Information & Security

Published since 1998

S. Dotsenko, O. Illiashenko,
S. Kamenskyi & V. Kharchenko
vol. 43, no. 3 (2019): 294-304
https://doi.org/10.11610/isij.4322
ISSN 0861-5160 (print), ISSN 1314-2119 (online)

Research Article

Integrated Security Management System for Enterprises in Industry 4.0

Sergiy Dotsenko [a], ***Oleg Illiashenko*** [b] (✉),
Sergii Kamenskyi [a], ***Vyacheslav Kharchenko*** [b]

[a] *Ukrainian State University of Railway Transport, Kharkiv, Ukraine*
http://kart.edu.ua/en

[b] *National Aerospace University "KhAI", Kharkiv, Ukraine*
https://khai.edu

ABSTRACT:

This paper presents results from the analysis of methodologies and standards aiming to meet the requirements to security management of enterprises implementing Industry 4.0 principles. Key standards such as ISO/IEC 7498, 15408, 18045, 20000, 27000 have been analysed to suggest an approach to the development of integrated security and safety management system structure considering threats of intrusion into physical, information and signal spaces. This system, based on the cybernetic principles of control, is part of the enterprise management system. Security subsystems check and control according to individual and general objectives for physical, information and signal spaces and respective requirements-based models. On that basis the paper presents results and recommendations for enhancing and implementing integrated security management systems.

ARTICLE INFO:

RECEIVED: 20 AUG 2019
REVISED: 03 SEP 2019
ONLINE: 22 SEP 2019

KEYWORDS:

security, safety, enterprise management system, control system, standards, integrated security management system, industry 4.0

✉ Corresponding Author: Tel.: +380954676066; E-mail: o.illiashenko@khai.edu

Introduction

The task of developing and implementing the enterprise security management systems is becoming increasingly important at the point of view of the losses associated with a security breach resulting from management.[1,2] Additional challenges for creating security management systems take place while developing the Industry 4.0 strategy.[3,4,5] The goal of implementing the enterprise security management systems is to have insurance that only authorized personnel can make changes to the process or influence to production in a permissible way.[6]

According to ISO / IEC 7498-2:99 [7] to achieve this goal the following tasks have to be completed:

- granting the physical security by limiting access to the objects;
- realization of the control under the information flow that comes out of objects to protect intellectual property;
- realization of the control under the information flow that comes out of objects to control data transmissions;
- avoidance of influencing the production process by unauthorized remote access.

ISO / IEC 7498-2:99 [7] recommends to distribute the control object for the enterprise security management system into two components, specifically:

- technological process, that are realized in a real-time mode;
- organizational processes that are implemented beyond the boundaries of technological processes (physical processes) and provide the organization of technological processes.

In the theory of automatic control, the development of an appropriate control system begins with the study of the model of the control object. Having investigated the model of the control object, decisions are made on the application of the control laws of the corresponding control object. The basic control law is the negative feedback control.

On the other hand, in the theory of management for the organization of the control system it is enough to define the elements of the management cycle. A classic example of such a system is the quality management system according to the standards of the ISO 9000 series. In this methodology a management cycle is used, known as the Deming-Shewhart cycle, specifically: “Plan – Act – Check – Implement.” At the same time, the objects of management are products, processes and systems.

Another situation arises during enterprise security system management. In this case, all possible aspects of the organization and activities of the enterprise have to be potentially analysed as a security system. At the same time, it is previously unknown which of the aspects of the organization and activity of the enterprise has the greatest importance.

The special attention should be paid to the following circumstances. Formation of the enterprise security system should begin to be engaged at the

stage of formation of the enterprise. After all, security problems could be already identified at the stage of enterprise formation.

So, it is necessary to compare two methodologies for the formation of a security control system. The *object of control* for each of these methodologies has to be the *enterprise security system*. Therefore, the task is the formation of a control object in the form of a security system. On the basis of its analysis, it will become clear which control methodology should be implemented to provide the required quality for the management of security system. Additionally, it is important to determine the features of its construction for modern enterprises in the era of Industry 4.0 and integration in the overall structure of the management of such enterprises.

