

# Creation of Integrated of Industrial Security with the use of Modern Information Technology

Sh.B.Sattarov<sup>1</sup>, F.T.Adilov<sup>2</sup>, A.I.Ivanyan<sup>3,\*</sup>

## Abstract

This article considers Honeywell solutions in the branch of integration of subsystems of industrial safety and security for industrial enterprises with the creation of a unified Human-machine interface for centralized management and control of safety at the plant.

**Key Words:** Industrial safety and security, KITSO, EIS, HMI, Virtualization, DSA, EPKS.

## I. INTRODUCTION

The concept of a unified centralized system of safety and security management in the enterprise certainly is one of the strategic decisions of company management and is based on the characteristics of the organizational structure of the enterprise, scheme of interaction of its units, rules of the process conditions and other factors.

## II. Statement of a Problem

Often a enterprise management decision determines the creation of pre-defined completely independent autonomous control subsystems of the various functional components in the operation of an industrial facility (an independent protection system, an independent fire safety system, an independent video surveillance system, independent safety instrumented systems, etc.).

But in recent times, an increasing number of large industrial enterprises are showing interest in building a unified security management system, which, on the one hand, will provide authorized employees with a centralized security control for the object, and on the other hand, will be sufficient to have the software and technical features, guaranteeing the required levels of information

security and protection against unauthorized access, as for an object in general and in the structure of interaction between subsystems of industrial safety and security [1].

As fulfilled answer to this requirement of the modern market of information technologies can be considered a comprehensive solution of Honeywell - Experion Industrial Security (EIS) which offers a common software and hardware platform for all top-level subsystems of safety and security in the industrial object [2,3].

## III. The Concept of the Problem Decision and Concept Realization

### 2.1. The features of Experion Industrial Security (EIS) technical solution

Technical solution Experion Industrial Security (EIS) from Honeywell company is a software and hardware platform for top-level, combining subsystems of access control (ACS), closed circuit television (CCTV), monitoring and control in real-time, perimeter intrusion detection, protection of life and health of employees, dynamic acoustic sounding. Furthermore, this classical model, including the basic subsystems of a complex of engineering-technical means of protection (KITSO), is not dogmatic. Hardware and software platform of Experion provides a maximum flexibility of interfaces and has a full

---

Manuscript received August 4, 2015; Revised September 30, 2015; Accepted October 26, 2015. (ID No. JMIS-2015-23)  
Corresponding Author (\*): A.I. Ivanyan, Niyozbek yuli-1 Street, 100000, Tashkent city, Republic of Uzbekistan ,  
[arsen.ivanyan@himavtomatika.uz](mailto:arsen.ivanyan@himavtomatika.uz) .

<sup>1</sup>Eriell Corporation S.R.O Company, Czech Republic, [shakhrukh@eriell.com](mailto:shakhrukh@eriell.com)

<sup>2</sup>Tashkent State Technical University, Uzbekistan, Tashkent, Uzbekistan, [Farukh.Adilov@himavtomatika.uz](mailto:Farukh.Adilov@himavtomatika.uz)

---

set of tools for the integration of the entire spectrum of modern subsystems of industrial safety and security.

Clearly the classical scheme of KITSO subsystems complex which is combined for centralized management on the basis of EIS technical solution, is presented in Figure 1 below.

Experion Industrial Security (EIS) system solution is based on client-server architecture with the use of information networks of personal computers, standard operating systems and communication protocols.

EIS System solution allows the distribution of system functions, such as monitoring and control using a graphical user interface on all nodes in the network that provides maximum flexibility and performance. The system architecture is built on the principle of support of different widely used networks and uses customized hardware and software to access all the network nodes. The protocols relate to the stack of TCP/IP protocols. The EIS also works in remote configuration modes and access via a standard intranet and Internet connections. The EIS system enables communication with a wide variety of control devices using ready-made driver packages. It supports such standard protocols like LON, BACnet, Modbus and OPC, thereby guaranteeing the openness of the system. For integration at the corporate level of the enterprise system EIS also equipped with means to support a service-oriented architecture (SOA) based on Web 2.0 standards of web services.

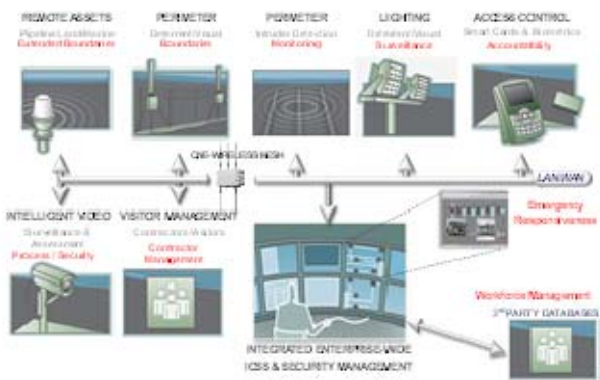


Fig.1. The classical scheme of KITSO complex of subsystems, combined on the basis of Experion Industrial Security (EIS) technical solution from Honeywell

Like all software-hardware platforms of the Experion family EIS system supports the concept of full redundancy in hardware at the level of server hardware, as well as at the level of network equipment.

