Control of information security monitoring perimeter of industrial facilities

R. Fatkieva and E. Evnevich

St. Petersburg Research Center of the Russian Academy of Sciences, St. Petersburg, Russia
E-mail: rikki@mail.ru

Abstract. In the process of monitoring industrial facilities information security, the sets of heterogeneous data are generated by different monitoring tools which are to be processed according to various regulatory documents not always compatible with each other. Definition of a set of security characteristics based on perimeter monitoring data and determination of security level carried out mostly by calculating integral indicator do not take into account some aspects of security. The method is proposed for the harmonization of industrial facilities interaction and for the formation of a set of security indicators on the basis of formalized subject domain description and unified data description scheme.

1. Introduction

One of the main problems of harmonization of the systems of industrial facility (IF) monitoring and control is the underdevelopment of methodological recommendations for measurement, interpretation and estimation of performance parameters, which are represented by heterogeneous data obtained both by direct measurements and indirectly.

Solving the problem in the situation of a large number of various monitoring tools being included in the perimeter of IF requires introducing departmental legislation in the industry or making amendments to the existing operational rules within the group of enterprises of IF [1, 2]. However, such changes in regulatory documents are most often based on the integral assessments according to the criterion of achieving some objective function, which cannot always provide a required level of secure maintenance and stability of the IF complex [3-6]. All the above said reaffirms the need for harmonization procedure [2] by means of creation of self-consistent formal description of the subject domain and development of application software to support unified data scheme including the construction of terminology taxonomies, predicative relationships, descriptive restrictions for obtaining new data on the performance indicators and for expanding the set of inference rules [7-9].

1.1. Approaches to IFs control

The following approaches to control IFs distributed group are developed at the moment:

- semantic ones – those based on the analysis of terminology and conceptual descriptive apparatus of products, processes and resources of IFs and on the construction of the subject domain ontologies;
- project-framework ones – based on logical analysis of processes at different stages of the IF life cycle;
• dynamic ones – based on current monitoring state and on assessment of IF indicators such as reliability, security and resources efficiency.

In connection with the development of the industrial Internet the trend and the requirements for the development of monitoring systems with a single control center are just beginning to form. National standard (GOST) [3] explicitly indicates, for example, the possibility of using both centralized and polycentric methods of organizing monitoring and control systems. Under the above circumstances the issue of the uniformity of measurement, processing and transfer of information which is necessary for decision-making in the process of control of joint IFs performance became of special importance. In order to achieve the required level of joint operation the system coordination is required as regards all control means, methods and measures, hence the methods and algorithms for coordination of IF operational processes should be developed.

2. Harmonization method of industrial facilities interaction

Step-by-step description of the method is given below.

Step 1. Formalization of the operational processes and procedures for harmonizing the set of indicators for activities assessment (Figure 1).

Step 2. Determination of the perimeter with ensured attainment of target indicators specified at step 1 with the possibility of their modification during operation (Figure 2):

2.1. Forming a group of IFs and their operational processes for monitoring. Determination of perimeter boundaries and methods of identification of perimeter violation.

2.2. Determination of the identification policies of elements included in the IF (digital signatures, identifier hashing, tunneling) with the assignment of unique identifiers (platform metadata, keys, etc.)
according to the identification policy. The latter would enable to trace the displacement of monitoring elements within the perimeter.

2.3. IF certification.

2.4. Initializing the choice of dataset for monitoring according to the formed interaction policy.

Step 3. Development of the response system for each of the IF systems and for IF activities as a whole includes the following steps (Figure 3):

3.1. Measurements and collection of data on the system (definition of monitoring period of data collection on dynamics of objects perimeter changes).

3.2. Data processing (aggregation, definition of key information, search of signatures according to the current set of indicators changes, classification of indicators types).

3.3. Analysis of the current state (comparison with a priori created template (search for strings, regular expressions, etc.), recognition (step-by-step comparison with all signatures, comparison tree, decomposition, associative access).

3.4. Evaluation of results (analysis of distribution function changes, system topology changes, system performance changes, etc.).

3.5. State forecasting (analysis and selection of prediction algorithm depending on level, depth, horizon and distribution function change, forecast creation).

3.6. Elaboration of information security assurance measures to be undertaken.
3. Method application
Perimeter control method approbation was carried out at the industrial facility under pursuing strategic goal of reduction of integral losses by virtue of optimization of purchased tools nomenclature. In the process of the goal achievement it became necessary to make closer interaction with tools suppliers followed by the creation of unified testing base for the tools purchased being intended for cutting modes optimization. Communications with the equipment suppliers on the issues of tools ordering and tools testing via e-documents circulation and access of suppliers to testing resulted in the urgent need for perimeter monitoring with the purpose of information security assurance of the IF functioning during its interaction with the suppliers.