The goal of this research is to analyse the methodologies for developing an integrated security management system structure as a component of enterprise management systems in the context of Industry 4.0.

Analysis of Methods of Forming Enterprise Security Systems

Enterprise security systems are based on the approach introduced in a series of ISO / IEC 15408 standards [8, 9, 10] and is intended to protect information from unauthorized disclosure, modification or loss of its usability. Security categories related to these three types of security breaches are commonly called *privacy*, *integrity*, and *availability*.

This system of standards refers to the security system of information technology objects that the consumer intends to put in their own activities. This standard series introduces a different approach to presenting enterprise security. Of the five security services that are dealt with in the standard ISO / IEC 7498 – 2 [7] examines three types of security breaches that are relevant to the specified services, specifically: *confidentiality*, *integrity*, *availability*.

According to ISO / IEC 15408-1 [8] security is concerned with the protection of assets. Many assets are represented in the form of information that is stored, processed and transmitted by IT products to meet the requirements laid down by the owners of the information. Availability, distribution and modification of any such information have to be strictly controlled and the assets have to be protected from threats by countermeasures. In this security system, the main object of control is the *risk*. To provide a specified level of risk, an assessment of the Target of Evaluation (TOE) and development of appropriate countermeasures should be done. TOE according to ISO / IEC 15408-2 [9] is defined as a set of software and firmware complexes accompanied by user and administrator guidance documentation.

The evaluation is carried out by special construction, specifically: security target (ST). According to ISO / IEC 15408-1 [8] the ST begins with describing the assets and the threats to those assets. The ST then describes the countermeasures (in the form of Security Objectives) and demonstrates that these countermeasures are sufficient to counter these threats: if the countermeasures do what they claim to do, the threats are countered.

To unify the activities for the development of ST in the standard [8] the universal design in the form of a Protection Profile (PP) is proposed. Term "Security functional requirements" provided on the base of "Functional requirements paradigm."[9] Functional safety components are implemented based on functional safety requirements.

According to ISO / IEC 15408-2 [9] TOE is concerned primarily with ensuring that a defined set of security functional requirements (SFRs) is enforced over the TOE resources. The SFRs define the rules by which the TOE governs access to and use of its resources, and thus information and services controlled by the TOE.

From this thesis it follows that the TOE manages the use and access to its resources. It follows that the structure of the TOE should include appropriate methods of management. The security mechanism is the implementation of the TOE Security Functionality (TSF), which are defined by the SFR at the stage of formation and implemented through the mechanisms that follows the established rules. The implementation of these rules provides security capabilities.

From the abovementioned follows that the provision of information security on the stage of development and implementation of the TOE is an important part of the management of enterprise security system.

From the above analysis of the methods of forming enterprise security systems it follows that there are two independent methods for the formation of such systems, specifically:

- formation of the security system of information technologies, which are implemented and operated at the enterprise (ISO / IEC 7498);
- formation of the security system of information technologies, which are at the development stage (ISO/IEC 15408, ISO/IEC 18045).

In investigated security systems the information technologies are considered as assets.

In ISO/IEC 15408 for information technologies the functional security requirements (ISO/IEC 15408-2 [9]) are described and the level of assurance is determined. Functional requirements relate to the relevant functions that need to be implemented in the activity.

It is clear that any security system requires proper management, so the task of analysing existing management methodologies, which is recommended for using, is appeared.

Analysis of Methods for Managing Security Systems

Information security management at the stage of development and implementation of information technologies is based on the requirements of ISO/ IEC 27001 and ISO / IEC 27002 standards as specified in ISO / IEC 15408-1. [8]

The methodological basis of this set of standards is the methodology of the formation of management systems. The most famous system of this class is the quality management system (QMS) according to the standards of the ISO 9000 series.

The management of the providing of information security services at the stage of development and implementation of information technologies is based on the requirements for management system for providing security services. This management system is based on the requirements of a set of ISO/IEC 20000 standards. This standard requires an integrated process approach at the time of planning, development, deployment, operation, monitoring, review, support and improvement of the service management system. According to the standard, a system of service provision is introduced that can be applied to provide services to the company to ensure its security. But the form of this security is not defined, that is, the model of the control object for which this system is formed is not defined.

