Application of Digital Twin Technology for Modelling of Information Security Level of Industrial Plant

Natalia Mikhailovna. Kuznetsova.[1,*], *Tatyana Vladimirovna* Karlova[2,*]

[1]Candidate of technical science, docent, Automated Control Systems and Information Processing Department, Moscow State University of Technology "STANKIN", RU-127055, Moscow, Russia
[2]Doctor of sociological Science, candidate of technical science, Professor, Automated Control Systems and Information Processing Department, Moscow State University of Technology "STANKIN", RU-127055, Moscow, Russia

Abstract. Maintaining the high level of information security at all stages of production is one of the most important tasks of modern industrial plans. In this case, the complex (integrated) approach plays a special role in which information security is realized on maximum number of automated systems and communication channels. The article is devoted to the mechanism of modelling the realization of external and internal information security threats by means of digital twin application. The presented model is a generalized digital copy of all industrial automated systems.

1 Introduction

Digital twin technology is becoming more popular among industrial enterprises. The main purpose of the technology is creating the model (copy) that is closest to reality. These models should contain the complex of detailed digital copies of physical objects in all automated systems (further AS).

Digital twin technology is at the intersection of technologies "Industry 4.0" and "Industrial Internet of things" [1].

Detailed digital twins could be used for maintaining (and increasing) the level industrial information security. This requires:

- creating the detailed digital model of all AS and communication channels of enterprise:
  a) creating the digital models of computing complexes (further CC);
  b) creating the digital models of data stores (further DS);
  c) creating the digital models of local area networks (further LAN);
  d) creating the digital models of automated workstations (further AW) for employees;
- modelling the information security incidents:
  a) modelling (simulation) employee behavior;
  b) modelling (simulation) "behavior" of active equipment (technics);
  c) modelling (simulation) "behavior" of passive equipment (communication channels);
  d) modelling (simulation) of changes in environment parameters;
- integrated modelling of all systems and incidents:
  a) building incident trees (in particular for the study of avalanche effects);
  b) using Swiss Cheese Model (from risk theory) [2].

2 Detailed digital model of all enterprise automated systems

Architecture scheme of interaction between main enterprises AS elements is shown on Figure 1.

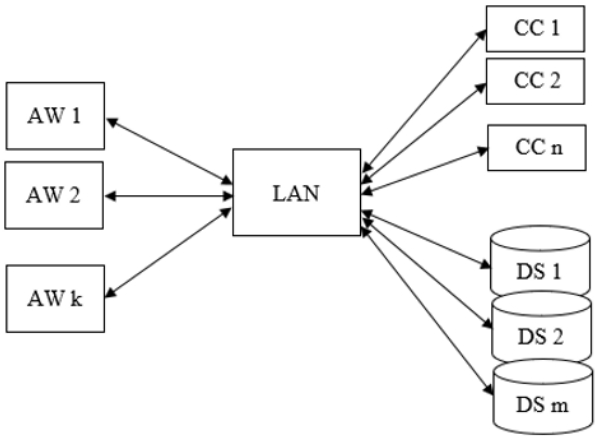

Fig. 1. Architecture scheme of interaction between main enterprise AS elements.

2.1 Digital Model of CC

Digital model of CC should contain:

- the logic of all information processing algorithms;
- the logic of interaction between clusters;
- technical characteristics of the equipment;

* Corresponding authors: knm87@mail.ru, karlova-t@yandex.ru

- technical characteristics of data transmission channels within CCi and between CC;
- data exchange interfaces (e.g. MPI – Message Passing Interface);
- features of the operation of RAM (Random Access Memory) and permanent memory;
- environmental conditions:
  a) wet;
  b) temperature;
  c) electromagnetic compatibility of equipment (including TEMPEST or "Compromising emanation") etc.;
- territorial location, etc.

2.2 Digital model of DS

Digital model of DS should contain:
- feature of applied storage technologies (access mode, backup mode, protocols used, etc.);
- technical characteristics of the equipment;
- technical characteristics of data transmission channels within DSj and between DS;
- territorial location;
- environmental conditions, etc.

