RISK AND HAZARD PREVENTION USING REMOTE INTERVENTION

Luiza OCHEANĂ[1], Dan POPESCU[2], Gheorghe FLOREA[3]

In aceasta lucrare propunem un nou nivel de protectie in arhitectura actuala reprezentat de un sistem de interventie de la distanta avand ca scop monitorizarea, diagnoza si controlul unei instalatii industriale folosind infrastructura de comunicatie oferita de Internet. Sistemul va oferi suport tehnic pentru operatorii din camerele de comanda si resurse de calcul pentru a simula procese complexe, pentru a identifica probleme si pentru a oferi solutii de optimizare, diagnoza si imbunatatire a strategiilor de control. Lucrarea prezinta arhitectura de sistem a noului concept, precum si avantajele acestuia raportate la solutiile actuale.

This paper introduces a new level of protection in the current industrial architecture represented by a remote intervention system having the purpose to monitor, diagnose and control a facility remote, using the Internet infrastructure. The system will provide technical support for the operators and computational resources to simulate complex processes, to identify problems and give solutions for plant optimization, diagnosis and creating new control strategies. The paper presents the system architecture of the new concept in process control industry and its advantages related to present solutions.

Keywords: levels of protection, remote monitoring and intervention, risk and hazard in industrial processes

1. 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:

[1] PhD student, The Faculty of Automatic Control and Computers, University POLITEHNICA of Bucharest, Romania, e-mail: luiza.ocheana@yahoo.com

[2] Prof., The Faculty of Automatic Control and Computers, University POLITEHNICA of Bucharest, Romania, e-mail: dan_popescu_2002@yahoo.com

[3] PhD student, The Faculty of Automatic Control and Computers, University POLITEHNICA of Bucharest, Romania, e-mail: gelu.florea@sis.ro

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

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.

This paper introduces a new level of protection, between OI and ESD layers, having the main function to prevent hazardous situations in order to avoid the ESD intervention. Fig. 1 shows the position of the new layer in the current architecture.

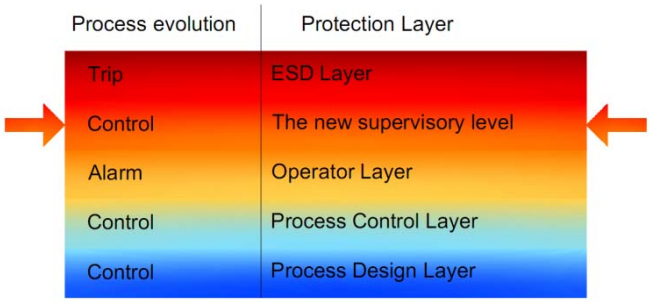

Fig. 1. Layers of protection

Poor performance costs money in lost production and plant damage and weakens a very important line of defence against hazards to people [2]. 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. That is why this project aims to develop a system that will connect to multiple plants to monitor and detect abnormal functioning as shown in Fig. 2. The system will be able to intervene in hazardous situations and provide solutions to system operators.

The challenges that must be answered in order to achieve the expected results are:

- ¬ Creating a safe remote connection over the Internet;
- ¬ Developing a system for the diagnosis and debugging of plants;
- ¬ Implementing a generic approach (the system will be able to connect to any plant, no matter the automation controller, the communication type between the automation equipment);
- ¬ Creating a comprehensive database to gather the system experience gained from different clients;
- ¬ Providing support by remote access and help files for plant operators;
- ¬ Defining a methodology for plant optimization;
- ¬ Defining a methodology for failure detection.

In the next sections we will present the functional architecture of the system, the main components and two particular implementations.

2. System Architecture

The system architecture is presented in Fig. 2. The main components of the system are:

- ¬ Client's plant and BPCS;
- ¬ Communication infrastructure;
- ¬ Remote control system.

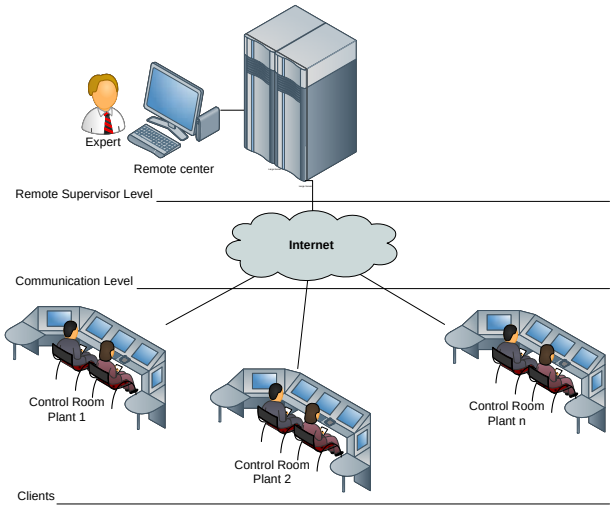

Fig. 2. System architecture

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.

