

The system of technical diagnostics of the industrial safety information network

P V Repp¹

¹ Perm National Research Polytechnic University, 29, Komsomolsky Ave., Perm, 614990, Russia

E-mail: polina.repp@gmail.com

Abstract. This research is devoted to problems of safety of the industrial information network. Basic sub-networks, ensuring reliable operation of the elements of the industrial Automatic Process Control System, were identified. The core tasks of technical diagnostics of industrial information safety were presented. The structure of the technical diagnostics system of the information safety was proposed. It includes two parts: a generator of cyber-attacks and the virtual model of the enterprise information network. The virtual model was obtained by scanning a real enterprise network. A new classification of cyber-attacks was proposed. This classification enables one to design an efficient generator of cyber-attacks sets for testing the virtual modes of the industrial information network. The numerical method of the Monte Carlo (with LP τ - sequences of Sobol), and Markov chain was considered as the design method for the cyber-attacks generation algorithm. The proposed system also includes a diagnostic analyzer, performing expert functions. As an integrative quantitative indicator of the network reliability the stability factor (Kstab) was selected. This factor is determined by the weight of sets of cyber-attacks, identifying the vulnerability of the network. The weight depends on the frequency and complexity of cyber-attacks, the degree of damage, complexity of remediation. The proposed Kstab is an effective integral quantitative measure of the information network reliability.

1. Introduction

The problem of industrial safety is one of the most important modern problems. In accordance with the socio-economic requirements, the regulatory and the legal base, technical regulations and control algorithms are changing. Since modern society cannot exist without information technology, the protection against cyber threats is an actual problem. The design of security algorithms and creation of new ways of hacking is a mutually interconnected and dynamic process. The evolution of cyber danger moves from localized to global threats. Since 2008, there has been a special international RISI database, which has contained general information on these incidents since 1982. So the protection of industrial networks and timely diagnosis of its vulnerability have become an urgent task.

A typical structure of the enterprise automated technological process control system (APCS) includes production, storage, distribution, transportation, support and office activities, shown in Figure 1.



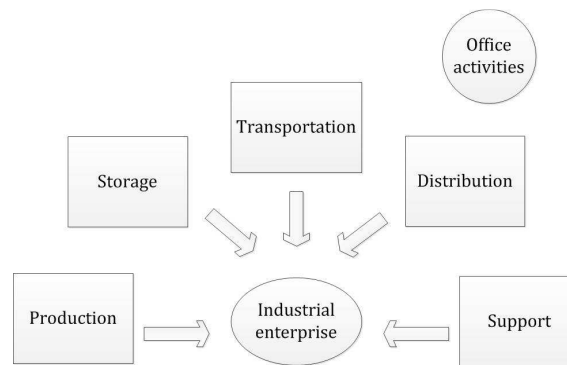


Figure 1. The typical structure of APCS.

Each element has its own sub-network which generates a set of the industrial enterprise networks. Despite the fact that each of these is equally vulnerable to cyber-attacks, the specificity of attacks influence for each sub-network is different.

A simple solution to the problem is the localization of the entire information flow within the enterprise or infrastructure. But modern automation systems providers require their customers to have a remote access for the remote support of their product. This means fabricators are required to have a permanent channel in the Internet, for example, to access the update servers for the installed software. In Russia, this problem is tried to be solved by developing own unique software products and releasing regularly updates which has to actualize this software independently, in accordance with changes in external parameters. In addition to the contradictions of the global unification trend, this approach has additional security issues. In particular, the human factor is not being considered. In order to have leverage over the customer's administration, developers supply their product with backdoors - deliberately altered fragments of the program, allowing the attacker (in this case the developer) to carry out unauthorized access to the information network resources based on changes in the protection system properties.

The modern IT-market offers a range of turnkey solutions for enterprise information security at any level and scale: software and hardware, and outsourcing services. In addition, there are approved standards, protocols, technical documentation and certification, designed to regulate the sphere of information security. Though, among the existing varieties of products there are no network diagnostics. That means the company that is acquiring (or building) their information security system has no opportunity to test its effectiveness before the actual cyber-attack will be carried out..

Thus, due to the obvious danger and the possible catastrophic consequences of global cyber threats for modern industrial and social infrastructure, an important challenge is to provide effective tools to combat them. The proposed system of identification, diagnosis and expert assessment of the significance of threats to the security of industrial networks can be considered.

2. Materials and methods

The main purpose of technical diagnostics is to organize efficient processes determining the technical condition of the complex, multi-component objects, which should include the industrial information network of an enterprise. Diagnosis is performed by hardware or software, internal or external technical tools implementing a particular algorithm for diagnosis.

