Remote Risk and Hazard Control

Luiza Ocheana[#1], Dan Popescu[#2], Oana Rohat[#3]

#1 PhD Student, University Politehnica of Bucharest, +40766264325,
luiza.ocheana@yahoo.com
#2 Professor PhD, Politehnica University of Bucharest, +40766218363,
dan_ popescu_2002@yahoo.com
#3 PhD Student, University Politehnica of Bucharest, +40721877478,
ratzoni_18@yahoo.com

ABSTRACT

Most of industrial environments share the need for a higher-level decision and control system to improve and optimize plant operation. Different research projects have been developed worldwide in this area and their results will be considered in designing and implementing the system. Hazard analysis studies are developed during the design phase of an installation to assess and document the possible faults that might appear during the plant functioning. Changes are made to the design so that any hazard that might appear will have a limited effect on the installation. That is in the ideal case. The truth is you cannot really imagine all the faults that might appear, neither their effect on the functioning of the entire system. Partially, that is because it also depends on how the plant operator interferes in the process, how he commands the installation, how he acts when he detects faults or acknowledges alarms. The solution we propose in this paper is to implement a higher decision control system to take the control over the plant in cases of hazard, risk or abnormal situations, a system that will make sure that the correct decisions are taken in the given situations.

Key words: Diagnostics, Hierarchical decision, Remote intervention, Risk and hazard assessment, Safety and security.

Corresponding Author: Luiza Ocheana

INTRODUCTION

Most of industrial environments share the need for a higher-level decision and control system to improve and optimize plant operation. Plants often need to operate near criticality, meaning in conditions far from the designed ones from the point of view of control and stability. This leads to the need for the enhancement of process operations at plant production management level. Industrial processes are usually very complex, difficult to model and to keep under control. There is also a need for complex and more versatile simulation and modeling tools but no product in the market offers the necessary capabilities to deal with the uncertain nature of complex plants and the safety and security threats.

Safety has become a very important issue nowadays that receives an increasing amount of focus. The reason is, unfortunately, the number of accidents that occurred in industry plants and which require the process industry to take a hard look at current practices like process design, process control, risk analysis and control, risk assessment (for example the nuclear

plant accident in Harrisburg [1]). Engineering organizations have developed standards for the engineering of process safety. For example, IEC released two standards:
IEC 61508 includes electrical, electronic and Programmable electronic Systems for safety related function and usability [2] – targets the suppliers of safety equipments.
IEC 61511 developed for the end-users of process safety equipment [3].
All the development phases must be taken into consideration in order to achieve the required degree of safety and security: analyze the risks and their control, design, implementation and maintenance of the plant.

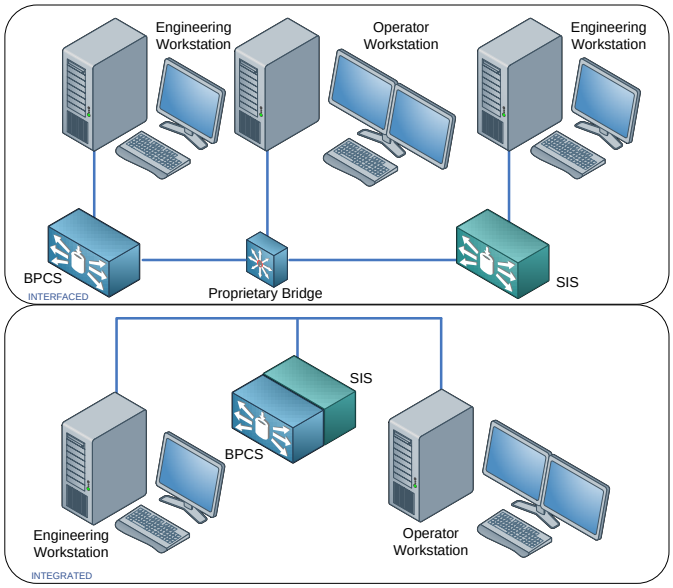

Fig. 1 - SIS and BPCS Integration Levels

Another important issue nowadays is whether or not safety and control systems should be integrated. Increasingly more manufacturers offer support for integrated control and safety system [4]. The entire issue of integrating or interfacing BPCS and SIS is presented in [5].

