DOI 10.15622/sp.59.5

A.A. TEILANS, A.V. ROMANOVS, Yu. A. MERKURYEV, P.P. DOROGOVS, A.YA. KLEINS, S.A. POTRYASAEV

ASSESSMENT OF CYBER PHYSICAL SYSTEM RISKS WITH DOMAIN SPECIFIC MODELLING AND SIMULATION

Teilans A.A., Romanovs A.V., Merkuryev Yu.A., Dorogovs P.P., Kleins A.Ya., Potryasaev S.A. **Assessment of Cyber Physical System Risks with Domain Specific Modelling and Simulation.**

Abstract. Nowadays, the systems developed to integrate real physical processes and virtual computational processes — the cyber-physical systems (CPS), are used in multiple areas of industry and critical national infrastructure, such as manufacturing, medicine, traffic management and security, automotive engineering, industrial process control, energy saving, ecological management, industrial robots, technical infrastructure management, distributed robotic systems, protection target systems, nanotechnology and biological systems technology. With wide use, the level of IT and cyberrisks increases drastically and successful attacks against the CPS will lead to unmanageable and unimaginable consequence. Thus, the need in well-designed risk assessment system of CPS is clear and such system can provide an overall view of CPS security status and support efficient allocations of safeguard resources. The nature of CPS differs from IT mainly with the requirement for real-time operations, thus, traditional risk assessment method for IT system can be adopted in CPS. Design of a unified modelling language based domain specific language described in this paper achieves synergy from in IT industry widely used UML modelling technique and the domain specific risk management extensions. As a novelty for UML modelling, especially for simulation purposes, the presented DSL is enriched by a set of stochastic attributes of modelled activities. Such stochastic attributes are usable for further implementation of discrete-event system simulators.

Keywords: Cyber Physical System, IT, Risks, Risk Assessment, Domain Specific Language, Modelling, UML, CORAS, Disaster Tolerance Cyber Physical System, Structure Dynamic Control System.

1. Introduction. New competitive approach to the physical and virtual world integration with cyber-physical systems is one of the European Union research priorities. Cyber-physical systems (CPS) will change the way people interface with systems, the same way as the Internet has transformed the way people interface with information.

Concept of cyber-physical systems, their history and main components and characteristics are considered in this paper. Main accent is directed to the great influence of effective risk management on profit abilities in modern business systems, especially highly automated ones with complex use of Information Technology. IT risk consists not only of breakdowns in computer software or hardware, or lack of expertise of the IT staff. IT risk also may relate to risk of loss resulting from theft of company's data or client information. IT risk also may be the risk of loss that originates from computer software malfunction, such as a manufacturer's software license expiration or glitches, and the ways it affects corporate activities [1, 2]. A risk assessment initiative for IT systems

generally helps management understand areas in which significant losses may arise. IT risk assessment is carried out by identifying and evaluating assets, vulnerabilities and threats of using information technologies in business. An asset is anything that has value to the company — hardware, software, people, infrastructure, data, suppliers and partners, etc [3].

Taking into consideration the extreme complexity of IT risk assessment, we conclude that there is necessity to apply international frameworks of IT governance and risk management, such as Enterprise Risk Management Framework by Committee of Sponsoring Organizations of the Treadway Commission, Control Objectives for Information and related Technology, Code of Practice for Information Security Management, Information Technology Infrastructure Library, etc [4, 5].

Within our research, an IT risk management domain specific language is developed [6]. Nowadays, in the IT industry, majority of system specifications and procedure descriptions are made using the Unified Modelling Language (UML). UML is a graphical language and it consists from diagrams which are united in a model. The description of a system can be made from just a few diagrams in case of simple system or from hundreds of diagrams in case of a complex system. These diagrams are designed by system architects and system analysts.They are used in whole life cycle of a system. These models are frequently the main documentation for the system that is used for its operation and maintenance. That is why the authors have chosen UML as the base for designing the IT risk analysis DSL. UML uses general system organization terms such as Use Case, Activity, Action, State, Event etc. However, risk analysis professionals work with terms such as Threat, Vulnerability, Asset, Incident, Risk, Treatment etc. Therefore, to create an IT risk analysis tool, it was necessary to extend UML modelling approach with elements used by risk analysts. In fact there was an attempt to develop our own Risk analysis Domain specific modelling language, suitable for system developers and maintenance personnel and for risk analysts as well. Design of modelling tools necessary for risk analysts was based on CORAS language which is well known in professional community [7]. The CORAS language is a graphical modelling language for communication, documentation and analysis of security threat and risk scenarios in security risk analyses. This paper explains how the authors use CORAS Threat and Treatment diagrams, connecting them with UML Uses Case and Activity diagrams [8]. The result of this work provides means to unify both risk analysis model and IT system model.

2. Concept of a cyber-physical system. Cyber-physical systems are developed to integrate real physical processes and virtual computational processes. Many objects used in modern daily life are cyber-physical systems. Concept of CPS is complicated, it can be illustrated with a concept map (see Figure 1), developed in Berkley University [9, 10].

The definition of Cyber-physical system from Cyber-Physical Systems Week (www.cpsweek.org): "Cyber-physical systems (CPS) are complex engineering systems that rely on the integration of physical, computation, and communication processes to function."