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 system will be based on four main functions:

i. Help Center;
ii. Remote Monitoring and Diagnosis.
iii. Remote Intervention;
iv. Remote Back-up and Recovery.

The Help Center function will provide plant operator support using various communication methods like help files, remote access assistance, instant messaging. In case of remote access, we need to establish a secure VPN (Virtual Private Network) connection between the plant and the center site. A VPN is "a communications environment in which access is controlled to permit peer connections only within a defined community of interest" [3].

Another important problem is alarm management. "The purpose of an alarm is to draw the operator's attention to abnormal conditions requiring action" [4]. The system will define an efficient alarm management system allowing the operator to focus on real emergency situations. The system will be able to read the plant instruments status, to make the difference between operating alarms and maintenance alarms, leading to a better alarm management and faster intervention.

The remote monitoring needs to assess two main problems [5]. On one hand, the system will need to be able to connect to any existing plant, to retrieve data and status information in a format it will be able to understand. From this point of view, the solution will be OPC (OLE for Process Control; Object Linking and Embedding) automation standard. Using an OPC server for a specific controller, real-time data, alarm information and even history files can be sent over the Internet and included in the monitoring and control applications. The advantage is that almost all DCS or PLC manufacturers provide support for interface using this standard.

Remote monitoring is strongly related to the data acquisition. Data will be integrated in a historian database where it will be centralized with information received from other plants and the time when the acquisition was performed will be recorded to better empathize the process characteristics. This way, besides the actual data monitoring, the analysis for the PLC and DCS state can be performed, vital parameters can be calibrated accordingly, one can monitor the maintenance level, perform fault diagnosis and predict future failures etc. Collecting and transporting data must comply with the security and flexibility standards.

Security of data transfer must be managed and refined in order to ensure confidentiality, integrity, and availability of the services and systems. For this we used dedicated software packages to create VPN's through the Internet. Because the system must be available at any time and any place, a redundant connection will be set up. Wireless access must also be taken into consideration, using dedicated technologies like WiMAX for example, that defines two layers of the protocol stack, physical (PHY) and medium access control (MAC) [6].

The system will also offer solutions for plant optimization, by creating new strategies based on the modelling and simulation of the plant, or by an efficient tuning of the control loops, which are constantly under different perturbations. Modelling a industrial process is a difficult task because relevant models need to be dynamic and have a large operational range, but in the same time, it should not be too complicated, easy to assign parameters to it and easy to combine [7].

In large systems, every single component is designed to provide a certain function so the overall system works in optimal conditions only if all components provide the service they are designed for. This is why a fault in a single component usually changes the performance of the overall system. In order to avoid production deteriorations or damage to machines and humans, faults have to be found as quickly as possible and decisions that stop the propagation of their effects have to be made [8].

The remote intervention function will be used in order to react to the existence of the fault by adjusting its activities to the faulty behavior of the plant (Fig. 3).

The intervention will consist in two steps:

- Fault diagnosis - The existence of a fault has to be detected and the fault identified.
- Control re-design: The controller has to be adapted to the faulty situation so that the overall system continues to satisfy its goal.

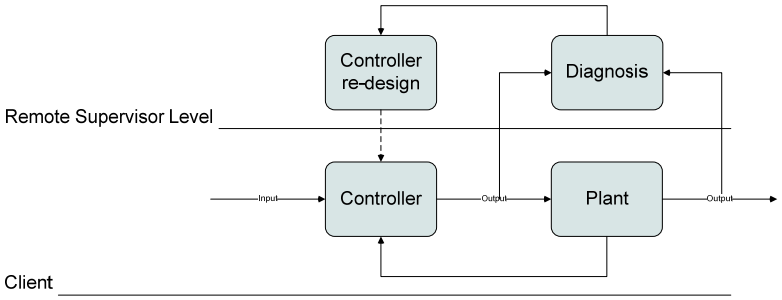

Fig. 3 – Remote intervention – fault diagnosis and re-design

The remote back-up and recovery function will have two components:

- Back-up of program and configuration data – to restore the entire system if needed.
- Back-up of historical data - to recover data from a historical period of time within the constraints of a user-defined.