RISK ASSESSMENT

Risk assessment is the first process in the risk management process used to determine the potential threats and the risk associated within a system [6]. The procedure includes 10 steps:

- Step 1 – system characterization – deals with the technical specification of the system and how it will be used;
  - Inputs: hardware and software configuration, system interfaces, equipments, utilities, personnel, raw materials, system scope;
  - Outputs: system boundary, system functions, system and data criticality, system and data sensitivity.
- Step 2 – Threat identification:
  - Inputs: history of process risk, data from the process, hazard estimation;
  - Outputs: threat report.
- Step 3 – vulnerability identification:
  - Inputs: reports from previous risk assessments, audit comments, security requirements, security test results;
  - Outputs: list of potential vulnerabilities.
- Step 4 – Control Analysis:

- Inputs: current controls, planned controls;
- Outputs: list of current and planned controls.

¬ Step 5 – Likelihood Determination:
- Inputs: potential risks, hazard capacity, threat-source motivation, threat capacity, nature of vulnerability, current controls;
- Outputs: risk assessment matrix.

¬ Step 6 – Impact Analysis – deals with the impact resulting from a successful threat exercise of vulnerability: Loss of Integrity, Loss of Availability, Loss of Control, Loss of Confidentiality:
- Inputs: mission impact analysis, asset criticality assessment, data criticality, data sensitivity;
- Outputs: impact rating.

¬ Step 7 – Risk Determination – assess the level of risk to the system;
- Inputs: likelihood of threat exploitation, magnitude of impact, adequacy of planned or current controls;
- Outputs: risks and associated risk levels.

¬ 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 behavior.

Hazard analysis studies are developed during the design phase to assess and document the possible faults that might appear during the plant functioning. Changes are made to the design so that any hazard that might appear will have a limited effect on the installation. That is in the ideal case. The truth is you cannot really imagine all the faults that might appear, neither their effect on the functioning of the entire system. Partially, that is because it also depends on how the plant operator interferes in the process, how he commands the installation, how he acts when he detects faults or acknowledges alarms.

There are many issues that can be discussed when it comes to plant efficiency and the things that must be done so that no accidents take place and the plant functioning is not stopped. One solution is allowing that a higher decision control system takes the control over the plant in cases of hazard, risk or abnormal situations, a system that will make sure that the correct decisions are taken in the given situations.

This higher-level decision system we propose has the main advantage of providing the plant with the experience of several engineers that will continuously monitor the plant activity. Even more, they will have access to information regarding the plant history, solutions and results in similar cases and high performance computing tools for testing, simulation and optimization. The diagnosis and debugging system will receive real time data from the plant over the Internet and the specialists will analyze it, will identify existing problems and will offer solutions remotely.

SAFETY STANDARDS

Process safety has gained a great importance recently, especially as a result of catastrophic incidents that took place in different plants. There is an increasing concern for complete sets of skills for engineers and operators and for developing safety guidelines for industrial processes. The current standard for electronic and programmable systems, IEC61508, is the result of concentrated efforts of authorities and industrial companies in the past 30 years. The

overall objective of this standard is to ensure the implementation of appropriate risk mitigation strategies by all areas in which the processes are dangerous, such as to prevent the occurrence of incidents mentioned above. This standard, together with the industry-specific standard, IEC61511, are essentially advisory. However, they are currently considered "best practice standards" by the authorities in Great Britain and other industrial countries, and a way to determine if a satisfactory level of safety within the electronic components and programs had been achieved. These standards are used as reference, but it is indented to be introduced as mandatory.