Cyber-physical systems have not appeared from nowhere, they have a long history of development, which continues. This paper is an introduction to cyber-physical systems, their history and overview of the main components and characteristics.

Always growing need for different purpose information management systems leads to optimization of computing tools design techniques. Most of the world's currently used information management systems are embedded systems and networks. They are closely related to the control or management objects.

From certain common computing systems' classifications best suited to the modern situation is classification proposed by David Patterson and John Hennesy [11]. Their classification was guided by the use of the system. They divided computing system into 3 categories: desktop computers, servers and embedded systems. Embedded systems by the area of use are separated into:

- Automatic control systems;
- Measuring systems and systems that read information from sensors;
- Real-time "question – answer" type information systems;
- Digital data transmission systems;
- Complex real-time systems;
- Moving objects management systems;
- A general purpose computer system subsystems;
- Multimedia systems.

The concept of embedded systems appeared in the early 50's and it is in rapid development even today. It is interesting to view the evolution of embedded systems:

- Information management systems, 60's;
- Embedded computing systems, 70's;
- Embedded distributed systems, 90's;
- Cyber-physical systems, from 2006.

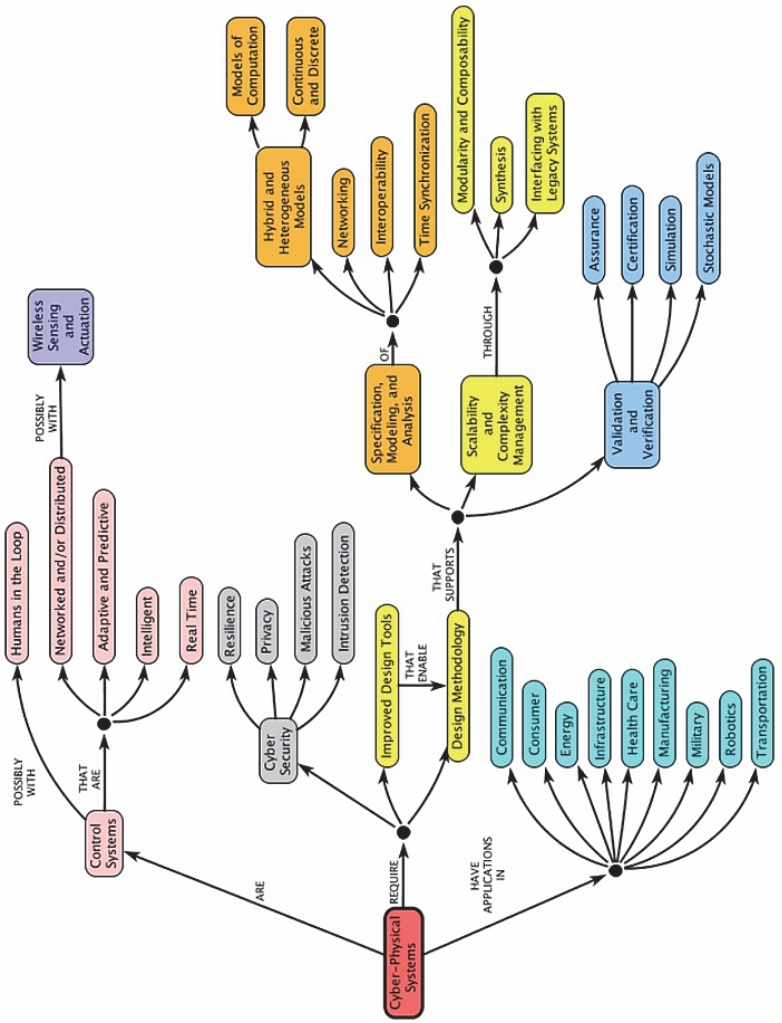

Fig. 1. A concept map of Cyber-physical systems

Information management system is a computing system designed for management purposes, but it is the most alienated from the control object. Integrated micro-scheme and microprocessors development led to information management system bringing directly to the management object. World had entered the era of embedded systems. System elements are gradually becoming cheaper and their integration increases, as well as the security level and the opportunity to combine them in controlled networks.

Downturn in embedded systems' elements prices and increasing connection with physical management objects led to appearance of cyber-physical systems.

Cyber-physical systems are specialized computing systems that interact with control or management objects. Cyber-physical systems integrate computing, communication, data storage with real world's objects and physical processes. All above said processes must occur in real-time, in safe, secure and efficient manner. Cyber-physical systems must be scalable, cost-effective and adaptive. Cyber-physical systems are in use in various areas such as smart medical technologies, environmental monitoring and traffic management.

Wireless sensor networks can become an important part of cyber-physical systems, because of high sensitivity capability it is one of the main driving factors of cyber-physical systems application distribution. The rapid development of WSN, medical sensors and cloud computing systems makes cyber-physical systems impressive candidates for use in inpatient and outpatient health care improvement [12]. Cloud computing maturity is a direct result of few technologies such as distributed computing, internet technology, system management and hardware development [13].

Cyber-physical systems integrate computing and physical processes. Compared with embedded systems much more physical components are involved in CPS. In embedded systems, the key focus is on the computing element, but in cyber-physical systems, it is on the link between computational and physical elements. Cyber-physical system parts exchange information with each other that is why the third component - communication is added there. For this reason, cyber-physical system is denoted by the symbol C3 (Computation, Communication and Control). Links improvement between computational and physical elements, extends cyber-physical systems usage possibilities.

