EAI Endorsed Transactions
on Energy Web

Research Article EAI.EU

Application of a Hybrid Method for Key Energy Facilities Safety Assessment

I.I. Livshitz [1,*], P.A. Lontsikh [2] and E.P. Kunakov[3]

[1]PhD, SPIIRAS, St. Petersburg, Livshitz.il@yandex.ru
[2]Doctor of Science, Irkutsk National Research Technical University, palon@list.ru
[3]Postgraduate, Irkutsk National Research Technical University, egor-kunakov@mail.ru

Abstract

Information Technologies (hereinafter – the “IT”) without security functions (hereinafter – the “SF”) are the exception rather than the rule nowadays [1 – 4]. Components of IT without SF are not a big problem since they can be replaced by analogs, which SF have, or can be supplemented by the necessary "imposed" SF, or we can "import" the required SF from the adjacent components of IT, which are an integral part of the information processing system (hereinafter – the “IPS”). Speaking further of IT, we will assume that the modern IT components presented in the competitive market for energy facilities (hereinafter – the “EF”) already have a certain set of SF and are able to support IT-security tasks (hereinafter – the “IST”).
Many scientists have done enough research on various safety issues at facilities and published their results [5 – 13]. These studies also concern the causes of various incidents at key facilities, especially energy ones, risk identification, and the analysis of the consequences for safety.
Against this background, the problem of adequate IT-security assessment of the EF is particularly relevant [14 – 16]. Indeed, why should we spend the resources on the implementation of additional "superimposed" SF in IPS, if there is an opportunity to optimize costs by using existing and practically "spent" SF? In this case, a reasonable solution would be to assess the existing level of IT-security related to the architecture of IPS resulting from the composition of IT-components that have SF for key EF [17 – 21]. Based on the results of the evaluation, it is possible to make a decision on the implementation of new additional SF in IPS based on documented facts.

Keywords: Fuel, energy, assessment, security, information, function, risk, vulnerability, threat, ISO, IEC, requirement.

Received on 05 May 2018, accepted on 03 July 2018, published on 28 January 2019

doi: 10.4108/eai.13-7-2018.156386

*Corresponding author. Email:Livshitz.il@yandex.ru

1. Problem-solving approaches

The problem in this IT-security subject area can be solved in the presence of the following types of expertize:

(i) Individual expertize (IE) inherent to its carrier. This is the well-known "mega light head". Advantages – compliance with the principle of "it is". Disadvantages – a search for a quality carrier is a non-trivial task, and the aggregation of several carriers is often difficult.

(ii) Template expertize (TE) recorded in the form of documented requirements. These are all well-known normative documents for EF of different levels (for example, IEC 61508, 61511). Advantages – primary sources are available. Disadvantages – a large "division price", hence – a significant error.

(iii) Calculation expertize (CE), based on the composition of measurement and calculation techniques. This is a typical modern approach to engineering and scientific problems. Advantages – accuracy due to

the qualified choice of the measuring instrument. Disadvantages – a certain qualification is required to select the instrument and determine the correct measurement technique that gives reproducible results.

A number of authors have noted only expert approaches (like IE), as various experts have been widely known and demanded for a long time. At the same time, there are very few examples of computational methods applications, i.e. those that provide numerical estimates (like CE). There are also few examples to ensure the safety of objects, complex technical systems, industrial facilities and key objects, because it is difficult to derive accurate mathematical formulas for them [5 – 13]. For key energy facilities, it is particularly important to provide a chain of evidence of a particular management decision and provide evidence of its effectiveness to ensure safety [10, 11].

The problems can be successfully solved by using one type of expertize, and any combination thereof. Question is in search of the optimal combination of types expertize, providing for a particular EF mutual compensation of shortcomings and strengthening of advantages. Graphically, the area of combinations of expertize can be represented as a triangle (see figure 1).

From this follows that for IPS the point of combination of examinations "A" lies on the side of the triangle IE-TE. It is clear that such position of the point is not a "a limit to somebody's ambitions", and resources for a more accurate assessment of IPS safety are available. To do this, it is necessary to shift the point of combination of expertize from the side of the IE-TE into the triangle in the direction of the CE vertex (point "B").

