocated to tasks according to several prioritization strategies such as first-come-first-served, infinite servers, last-come-first-served, processor-sharing. System parameters such as response times, rate of use, 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 later to implement the appropriate Distributed Control System (DCS) or Programmable Logic Controller (PLC) and Supervisory Control And Data Acquisition (SCADA) strategies to run on site or remote.

- System Identification

Data handling and processing power available today enables not only standard on-line identification techniques but also sophisticated, empirical model development methods that in the past were not feasible. Tools are available for today's simulators to help gather perturbation data from the process and develop empirical models that sometimes boast more fidelity than classical models. Although system identification theory has been around for a long time, only recently these theoretical tools become practicable because of the large amount of data processing required.

V. Emerging Technologies

Emerging technologies analyzed helped us to establish the most important of them to be used in our project.

a) Concurrent Engineering (CE)

An activity that requires a high degree of effort from a design company, but not without a rewarding return on investment is CE. This design paradigm is based upon the principle that the process and the associated control strategy are designed in parallel before the process is built. Trade-off analysis is performed in advance, in order to prevent conflicting criteria of the two designs. Dynamic process simulators are combined with traditional static simulators to assess transient behavior and controllability of the process.

The CE approach is based on the following key elements:

- the system engineering process;
- a multidisciplinary team (process, control, safety and security, management, accounting, inventory)
- a collaborative platform, control environment and data & information distribution
- supporting tools and facilities.

The approach can evolve into an Integrated System Development based on cross functional System / Process Teams for all systems and services, and a System Engineering and Team to cover the system issues, performances, balance requirements.

By applying CE to plant design and installation, non-value added activities both in the upstream and downstream activities of the plant can be eliminated at the early stage of the design process, plant, operations and control. Plant wide controllability analysis in the conceptual design stage is an issue that has been raised by process industry [15].

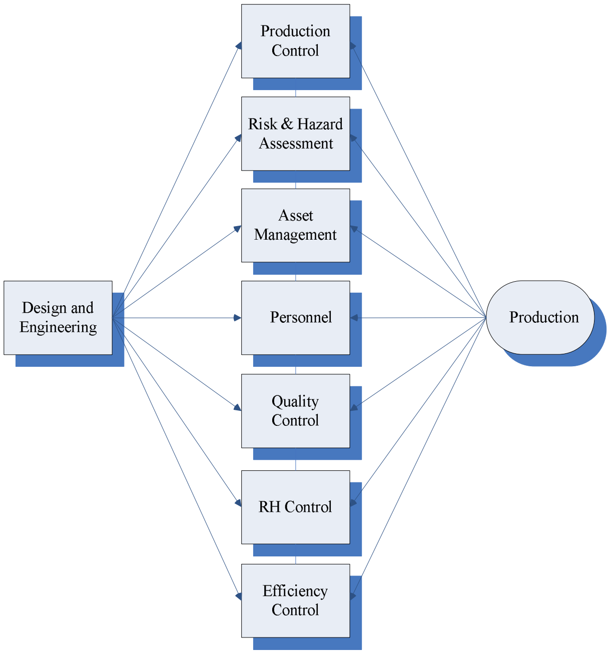


Figure 6 - Concurrent engineering apply to process control

The role of CE is obvious since it reflects that opportunities exist even at the conceptual design stage, to optimize the downstream operations including the capabilities to run the process instead of risks and hazards. This is against the conventional approach of the control as an add-on to process design after the flow sheet structure has already been determined.

There are a number of tools available for the design of process using CE including: simulation, process modeling, on – line identification, asset assessment, risk and hazard analysis. Including all this we can have a conceptual framework for the implementation of CE in process control.

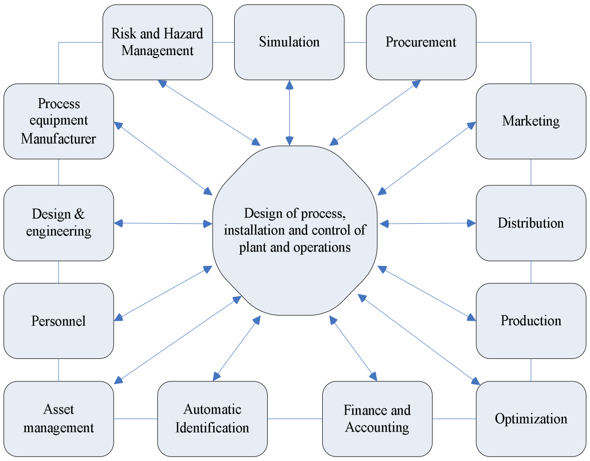


Figure 7 – Conceptual framework

b) Controller Testing

Using simulators to test control systems is an increasing trend in almost every industry. Simulator-based testing takes the control software development from the project critical path. Tests using simulators can be more comprehensive than a test using the actual process because the normal safety or process operational limits are not a concern, so the virtual test can exceed 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 architecture than in the past when individual wiring terminations were required.

c) 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 Figure 8, a difference between the two indicates a fault. Advanced fault-detection algorithms will lead the RH control or the supervisory engineers to the appropriate action.