3. Particular Implementations

For the first implementation we chose to simulate the process of controlling the level of liquid in a tank. The control of the process is done using Proportional-Integral (PI) control algorithm. The PI regulator uses the reference level of the tank and the perturbation as inputs and commands the evacuation in order to keep the tank level constant. Simulation results of the PI algorithm are presented in Table 1 and Fig. 4, for the following function [9]:

$$u(t) = k_p e(t) + k_i \int e(t)dt \quad (1)$$

Table 1

The parameter values after PID simulation

				Fixed output flow				Variable output flow			
Time	Level Set Point	Kp	Ki	In flow	Out flow	Level	CMD	In flow	Out flow	Level	CMD
49	**0.75**	**0.011**	**0.015**	12.4999	5.00	0.7500	1.2500	12.4999	5.00	0.7500	1.2500
50	**0.75**	**0.011**	**0.015**	12.4999	5.00	0.7500	1.2500	12.4999	5.00	0.7500	1.2500
51	**0.20**	**0.011**	**0.015**	12.4999	5.00	0.7500	1.1070	12.4999	5.00	0.7500	1.1070
52	**0.20**	**0.011**	**0.015**	11.0699	5.00	0.6070	1.0616	11.0699	5.00	0.6070	1.0616
...	**...**	**...**	**...**	...	...	...	...	...	...	...	...
122	**0.20**	**0.011**	**0.015**	7.0001	5.00	0.2000	0.7000	7.0001	5.00	0.2000	0.7000
123	**0.20**	**0.011**	**0.015**	7.0001	5.00	0.2000	0.7000	7.0001	6.00	0.1000	0.7260
124	**0.20**	**0.011**	**0.015**	7.0001	5.00	0.2000	0.7000	7.2601	6.00	0.1260	0.7342
...	**...**	**...**	**...**	...	...	...	...	...	...	...	...
152	**0.20**	**0.011**	**0.015**	7.0000	5.00	0.2000	0.7000	7.9861	6.00	0.1986	0.7988
153	**0.20**	**0.011**	**0.015**	7.0000	5.00	0.2000	0.7000	7.9879	6.00	0.1988	0.7989
154	**0.20**	**0.011**	**0.015**	7.0000	5.00	0.2000	0.7000	7.9895	6.00	0.1989	0.7991
...	**...**	**...**	**...**	...	...	...	...	...	...	...	...
178	**0.75**	**0.011**	**0.015**	7.0000	5.00	0.2000	0.8430	7.9996	6.00	0.1999	0.9429
179	**0.75**	**0.011**	**0.015**	8.4300	5.00	0.3430	0.8883	9.4297	6.00	0.3429	0.9882
180	**0.75**	**0.011**	**0.015**	8.8832	5.00	0.3883	0.9375	9.8829	6.00	0.3882	1.0375
...	**...**	**...**	**...**	...	...	...	...	...	...	...	...
259	**0.75**	**0.011**	**0.015**	12.4999	5.00	0.7500	1.2500	13.4999	6.00	0.7500	1.3500
260	**0.75**	**0.011**	**0.015**	12.4999	5.00	0.7500	1.2500	13.4999	6.00	0.7500	1.3500
261	**0.50**	**0.011**	**0.015**	12.4999	5.00	0.7500	1.1850	13.4999	6.00	0.7500	1.2850
262	**0.50**	**0.011**	**0.015**	11.8499	5.00	0.6850	1.1644	12.8499	6.00	0.6850	1.2644
...	**...**	**...**	**...**	...	...	...	...	...	...	...	...
327	**0.50**	**0.011**	**0.015**	10.0001	5.00	0.5000	1.0000	11.0001	6.00	0.5000	1.1000
328	**0.50**	**0.011**	**0.015**	10.0001	5.00	0.5000	1.0000	11.0001	6.00	0.5000	1.1000
329	**0.50**	**0.011**	**0.015**	10.0001	5.00	0.5000	1.0000	11.0001	6.00	0.5000	1.1000
330	**0.50**	**0.011**	**0.015**	10.0001	5.00	0.5000	1.0000	11.0001	3.00	0.8000	1.0220
331	**0.50**	**0.011**	**0.015**	10.0001	5.00	0.5000	1.0000	10.2201	3.00	0.7220	0.9972
332	**0.50**	**0.011**	**0.015**	10.0000	5.00	0.5000	1.0000	9.9728	3.00	0.6972	0.9704
...	**...**	**...**	**...**	...	...	...	...	...	...	...	...
403	**0.50**	**0.011**	**0.015**	10.0000	5.00	0.5000	1.0000	8.0000	3.00	0.5000	0.8000
404	**0.50**	**0.011**	**0.015**	10.0000	5.00	0.5000	1.0000	8.0000	3.00	0.5000	0.8000
405	**0.75**	**0.011**	**0.015**	10.0000	5.00	0.5000	1.0650	8.0000	3.00	0.5000	0.8650
406	**0.75**	**0.011**	**0.015**	10.6500	5.00	0.5650	1.0856	8.6500	3.00	0.5650	0.8856
...	**...**	**...**	**...**	...	...	...	...	...	...	...	...
450	**0.75**	**0.011**	**0.015**	12.4964	5.00	0.7496	1.2496	10.4964	3.00	0.7496	1.0496
451	**0.75**	**0.011**	**0.015**	12.4969	5.00	0.7496	1.2497	10.4969	3.00	0.7496	1.0497