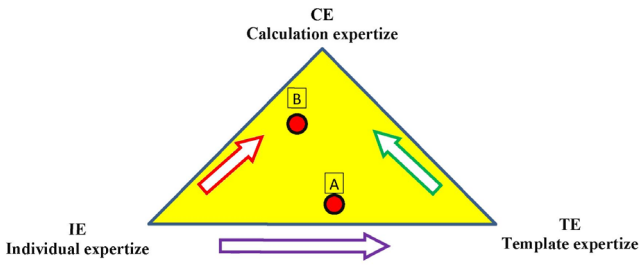

Figure 1. Combinations of expertizes

For filling the pole TE is recommended by well-known references [18, 19, 22 – 24]. Some comments should be defined about what ISO/IEC 15408 can be used not only for filling the "pole" of the TE, but also for filling the "pole" of the CE, due to a fairly small division and laid ISO/IEC 15408 opportunity almost any adaptation of the functional safety requirements and the requirements of the trust IT-security under the current need for specific solutions in the critical energy sector.

To fill the "pole" CE is also used time–tested tool: know-well Data flow diagram (hereinafter – DFD). DFD is one of the main tools of structural analysis and design of IT-systems and functional analysis. Despite the shift of emphasis from a structural to an object-oriented approach in the analysis and design of critical IT-systems, structural notations are still widely and effectively used in both business analysis and IPS analysis.

Based on known needs to provide the chain of evidence specific management decisions and evidence of their effectiveness for security for key energy facilities, you need to consider the particular factors which will help to solve this problem.

2. The new hybrid method

The main idea of the new proposed hybrid methodology for IT-security assessment is on the one hand shaping out a methodology, applicable to the IT-security assessment for any IT, on the other hand, a possibility to easily adapt the methodology to the specific features of a particular IPS.

None of the existing methods of IT-security assessment does allow to evaluate simultaneously and in the context of SF its components and in the context of management measures of the IST. The new proposed hybrid methodology for assessing IT-security based on ISO and ISO/IEC standards 15408, 27001, 27005 and DFD allows such assessment. Naturally, it implies the presence of experts with corresponding qualifications. It should be noted that the removal of at least one component from this methodology entails its complete disintegration.

If it is necessary to evaluate the IPS operating in the mode close to the real–time mode (hereinafter – RTM), the hybrid method of IT-security assessment based on ISO and ISO/IEC standards 15408, 27001, 27005 and DFD can be supplemented by provisions from the theory of automated control, functional safety requirements (for example, IEC 61508 and IEC 61511). At the same time, it should be noted that elimination of duplication, redundancy and inconsistency of requirements when adapting the hybrid method of IT-security assessment to the specifics of a particular IPS provides significant resource savings at the stage of IPS assessment. As an example, let us briefly consider the hybrid methodology of IT-security assessment based on ISO and ISO/IEC standards 15408, 27001, 27005 and DFD, applied to one example of the object of assessment (hereinafter – OA) functioning in the RTM. Evaluation is a traditional way of building trust.

It should be explained why in our opinion (as mentioned above) the new proposed hybrid methodology based on ISO and ISO/IEC standards 15408, 27001, 27005 and DFD is minimum required methodology for assessing IT-security. It is not possible to remove the ISO/IEC 15408, as this standard is the "core" of the methodology and the source of functional safety requirements and safety credibility requirements. It is not possible to remove ISO/IEC 27005 because this standard applies to risk assessment. It is not possible to remove

DFD because this tool is used to model IPS and determine its structure. It is not possible to remove ISO/IEC 27001 as this standard applies as the only "standard of requirements" when formulating requirements to management of IST.

Taking advantage of the fact that ISO/IEC 15408 "provides flexibility allowing the use of a variety of assessment methods in relation to a variety of security properties of a variety of it products", ISO/IEC 15408 used to the extent, and in a format in which it was possible to avoid excessive complication of the procedure for assessing the security of such complex and multidimensional composition of the OA. It was taken into account that "users of this standard should exclude the possibility of misuse of this flexibility of the standard". That is why the hybrid IT-security assessment methodology does not provide for the development of a single IST, or a set of IST, as could be done if the ISO/IEC 15408 is followed literally and dogmatically.

