Risk and Hazard control hosted on Cloud

G. Florea, R. Dobrescu

***Abstract*—** 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 towards full control systems and the requirement specifications for Safety Instrumented Systems (SIS) forms the central network for the process risk and hazard assessment to be carried out. Process Control has evolved very much in the last years. Plants become more complex, they require more efficiency and reduced costs while maintaining the product quality. Advanced process control appeared to be the most effective technology to realize these objectives, but it is not enough anymore. 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. Risk and hazard control is for sure one modern approach to keep plant running even under big perturbations or uncertainty. Emerging technologies used for design and implementation; modeling, simulation, concurrent engineering, on line diagnosis, merger techniques needs big computational capabilities that Cloud can offer.

***Keywords*—** risk and hazard control, levels of protection, concurrent engineering, algorithms for hazard and risk management, generic algorithm representation.

I. Introduction

Process Control has evolved very much in the last years. Plants become more complex, they require more efficiency and reduced costs while maintaining the product quality. Advanced process control appeared to be the most effective technology to realize these objectives, but it is not enough anymore.

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 [1]. The solution is to use multiple layers of protection. The current architecture of the process control systems uses three levels:

- ¬ Basic Process Control System Layer (BPCS);
- ¬ Operator Intervention Layer (OI);
- ¬ Emergency Shut Down system Layer (ESD);

G. Florea is with Society of Syste,s Engineering SA, Romania. (corresponding author to provide phone: +40 212525577; fax: +40 212525694; e-mail: gelu.florea@sis.ro).

R. Dobrescu is with the University Politehnica of Bucharest, Romania (e-mail: radu.dobrescu@sis.ro).

BPCS represents the lowest layer of protection and is responsible for the operation of the plant in normal conditions. If it fails or is not capable of maintaining control, then, the second layer, the Operator Intervention (OI) Layer attempts to solve the problem. If the operator also cannot maintain control within the requested limits, then the ESD Layer must attempt to bring the plant in a safe condition, usually meaning turning off the process. If ESD also fails in restoring to the normal operation, the hazard occurs.

The operators in the control room are constantly monitoring the plant but their intervention is limited to reacting to the hazardous situations that may occur. The operator reacts to the problem that appears in order to correct it and to restore the plant in normal operating conditions.

Therefore, a new level of protection is needed, to take action between OI and ESD layers, having the main function to prevent hazardous situations in order to avoid the ESD intervention [2]. Fig. 1 shows the position of the new layer in the current architecture.

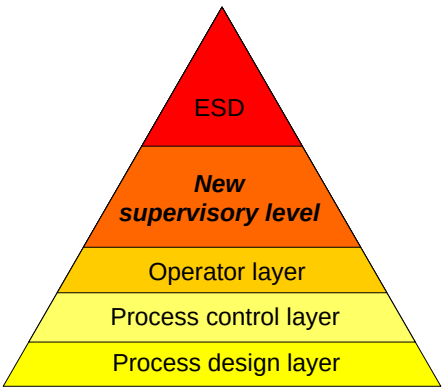

Fig. 1. Layers of protection

Poor performance costs money in lost production and plant damage and weakens a very important line of defense against hazards to people [3]. Studies show that the start-up of a refinery for example is estimated at two million EURO, meaning huge costs for the owner. The need of specialized and experienced engineers in the control room of a plant, especially when a hazard or an abnormal situation appears is obvious. These engineers should know how to intervene in the plant functioning so that they can prevent failures and, most important, to prevent the ESD controller action that will shut down the plant and cause great money loss. Usually, the operator cannot face these situations.

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].

Risk assessment means that a quantitative value is assigned to a task, action, or event.

Types of Risk:

Total Risk - The sum of identified and unidentified risks.

Identified Risk - Risk that has been determined through various analysis techniques. The first task of system safety is to identify, within practical limitations, all possible risks.

Unidentified Risk - Risk not yet identified. Some unidentified risks are subsequently identified when a mishap occurs. Some risk is never known.

Unacceptable Risk - Risk that cannot be tolerated by the managing activity. It is a subset of identified risk that must be eliminated or controlled.

Acceptable Risk - Acceptable risk is the part of identified risk that is allowed to persist without further engineering or management action. Making this decision is a difficult yet necessary responsibility of the managing activity. This decision is made with full knowledge that it is the user who is exposed to this risk.