At the client location the process is monitored and controlled through a SCADA (Supervisory Control And Data Acquisition) system, representing the BPCS, which also includes an OPC server. OPC is an open industrial standard created by hardware and software automation manufacturers together with Microsoft [10]. The standard creates a common interface for communication between several components that control the technological processes.

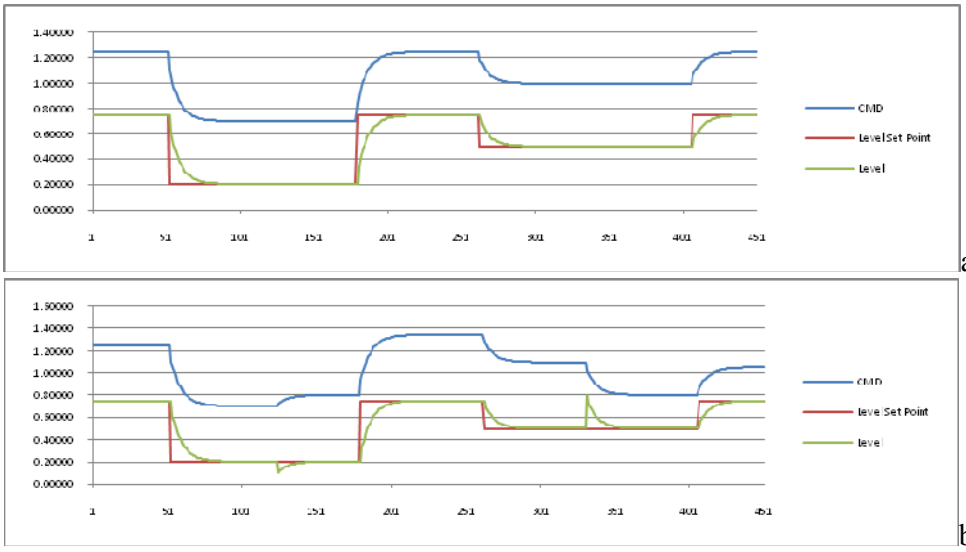

Fig. 4 - Simulation results of the PID algorithm a) Fixed output flow, b) Variable output flow

Although OPC was first designed for accessing data from a networked server, OPC interfaces can be used in many places within an application. This architecture and design made it possible to realize an OPC Server that allows a client application to access data from many OPC Servers provided by many different OPC vendors running on different nodes via a single object.

SCADA system allows operators to monitor the process and interact with it if necessary, ensuring the second layer of protection (OI). The communication between the client system (BPCS) and the remote one was done through Internet. In order to prevent data alteration, strong security measures are recommended. In this way, the confidence of the clients will also be increased in allowing remote access to their private data and even to the decisions taken in order to control of the process.

A solution to provide data security when using Internet access is to create a VPN connection, which is the solution we chose for the application. Open VPN is a complete solution that combines remote access, VPN site-to-site, Wi-Fi security, and so on. The security model of Open VPN is based on SSL (Secure Sockets Layer), the general used standard for encrypted communication over the

Internet [11]. The main advantages of Open VPN are portability, an easy configuration process and compatibility with Network Address Translation (NAT) and Dynamic Addressing [12]. This solution involves a reduced effort for design, implementation, operation and maintaining the security of data. These are the arguments that were taken into account when choosing Open VPN as security solution implemented for the application, on both customer location and central location.