Therefore, the new hybrid methodology for assessing IT-security provides for the decomposition of IT, as OA, into two parts: "clean IT" and the boundaries of trust, defined as part of IT on the IPS model using DFD. It is the boundaries of trust (in the notation ISO/IEC 15408 – trusted boundary", TB) that are put in line, on the one hand, the functional requirements of safety and security requirements of ISO/IEC 15408, and the requirements for the management of IST based on ISO/IEC 27001, and on the other hand, the means of processing information in which the boundaries of trust are implemented. The new hybrid method of IT-security assessment for EF provides the following sequence of steps:

- IT structuring;
- Structuring of physical space;
- Formation of the SOY model;
- Definition of security problems;
- Definition of safety objectives;
- Definition of security requirements;
- Brief specification of the object of assessment.

IT Structuring

Perform structuring of the IT totality, ensuring automatization of business-processes of the complex objects, several fields (hereinafter – Realm, R).

The structuring of physical space

Running the structuring of physical space occupied by the assets of the organization, in several locations (hereinafter – Location, L).

3. The formation of the IPS model

Formation of IPS model, on the basis of which it is implemented, is based on DFD. The number of developing models of IPS was determined based on considerations of convenience, the sake of completeness IT based on the specific details to achieve the objectives of the evaluation.

For one IPS, if necessary, more than one model can be formed. At the same time a few IPS are similar to each other and can be formed by one model. It is possible to form a single partial model for several partially similar to each other IPS and the formation of various partial models for parts of IPS that are not exactly similar to each other. An example of a IPS model of a real OA operating in RTM is shown in figure 2.

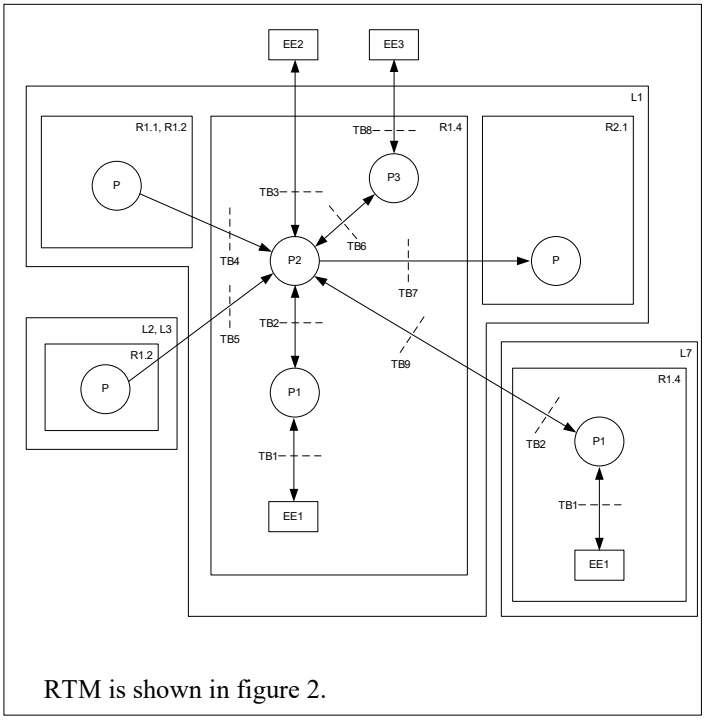

Figure 2. An example of a IPS model of a real OA operating in RTM

Here it is necessary to make a retreat and focus attention on the fact that threats are determined precisely through risks, as typically shown by the international practice [18, 19], for the real world objects, first of all – for fuel and energy facilities. In accordance with Annex C of requirements ISO/IEC standard 27005, a certain list of typical threats shall be taken into account.

In accordance with Annex C of standard [19], applicable threats are ranked by defining a risk measure. The definition of the risk measure and the results of the ranking of the applicable threats are presented in table 1. The degree of probability and the magnitude of the effects are determined by the ranking scale in ascending order from 1 (minimum) to 5 (maximum). The above-mentioned ST without specification of the type of threat source [19] (it can be personnel, natural phenomena or manifestations of technical disasters), carries main types of threats [22 – 24].