2.3 Digital model of LAN

Digital model of LAN should contain:
- network topology;
- technical characteristics of data transmission channels;
- territorial location of all network parts;
- heterogeneity of data transmission medium (on physical level);
- environmental conditions, etc.

2.4 Digital model of AW

Digital model of AW should contain:
- first, all data "entry points":
  a) USB-ports;
  b) floppy drives;
  c) printers;
  d) faxes etc. [3-5]
- technical characteristics of the equipment.

It is important to note, that creating all kind of enterprise AS is needed for modelling (including all stages of life cycle of the enterprise target product) [6]:
- integrated monitoring and control design system:
  a) CAD (Computer-Aided Design) / CAM (Computer-Aided Manufacturing) / CAE (Computer-Aided Engineering);
  b) SCADA (Supervisory Control And Data Acquisition);
- integrated resource management system:
  a) ERP (Enterprise Resource Planning);
  b) MRP (Material Requirements Planning);
- document management system;
- tasks trackers;
- common programming environments.

3 Modelling the information security incidents

When the complete (detailed) digital copy of AS is created, development of event scenarios is needed. Event scenarios should depend on employees' behavior, equipment condition and the external environment.

If the behavior of equipment and environment could be predicted by changing a relatively small number of parameters, then employees' behavior modelling requires research on psychological, emotional, moral and motivation factors.

Modelling of equipment reliability can be carried out by mean of Monte-Carlo method [6]. For this, the technical characteristics AS equipment should be used as parameters. Also, this method could be used for modelling of external environment parameters.

It is important to note, that Monte-Carlo method assumes the presence of a large amount of computing resources.

When employee's behavior modelling, it is necessary to take into account:
- human factor:
  a) tiredness;
  b) tensity;
  c) neuropsychic stability;
  d) stress level etc.;
- psycho-emotional state:
  a) suffered shocks [7];
  b) love etc.;
- morals and principles:
  a) upbringing;
  b) education;
  c) origin;
  d) religiosity etc.

Based on the listed characteristics possible "personal portraits" of employees are formed. For correct modelling, "personal portraits" (which saved in database) are discussed and coordinated with experts-psychoanalysts.

4 Integrated modelling of all systems and incidents

4.1 Incident tree

While modelling of employee's, equipment and environment behavior the possibility of a series of interrelated events should be taken into account – avalanche effect, in which each of the events does not pose a serious threat, but their combination can lead to a decrease in the enterprise information security level.

4.2 Model "Cheese holes" (Swiss Cheese Model)

Model "Cheese holes" (Swiss Cheese Model) assumes that in any system there are vulnerability at different levels. However, the levels of protection ("cheese layers") overlaps, and therefore the general state of

system is stable (Figure 2a). However, there is the possibility that "cheese holes" would be overlapped not by cheese layers, but by the "holes" (lined up), which would lead to the global (system) information security threat implementation (Figure 2b).

In order to minimize the likelihood of lowering the information security level, it is necessary to:

- reduce the number of cheese "holes";
- reduce in the size of "cheese holes".

"Cheese holes" could be any kind of vulnerabilities in any part of enterprise AS in any time. Thereby while creating the model of "Cheese holes" it is necessary to consider both special and temporal aspects of information security [8].