At the central location the diagnosis function was implemented. The system is counting the alarms for analysis: an increased number of alarms may indicate an evolving problem into the system, while a decrease of the number of alarms indicates the fact that problem was solved. On the other hand, the alarms per subsystem are also counted. The experts from the remote center will analyze the data received and will notice an abnormal behavior. Creating groups of alarms will increase the operator's efficiency and will help detecting a fault into the system. In Fig. 5, the client's screen is visualized remote using the Internet connection. Because the level inside the tank is lower that the Low Low (LL) limit, the alarm is shown in the list and also the process parameters evolution is shown on the graphic.

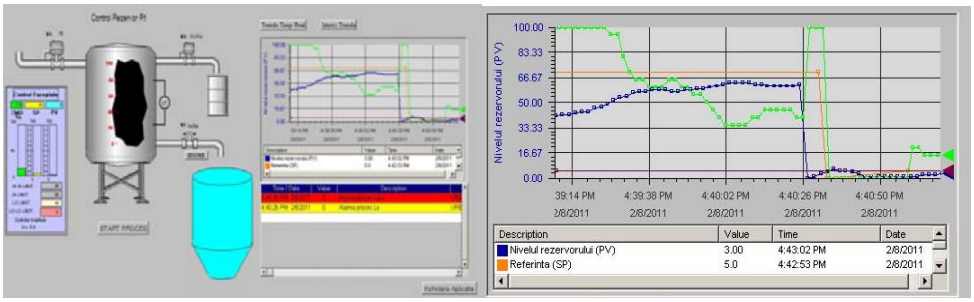

Fig. 5. The operator screen visualized from the remote center (LL alarm)

The system also allows post-incident analysis – the data acquired from the process is stored in order for the experts to analyze and to find a solution to prevent the incident in the future.

Alarm management is done by erasing the minor alarms in order for the operator to focus on the critical ones. The alarms are filtered, stored in a structured database and presented in graphical easy to use reports.

Performances supervision is another important task: the data acquired from the process is continuously monitored in order to optimize the performances and to improve the accuracy of prediction of the behavior of the system.

At the remote location, not only the client's screen is shown, but also a model of the process was implemented, having a similar operator screen, which will be used to estimate the behavior of the system. Different scenarios can run on the model in order to improve the control parameters and future actions. A

situation of alarm is shown in Fig. 6, the level inside the tank has reached the High High (HH) limit.

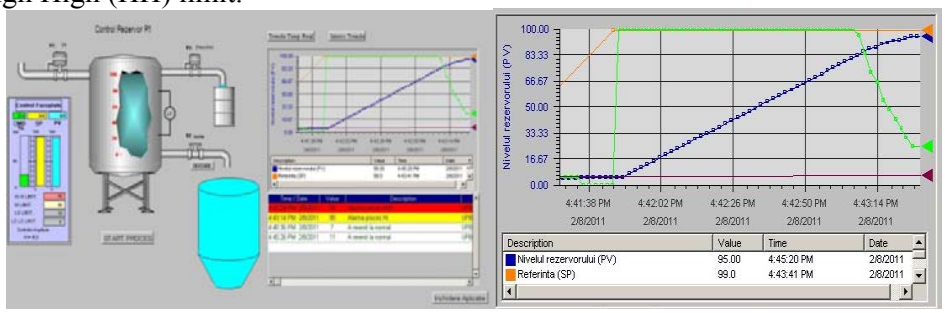

Fig. 6. The simulated process (HH alarm)

The second implemented application is for a Building Management System (BMS) designed for a supermarket. BMS is a centralized system that monitors and controls the mechanical and electrical equipments (HVAC, lightning, fire detection, access control, and so on). The system monitors the evolution of parameters, displays the events, controls different equipments (vents, doors) in case of abnormal situations.

The operator screen is shown through Internet connection in the remote center. Fig. 7 left shows the main screen and its menu while Fig. 7 right shows the controllers and their status, both seen from the remote center. In this case, the remote connection was proved to be very helpful in the commissioning stage of the BMS because all needed interventions were done quickly and efficient without the actual presence of the experts at the client's site.