Table 1. Definition of risk measure and ranking of applicable threats

IT-Security Threats	Severity	Probability	Risk	Risk Treatment
Fire	5	1	5	Need
Major accident	5	1	5	Need
Disclosure	2	1	2	No
Criminal use of hardware	2	1	2	No
Criminal use of the software	2	1	2	No
Equipment failure	1	1	1	No
Violation of information system maintenance	2	1	2	No
Error while using	1	1	1	No
Abuse of rights	1	2	2	No
Denial of action	2	1	2	No
Violation of staff performance	2	1	2	No

Identify a security problem

Identification of the IT-security problem for key EF implies a consistent identification of security threats (hereinafter – STr), security policy of the company and security assumptions for the operation environment.

It is important to take into account that solutions to the safety issue of key energy facilities should consider the requirements of compliance with the recognized international standards in this area ([18, 20, 22 – 24]).

IT-Security threats

The threats that should be opposed to the OA are determined by the risk register (e.g. increasing importance). The register of risks for EF is either formed on the model of IPS, or it uses the already existing one in the company [18, 19]. In the practice of IT-security audits, as a rule, a good "starting point" is the result of audits, for example, compliance with the requirements of ISO/IEC standard 27001 [14 – 16]. It is important to take into account that for key energy facilities the solution of the security problem requires to consider vulnerabilities and threat analysis, as suggested in a number of works [3 – 9]. Such requirements may be provided in compliance with applicable international standards [18, 19].

Safety objective

The security objectives are a concise and abstract statement of the intended solution to the issue outlined above. Security objectives have a triple role:

- provide a high-level natural language description of the issue;
- divide this decision into two parts (object of evaluation and the environment of operation), reflecting that different entities solve their part of the problem;
- show that these parts of the solution form a complete solution.

Based on the security objectives and justification of security objectives, it is concluded that in case all security objectives are achieved, the security problem stated above is solved, that is, all threats are met, all security policies of EF are implemented, as well as all security assumptions.

Brief specification of the object of assessment

Brief specification of OA contains information for the owner of OA about how a specific OA meets functional safety requirements, IT-security requirements [22 – 24] and the requirements for management of IST [18, 19]. The correlation between the IPS model and its corresponding real IPS is described in the natural language. Each DFD notation of the model is associated with the specific tool of IT processing, a communication channel, or method of TB implementing.

4. Assessment results

The new proposed hybrid methods of IT-security assessment for the EF result in documentary evidences of the countermeasures sufficiency and correctness that the OA owner receives. Sufficiency level of the countermeasures is determined in the measuring units – functional security requirements mapped to the TB. The correctness of countermeasures is determined in measured units – the requirements of confidence in the security and management requirements of the IST. Sufficient and correct countermeasures minimize the risks to the assets of a particular EF. Thus, trust is achieved through evaluation of IT-security assessment).

This methodology provides reproducible and objective evidence of the OA assessment, which can be presented for verification to an independent group of properly qualified appraisers . The assessment report is a strong argument in favor of IT-security expressed in measurable values, based on the system [22 – 24], which allows to operate them for the benefit of any key EF. For key energy facilities the solution to the issue of security requires mandatory compliance audits. This process means that any facility must provide comparable and impartial security assessments. These assessments can only be obtained by independent groups of auditors that perform compliance assessments based on recognized standards and reliable data [14, 16].

Conclusion

A characteristic feature of the presented new hybrid method is that it allows to conduct IT-security assessment on key energy facilities (like OA) of any scale, including

complex EF that work in RTM mode, when the appropriate level of detail is set. At the same time, the evaluation process must stay within the normative field of the relevant International standards, adequate to the current level of their development in the world (for example, ISO and ISO/IEC standards series 15408, 27001).

References

[1] Sokolov B. V., Yusupov R. M. Neokibernatika in the modern structure of system knowledge // Robotics and technical Cybernetics, 2014, vol. 3, Pp. 3 – 11.

[2] Yusupov R. M., Shishkin V. M. Some contradictions in the decision of information security problems // Proceedings of SPIIRAS. Vol. 6. — SPb.: Science, 2008. Pp. 39-59.