IEC61508: Functional Safety of Electrical, Electronic and Programmable Electronic Safety Related Systems [7] is a generic standard on which safety standards specific to each sector should be based on. For the process area we have IEC61511 and its U.S. equivalent, ANSI / ISA S84 [8]. IEC61508 tends to become an European standard and can be applied to a wide range of security systems such as:

- ¬ Emergency Shut Down Systems;
- ¬ Fire and gas leaks detection and warning systems;
- ¬ Turbine control systems;
- ¬ Burner management systems;
- ¬ Railway signaling systems;
- ¬ Interlock systems.

IEC61508 is made of seven parts that provide specific instructions for operating safety systems. Developed by the International Electrotechnical Commission (IEC, Geneva, Switzerland), the standard refers to managing all components of safety systems, from sensors and controllers, to the features and applications that are designed to drive the process to a safe state described by predetermined conditions. The standard applies to the entire life cycle of the safety system, from the initial concept development, specifications, technical design, implementation, operation and maintenance. The first three parts of the standard provide information on the management, development, implementation and operation of the system hardware. Sections 4 to 7 of the standard present definitions, applications and additional information.

The Safety Integrity Level (SIL) and its availability are statistical representations of the availability of SIS in critical situations. This is the core of the design of a SIS compliant and includes the following factors:

- ¬ Component integrity;
- ¬ Diagnosis;
- ¬ Systematic and common cause faults;
- ¬ Testing methods;
- ¬ Operating procedures;
- ¬ Maintenance procedures.

The safety availability, meaning the period of time when the system is in operation, depends on:

- ¬ The rate of failure and fault modes of the components;
- ¬ Redundancy;
- ¬ The chosen scheme of voting;
- ¬ The testing frequency.

When the risk assessment and hazard identification concludes that a SIS is needed, we also have to determine the degree of risk reduction desired as a SIL level determination form. The effectiveness of SIS as an independent level of protection is described in terms of probability of failure to perform the functions provided when requested. This is known as the probability of failure (PFD) or reliability. In practice, we use the average PFD (PFDavg). The table below shows the relationship between PFDavg availability, MTBF and the SIL.

Table 1 - SIL according to IEC61508 and ways of measurement

SIL	Availability	PFDavg	MTBF
4	>99.99%	10–5 … <10–4	100000 … 10000
3	99.9%	10–4 … <10–3	10000 … 1000
2	99–99.9%	10–3 … <10–2	1000 … 100
1	90–99%	10–2 … <10–1	100 … 10

Assigning a SIL is a decision based on risk management and risk tolerance philosophy, specific to each company. IEC61508 requires that its establishment is carried out with great care, be well documented and provides guidance tables.

IEC61511 defines methods for risk assessment of certain hazardous processes and determines the level of risk reduction that must be provided by the SIS. The standard requires reducing risks to a level as low as possible. It does not impose specific technologies or architectures.

IEC61511 covers all phases, from design to management requirements for SIS. It includes: initial concept, design, implementation, commissioning, operation, and maintenance. The standard also contains sections relating to modifications to the system that may occur after commissioning and even decommissioning activities.

The standard is divided into three parts:

- ¬ Framework, definitions, hardware and software requirements;
- ¬ A guideline for implementing IEC61511;
- ¬ Guidelines for determining the required level of safety.

IEC61511 requires a management system for each identified SIS. A SIS is made of independent combinations of sensors, actuators, controllers and support systems designed and operated to ensure a specified SIL. A SIS may implement one or more functions for certain situations and events. The management system should define how the owner / operator will evaluate, design, install, verify, validate, operate, maintain and continually improve the system. Specific rules and procedures must be developed for the key personnel to support their work.

COMMUNICATION

A Virtual Private Network (VPN) provides a way of establishing secure communication through an insecure network. Using a VPN connection, two sides can communicate in the same safe conditions as those provided by a local network. The term "private" underlines the restrictive access to a specified set of entities and facilities, in this case private access to the content of communication. A VPN is at the same time:

- ¬ A computer network in which the links between nodes are ensured by "virtual circuits" within a larger network (usually the Internet) instead of physical connections (cables). The protocols used by the virtual network connection are called “tunnels" through the larger network. In general, a VPN allows the computers to appear at a different IP address than the one that connects them to the Internet.