Cyber-physical systems are used in multiple areas such as medicine, traffic management and security, automotive engineering, industrial and process control, energy saving, ecological monitoring and management, avionics and space equipment, industrial robots, technical infrastructure management, distributed robotic systems, protection target systems,

nanotechnology and biological systems technology. In all cases increased use of CPS are closely tied with cyber and IT risks, that need to be managed well.

3. Common IT risk management problems. It is possible to indicate a set of IT risks management problems which are typical for Latvian business [4]. They are:

– customer service malfunction due to interruptions of continuous access to IT services;

– unsatisfied demand for qualified IT personnel;

– delayed modernization of information systems software and hardware;

– insufficient IT qualification of information system users;

– inadequate level of existing IT services quality monitoring;

– inadequate level of cooperation between IT specialists and other employees;

– inadequate assessment of financial losses resulting from failures or interruptions within information systems;

– absence of IT system development strategic plan, based on a general development plan of company;

– inadequately low IT security level;

– absence of strategy of IT system restoration after potential failures and interruptions.

Taking into consideration the extreme complexity of IT risk management within the framework of operational risk management system, it could be concluded that it is necessary to apply international standards and frameworks of IT governance, such as Information Technology Infrastructure Library, Control Objectives for Information and related Technology, Code of Practice for Information Security Management.

The proposed technique for IT risk assessment and management could be successfully used as a start point for development of the IT risks assessment support systems prototype, based on an IT risk management domain specification language with a metamodel that defines an abstract UML based language for graphical approach to identify, explain and document security threats and risk scenarios. The next chapter describes the Domain Specific Language (DSL) for IT risk analysis modelling and simulation. The presented tool will provide both IT process modelling and documentation as well as connection of these processes with identified risks.

4. DSL for IT risk analysis. A Domain specific language (DSL) is language for programming, specification or modelling suitable for particular problem domain specialists to solve their specific technical tasks [14, 15]. This chapter describes domain specific language for IT risk analysis designed by the authors. This language has organically emerged from

unifying several methods and graphical languages which are used by developers and maintenance specialists from information systems domain, and also analysts responsible for risk analysis and risk mitigation activities for IT systems. The designed DSL (see Fig. 2) is based on approach to Unified Modelling Language (UML), CORAS method and Misuse Case Alignment Method [7, 8, 16, 17].

Currently, using UML is one of the most commonly used approaches in IT system modelling. The authors' experience acquired while working in IT and UML belongs to the group of graphical modelling languages. Initially UML was built for information systems modelling to facilitate the development and maintenance processes. Nowadays the usage of UML is broadened. This language is used for building business models, which exceed the initial task of modelling of information systems. Industry shows that UML modelling is used to some extent in all medium and large scale projects.

UML belongs to the group of graphical modelling languages. Initially UML was built for information systems modelling to facilitate the development and maintenance processes. Nowadays the usage of UML is broadened. This language is used for building business models, which exceed the initial task of modelling of information systems.

As regards system modelling, UML modelling is widely used at systems development or enhancement phases. UML modelling describes the structure and behaviour of the system. This language consists of graphical notations called diagrams and builds up an abstract model of a system. The UML standard is maintained by OMG (Object Management Group). In the beginning, UML was built for specification visualization and documentation of IT systems development. Nowadays usages of UML are not only limited to tasks of software engineering. UML is also used for business process modelling and for the development of systems which are not pure information systems.

Modelling with UML promotes model-driven technologies, such as Model Driven Development (MDD), Model Driven Engineering (MDE) and Model Driven Architecture (MDA). Supplementing graphical notations with terms such as class, component, generalization, aggregation and behaviour, helps save system designer's time for system architectural tasks and design.

A UML model consists of a set of diagrams. A diagram is a partial representation of the model. A system model could be divided into two parts. The first part is a functional model, which reflects functionality of a system from the system user's point of view. This kind of model is constructed using Use Case diagrams. The second part is the dynamical model that reflects internal behaviour of the system. A model of that kind is constructed using Activity, State, Sequence and Collaboration diagrams.