During studying, development and implementation of diagnosis processes of the industrial information network technical condition, it is necessary to solve the same problems, which arise during the studying, development and implementation of all management processes. In the first place, it is the task of studying the physical properties of an information network and its security vulnerabilities, the problem of constructing mathematical models and information network vulnerabilities models. The following are the problems of model information network analysis, which is needed to obtain necessary data for the construction of the diagnosis algorithms. The next group

consists of tasks related to the development of construction principles, pilot testing and commercialization of the information network diagnostic system. Finally, there is the diagnostic system design problem in general and the study of its characteristics and properties (including experimental testing) [1]. The main subject of research of the industrial information network system is a design classification tree of the technical diagnostics shown in Figure 2.

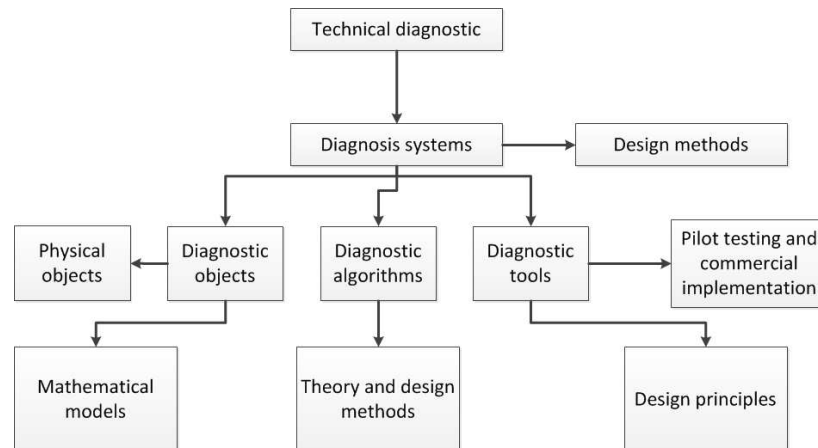


Figure 2. The main subjects of research of the design classification tree of technical diagnostics of the industrial information network system.

In this study, the problem of determining the diagnostic objects, diagnostic algorithms and diagnostics tools of the industrial information network is solved.

2.1. Diagnostic objects (Block 1).

The object of diagnosis is a mathematical model of the tested industrial enterprise network. As it was specified in the introduction, the industrial enterprise (both mining and processing) in case of damages, accidents and technological processes stoppages could cause a global catastrophe. Therefore, it is impractical to carry out testing and diagnostics of the enterprise's network at the moment of its work. It was proposed to solve this problem by means of a mathematical model design for the tested network. We should consider the network that may change significantly affecting the results of the diagnostics after the reading of the network characteristics for building its virtual model. To improve the reliability of the results, it is necessary to perform a series of tests with given Δ , sufficient to provide reliable statistics. This parameter is determined by the structural, technical and functional characteristics of the process implemented by the company. The proposed solution will help to update the status of the tested network.

2.2. Diagnostic algorithm (Block 2).

The core of the diagnostic algorithm is a model of cyber attacks. It is possible to build a cyber-attacks model in two ways. The first method is based on the use of numerical probabilistic methods (e.g. Monte Carlo). In this case, the sets (combinations) of attacks are formed by using a random number generator built on the Sobol sequence (LP sequence). As a criterion for the worst-case vulnerability, $\min K_{sta}$ is chosen. A limit of not more than three attacks at the same time is introduced. In the second case, the test is carried out in steps. The test at each step is determined by the previous results. That means the first set of attacks determines the most probable vulnerability. Then other cyber-threats matching this vulnerability are determined; and for this information a new cyber-attacks test kit is formed. The dimension of the sets can be increased. The basis of this diagnostic algorithm is the Markov chain. A table of conditional probabilities of correspondence between cyber-attacks, cyber threats and vulnerabilities is created for the operations. Conditional probability describes how likely

this cyber-threat will lead to this cyber-attack for a given vulnerability. To improve the reliability of the test results, it is suggested to use both methods in turn.

2.3. Diagnostics tools.

The use of the software - a set of software products designed specifically for the performance of current diagnostic tasks - is proposed as diagnostic tools.

Thus, experiments of the real existing network of a running enterprise are not allowed and process technology stops can cause unwanted effects, the proposed diagnostic system presupposes the existence of two structural blocks, shown in Figure 3:

- The industrial network virtual model, based on the scan selected nodal points, and
- The generator of cyber-attacks sets.

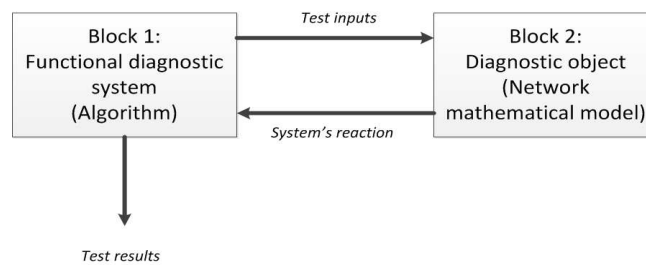


Figure 3. The functional diagram of the technical diagnosis system of the security state of the industrial enterprise network.