From the mentioned above it follows that there are two approaches of ensuring enterprise security, specifically:

- security system for the reference model of interconnected open systems (ISO/IEC 7498-99);
- providing security of information technologies that are used in enterprises in the form of providing functional security and assurance to its evaluation.

At the same time, for the aforementioned approaches to ensure the enterprise security, respectively, different management methods are used, specifically:

- administrative management of system security, security services, security mechanisms, as well as the system of administrative management of security of interconnected open systems;
- management system in two alternative variants: according to ISO/IEC 20000 or to ISO/IEC 27000.

The question arises how these two security management methods are related. To answer this question, the existing methods of integration of management systems and enterprise management systems are considered.

Integration of Management Systems and Enterprise Security Management Systems

Integration of Management Systems

Integration of enterprise management systems is based on the publicly available specifications PAS 99: 2006. ISO Guide 72 for standards developers includes the basis for common requirements set in standards for management systems. The public technical specifications PAS 99: 2006 are applicable to the standards of the ISO/IEC 27001 series, ISO/IEC 20000-1, ISO/IEC 20000-2, that is, to the standards that are applied to ensure the information security of the enterprise.

While choosing for application the standards of series ISO/IEC 27000 or ISO/IEC 20000 the following uncertainties are arisen. The ISO/IEC 20000 series of standards is *explicitly* based on the ISO 9000 series methodology, for which the method of forming a management object model is not defined. The ISO/IEC

27000 series of standards is *implicitly* based on the ISO 9000 series methodology, but the management object model is explicitly defined in the form of "activities (as processes) for providing information security" for it.

Integrated Enterprise Security Management System

The integration of enterprise management systems is based on the series of standards IEC 62264-1-2014. In this case, integration means the following: [11] "Successfully addressing the issue of enterprise-control system integration requires identifying the boundary between the enterprise and the manufacturing operations and control domains (MO&C). The boundary is identified using relevant models that represent functions, physical equipment, information within the MO&C domain, and information flows between the domains."

This method of integration is based on the functional representation of the enterprise. It involves the integration of enterprise management systems and production process management systems, that is, the integration of the two control systems of parts of the enterprise into a whole one.

From the analysis of the mentioned integration methods it follows that at present time two methods of integration of enterprise management systems are proposed, specifically:

- integration of management systems based on a single element set of the management cycle (ISO 72);
- integration of two forms of management systems, specifically: the enterprise management system and production process management system (IEC 62264-1-2014).

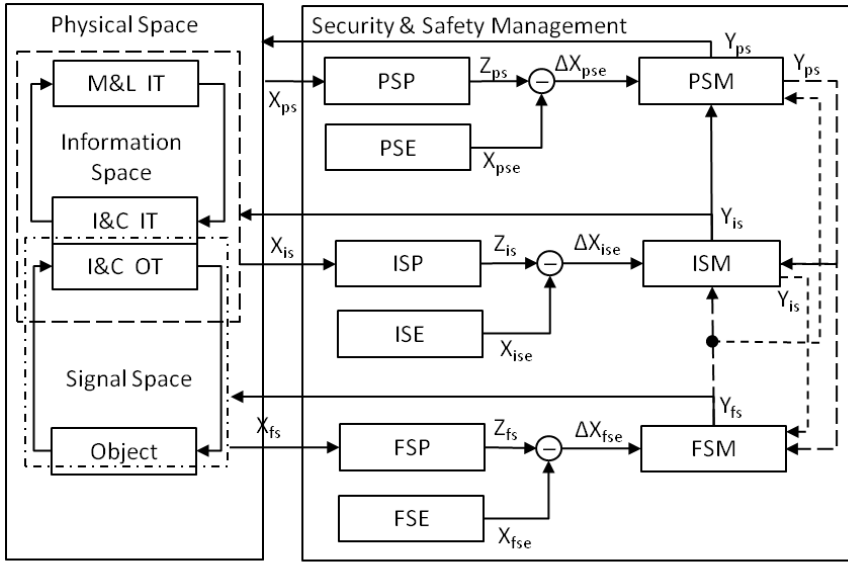
The basis of these two forms of integration is the functional representation of the enterprise.