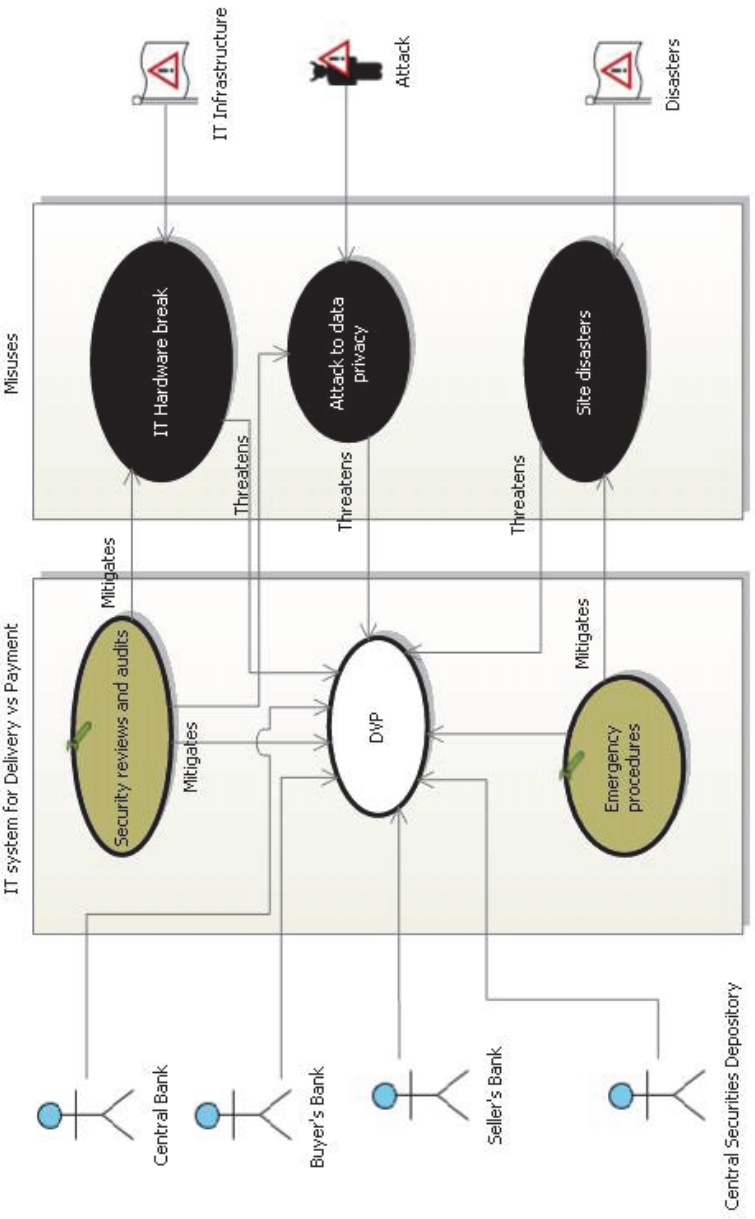

Fig. 2. DVP IT System Use cases

A system model to be created with UML language should not necessarily contain all diagrams. For example, when creating Information System vision model or requirement specification, it is enough for the system analyst to create Use Case and Activity diagrams. Use Case diagram answers a question – what a system does. Activity diagrams describe scenarios of every Use Case, i.e., Business processes. Therefore we prefer this work use only Use Case and Activity diagrams.

As mentioned above, IT industry use of UML is mostly directed to specification and documentation of a system [14].

The authors as representatives of simulationist community would like to improve this situation and to add more dynamic to this static construction. Obviously simulation of the model can give to developer's possibilities to evaluate and forecast behaviour of a target system. The authors already addressed this issue in [8]. During development of the presented DSL for IT risk analysis, which is based on UML, one of the objectives was possibility of simulation of a model. Activity Diagram elements are complemented with stochastic attributes for simulation purposes (Table 1).

Table 1. Stohastic attributes of Activity diagram

UML element	Stohastic attribute
Task	Duration
Branch	Decision probabilities
Timer	Start Delay
	Number of Events in group
	Delay between groups
	Number of Groups

One more approach for the developed DSL is application of Misuse Case in a UML Use Case model. Misuse cases improve UML diagrams with a better support to analyse problems of IT risk management. The *Use Case* diagram is extended with graphically black *Use case*, called *Misuse Case* and black *Actor* called *Misuser*. *Misusers* are related with *Misuse Case*. *Misuse cases* are related to *Use Cases* with relation <threatens>. During risk analysis stage *Use Case* diagrams are extended with additional *Use Cases* for risk mitigation, which are connected with system *Use Case* with relation <include> and with *Misuse Case* with relation <mitigate> (see Figure 2).

Considering that the task to be solved by the authors was to provide a government institution responsible for IT risk evaluation with

tools necessary for such tasks, the third technology used in this work is security risk modelling, analysis and documentation language CORAS. The initial CORAS approach was developed within the CORAS project funded by the European Commission that ran from 2001 until 2003. CORAS is both a language and a methodology for its application, described in the book [7]. Although initially CORAS was designed for security risk analysis, its syntax and semantics allows applying this language to complete IT risk analysis scope. In the developed prototype only one CORAS language diagram – the Treatment diagram – Is used. Treatment diagram is CORAS method all-inclusive diagram, in which all main risk analysis entities – *Threat*, *Vulnerability*, *Risk*, *Asset*, *Threat Scenario*, *Unwanted Incident* and *Treatment Scenario* are included. In turn, by methodology developed by the authors, *Unwanted Incident* is common entity, which connects risk analysis Treatment diagram with UML Activity diagram used in IT system Activity diagram model (see Figure 3).

Additionally, we did similar enhancements to CORAS Treatment diagram as we did with UML activity diagram. For simulation purposes, Treatment diagram is complemented with stochastic attributes (Table 2).

Table 2. Stohastic attributes of Treatment diagram

Diagramm element	Stohastic attribute
Relation between Risk and Asset	Impact
Unwanted incident	Used as connector between risk and system models. Transfer events from treatment scenario to system model. Event raises a disability of selected activity of a system model
	Duration of disability
TreatmentScenario	Start Delay
	Number of Threat events in group
	Delay between groups
	Number of Groups

Using the DSL described in the paper, a corresponding Activity diagram describing IT system functionality should be designed for each system Use case, a corresponding risk mitigation Activity diagram for each risk mitigation Use case should be designed, and Treatment diagram should be designed for each Misuse Case (see Figure 3).