Residual Risk - Residual risk is the risk remaining after system safety efforts have been fully employed. It is not necessarily the same as acceptable risk. Residual risk is the sum of acceptable risk and unidentified risk. This is the total risk passed on to the user [5].

Using a risk assessment matrix helps differentiate between low-risk and high-risk:

Table 1 - Risk assessment matrix

Severity			
Catastrophic	Critical	Marginal	Negligible
High	High	Serious	Medium
High	Serious	Medium	Low
Serious	Medium	Medium	Low
Medium	Medium	Medium	Low

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. The design of the Control System architecture must take into consideration the result of risk and assessment analysis.

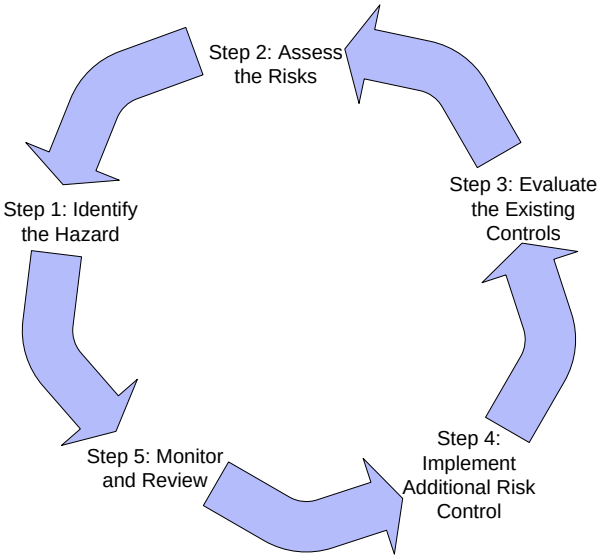

Fig 2 Risk and assessment procedure

The extended risk assessment procedure, consisting in 10 steps is described in [6]:

- Step 1 – 5 – deal with current situation, threat, vulnerability and likelihood identification, current and planned controls;
- Step 6 – deals with the impact resulting from a successful threat exercise of a vulnerability;
- Step 7 – assess the level of risk to the system;
- Step 8 – implement controls that could mitigate or eliminate the identified risks;
- Step 9 – once the risk assessment has been completed, the results should be documented in an official report.
- Step 10 – monitoring the process behaviour.

Today, integrating safety and control has become a cost effective way for manufacturers that could not justify a separate SIS in the past. As a process manufacturer, you need to perform rigorous hazard and risk analysis based on IEC 61511 or ANSI/ISA-84.00.01 safety standards to decide on the right level of protection required for your manufacturing plants. You may follow that by selecting an SIS that provides close integration with the software tools of your BPCS while still providing the required degree of separation.

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.

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 [7]. 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 behaviour.

The industry has heavily invested (and still investing) in both ACS and also Management Information Systems (MIS) like MES, R/PE, ERP, SCM or SSM (OMG Manufacturing Domain Task Force, 1998). Information systems in plants are hierarchically structured in order to deal with the large collection of functional components. Complex software systems tend to be unpredictable and this is not acceptable in some types of plants. Heterogeneous environments are the common infrastructure for advanced control systems. Almost everybody recognizes the need for better and more extensive solutions for tackling problems belonging to the tactical and strategic layers of control. They also recognize the need for vertical integration of the layers (in terms of flow of information. In the mean time the safety and security are major problems in the real time world.

The introduction of chaos control to solve uncertainties is another approach to be taken into consideration Instead of conventional chaos control that follow to reach single control objective at each time and another control objective can be realized at another time a new research direction of control chaos -- multi-objective control (MOC) [8] is naturally raised and needed in practical applications, such as in communication engineering, biological systems, social networks and so on since these systems have more than one unstable equilibrium and infinite unstable periods or time-space patterns.

Based on our experience the only performing approach is toward a totally integrated system. The three important levels cover the process, the management and the business control but we aid the new one; RH Control.

II. 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:

  - Bus adapter and shared memory
  - Data broadcast network
  - 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 allow 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.

- Fuzzy logic

Fuzzy logic has many applications in many fields, from control theory to artificial intelligence and for sure is an approach that can give many solutions to implement risk and hazard control. Typical examples include control software for monitoring safety-critical and risky industrial applications. In [9] the authors focuses on the problem of decreasing the response time of fuzzy rule-based systems analyzing some algorithms for off-line computing of the compiled fuzzy models, for the Variable Linking Network (VLN).