To construct the block generating cyber-attacks, a multi-level classification of cyber-attacks has been proposed. Practical significance of this problem is emphasized in [2]. The authors describe a number of available simulators of computer attacks (ARENA, Cohen, Secusim, OPNET Modeler, Sakhardante, NetENGINE etc.), noting the lack of cooperation between the private sector and the government (military sector) in the development. Also, the lack of available simulators with the “prediction” function of the consequences for a particular attack for a particular network is mentioned.

Furthermore, foreign scientists have made lots of attempts to create a unified cyber-attacks classification. One of the main problems was the lack of universal terminology, as the authors [3] mark. Moreover, most classifications do not satisfy such requirements as comprehensible and unambiguous ones. For example, in [4], the authors used an intuitive approach. Classifications by a number of authors [5], [6], [7] are unambiguous, complete and comprehensible. The work by [8] has undeniable advantages, but it does not meet the requirement of an exhaustive survey.

3. Results and Discussion

In this case, it should be noted that an adequate classification is a prerequisite for creating both a simulation of cyber-attacks and an expert system for assessing the safety of industrial information networks. In general, it is purposed to divide cyber-attacks into two groups: external and internal. External threats include nine categories, most of which are divided into subcategories. Internal threats include two categories: “Vulnerabilities in software” (which is the responsibility of its vendor) and “Data leakage” (which is the responsibility of company’s HR). Figure 4 shows the classification scheme of cyber-attacks. Due to the fact that computer viruses are the most wide spread type of cyber-attacks, detailing was made only for the corresponding block. This is the most common type of cyber threats. The scheme will allow designing an effective search form for the diagnostics software interface.

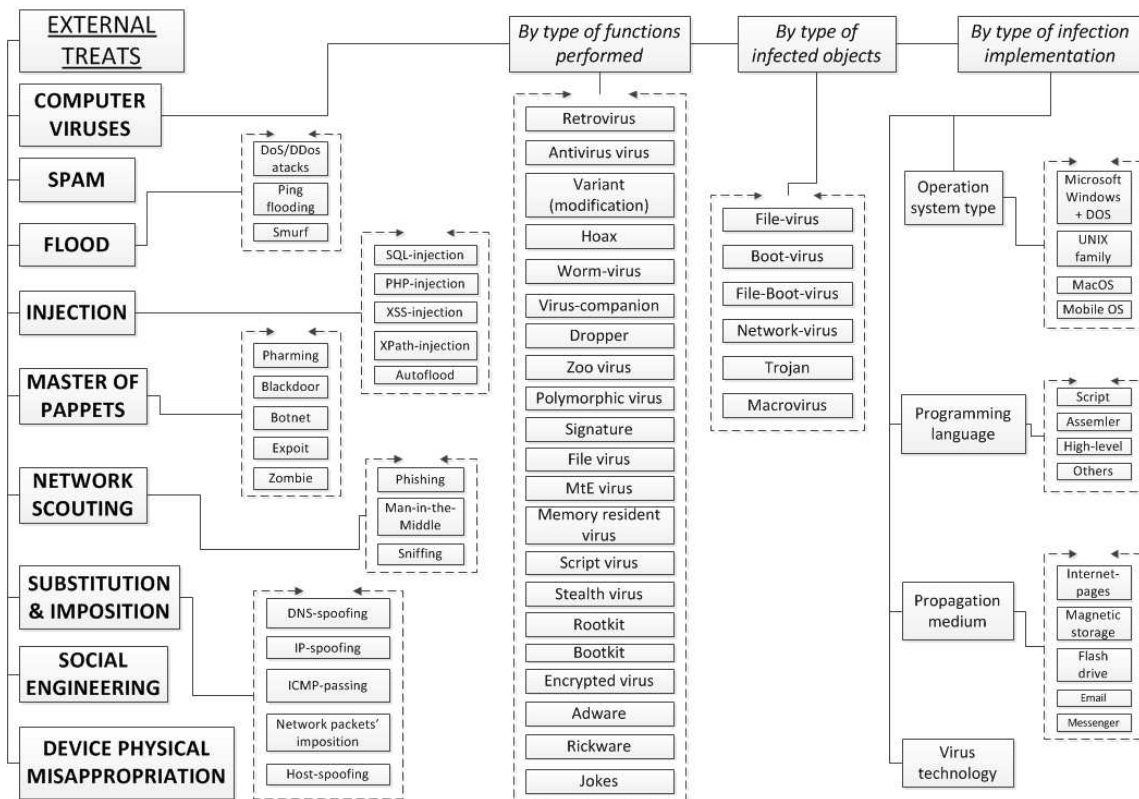


Figure 4. The classification scheme for cyber-attacks.