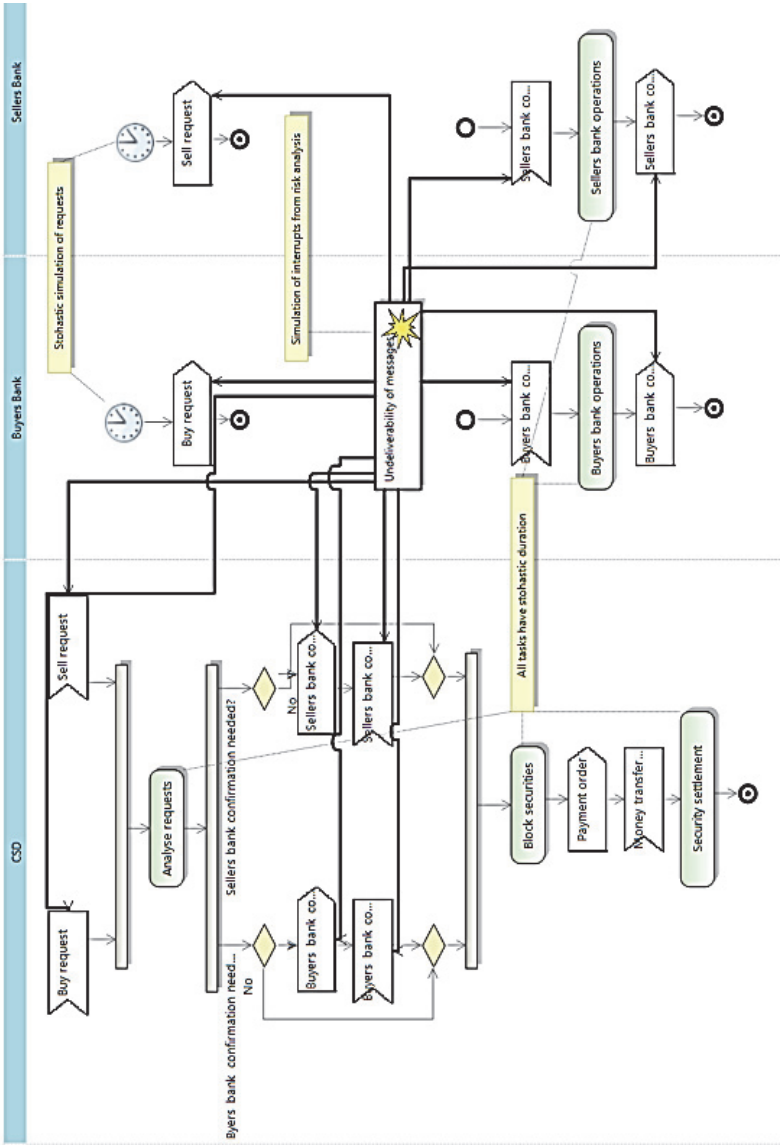

Fig.3. DVP Activity diagram

Simulation will allow to perform simulation experiments on two models simultaneously – the risk analysis model (see Figure 4) and IT system model (see Figure 3) and gather more adequate risk estimation results.

For such IT risk analysis approach, a tool prototype which is based on Microsoft Visualization and Modelling SDK (VMSDK) is developed while designing DSL. This implemented modelling tool is functioning inside Microsoft Visual Studio Shell. It could be distributed either with Microsoft Visual Studio Shell, or as Microsoft Visual Studio Add-In (see Figure 5). Additionally this approach ensures ability of simulation program code generation, compilation and execution for any Microsoft .NET Framework supported language. Specially designed templates ar used for code generation purposes, and they consist of code snippets for simulation of diagram elements. The authors currently are working on this solution.

Another approach is code generation from DSL diagrams for some general purpose simulation package (for example ARENA).

5. Reducing managerial risks by the use of disaster-tolerant CPS. Currently, there is a widespread of opportunities, provided by the Internet of Things and the Industrial Internet of Things both in terms of created systems of technologies and services, provided by these systems [18, 19]. In these conditions, ensuring the continuity of business-processes (BP) and improving disaster tolerance of relevant business-systems (BS) are one of the most important strategic directions of any organization (company) development. At the same time ubiquitous implementation of cyber physical systems as basic components and subsystems in existing and perspective information systems (IS), that make up the main core of large and commercial crucial infrastructure, leads to the need of giving them such an important system-cybernetic property as disaster tolerance [20]. Further, under the disaster tolerance of CPS should be understood the ability distributed computer complex, consisting of several CPS, to store critically important data and structure, and also continue to perform their functions after a massive (perhaps, purposeful) destruction of their components as a result of various cataclysms not only natural character, but also human-inspired [20–22]. This definition is accurately corresponds to the English term "Disaster Tolerance" (DT), but generally the term "Disaster Recovery" (DR) (literally "recovery after catastrophe") can also be translate as "Disaster Tolerance". The difference between DR and DT is that DR focuses on the security of data (with strictly controlled losses, if they unavoidable), and the means for continuing full-fledged work are in many cases assumed external to the actual disaster-tolerant part of the complex. Thus, the disaster tolerance of CPS supposes first of all ensuring the safety of data, and the possibility to recover the data after a major local or global cataclysm, and at the same time an appropriate level of reliability (traditional, "local", fault-tolerant) of all or critical subsystems is provided by the same means [20-22].