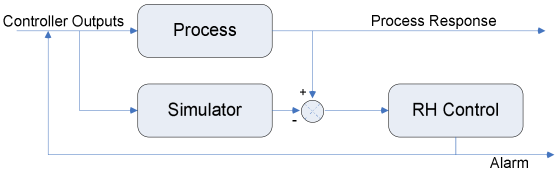


Figure 8 - Online diagnostics

d) Internet Applications

This technology offers today the capability to interconnect the on-site system with a remote control center (PH center) and to perform simulation, on-line identification [16], RH strategies, on-line tests and training, back-up and restoration. Operating remote from the site, the Process Help Center will host not only a copy of the process control system but the strategy and algorithms to fulfill the safety task and to keep the process running even in RH conditions.

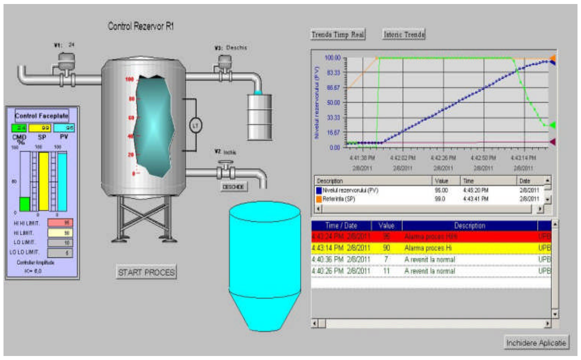
VI. RESULTS

The new approach in process control system engineering, based on new algorithms, scalable and modular architectures and platforms, RH control, is industry independent. The capability of the systems to model and implement the 4 states, start-up, nominal, RH, shut-down, having 4 different strategies and the capability to change the state according to the functional parameters can be taken in consideration by CE. The diagnosis system, hosted remotely, will be continuously improved by gathering knowledge from various applications, based on identified problems, the solutions offered and their impact on the plant performance. The correlation factor between these different applications will influence future decisions. This way, the required period of time for solving a problem will be minimized, as well as the time that a plant needs to be shut down because of the instrumentation process control strategy.

Some of the expected results are an integrated exploitation of a collection of heterogeneous technologies for the prevention of anomalous situations related to the safety of an industrial complex and determining 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 separate ways. Another advantage arises from being able to automatically take into account 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 to develop and implement the hierarchically superior level for safety and security problems. The work carried out in the project establishes the baselines for a new architecture of process control taking into consideration the remote operation.



Description	Value	Time	Date
Nivelul rezervorului (PV)	95.00	4:45:20 PM	2/8/2011
Referinta (SP)	99.0	4:43:41 PM	2/8/2011

Time / Date	Value	Description	
4:43:24 PM 2/8/2011	95	Alarma proces HiHi	UPB
4:43:14 PM 2/8/2011	90	Alarma proces Hi	UPB
4:40:36 PM 2/8/2011	7	A revenit la normal	UPB
4:40:26 PM 2/8/2011	11	A revenit la normal	UPB

Figure 9 - The simulated process

In the meantime, the results achieved underlay the feasibility of the idea. This statement is based on two reasons:

- Two demo-applications have been designed according to real plant requirements with a large involvement of plant staff. At present, two applications are installed and under operation after a period of user validation and evaluation:

- a simulator for a simple process - controlling the level of liquid in a tank – Figure 9.

- a Building Management System (BMS) designed for a supermarket – Figure 10.

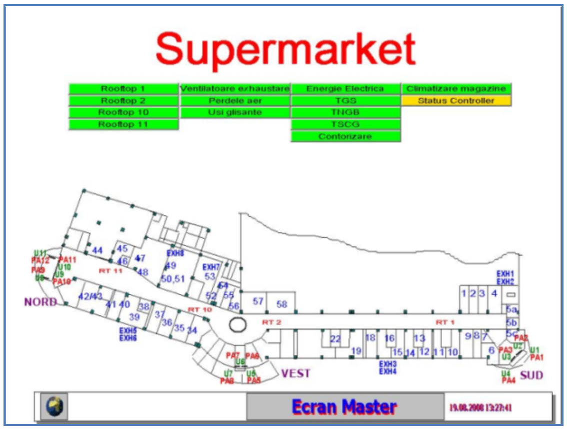


Figure 10 - Supermarket BMS – remote connection main screen

Also, we are currently working on including a new connection to the PH Center, a DCS control system (Experion - Honeywell) from LPG terminal, Midia, Navodari (Figure 11).