- A shared network where private data are separated from the rest, so the only real recipient has access to them. VPN term was first used to describe a secure connection over the Internet. A key aspect of data security in VPNs is that they, in their course to the recipient, are protected by encryption technology. Private networks lack of data security, allowing the network entry and access. Instead, virtual private networks use advanced cryptographic techniques to secure data.

Private network does not necessarily mean a physical system of private communication. To build a private network, an organization could rent private circuits from a telecommunications service provider and build the network using these circuits. It can be built between two or more systems, between two or more organizations and even between certain individual applications.

For VPN, private communication occurs within a distributed infrastructure. A VPN does not necessarily imply the isolation of the communication, but the implementation of controlled segments of communications for groups with common interests over a distributed infrastructure.

The cost of setting up a VPN depends crucially on the level of security requirements in conjunction with the level of risk that the beneficiary organization accepts. Also on behalf of the organization a large part of their VPN performance can be ensured through the appropriate choice of WAN services and the use of data compression techniques. In the long term, new technologies promise to continuously ensure stable performance between suppliers and customers.

A VPN connection usually provides the following functions:

- Authentication - using passwords or other methods, the two sides of a communication can prove their identity before accepting a connection. Once the connection was established, the communication can take place in both directions through that it.
- Encoding - the encoding of all data sent between the two points of the public network, the packets can be seen but cannot be read by a hacker. This process is known as "tunneling".

RESULTS

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" were used to connect two industrial plants to the superior level. Based on the general architecture presented in [9], we established the connection to a compressor station and a fuel tank farm.

Compressor station:

The plant was developed in order to compress the gas extracted in the upstream using a gas compressor and the associated piping network. The station was equipped with an ESD system that shuts down the compressor and isolates the station in case of any alarm. The field equipments are:

- two valves on the gas piping system: XV3, XV4;
- two valves on the ventilation piping system: XV1, XV2.

The initial state is the same as the safe state of the plant and is described as following:

- Compressor stopped;
- Valves XV1, XV2 – opened;
- Valves XV3, XV4 – closed.

The normal operation state:

- ¬ Compressor in operation;
- ¬ Valves XV1, XV2 – closed;
- ¬ Valves XV3, XV4 – opened.

In case of alarm (fire, gas leakages, manual alarm), the ESD system shuts down the compressor, opens XV1, XV2 and closed XV3, XV4.

The ESD system is a small HiQuad configuration manufactured by HIMA [10], certified SIL3. It includes a network module for data transmission over Ethernet, using Modbus TCP/IP. The valves are monitored using led lamps mounted on the front panel. There is no operator station installed.

The client asked for the following services to be provided by the remote center: plant monitoring, alarm counting, intervention in case of emergency, online technical support, back-up and restore the ESD logic.

In order to connect the ESD system to the remote center, we need to add a data acquisition device (local station) and an Internet link (Fig. 2). The minimum requirements for the device are: operating system, antivirus, SCADA software, PLC programming software, VPN software. We chose to use LogMeIn Hamachi [11] to establish a direct link between the local station and the remote center. The software establishes a connection over the Internet that emulates the links between computers in a local network.