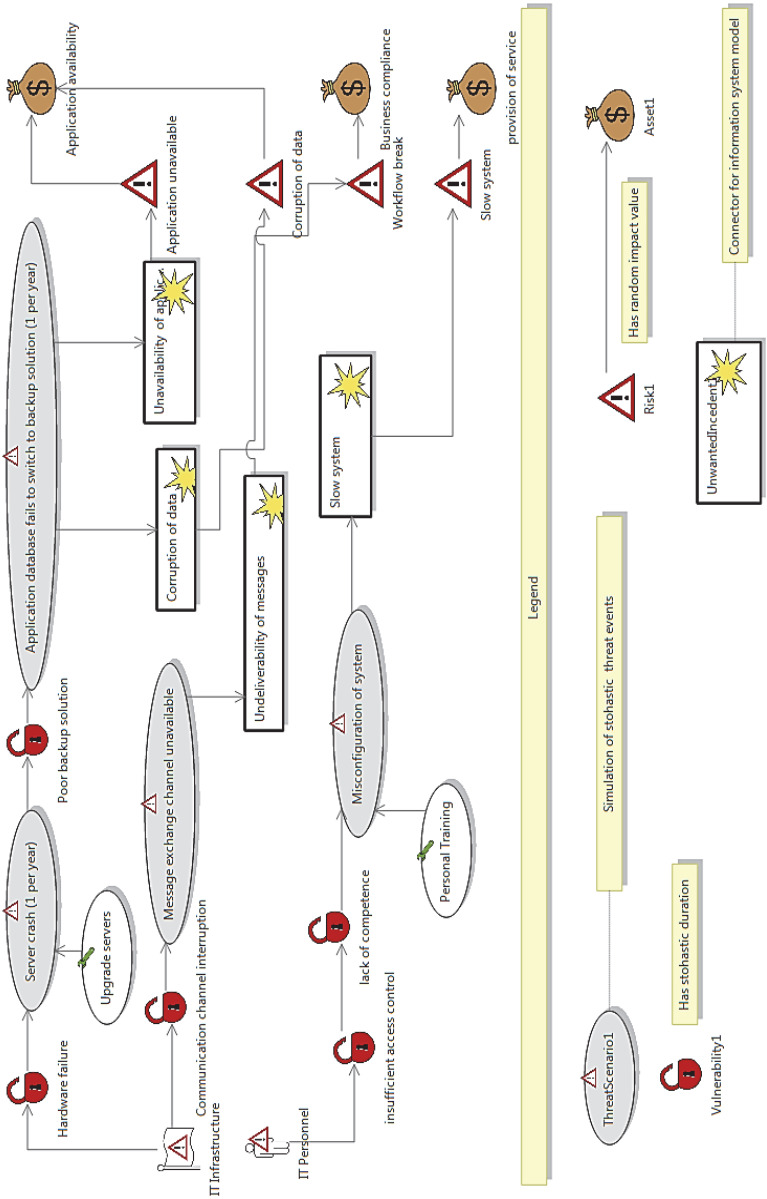

Fig. 4. Treatment diagram for IT Hardware break

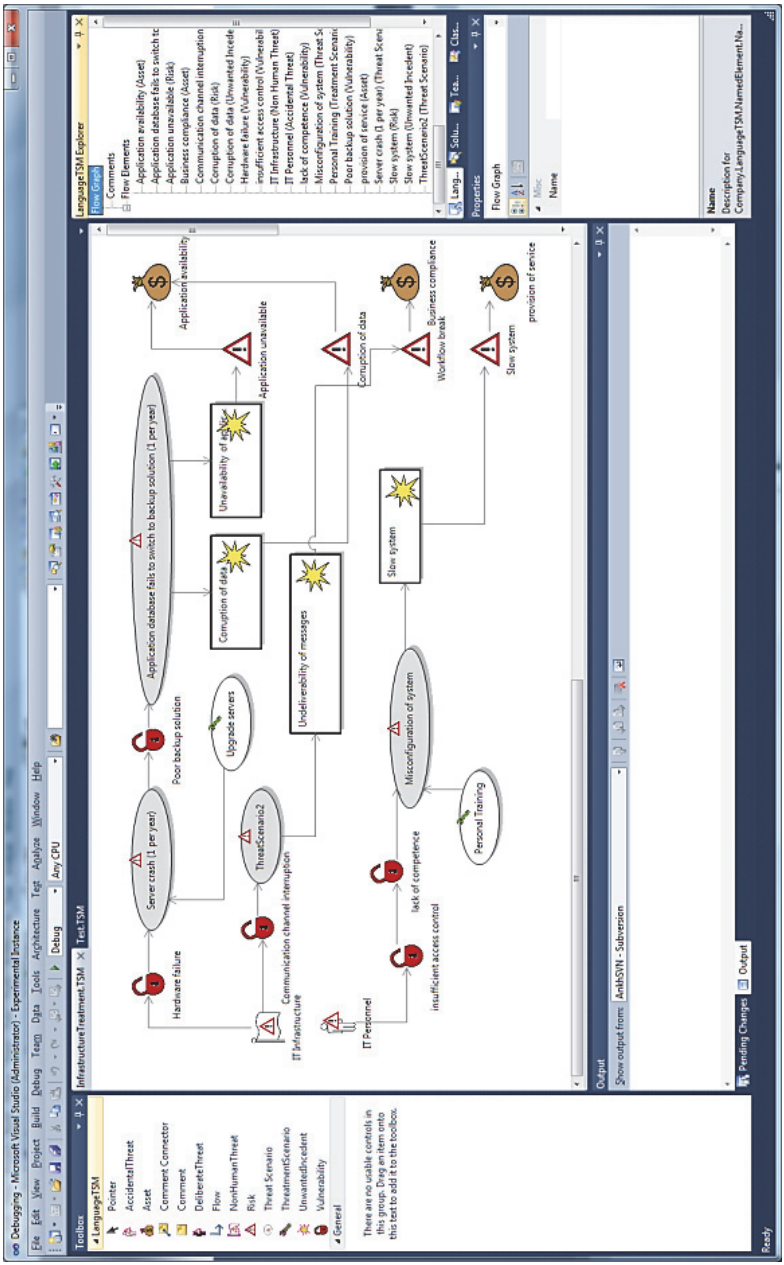

Fig. 5. IT risk analysis tool

As subsystems of modern corporate IS (CIS), which include the CFS, are distributed, in case of mass failures on one site, the main performance can be removed to another site. The listed features of disaster-tolerant CPS lead to the need for principally new approaches to solving bothproblems of creation and development of this class CPS, and the problem of assessing the managerial risks associated with their application, that is considered at this paper.

Studies have shown, that in order to neutralize threats and minimize losses caused by abnormal, emergency, extreme and catastrophic situations, leading to an avalanche-like increase in degradation processes and destruction of CPS, management of the relevant organizational structures, (business-systems (BS)) must be prepared in advance for the solution of at least the following five groups of interrelated problems [23]:

– identification of potential threats to possible emergencies due to socio-economic crises, natural and technogenic disasters, development of model options solutions for their prevention, localization and stabilization;

– development of proposals and draft decisions aimed at increasing sustainability objects of the BS infrastructure to the action of destabilizing and destructive factors possible emergencies;

– identify trends and early detection of potential threats, estimate and predicting the possibility of emergencies;

– prompt formation and justification of decisions on management of all types of CPS and BS resources as a whole in order to minimize the negative consequences of destructive and destabilizing factors in the conditions of the emerged emergency situation;

– assessment of the negative consequences of an emergency situation and the development of draft decisions, aimed at their elimination with minimal costs.

Preliminary analysis of problems and tasks that need to be solved at various stages of CPS life cycle and the existing theoretical methods and approaches to their solution shows that within the framework of the earlier developed theories and methodologies for managing complex systems, these issues, as a separate subject of research, from a single system-wide point vision was practically not considered. In this case, the subject area covering them has a number of significant features, radically different from the subject of research existing theories of managing complex systems. Among them you can specify, in particular following features [21, 23]:

– extreme and catastrophic situations, as a rule, are difficult to predict and arise suddenly (temporary uncertainty in the provision of readiness for management);

– the scale of the negative consequences associated with them is also difficult to predict; they can quickly increase over time and have various long-term negative consequences for heterogeneous, including territorially distributed objects (uncertainty boundaries and content of the subject area);

– information about such situations, as a rule, is contradictory and bad predictable in its composition and volume character and enters the management system with different time delays (uncertainty in the identification of current situations);

– decision making in such situations is carried out in conditions of a strict limit time, risks and various limitations in the options for selecting and implementing managers effects, etc.

Accounting for these and a number of other specific features of management processes of complex systems in emergency and catastrophic situations requires the development of fundamentally new, special principles and methods of monitoring, analysis and forecasting situations, developing options for management decisions, procedures for their selection and implementation.

Thus, for example, analysis shows that the principles and methods of traditional diagnostic systems are conceptually failures, faults, defects and oriented to diagnose the standard mode. This does not take into account a number of important properties of the dynamics of the functioning of complex objects in abnormal and critical conditions situations. In particular, the specificity of their probabilistic properties is not taken into account, the possibility sudden appearance of dynamic chaos in the form of disordered processes in deterministic systems, the "fine" structure of the dynamics of the mechanisms of aging and destruction materials and structures, as well as a number of other practically important properties of the dynamics of non-standard and critical situations. Many conceptual problems related to management of the structural dynamics of complex systems with their various degradations, assessments and forecasting of risks of occurrence of supernumerary and critical situations, and also risks selection and implementation of relevant management decisions, etc. [21, 23, 24].