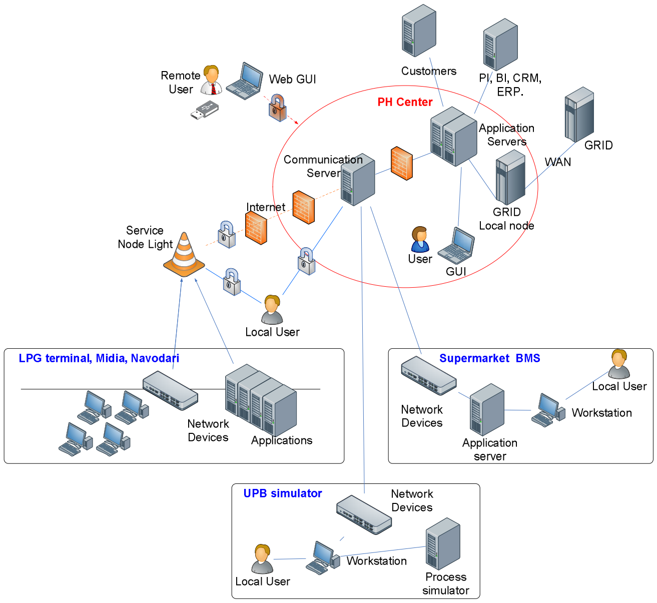


Figure 11 – PH Center connected to DCS

- The three generic products constructed within the project are truly reusable and can be exploitable components of other implementations.

This approach demonstrates that advanced control technology can be modularized, deployed and integrated with legacy control systems, progressing effectively towards complete automatic operation.

VII. Conclusions

In the past, SIS were strictly separated from the BPCS, mainly to segregate the safety and control functions and to have higher availability and reliability. Lately, many "integrated" control systems were deployed that have both BPCS and SIS systems in the same package

Hazard identification, risk assessment and control are on-going processes that involve a critical sequence of information gathering and also the application of a decision-making process. They 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 exist for preventing and mitigating a major accident (control measures). The state of the art has no real and integrated solution. The work done by authors and the team has proposed:

- ✓ The new concept: Risk and Hazard Control;
- ✓ A new system architecture of process control;
- ✓ The guidelines and advantage of using CE to the design of process control system.

REFERENCES

[1] Gheorghe Florea, Luiza Ocheana, Radu Dobrescu, and Dan Popescu - Emerging Technologies - the base for the next goal of Process Control - Risk and Hazard Control, Proceedings of WSEAS International Conference, 2011, pp. 227 – 232.

[2] American Institute of Chemical Engineers - Guidelines for Safe and Reliable Instrumented Protective Systems, 2007.

[3] Asish Ghosh and Dave Woll - Business Issues Driving Safety System Integration, ARC White Paper, 2006.

[4] Ged Farnaby - Protect the plant. Leading edge trends in process control safety, InTech, June 2005.

[5] Wes Iversen - The Great Safety Debate, Automation World april 2007, pp. 30.

[6] David Hatch and Todd Stauffer - Operators on alert. Operator response, alarm standards, protection layers keys to safe plants. InTech, Cover Story, September 2009.

[7] Merry Spooner and Trevor MacDougall - Safety Instrumented Systems can they be integrated but separate?, ABB White Paper, 2011.

[8] Gary Stoneburner, Alice Goguen, and Alexis Feringa - Risk Management Guide for Information Technology Systems. Recommendations of the National Institute for Standards and Technology, 2002.

[9] Ricardo Sanz, Miguel Segarra, Angel de Antonio, and Idoia Alarcon - Plantwide Risk Management Using Distributed Objects, Proceedings of IFAC Symposium on Fault Detection, Supervision and Safety for Technical Processes 2, 2000, pp. 14 – 16.

[10] Michael Guttman and Jason R. Matthews - The Object Revolution, Wiley, New York, 1995.

[11] Stefan-Helmut Leitner and Wolfgang Mahnke. OPC UA – Service – oriented Architecture for Industrial Applications. ABB White Paper, 2006.

[12] Ruppel Francis and Wysor Wes - Mighty microprocessors boost process simulation, InTech, September 1997.

[13] David Harel - Statecharts: A Visual Formalism for Complex Systems, Science of Computer Programming vol.8, 1987, pp. 231 – 274.

[14] Christos Cassandras - Discrete Events Systems: Modeling and Performing Analysis, IFAC Best Control Engineering Textbook, 1999.

[15] Angappa Gunasekaran - Concurrent engineering: a competitive strategy for process industries, Journal of the Operational Research Society, Volume: 49, 1998, pp. 758-775.

[16] Mauro Coccoli and Antonio Boccalatte - Future Directions of Internet-based Control Systems, Journal of Computing and Information Technology, 2002, pp. 115–124.