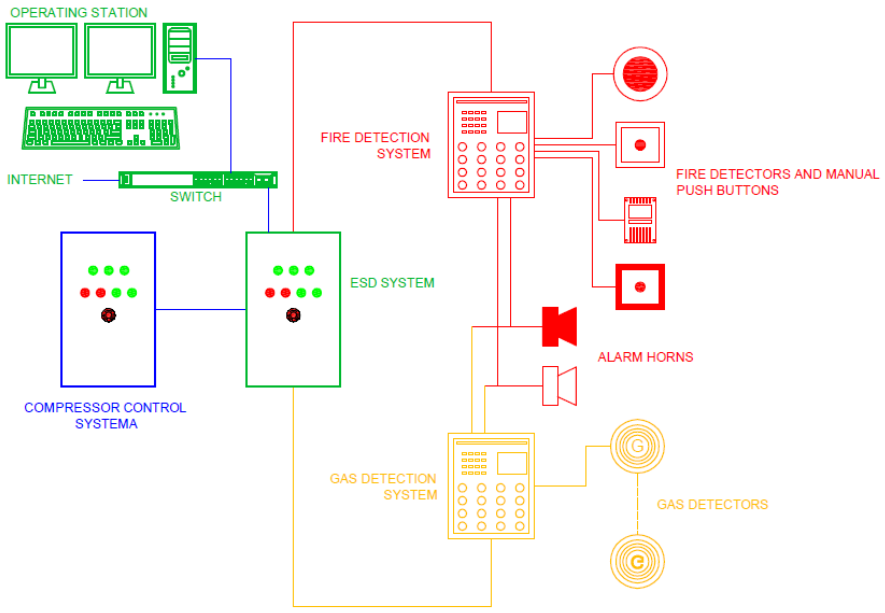

Fig. 2 – Compressor station – system architecture

For the local station we need a small SCADA application in order to retrieve the data from the ESD and transfer it to the remote center. Next, we need another SCADA application for the remote center station that ensures the plant monitoring, alarm counting and the intervention in case of emergency.

Technical support will be provided by email and phone on request. In addition, LogMeIn application needs to be installed on the local station in order to ensure the back-up function. To this end, the client needs to provide the exact files that were uploaded on the ESD controller.

Tank farm:

The terminal is used to transfer the fuel between tanks and tank trucks and stores it for a period of time. The automation system is based on a PcVue SCADA application [12] and S7-300 manufactured by Siemens, certified SIL 3 [13]. There are three hierarchical levels: the field devices (sensors, transducers, actuators), the level of automation (S7-300 controller with appropriate software logic) and the upper level – the operator station (SCADA application) (Fig. 3).

The operator station ensures the following functions (Fig. 4):

- communicates with other equipments;
- displays comprehensive data on process synoptic diagrams;
- allows the operator to access alarms and events files;
- displays real-time trends and historical data;
- displays the status of functionality (valve closed - open, etc.;
- generates trends (hourly, daily, weekly, monthly, yearly operator custom);
- allows access to information based on predefined hierarchical levels of passwords.