[3] Andrew Jaquith. Security Metrics: Replacing Fear, Uncertainty, and Doubt 1st Edition. Addison-Wwsley, 2007, ISBN 0785342349986/

[4] Bohme R. and S. Koble, "On the Viability of Privacy-Enhancing Technologies in a Self-regulated Businessto-Consumer Market: Will Privacy Remain a Luxury Good?," Proc. Workshop on Economics of Information Security (WEIS 07), 2007.

[5] Lo K. A critical review of China's rapidly developing renewable energy and energy efficiency policies / Renewable and Sustainable Energy Reviews. 2014. V. 29. Pp. 508-516.

[6] Bouzarovski S. Post-socialist energy reforms in critical perspactive: Entangled boundaries, scales and trajectories of change / European Urban and Regional Studies. 2010. V. 17. № 2. Pp. 167-182.

[7] Steiner A., Kohler C., Metzinger I., Ritter B., Braun A., Zirkelbach M., Ernst D., Tran P. Critical weather situations for renewable energies – Part A: Cyclone detection for wind power / Renewable Energy. 2017. V. 101. Pp. 41-50.

[8] Kramida A. Critical evaluation of gata on atomic energy levels, wavelengths, and transition probabilities / Fusion Science and Technology. 2013. V. 63. № 3. Pp. 313-323.

[9] Meyar-Naimi H., Vaez-Zadeh S. Sustainable development based energy policy making framework, a critical review / Energy Policy. 2012. T. 43. C. 351-361.

[10] Massel A.G. Cybersecurity of Russian energy infrastructure as one of critical infrastructures / Proceeding of Iternational Workshop CM/IA/CS/CI-2016. Melentiev Energy Systems Institute; Russian Academy of Science Siberian Branch. 2016. Pp. 17-18.

[11] Kumar R. A critical review on energy, exergy, exergoeconomic and economic (4-E) Analysis of thermal power plants / Engineering Science and Technology, an International Journal. 2017. V. 20. № 1. Pp. 283-292.

[12] Gaskova D.A., Massel A.G. Methods to identify critical facilities in energy with regard to analysis of cyber threats / Critical Infrastructures: Contingency Management, Intelligent, Agent-based, Cloud Computing and Cyber Security CI: CM/IACC/CS – 2018 Proceeding and programm of International Workshop. 2018. Pp. 47-50.

[13] Bilgin M. Energy transitions and international security in the twenty-first century / Political Science and International Relations, Bahcesehir University, Istanbul, 2012. Pp. 31-66

[14] Livshits I. I. Methodology of complex audits of industrial facilities for the effective implementation of energy management. Energobezopasnost' I energosberezhenie – 2015. - No. 3. - Pp. 10-15.

[15] Livshits I. I. Evaluation of the protection of objects of fuel and energy complex // energy security and energy efficiency – 2015. - No. 5. – Pp. 5-10.

[16] Livshits I. I. Introduction of energy management systems in accordance with the requirements of ISO 50001:2011 for industrial facilities // energy security and energy 2014. - No. 6. – Pp. 9-12.

[17] Livshits, I. I. The method of optimization of the audit program of integrated management systems // Proceedings of SPIIRAS. - 2016. – No. 5. – Pp. 52 – 68. DOI 10.15622 / sp.48.3.

[18] ISO/IEC 27001:2013 Information technology – Security techniques – Information security management systems – Requirements, International Organization for Standardization, 2013. – 23 pages.

[19] ISO/IEC 27005-2011 Information technology — Security techniques — Information security risk management, International Organization for Standardization, 2011. – 68 pages;

[20] ISO 19011:2018. Guidelines for auditing management systems

[21] I. I. Livshitz, D. V. Yurkin, A. A. Minyaev Formation of the Instantaneous Information Security Audit Concept. Distributed Computer and Communication Networks. Volume 678 of the series Communications in Computer and Information Science pp 314-324, DOI 10.1007/978-3-319-51917-3_28, ISBN: 978-3-319-51916-6.

[22] ISO/IEC 15408-1:2009 Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model

[23] ISO/IEC 15408-2:2008 Information technology – Security techniques – Evaluation criteria for IT security – Part 2: Security functional components

[24] ISO/IEC 15408-3:2008 Preview Information technology – Security techniques – Evaluation criteria for IT security– Part 3: Security assurance components.