However, based on the requirements of IEC 62264-1-2014, from a security point of view, the most significant should be the methodologies of enterprise modelling, in which the physical, informational and cybernetic (in the form of data transmission) representations should be presented in an explicit form.

On this basis this, Figure 1 presents an integrated enterprise security management system, which is proposed in. [12] The architecture of each channels of this management system is similar to the architecture of the operation management system.[13]

For the composition of the system it is proposed to introduce three mutually connected areas of security on the levels of *physical*, *information* and *signal spaces*.

Let us examine the work of the system on the example of the safety management channel "Physical Space." Signals about the enterprise security state as a physical object (X_{ps}) are transmitted to the PSP block where the appropriate diagnosis (Z_{ps}) is formed. This diagnosis is transferred to the adder. In the adder it is compared with the reference value (X_{pse}), which is formed in the PSE block, and the formation of the control signal as the difference (ΔX_{pse}) = (Z_{ps}) - (X_{pse}) is provided. Under the action of the resulting signal in the PSM block, a *control*



M&L – management & logistic; I&C – instrumentation & control;
OT – operation technical; IT – information technical; PS – Physical Security
IS – Information Security; P – processing; E – Etalon; M - Maker

Figure 1: Integrated Safety-Security Management System.

action is formed that guides to the processes in the *"Physical Space*." A similar algorithm is implemented in the "Information Space" and "*Signal Space*" channels.

The integration of control channels is carried out by transferring control signals from the "Physical Space" (PSM block) channel to the inputs of the ISM and FSM units. Due to this, "Information Space" and "Signal Space" channels are controlled taking into account the state of the "Physical Space" management channel.

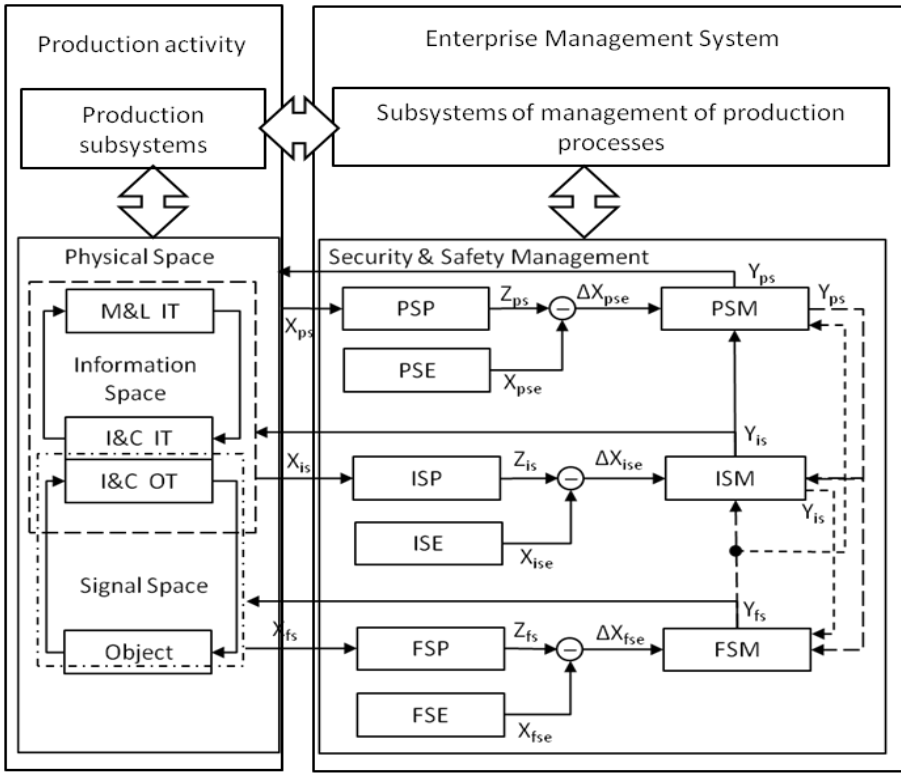
Additionally, the control commands from the ISM and FSM units proceed to the PSM block. For this reason, control action in the PSM block is formed taking into account the state of the channels "Information Space" and "Signal Space."