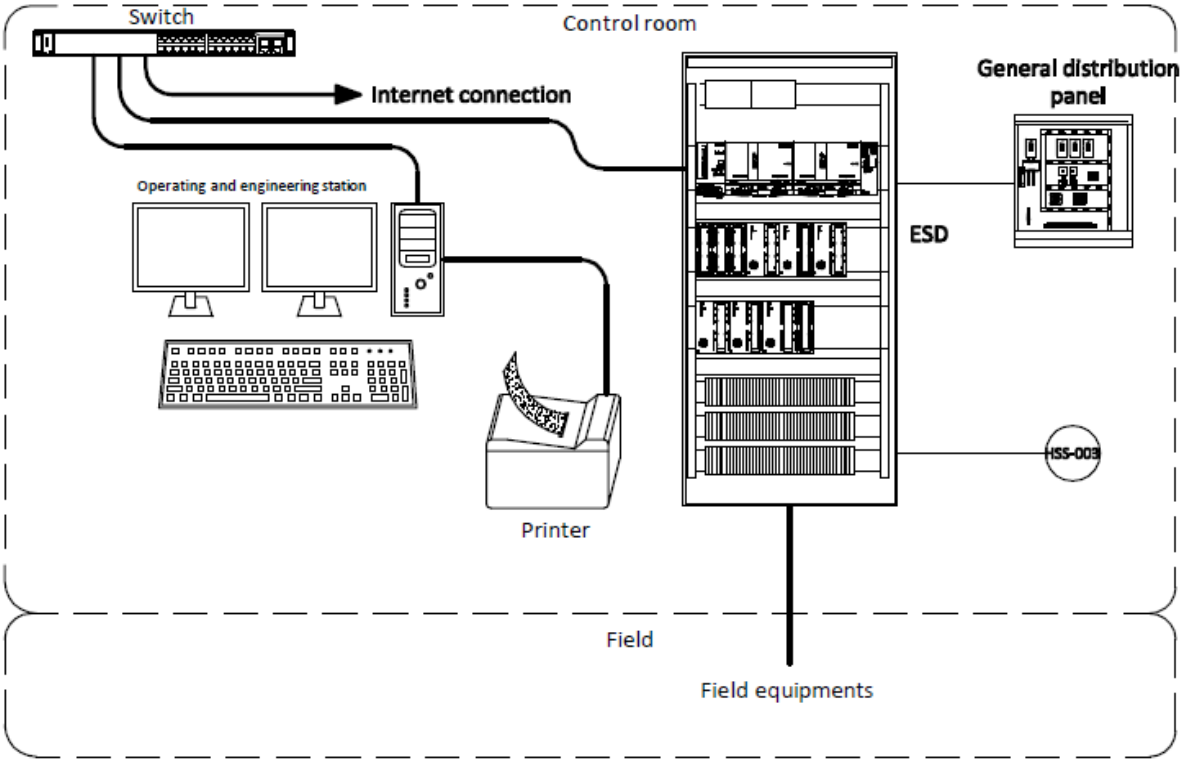

Fig. 3 – Tank farm – system architecture

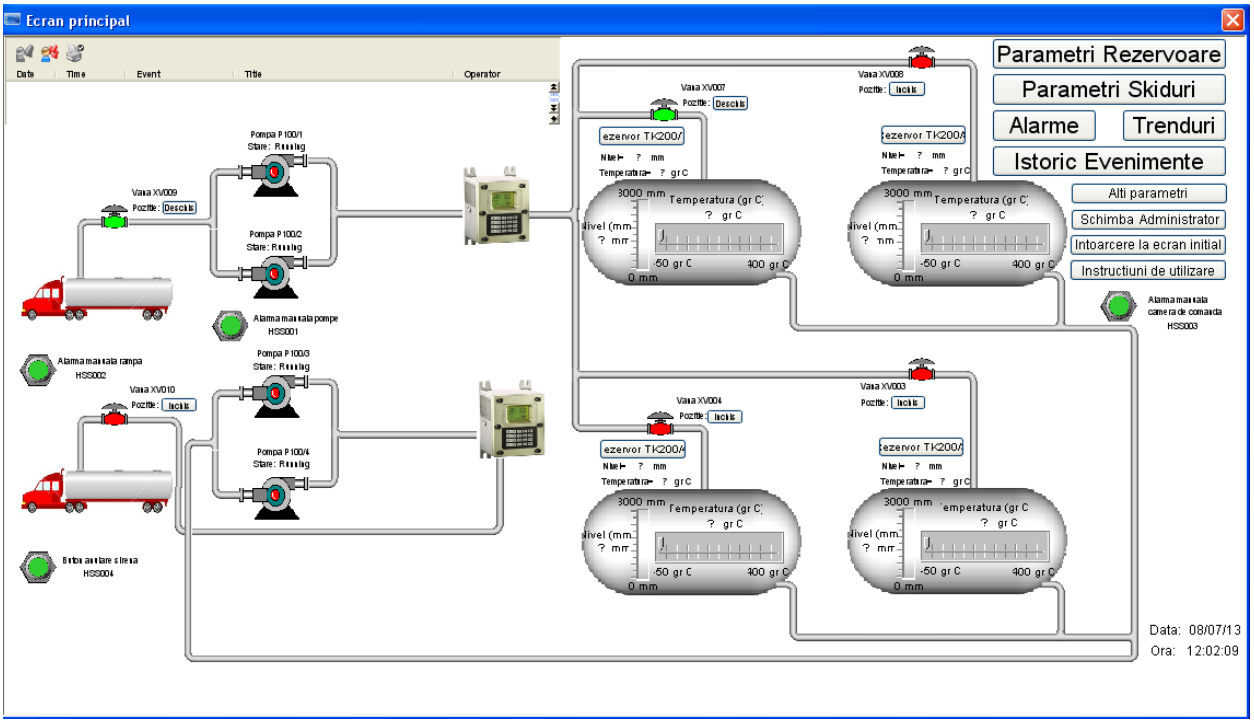

Fig. 4 – Tank farm – synoptic diagram

The client asked for the following services to be provided by the remote center: plant monitoring, alarm counting, intervention in case of emergency, online technical support, back-up and restore for the operating station – system image.

Because the control room was provided with an operator station including an OPC server, we only need two more components: an Internet connection and a VPN application. Using LogMeIn Hamachi we create a virtual network between the operator station and the remote center. At the center, we need to implement the same synoptic diagrams and to display the data transferred by OPC. In addition, the remote center will allow the experts to take over the control of the installation when needed.

Technical support will be provided by email and phone on request. In addition, LogMeIn application needs to be installed on the local station in order to ensure the intervention from the remote center at any time. This software will also be used to create a system image after any modification. The center will keep all the revisions of the operating station so anyone will be able to return to any of them later.

CONCLUSIONS

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, 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).

This paper presents a new layer of protection represented by a remote supervisory center, connected to multiple plants in order to reduce the risks and prevent accidents along with the disposal of costs brought by unnecessary shut downs.

The remote connection can be set up using virtual private networks and OPC industrial standards that ensure both the security of communication and the compatibility between applications.

REFERENCES