- 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 [10]. The use of state-transition diagrams allows the behaviour 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 (RH state) to keep process under control.

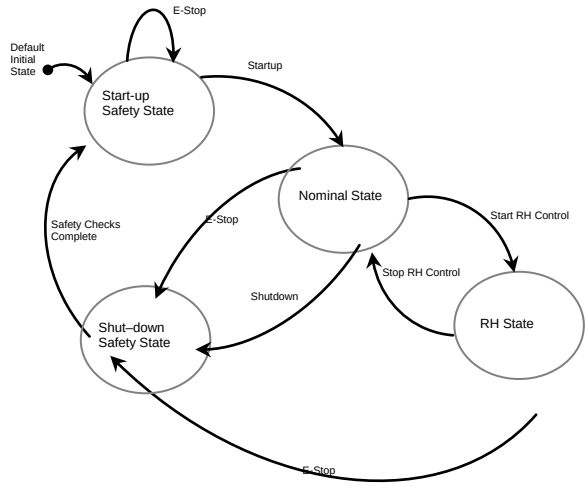

Fig. 3 - Operational states

User/resource analyzes tools queuing systems that can be characterized by a collection of resources and tasks using these resources [11]. The modelling tools allow resources to service tasks in many priorities such as firs-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 whole 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 [12, 13]. 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 to assess transient behaviour and controllability of the process.

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. 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 [14]) offers today the capability to interconnect the on-site system with a remote control center [15], PH Center 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.

More information's about emerging technologies can be found in [16].

III. 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 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. 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.

These applications 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 restore the 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. 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.

In [17] RH Control, the next level of decision and intervention we have proposed the System architecture incorporating Risk and Hazard control.

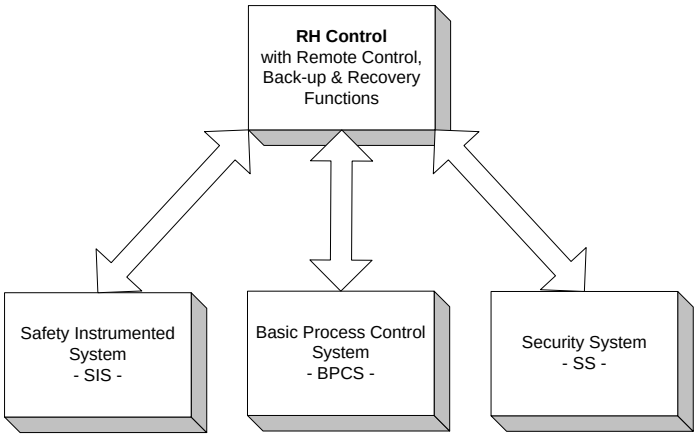

Fig 4 Functional Architecture incorporating Risk and hazard control

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.

The system as described will be able to automatically diagnose and control a plant preventing the occurrence of hazardous situations.

The system architecture presented in fig 5 consists in connecting different control systems located in different plants to the remote center using the Internet, creating a "system of systems".

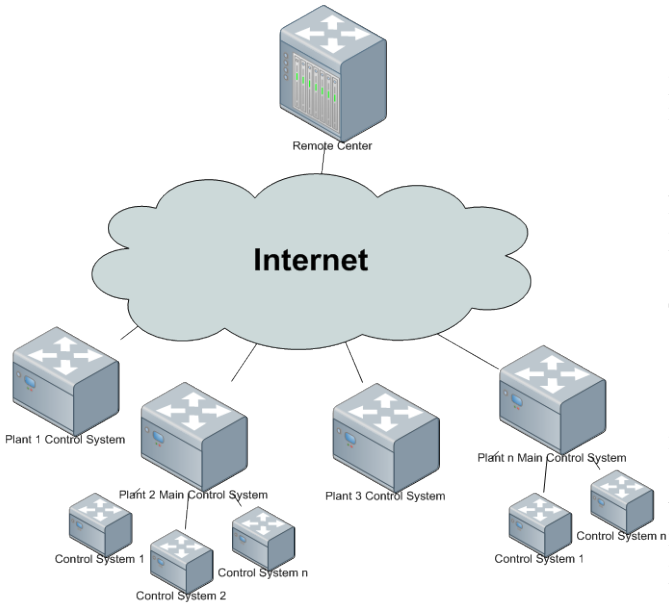

Fig. 5. System Architecture

The communication infrastructure between client's BPCS and the remote supervisory system will be done through Internet connection. The system will work in parallel with the existing systems but will be independent of them and will use a complex library of open standard function blocks.