Human machine interface (HMI) provided by the EIS system, ensures effective communication of operational data in emergency situations. The system is a set of software tools (processing of alarms, monitoring of the status of hardware means of the system, a set of standard

displays for settings and navigation throughout the system, a versatile tool set for configuring custom displays based on the HMI Web Display Builder software).

To ensure reliable protection against unauthorized access the EIS system provides a concept of protection levels for the system data access. By default it is offered the 6 levels of access with the characteristics described below, but this configuration is easy by changing the embedded toolbox set considered in the EIS system:

- Level 1: Sign-off mode. Visualization of only the initial display of the HMI.

- Level 2: Mode, limited for the view only. Allows the user only to view the displays. Usually installed for inexperienced users.

- Level 3: Allows all actions which are permitted for levels 1 and 2 and allows the user some control functions such as start/stop, enable/disable and acknowledge the alarm in case of its occurrence.

- Level 4: Allows all actions which are permitted for levels from the first to the third, and also provides the user with access to information on schedules and graphs to the system peripherals, allows changing the parameters of the points of the control system, allows configuration of the reporting documentation and provides complete access to all standard displays configuration. This level of access, usually established for an employee with authorized functions of the supervisor.

- Level 5: Allows all actions which are permitted for levels from first to fourth, and also provides access to engineering of system functions such as creating custom HMI displays and linking them together, the appointment and reappointment of the properties of the shortcut to the user keyboard, etc. This level of access, usually established for the employee responsible for the system engineering.

- Level 6: The highest level of security on the user station. Provides unlimited access to all features of the system. This level of access, usually installed by a duly authorized representative of the management.

We would like to note again that the above features propose a unified HMI for all subsystems of industrial safety and security at the facility, offering thus a unique variant of integration in "one window" for the management of the enterprise.

Figure 2 below shows the architecture of an EIS system, reflecting all aspects of the integration of subsystems of industrial safety and security of the object.



Fig.2. Experion Industrial Security (EIS) system architecture form Honeywell company

## 2.1. KITSO subsystems combined in the upper level of EIS

EIS technical solution is a multi-functional integrated solution and gives a huge technological advantage in combination with products from Honeywell, proposed to build the KITSO subsystems integrated into the EIS.

### 2.1.1. Temaline Access Control System solution as base for access control subsystem

Temaline Access Control System solution for access control subsystems (ACS) provides the following advantageous characteristics:

- 1) Excellent fault tolerance at the controller level in combination with a robust and accelerated intercontroller information exchange;
- 2) Scalability of the system, constructed on the basis of TCP/IP stack of protocols;
- 3) Multifunctionality of the system - ability to track records time and attendance, checking data on intrusion detection for protected areas, direct integration with the information systems of enterprise resource planning (SAP) layer;
- 4) Advanced security settings of ACS system:
  - control of the route by forcing readers for maintaining a fixed path to the destination;
  - single and double transit, allowing access only in the case of two active cards in the reader;
  - the function of escort, allowing access of an employee to a specific zone only if the support of the employee by another authorized employee;
  - zones control, enabling the configuration of a specific access to certain areas according to the required conditions (the maximum number employees in the zone, the minimum number of employees in the area, a limit on the time an employee spent in the area, etc.).

### 2.1.2. DVM Video Management System solution as base for CCTV subsystem

DVM Video Management System solution for video surveillance subsystems, monitoring and control in real-time mode ensures the achievement of the following predominant characteristics:

- 1) Scalability of the system;
- 2) Possibility of simultaneous observation of multiple objects;
- 3) Improvements in the efficiency of operational activity and notifications about emergency situations - setting the standard automated tasks in the alarms lists, quick access to video from any display of subsystems of the Experion family, fast analysis with simultaneous playback and search functionality of motion in the video;
- 4) Optimized cost effectiveness of solution based on the use of existing data networks;
- 5) Highly reliable architecture based on redundant servers;
- 6) Possibility of access using various types of HMI - web access, specialized surveillance station, Experion control systems operators station;
- 7) Optimized hardware, made on the basis of last generation information technology - Virtualization.

Here we would like to digress to tell you about another unique information technology used by Honeywell as part of a comprehensive Experion solution - Virtualization technology.