[1] John G. Kemeny, Report of the president's commission on the accident at Three Mile Island, http://www.threemileisland.org, 1979.
[2] Börcsök J. Schwarz M.H. - A Survey on the Development and Design Strategies for Safety Related Systems according the Standard IEC/EN 61508, Proceedings of the 6th WSEAS International Conference on Applied Computer Science, 2006.
[3] Tino Vande Capelle and Michel Houtermans - Functional Safety: A Practical Approach For End-Users And System Integrators, Proceedings of the 10th WSEAS International Conference on Communications, 2006.
[4] Asish Ghosh and Dave Woll - Business Issues Driving Safety System Integration, ARC White Paper, 2006.
[5] Luiza Ocheana, Dan Popescu, Gheorghe Florea - Integrating versus interfacing safety and security with process control system, 19th International Conference on Control Systems and Computer Science, 2013.
[6] Gary Stoneburner, Alice Goguen, and Alexis Feringa - Risk Management Guide for Information Technology Systems. Recommendations of the National Institute for Standards and Technology, 2002.
[7] IEC61508 Parts 1–7: 1998, Functional Safety of Electrical/Electronic/Programmable Electronic Safety–Related Systems, International Electrotechnical Commission, Geneva, Switzerland.
[8] ANSI/ISA Standard S84.01–1996, Application of Safety Instrumented Systems to the Process Industries, International Society for Measurement & Control, Research Triangle Park, NC, (1996)
[9] Gheorghe Florea, Luiza Ocheana, Dan Popescu, Oana Rohat (2011). Emerging Technologies – the base for the next goal of Process Control – Risk and Hazard Control, Proceedings of the 11th WSEAS International Confference on Systems Theory and Scientific Computation, pp. 227 – 232.
[10] http://hima.com/Products/HIQuad_default.php.
[11] https://secure.logmein.com/products/hamachi/download.aspx
[12] http://www.arcinfo.com/.
[13] http://www.automation.siemens.com/mcms/programmable-logic-controller/en/simatic-s7-controller/s7-300/pages/default.aspx.