The system will continuously monitor the overall state of the process in order to identify possible risks but will act only when necessary. Remote assistance of the production system is an important component for any company that wants high financial performance. The remote center will provide predictive control, diagnose and intervention based on complex algorithms.

During the past years, significant progress has been made with regards to the automated control of large – scale industrial plants. The motivation consists in the fact that the complexity level of such plants is gradually increasing and thus the control requirements diversify. It is no longer sufficient for the automated control system to ensure that the plant operating parameters are located within their normal admissible ranges dictated by the plant operating regime, but it becomes increasingly obvious that more complex control solutions are needed in order to address the problematic of large – scale distributed process control. Until now, most of the risk analysis platforms developed were based on offline data computing and were destined to the plant design phase and not to on – line monitoring. By performing real – time fault detection and diagnosis and event tree analysis in addition to the classical risk computing algorithms, the hazard analysis process can be integrated by the supervisor functions. In addition, fault – tolerant control algorithms concurred with sequential control strategies contribute to successful hazard prevention.

The challenges become even greater in the case of distributed systems and networks, such as large industrial platforms which, by their nature, require control and estimation in a distributed setting. Requirements and specifications can also be widely variable between safety critical and socially/economically significant systems. Control, communications and computation need to be synergistically combined [18] through a 'universal formalism' and novel paradigms that combine logical operations (symbolic reasoning and decision making) with analytical constructs (mathematical algorithms) and continuous quantities (throughput, subsystem interconnections), in order to handle heterogeneity, a synchronicity, real time functionality, properties that typically characterize distributed systems/networks.

The main motivation and the driving force for implementing a common framework for integrated process control, safety and security systems 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 [19] 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.

Efficient and sustainable progress both in the process control environment and also in the research and development areas can be achieved with the correct tools for sharing results in the algorithms development, integrated with the feedback from the industrial implementation, formulating problems based on real life cases and finding solutions together. That is why there is a strong need for a common library and a generic algorithm representation methodology that will ease the communication and sharing of information [20].

Sharing information about the latest research algorithms can build stronger relationships between the academic and industrial research centers, and more important will help integrate the latest algorithms in the process functioning, closing the gap between mathematical development and real-time implementation.

The architecture of the library of complex poly-functional process control algorithms is presented in a generic representation so that they could be adapted to different classes of practical systems, with the associated program performances and process interface capabilities. The library will be used by the remote control system in order to control, optimize and prevent hazard situations.

Based on the diversity of the processes in which the algorithms can be used, we expect a large variety of mathematical functions for signal processing, system identification, controller design, strategies for hazard and risk management, fault analysis and assessment. A complex

architecture that will provide the support for the project development is presented in 5.

This architecture includes all the functional components that are necessary for the implementation. We considered the possibility of viewing and saving algorithms, of adding different characteristics for them in order to have an idea regarding the processes where they can be used, adding new algorithms after their testing and validation and also their optimization and configuration on specific applications. The algorithms will be provided as files containing the definition of the function block. This function block will be represented based on a methodology and an open standard so that it can be included in the existing control logic of a plant.