The enterprise security management system, which is shown in Figure 1 corresponds to the principle of constructing the hierarchical control systems based on the integration of the appropriate channels of the control system. By the content of the *control law*, this system refers to *cybernetic control systems with feedback,* so it can be described with the appropriate mathematical apparatus. This will ensure its formation as an *automated system of dialog enterprise security management*, or a *decision support system* in the management of enterprise security.

It should also be noted that the usage of the developed security management system has certain features. It differs for enterprises that are software developers or project designers. They do not have a level of functional security (I&C OT) and a sub-level of information security (I&C IT).

Embedding of Integrated Security Management System into Enterprise Management Systems in the Context of Industry 4.0

The considered system (Figure 1) is part of the overall enterprise management system. Integrated enterprise management system with enterprise security management system is presented in Figure 2.



M&L – management & logistic; I&C – instrumentation & control;
OT – operation technical; IT – information technical; PS – Physical Security
IS – Information Security; P – processing; E – Etalon; M - Maker

Figure 2: Integrated Enterprise Management System with the Enterprise Security Management System.

The integration of the enterprise security management system into the enterprise management system involves the interaction of the subsystems of production process management with the security management subsystems. Similar interaction exists between production subsystems and subsystems that describe the signalling, information and physical security levels.

It should be noted that the formation of security subsystems the indicated levels can be carried out using various methods of forming management systems, and management, which were described above.

It has been shown above that the developed and applied information technologies are based on a functional representation. At the same time, the standard of the IEC series 62264-1-2014 establishes that the most significant should be the methodology of modelling the enterprise in which the physical, informational and cybernetic (in the form of data transmission) views should be presented in an explicit form. This requirement is especially important for Industry 4.0. Global industry digitization raises the problem of cybernetic threats for any of the information processes implemented with the use of digital technologies for receiving, transmitting, storing and presenting data and information.

Conclusions

There are two independent methods of developing security systems for enterprise systems such as:

- formation of a security system for *information technologies,* that is implemented and operated by an enterprise (ISO / IEC 7498-2: 99);
- formation of a security system for *information technologies*, which are at the stage of development (ISO / IEC 15408, ISO / IEC 18045: 2008).

At the point, for the aforementioned approaches to ensure the security of enterprises different management methods are used, respectively:

- *administrative* management of system security, security services, mechanisms of security, as well as the system of administrative control of interconnected open systems;
- *management system* in two alternatives: according to ISO / IEC 20000-1 or ISO / IEC 27000.

The enterprise security management system, which is shown in Figure 1 corresponds to the principle of constructing the hierarchical control systems based on the integration of the corresponding channels of the control system. By the content of the control law, this system refers to cybernetic control systems with feedback, so it can be described with the appropriate mathematical apparatus. This will ensure its formation as an automated system of enterprise security dialogue management, or a decision support system in the management of enterprise security.

The subsystems of the integrated enterprise management system with the enterprise security management system should be formed taking into account the forms of production subsystems of the enterprise and security subsystems,

specifically: signalling, information and physical views. For the effective implementation of the Industry 4.0 concept, it is expedient to integrate the integrated enterprise security system into the enterprise management system.

The developed safety and security management system conception and models have been adopted and implemented at the PC "RPC Radiy," Kropyvnytskyi, Ukraine and PrJSC FED Kharkiv Ukraine.

Acknowledgements

This work was supported by the ECHO project which has received funding from the European Union's Horizon 2020 research and innovation programme under the grant agreement no. 830943.

The authors appreciate the scientific society of the ECHO consortium and in particular the staff of Department of Computer Systems, Networks and Cybersecurity of the National Aerospace University "Kharkiv Aviation Institute" for invaluable inspiration, hardworking and creative analysis during the preparation of this paper.