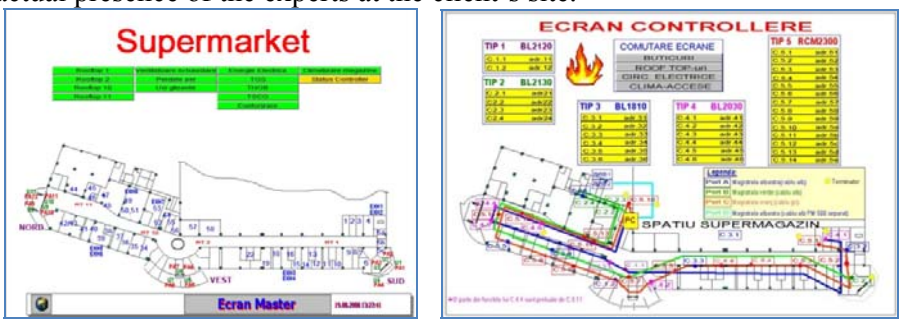

Fig. 7. Supermarket BMS – remote connection screens

4. Conclusions and Future Work

The work that had been developed so far represents only the first step for building the next level of supervision and control. The main advantages of the solution are scalability and flexibility, because the system can easily integrate different types of processes, using a cost effective and secure solution over the

Internet. The simulator of the real process can be used in order to evaluate new solutions, to compare them with the existing ones and to materialize direct or indirect intervention. The simulator can also be used for operator training.

The alarm management component will help the operators from the control room to focus on the critical alarms. Advanced alarm management algorithms must be studied and implemented in order to improve the performance of the system.

Loop optimization and tuning components also need improvement in order to increase plant efficiency and reduce operating costs.

Original work was validated by implementing a pilot system of two units: an academic (Universitatea POLITEHNICA Bucuresti) and a SME one (Societatea de Inginerie Sisteme).

The work was partially supported by national research program PN2 (project 81.060/2007) and doctoral program DocInvest/2010.

Future work will include the expansion of the system in two directions:

- adding new applications to the system, more complex processes;
- improving the implemented algorithms for simulation, control, alarm management, optimization, tuning, and so on.

REFERENCES

[1] *Hatch, D. and Stauffer T*, "Operators on Alert. Alarm Standards, Protection Layers, HMI Keys to Keep Plants Safe", InTech, september 2009.

[2] *Bransby M.L. and Jenkinson J.*, "The Management of Alarm Systems", HSE Contract Research Report 166/1998, ISBN 07176 15154, 1998.

[3] *Paul Ferguson and Geoff Huston*, "Whitepaper: What is a VPN?", Revision 1, under "Presentations, Slideware, and Assorted Cruft", 1998.

[4] *Todd Stauffer, Nicholas P. Sands and Donald G. Dunn*, "Alarm Management and ISA-18 – a Journey, not a Destination", Texas A&M Instrumentation Symposium, 2010.

[5] *Luiza Ocheană, Dan Popescu, Gheorghe Florea,* "Remote Diagnosis and Intervention – a New Layer of Protection for Industrial Processes", Proceedings CSCS-18 18th International Conference on Control Systems and Computer Science, 2011.

[6] *Cătălin-Teodor Dogaru, Teodor Petrescu*, "WIMAX 802.16 Network – Secure Communications", U.P.B. Sci. Bull., Series C, Vol. 71, Iss. 2, 2009.

[7] *Kaj Juslin*, "A Companion Model Approach to Modelling and Simulation of Industrial Processes", VTT Publications, 2005.

[8] *Andrea Paoli*, "Fault Detection and Fault Tolerant Control for Distributed Systems. A General Framework - Ph.D. Thesis", University of Bologna, 2003

[9] *Dumitrache I.*, "Ingineria Reglării Automate" (Automatic Control Engineering), Politehnica Press, Bucureşti, 2005.

[10] *OPCFoundation*, "What is OPC?", http://www.opcfoundation.org/Default.aspx/01_about/01_whatis.asp?MID=AboutOPC, 2011

[11] *Daniel Merezeanu, Dan Popescu, Gheorghe Florea*, *Corneliu Rusu*, "PHcenter: A Platform for Process Diagnosis and Control via Internet", Proceedings of the 2010 Second International Conference on Advances in Future Internet, 2010.

[12] *Guha,S., Ed. Cornell, and U.K. Biswas*, "NAT Behavioral Requirements for TCP", IETF 66, 2006.