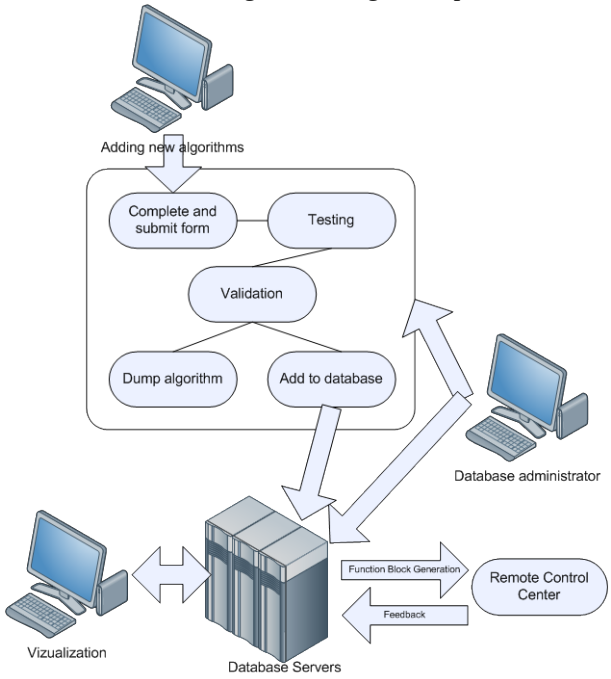

Fig. 6. Cloud based library Architecture

In order to have access to these algorithms, we will develop an application that will connect to a database for solving the user requests. The application will allow access to three types of users:

- unregistered users, that will have visualization rights, they will be able to download algorithms and to add comments
- registered users, that will be able to contribute to the library development by adding new algorithms and will be able to adjust different algorithms so that they can suite specific applications
- System administrators that will manage the database by validating the operations of adding or deleting algorithms, as well as the library application functional management.

The architecture shows how different users will interact with the system, how new algorithms can be added, the selection process and how they can be integrated in the industrial environment.

For the data representation we needed to find an open standard that will provide the capability of developing reusable function blocks that could be integrated in the control logic of an automation system. For this matter we decided that a common way of representation is using the IEC 61131 standards and its improved version IEC 61499. These standards provide support for developing function blocks on several design levels, similar to object oriented programming. Based on predefined basic functions, one can develop a function with specific inputs and outputs that can later be used inside another function block.

The main PLC manufacturers (like Allen Bradley, Siemens, HIMA, GeFanuc, Mitsubishi etc.) use for logic programming software tools that are compatible with the IEC 61131 standard. The IEC 61499 is an improvement that adds new functionalities specific for distributed systems which will allow including them in a larger variety of applications. Also, in the last years there is a great interest in the large scale development and implementation of applications based on this standard. The most relevant work was conducted by the O3neida consortium and the Rockwell Automation company. They also developed the first commercial application that allows developing control strategies based on the two function block standards.

The adaptability of this representation to different applications depends on the type of the application where it is needed. For example, for the design phase one can use a top down approach and start from an overall view and then develop individual components so that in the end the connection to the hardware components is defined. The application modeling is done on its specific components. A function block can be seen as a software component that can be used independently and that has a fix set of interfaces that can be used in a specific context. The interaction with the physical inputs and outputs is made based on certain events.

Another aspect that needed to be considered is to ease the collaboration between scientific researchers, that are usually familiar with software tools like Matlab, and system integrators, that can develop control strategies using the above mentioned standards. For this matter, Matlab has a specific component called “Simulink PLC coder” that allows converting algorithms to a function block representation based on IEC 61311. Unfortunately, DCS manufacturers usually have their own programming environment that is not based on standardized regulations. In this case, a solution can be implementing the algorithms as executable files that can be interfaced with different control system parameters based on OLE for Process Control - OPC client server architecture or using a direct database interface.

An interesting aspect refers to the way data will be organized inside the database. Database management raises problems regarding algorithm storage mechanisms, their indexing that will be used in item search, their associated characteristics that will define the processes and applications for which an algorithm is suitable and replication problems in the idea that two slightly different algorithms may accomplish the same function in a different way. These problems need to be considered when developing the database structure and the mechanisms for adding and testing the corresponding

algorithms. There is the need to particularize a certain algorithm to the special needs of an application. That means that adaptability and reusability play important roles in correct algorithms development. A support for that matter is offered by the object databases. When database capabilities are combined with object programming language capabilities, the result is an object database management system (ODBMS). An ODBMS represents database items as programming language objects in one or more object programming languages. This way, the results of a database interrogation can be instances of an algorithm, particularized for a specific application. Also there are software products, like Objectivity DB, that offers support for this kind of applications. For the moment there are little tools that allow the interaction with this kind of databases and also their documenting is poor. This means we will have to find solutions for the representation of function blocks in object-oriented format.

The library components will need to be integrated directly in the control logic of a control system. The problem is that not all manufacturers provide support for using functions blocks according to the IEC 61311 or 61499 standards (Gerber et. All, 2007). Also, the current programming environments of specific manufacturers (like for example STEP7 for Siemens controllers) don't allow importing function locks from other environments, even if the use the same representation standard. This is why we will need to use a programming language that is independent of the manufacturer, like ISaGRAF, for implementing the function block in the control strategy.