Virtualization of an Experion system involves allocating Experion system and application nodes to virtual machines rather than physical machines. A key aspect of an Experion system that is deployed with virtualization is the addition of the virtual infrastructure. The virtual infrastructure is comprised of the hardware and software components required to host and manage the system. Some important characteristics of a virtualized Experion system that include:

- The Experion production workload is consolidated on ESXi server grade hosts and connected to a production network;
- The production ESXi hosts are also connected to a separate management network to isolate the traffic generated from management of the ESXi hosts and virtual machines from that of the production network;
- The production ESXi hosts are optionally connected to a separate storage network;
- The virtual infrastructure management workload is consolidated on a separate ESXi host that can be shared between production and application levels of the system;
- Workload distribution strategies for optimum performance and minimal scope of loss;
- Use of thin clients to provide user interaction with virtual desktops. No Experion application software is installed on the thin client;
- Workload backup and recovery strategies to minimize downtime in the event of a host or virtual machine failure;
- Hardware and software update strategies to maximize efficiency and minimize downtime and/or scope of loss.

Virtualization of Experion system is a prime example showing the replacement of system hardware and software part through the introduction of advanced information technology, which significantly reduces costs and

simplifies maintenance of management systems.

### 2.1.3. Perimeter intrusion detection subsystem

This subsystem can be built on different technical solutions being used in the early stages of construction, and selected on the basis of landscape features of the object's location, climate and weather conditions and be easy to deploy this specific system in the conditions of the region.

Here it is possible to highlight the technology of strip sensitive fiber-optic cable, allowing:

- to provide a detection of signal when approaching to main gas and oil pipelines, as well as tracking the movement of the scraper (pig) in real time;
- to provide intrusion detection at the perimeter of industrial facilities;
- to provide remote monitoring of the working conditions of rotating machines;
- to provide additional functionality to detect leaks of gaseous products.

### 2.1.4. Radar video surveillance (RVS) technology as base for Dynamic acoustic sensing subsystem

This subsystem refers to the number of advanced control systems for extended perimeter and provides:

- reduction of expenses on implementation due to the minimum quantities necessary equipment, able to cover the desired coverage area;
- the possibility of observation in all weather conditions, at any time without gaps in the aspect of industrial safety and security;
- greater accuracy of location determination and tracking of suspicious objects outside the perimeter;
- automatic simultaneous tracking of multiple objects;
- enhanced perimeter protection with fewer false alarms.

### 2.1.5. Life Safety Manager solution as base for protection of life and health of employees

Integration into the EIS of the Life Safety Manager subsystem provides a consolidated view of critical systems of an industrial facility during emergencies, and acts as a single point of management for quick response. Automation of complex system of relations through EIS, such as the inclusion of dampers, run vent fans, stopping processes and cut production units under the conditions of fire and gas detection, can save time and minimize damage when an emergency situation.

Integration of fire protection in EIS also means that other units of the enterprise are able to more prompt notification of alarms and response. The security system can support comprehensive protection of the object, providing a more efficient unlock of specific doors on the basis of the alarm to expedite emergency evacuation and access for emergency crews. Built-in digital video and audio provide a comprehensive assessment of the alarm at the EIS station, allowing the operator to immediately assess the incident and to provide a continuous record of any door that is used for output. Integration of Life Safety

Manager subsystem at EIS also provides the ability of making checking lists for collection of evacuated staff from the relevant point of an emergency evacuation.

Equally important is the question of testing and certification by a competent expert organizations when it comes to systems for the protection of life and health of employees. The technical solution of EIS Life Safety Manager has been tested and registered by the experts of the organization Underwriters Laboratories (UL) in several categories, including the most stringent Category for subsystems of fire control that allows it to be used as the primary means for the control and management of fire protection facility.

It's interesting to mention here that Safe Failure Fraction (SFF) parameter which is one of most important system reliability evidences is not less than 99,99 % which is excellent result.

Formula used for SFF parameter calculation tests is as below:

$$SFF = \frac{\sum \lambda_s + \sum \lambda_{DD}}{\sum \lambda_s + \sum \lambda_{DD} + \sum \lambda_{DU}} = \frac{\sum \lambda_s + \sum \lambda_{DD}}{\sum \lambda_s + \sum \lambda_o} = \frac{\sum \lambda_s + \sum \lambda_{DD}}{\sum \lambda}$$

where  $\lambda_{DD}$  – fault rate for detected dangerous failures;

$\lambda_{DU}$  – fault rate for undetected dangerous failures;

$\lambda_D$  – fault rate for all dangerous failures;

$\lambda_s$  – fault rate for safe failures.

### 2.1.6. Leading solution from Honeywell in the area of process control and industrial safety and security systems integration based on the Experion solutions

No doubt that absolutely unique software and hardware solution from Honeywell is to create a single, centralized system that combines all of the safety and security subsystems on the object and subsystems for automated control of production and auxiliary processes. The basis for this solution is a family of Experion software products, presented in this case by the Experion Industrial Security (EIS) system and Experion Process Knowledge System (EPKS).

A visual representation of the Honeywell solution for integration of Experion family systems is presented in figure 3.





This is blank Page