References

[1] Roberto Mejias, "An Integrative Model of Information Security Awareness for Assessing Information Systems Security Risk," *Proceedings of the Annual Hawaii International Conference on System Sciences* (2012): 3258-3267, https://doi.org/10.1109/HICSS.2012.104.

[2] Princely Ifinedo, "Understanding Information Systems Security Policy Compliance: An Integration of the Theory of Planned Behavior and the Protection Motivation Theory," *Computers& Security* 31, no. 1 (February 2012): 83-95, https://doi.org/10.1016/j.cose.2011.10.0076.

[3] "Smarter Security for Manufacturing in The Industry 4.0. Era: Industry 4.0 Cyber Resilience for the Manufacturing of the Future," White Paper, Symantec, 2017, https://www.symantec.com/content/dam/symantec/docs/solution-briefs/industry-4.0-en.pdf.

[4] "Systems Integration for Industry," *Automation.com*, November 03, 2015, https://www.automation.com/automation-news/article/systems-integration-for-industry-40.

[5] Adil Kondiloglu, Harun Bayer, Enes Celik, and Muhammet Atalay, "Information Security Breaches and Precautions on Industry 4.0," *Technology Audit and Production Reserves* 6, no. 38 (2017): 58-63.

[6] ISO/IEC 7498-1:99 Information technology - Open Systems Interconnection - Basic Reference Model, Part 1: The Basic Model, 1999.

[7] ISO/IEC 7498-2:99 Information technology - Open Systems Interconnection - Basic Reference Model, Part 2: Security Architecture, 1999.

[8] ISO/IEC 15408-1:2009 Information technology — Security techniques — Evaluation criteria for IT security, Part 1: Introduction and General Model, 2009.

[9] ISO/IEC 15408-2:2008 Information technology — Security techniques — Evaluation criteria for IT security, Part 2: Security functional components, 2008.

[10] ISO/IEC 15408-3:2008 Information technology — Security techniques — Evaluation criteria for IT security, Part 3: Security assurance components, 2008.

[11] IEC 62264-1-2014 Enterprise-control system integration - Part 1: Models and terminology, 2014.

[12] Vyacheslav Kharchenko, Sergiy Dotsenko, Oleg Illiashenko, and Sergiy Kamenskyi, "Integrated Cyber Safety and Security Management System: Industry 4.0 Issue," *Proc. of the 10th IEEE Dependable Systems, Services and Technologies Conference, DESSERT 2019*, Leeds, United Kingdom (2019): 197-201.

About the Authors

Sergiy **Dotsenko** is Doctor of technical sciences, associate professor, professor of department of specialized computer systems at Ukrainian State University of Railway Transport, Kharkiv, Ukraine. His research interests are in natural intelligent systems and intelligent information technologies.

Oleg **Illiashenko** holds a PhD in technical sciences. He is senior lecturer in the Department of Computer Systems, Networks and Cybersecurity, National aerospace university "Kharkov Aviation Institute," Kharkiv, Ukraine. His research interests are in models, methods and instrumentation tools for cybersecurity assessment, evaluation and assurance of cybersecurity of software and hardware, safety and cybersecurity co-engineering, dependability and resilience of embedded, web, cloud and IoT systems.

Sergii **Kamenskyi** is postgraduate student at the Ukrainian State University of Railway Transport, Kharkiv, Ukraine, and Head of the Complex Solutions department at the IPCOM group of companies. His research interests are in organizational structures, cybersecurity, devices in IOT systems, industrial controllers for remote monitoring systems.

Vyacheslav **Kharchenko** is Doctor of technical science, professor, Head of the Department of Computer Systems, Networks and Cybersecurity, National aerospace university "Kharkov Aviation Institute," Kharkiv, Ukraine, and Head of the Centre for safety infrastructure research and analysis, RPC Radiy. His research interests are in fundamentals and methods of critical computing, safety and security IT-engineering, technologies of regulation, development, assessment of dependable software and systems.