3.1. Step 1. Outlining the tasks for strategic goal achievement from the production part:
• reduction of losses by virtue of purchased tools nomenclature optimization, growth of the cutting modes variety, creation of electronic tools electronic data base;
• increase in tools and equipment sales and recycling.

At this step the strategic map is developed [10], set of indicators of the goal achievement together with their interrelations are outlined, scenarios of interaction in the autonomous mode and with the involvement of both internal participants and external ones – the suppliers – are formed (Figure 4).

3.2. Step 2. Formation of supplier – IF services interaction scenarios makes possible to determine:
• temporal intervals of processes under services interaction;
• intensities of state-to-state transitions;
• sets of processes performance indicators enabling to detect deviations from normal functioning;
• information assets to be protected.

Further it becomes possible to structure the list of information assets under protection, to determine the list of potential threats and to estimate probabilities of particular threats manifestation, to form sets of indicators and to determine the perimeter of protected information, the methods of protecting and identifying objects as well as to coordinate security policy between participants of the interaction.

3.3. Step 3. Certain sets of processes performance indicators serve as a basis for information security monitoring system development. Besides some new threats were identified during monitoring of the
task of optimizing the nomenclature of the purchased instrument that were not taken into account in the step 2:

- on-compliance of procured tools amount with production requirements;
- lack of coordination among the involved services and/or provision of doubtful and false information
- incorrect registration and violation of documents circulation due to software bookmarks.

Comprehensive taking into account potential threats ensured both refinement of the perimeter of protected information and identification of deviations in the production cycle and thus reduced the cost of the purchased tools by 40%.

In general the use of the method helps to optimize the purchase of a cutting tool, to reduce the number of information threats and to form e-document circulation system that enables inventory and automatic generation of replenishment orders by analyzing the dynamics of tool consumption over a calendar period.

4. Conclusion

Analysis of the results on the structural-parametric synthesis of an industrial facility and of the operational processes that take place in it demonstrated the need to introduce a system of indicators that reflect the dynamics of changes in characteristics at each level of the enterprise structure. In order to enhance the production quality it is purposeful to introduce a set of interconnected indicators of strategic goals achievement for interaction dynamics assessment and operational processes reconfiguration.

References

[1] Lakhno V, Boiko Y, Mishchenko A, Kozlovskii V, Pupchenko O 2017 Development of the intelligent decision making support system to manage cyber protection at the object of informatization Eastern-European J. of Enterprise Technologies, 2 (9–86), pp 53–61
[2] Lee B, Vanickis R, Rogelio F, Jacob P 2017 Situational awareness based risk-adaptable access control in enterprise networks Proc. of the 2nd Int. Conf. on Internet of Things, Big Data and Security (Porto: SciTePress) pp 400–405
[3] Bi Z M, Luo M, Miao Z, Zhang B, Zhang W J, Wang L 2021 Safety assurance mechanisms of collaborative robotic systems in manufacturing Robotics and Computer-Integrated Manufacturing, 67, art. no 102022
[4] Sarno R, Sinaga F, Sungkono K R 2020 Anomaly detection in business processes using process mining and fuzzy association rule learning J. of Big Data, 7 (1), art. no. 5
[5] Pal S, Hitchens M, Rabehaja T, Mukhopadhyay S 2020 Security requirements for the Internet of Things: A systematic approach Sensors (Switzerland), 20 (20), art. no. 5897, pp 1–34
[6] Gackowiec P, Podobinska-Staniec M, Brzychczy E, Kühlbach C, Özver T 2020 Review of key performance indicators for process monitoring in the mining industry Energies, 13 (19), art.no. 5169
[7] Salomon J, Broggi M, Kruse S, Weber S, Beer M 2020 Resilience decision-making for complex systems ASCE-ASME J. of Risk and Uncertainty in Engineering Systems, Part B: Mechanical Engineering, 6 (2), art. no. 020901-1
[8] Johannsen A, Kant D, Creutzburg R 2020 Measuring IT security, compliance and data governance within small and medium-sized IT enterprises IS and T Int. Symp. on Electronic Imaging Science and Technology, art. no. s5
[9] Bicaku A, Tauber M, Delsing J 2020 Security standard compliance and continuous verification for Industrial Internet of Things Int. J. of Distributed Sensor Networks, 16 (6)
[10] Xu M, Baraldi P, Al-Dahidi S, Zio E 2020 Fault prognostics by an ensemble of Echo State Networks in presence of event based measurements Engineering Applications of Artificial Intelligence, 87, art. no. 103346