For the manufacturers that don't provide support for the IEC 61311 or 61499 standards we will need to develop a standard plug-in generic interface for process connection. At the moment, the possibility of developing a generic interface that will allow integrating the algorithm no matter the type of the automation controller has two possible solutions: using the OPC standard or using web services.

OPC is an industrial standard primarily based on the Microsoft Distributed Component Object Model (DCOM) interface of the Remote Procedure Call (RPC) service [21]. The OPC standard provides a unified server-client interface solution that was accepted by most PLC and DCS manufacturers. It was developed with the initial purpose of allowing the interconnectivity between equipment from different manufacturers. At the moment most manufacturers have developed OPC Servers that allow connecting and modifying process variables without the need of implementing a specific driver for the automation system.

In other words, this solution will allow adding OPC data access functions to the developed algorithms so that they can be compiled and used in an executable stand-alone application. This application will run in parallel with the existing control logic of the process, providing unexpected situation management solutions.[22]

We chose for representation the most common control algorithm: the PID regulatory. The PID algorithm is the most popular feedback controller used within the process industries because of its simple structure and robust behavior. The transfer function for the PID algorithm is:

$$C(S) = K_p + K_i * \frac{1}{S} + K_d * S \qquad (1)$$

Where Kp, Ki and Kd are respectively the proportional, integral and derivative parameters of the PID controller. The value of the control action is calculated based on the error between the process value and the desired set-point.

An example on how to use the IEC 61499 function blocks to represent the PID algorithm is shown in "Modeling control systems using IEC 61499: applying function blocks to distributed systems" [23]. The algorithm can be represented as a composite function block as illustrated in Fig. . It uses the PID_CALC, DERIVATIVE_REAL and INTEGRAL_REAL function blocks to calculate the output XOUT based on the process value PV, the set-point SP and the PID parameters Kp, Ki and Td. MODE is used to select the auto mode (MODE = 1) where the output is calculated based on previous errors and PID parameter values, or the manual mode (MODE = 0) where XOUT sends the value received on the MANOUT input. INIT and RUN inputs control the event flow. When the INIT event is triggered, PID executes the initialization algorithms of the three function blocks: first the PID_CALC function block, then DERIVATIVE_REAL and last the INTEGRAL_REAL. The RUN event triggers the execution of the PRE algorithm in the PID_CALC function block. It calculates the value of the error between set-point and process value and passes it through the ERROR variable to the DERIVATIVE_REAL and the INTEGRAL_REAL function blocks. After the derivative and the integral components are calculated the POST event is triggered. It runs the algorithm that calculates one step of the PID algorithm based on the values of the KP, TD and KI parameters and outputs the control command.

The algorithm can be represented graphically using the FBEditor application [24] and can be stored in the database in XML format. The application also provides support for function block testing by entering different values as inputs. This way any developer that wants to add algorithms to the library has a free toll for the development and testing.

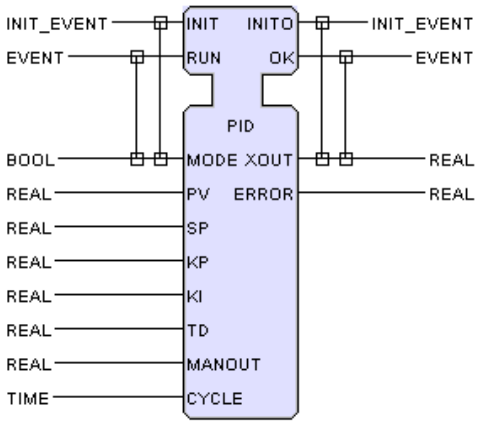

Fig. 7. The PID composite function block

The algorithm can be represented graphically using the FBEditor application and can be stored in the database in

XML format. The application also provides support for function block testing by entering different values as inputs. This way any developer that wants to add algorithms to the library has a free toll for the development and testing.

IV. CONCLUSIONS

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).