Block 1 designed on the basis of this classification generates attacks test sets in order to identify responses of the tested industrial network virtual model. Experiments are set with a sufficient sample to provide reliable statistics. In addition to the cyber-attacks generator, the system provides the analyzer, quantifies the degree of tested industrial information network safety.

There are many problems associated with access to effective quantitative characteristics of reliability of the information network. Firstly, all interested factors affecting safety can not always be quantified in a virtual network model. Many of these factors cannot be identified well enough or properly interpreted. Secondly, the concept of efficiency of the chosen safety measures may vary over time. The fact that at the moment something is an effective security feature, tomorrow it may become ineffective due to the ongoing continuous technological progress and an economic (environmental, political, etc.) conditions change. It should be noted that for one system one or more security measures may be appropriate simultaneously. Currently, 4 basic ones are used:

1. Availability.

There are 3 types of availability:

- Instantaneous availability - the probability that the system is ready for use at any randomly chosen time t ;
- Average uptime - the proportion of time in interval $(0, T)$, during which the considered system is ready for use;
- Steady-state availability- the proportion of time during which a given system is ready for use, if a given time interval is sufficiently large (i.e., when there is a statistical equilibrium in the system behavior).

2. Probability of survival.

This measure of reliability refers to the probability that the system for a predetermined time interval has reached a state of complete failure with the proviso that at the beginning of this interval, the system was in a state of serviceability. This measure is used mainly for systems unattended while working, or when maintenance is carried out only at specific time points (by schedule).

3. Meantime to failure (MTTF).

This measure depends on the maintenance conditions of the studied system. MTTF describes the expected time during which the system is in an operable state until the moment the whole equipment stops working. To use this reliability index, time is counted from the moment when the system was fully operational and until the time when all backup equipment does not fail, furthermore, the repairs are not started until the system fails completely. (MTTFF) describes the expected time during which the system is in order, allowing one to carry out repairs of separate failed pieces of the equipment, provided that at the initial moment of time they justify that the whole equipment was exploitable.

4. Duration of single downtimes.

The measure characterizes the time interval required to return the system performance, provided that at the initial time the system was faulty [9].

Quantitatively, these measures of reliability (and its prioritization) are largely determined by the type of a process, implemented at this industrial enterprise. Nevertheless, these measures have the same significance for the information networks.

The proposed safety diagnostic system for generating sets of cyber-attacks takes into account their weight (obtained as a result of statistical data processing), which affects the value of:

- Frequency of cyber-attacks (hackers' popularity).
- The complexity of implementation (technical and technological resources used).
- The possibility of preventing the attack during its execution (if detected).
- The degree of damage (magnitude of the consequences for the network and the whole enterprise).
- The complexity of remediation.

Thus, the proposed diagnostic system is also endowed with expert functions. The examination is conducted by determining stability factor (K_{stab}) for the tested network, depending on the detected vulnerabilities. Proposed K_{stab} is an effective quantitative integral measure (characteristic) of the information network reliability [10].

4. Conclusion

The design of the technical diagnostic system for the industrial networks was proposed to solve the problem with the use of new classification of cyber-attacks. The proposed algorithms allow achieving a higher diagnostic quality and safety of the industrial networks than similar models used in practice.

5. Acknowledgments

The reported study was done within the postgraduate research at Perm National Research Polytechnic University (Russia).

References

- [1] Karibskiy V V et al 1976 *Technical Diagnostics Fundamentals* Parkhomenko P P (Moscow: Energiya) **1** 464
- [2] Leblanc S P, Partington A, Chapman I, Bernier M 2011 *Proc. of MMS '11 (Boston, Massachusetts, USA)* 92-100.
- [3] Howard J D, Longstaff T A 1998 *SANDIA REPORT, SAND98-8667* 31
- [4] Simmons C B Shiva Sajjan G Bedi H, Dasgupta D 2014 *Proc. of 9th Annual Symposium On Information Assurance -ASIA'14 (Albany, NY)* 11 p
- [5] Hansman S, Han R 2005 *Computers and Security* **24(1)** 31-43
- [6] King J, Lakkaraju K, Slagell A 2009 *Proc. of SAC '09 (Honolulu, Hawaii, USA)* 8
- [7] Kjaerland M 2006 *Computers and Security* **25(7)** 522-538
- [8] Mirkovic J, Reiher P 2004 *ACM SIGCOMM Computer Communication Review* **34(2)** 39-53
- [9] Sandler G H 1963 *System reliability engineering* (Englewood Cliffs, NJ: Prentice-Hall) 300
- [10] Glazunov L P Smirnov A N 1982 *Design of technical diagnostics systems* (Leningrad: Energoatomizdat) 168