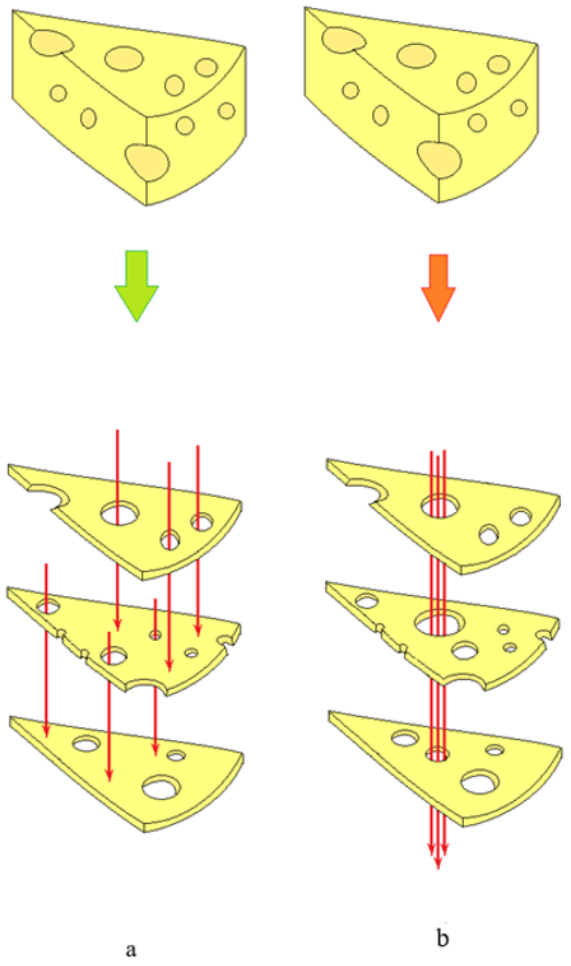

Fig. 2. Model «Cheese holes»:
a – «overlapping holes with layers of cheese»;
b – «overlapping holes».

5 Realization of modelling the digital twin

When using the concept of digital twins to simulate information security incidents and assess the protection level of all enterprise AS it is necessary to describe as accurate as possible all business processes and resources [9].

The cost of realization directly depends on degree of approximation of the digital model to reality. Also, the choice of modelling methods defines the realization cost.

6 Conclusion

Modelling physical systems using the conception of digital twins is a convenient tool for predicting the behavior of complex technical objects. The article is devoted to the methodology for using digital twins to estimate the information security level of the enterprise's automated systems. The methodology takes into account modelling of complex automated systems, communications, employees' actions, possible security incidents. In addition, methods of creating incident trees and "cheese holes" are presented as tools for integrate modelling. The methodology presented in the article allows to estimate the information security level as accurate as possible, to identify the "bottlenecks" and to take actions to eliminate vulnerabilities on time.

References

1. Digital twin. Available at: https://en.wikipedia.org/wiki/Digital_twin (accessed 15 October 2020)
2. Swiss Cheese Model. Available at: https://en.wikipedia.org/wiki/Swiss_cheese_model+ https://en.wikipedia.org/wiki/Chain_of_events_(accident_analysis) (accessed 15 October 2020)
3. N.M. Kuznetsova, T.V. Karlova, S.A. Sheptunov, Proceedings of the 2017 International Conference "Quality Management, Transport and Information Security, Information Technologies" (IT&QM&IS) – Proceedings Edited by S.Shaposhnikov 2017 St.Peterburg, Russia: Saint Petersburg Electrotechnical University "LETI", 199-202 (2017) ISBN 978-1-5386-0703-9 DOI:10.1109/ITMQIS.2017.8085797
4. Karlova, T.V., Bekmeshov, A.Y., Kuznetsova, N.M.. Proceedings of the 2019 IEEE International Conference "Quality Management, Transport and Information Security, Information Technologies" (IT&QM&IS) – Proceedings Edited by S. Shaposhnikov, St. Petersburg, Russia: Saint Petersburg Electrotechnical University "LETI", (2019) ISBN 978-1-7281-2594-7 DOI:10.1109/ITQMIS.2019.8928412
5. N.M. Kuznetsova, T.V. Karlova, S.A. Sheptunov, A.Y. Bekmeshov, IEEE Conference on Quality Management, Transport and Information Security, Information Technologies (IT&MQ&IS). Proceedings. – M.: "Quality", 23-27 (2016) ISBN 978-5-94768-071-3
6. A.M. Kolchuzhkin, N.M. Kuznetsova, Materials of XII scientific conference MSUT «STANKIN» and

«Education and scientific center for mathematical modelling MSUT «STANKIN» Collection of reports / Edited by O.A. Kazakov – M.: «STANKIN», 434 (2009)

7. Y.S. Shoigu, *Psychology of extreme situations* (S-Pb: Piter – 2019)
8. ICS cybersecurity. Available at: InfoWatch.ru (accessed 15 October 2020)
9. N.M. Kuznetsova, T.V. Karlova *Total Quality Management. Solving the problem of increasing the level of information security at an industrial enterprise as part of quality management system (course of lectures and laboratory workshops) Tutorial.* (M.: Janus-K, 2019) ISBN 978-5-8037-0779-0