The work carried out by the team has direct deliverables:

- the new paradigm - Risk and Hazard control
- a novel architecture
- library of algorithms and strategies on the cloud
- tools and methods to be used to develop such systems

Future work will address each separate component in terms of data organization and manipulation, types of algorithms for managing unexpected situations and their representation, determining how much a specific algorithm depends on the type of process in which it will be used, algorithm implementation and testing of process integration.
The final target is to achieve a scalable and flexible system, able to integrate different types of processes, to provide predictive control, diagnose and intervention functions, based on a standard function block based library.

REFERENCES

[1] D. Hatch, T. Stauffer, "Operators on alert. Alarm standards, protection layers, HMI keys to keep plants safe", InTech, 2009.

[2] L. Ocheană, D. Popescu, G. Florea (2011). Remote diagnosis and intervention – a new layer of protection for industrial processes. Proceedings of 18th International Conference on Control Systems and Computer Science.

[3] ML. Bransby, J. Jenkinson (1998). The Management of alarm systems, *HSE Contract Research Report 166/1998, ISBN 07176 15154, 1998*.

[4] M. Guttman, J.R. Matthews, "The Object Revolution", Wiley, New York, 1995.

[5] Aviation Glossary - http://aviationglossary.com/ aviation-safety-terms/risk/

[6] G. Florea, R. Dobrescu, "Risk and Hazard Control the new process control paradigm"- Systems, Control, Signal Processing and Informatics II Prague

[7] M.Gutman, J.R. Mattews, "The Object Revolution", Wiley, New York, 1995

[8]J.-Q. Fang, "A new research direction of chaos control: multi-objective control and its application" CONTROL'09 Proceedings of the 5th WSEAS international conference on Dynamical systems and control, 2009

[9]V. Mazilescu, C. Nistor, D. Sarpe, "A solution for decreasing the response time of knowledge based systems" Proceedings of the 9th WSEAS international conference on Applied informatics and communications

[10] D. Harel, "Statecharts: A Visual Formalism for Complex Systems", *Science of Computer Programming vol.8*, 1987, pp 231 – 274.

[11] C. Cassandras, "Discrete Events Systems: Modeling and Performing Analysis", *IFAC Best Control Engineering Textbook*, 1999.

[12] J. Estubier, S. Garcia, "Concurrent Engineering support in Software Engineering", 2006.

[13] G. Florea, L. Ocheana, "PH Center the result of concurrent engineering applied to implement Risk & Hazard Control" ESoCE-Net Rome

[14] FP6 Project Consortium - NEOXITE – Next Generation Open Control System Internet Ready, 2004.

[15] G. Florea, L. Ocheana - "Concurrent Engineering used to Implement Risk & Hazard Control", The Third International Conference on Advances in System Testing and Validation Lifecycle (VALID 2011), ISBN: 978-1-61208-168-7 2011

[16] G. Florea, L. Ocheana, D. Popescu, O. Rohat, "Emerging Technologies – the base for the next goal of Process Control – Risk and Hazard Control", 11th WSEAS International Conference on Systems Theory and Scientific Computation ISTASC '11, 2011

[17] G. Florea, L. Ocheana "RH Control, the next level of decision and intervention", - REV2011 - Remote Engineering & Virtual Instrumentation 2011

[18] L. Valavani, "Control and estimation theory: current trends, new challenges, & directions for the future"Proceedings of the 13th WSEAS international conference on Systems

[19] G. Florea, R. Dobrescu, "Architecture framework for control strategies under risk and hazard conditions-CONTROL STRATEG" Systems, Control, Signal Processing and Informatics II Prague

[20] L. Ocheană, O. Rohat, D. Popescu, G. Florea "Library of Reusable Algorithms for Internet-Based Diagnose and Control System", - 14th IFAC Symposium on Information Control Problems in Manufacturing - INCOM 2012

[21] E. Byres, J. Carter, M. Franz, B. Henning, J. Karsch, D. Peterson (2007). Focus on OPC. *ISA InTech Articles*, New York, London.

[22] G. Florea, L. Ocheanã, "Towards Total Integration Based on OPC Standards", - 14th IFAC Symposium on Information Control Problems in Manufacturing - INCOM 2012

[23] R. W. Lewis (2001). Modelling control systems using IEC 61499: applying function blocks to distributed systems. *IET, 2001 - Technology & Engineering*
[24] Holobloc Inc. (2011). Function bloc development kit and documentation, *http://www.holobloc.com*