In these conditions, it is necessary to investigate and solve the problems of ensuring the disaster tolerance of CPS within the framework of the interdisciplinary approach, interpreting them as tasks of structural dynamics control (SDC) of these systems. The tasks of SDC of CPS in its content belong to the class of problems of structural and functional synthesis of CPS shape and formation appropriate programs to manage their development (modernization). The main difficulty and singularity of

the class problems solution under consideration consists in the following. Determination of optimal programs and laws of main elements and subsystems of CPC management (planning) in a dynamically changing environment can only be carried out after the list of functions and algorithms of information processing and management becomes known, which should be implemented in the specified elements and subsystems. In its turn, the distribution of functions and algorithms for CPS elements and subsystems depends on the structure and parameters of the laws governing the management of these elements and subsystems. The difficulty of resolution this contradictory situation is aggravated by the fact that under the influence of various causes (objective, subjective, external and internal) over time, CPS composition and structure at various stages of its life cycle differs. By now the class of structural-functional synthesis tasks and management of CPS development has been investigated not deep enough. New scientific and practical results have been obtained in the following directions of research [21–24]: the synthesis of CPS technical structure under certain laws of functioning of the main CPS elements and subsystems (1st direction); synthesis of CPS functional structure, or, in another way, the synthesis of management programs of the CPS main elements and subsystems under the well-known CPS technical structure (2nd direction); of synthesis programs for the creation and development of new generations of CPS without taking into account the stage of joint functioning of the existing CPS and the implemented CPS. A number of iterative procedures for obtaining a joint solution of problems, the research of which is carried out within the framework of the 1 and the 2 directions. In general, all existing models and methods of CPS structural-functional synthesis appearance and the formation of programs for their development (modernization) are used in stages of external and internal design of CPS shape, i.e. when the time factor is not essential. However, in practice, when non-standard, critical and emergency situations in CPS, characterized by inaccurate and contradictory information, time becomes one of the most important parameters by means of which the effectiveness of activities, related to the maintenance and restoration of business processes.

Existing foreign and domestic business continuity planning tools (Business Continuity Planning) allow: using universal database architectures to simplify procedures for risk analysis and development plans for recovery and business continuity; simplify the processes of supporting current business continuity plans; synchronize and maintain up-to-date information using the interfaces of other applications; to adjust the management of the company taking into account business continuity plans.

At the same time, they do not provide for the comprehensive automation of the processes of managing the structural dynamics of CPS in order to improve their security, are poorly adapted to situations in which it is possible to create unrealistic abnormal situations.

Thus, at the present time it becomes very important to develop methodical and methodological foundations for the integrated automation of adaptive planning and scheduling of the modernization and operation of disaster-tolerant CPS based on the development of concepts, principles, models, methods and algorithms for analyzing and managing the structural dynamics of CPS in real conditions of incompleteness, uncertainty, inaccuracy and inconsistency of information about the emerging situation and in the presence of an unavoidable threshold time limitation on the cycle of the formation and implementation of solutions to prevent possible critical, emergency and extreme situations.

An important role in management theory development of complex organizational and organizational and technical systems in crisis situations should be given to issues of creation of appropriate model-algorithmic support for problem solving, planning and management of these systems under dynamically changing conditions.Resulting from what has been said so far, a conceptual scenarios of creation and functioning of CPS, possible approaches to organization and carrying out of complex modeling and multicriteria options estimation for the functioning of CPS under different conditions of the situation, as well as relevant risks of the choice of management decisions related to the application of both CPS and whole BS, in which they are included. In particular, the following list was proposed main CPS performance indicators: CPS availability indicators (total IS downtime for any reason, indicators that assess risks occurrence and development of accidents and disasters), indicators that assess the consequences of accidents and catastrophes for specific business processes (duration, scale and extent of damage), indicators that estimate the total time and completeness of the operations performed restoration of CPS working capacity, indicators evaluating, capital and operational costs to ensure the required level of catastrophic stability, costs of other types of resources, indicators assessing the degree of criticality of operations performed in CIS, the importance of resources and information used to provide the required level of disaster tolerance.

By now, a polimodel process description of creation and operation of disaster-tolerant CPS has been developed, providing work of the virtual enterprise (VE) in conditions of RFID technologies implementation. Part of this complex includes: deterministic and

stochastic static and dynamic models of CPS program management at various stages of their life cycle, allowing to describe both business processes performed within the framework of the VE, and processes of CPS modernization and functioning. Coordination of all listed models is based on the concepts and approaches developed by the proactive management theory of structural dynamics of complex technical objects (including CPS). Conducted preliminary analysis of the implementation of the concept of system modeling in the tasks of proactive CPS planning and scheduling shows the following advantages of joint use of the proposed static and logical-dynamic models of CPS proactive management:

– static models of CPS functioning allowed to take into account those factors (information losses, bandwidth limitations), which with dynamic modeling lead to the corresponding phase constraints;

– on the basis of static models, initial data are generated, dynamic model would not be possible (in this case, in fact, the aggregated variant of the technology of receiving, storing and processing data is determined);

– static models allowed, in the first approximation, to take into account the distribution and structural dynamics of the considered CPS, allowed to quantify the overall planned amount of data received, transmitted, processed or lost.

At the same time, a detailed description of the processes of information distribution and processing the operation of the VE with reference to specific time points in a static model is quite difficult. To do this, it was suggested to use a dynamic model of CPS functioning. In this case, the proposed dynamic description of the processes allows:

– to form and optimize such quality indicators of a manageable systemic dynamics (MSD) of CPS, which are difficult to describe in a static model (for example, estimating the uniformity (unevenness) of the use of CPS resources on the entire interval management and at each current time);

– to study the processes of CPS MSD involve an extremely rich mathematical apparatus of the theory of optimal control, allowing to solve a wide range of actual tasks of analysis and synthesis of management programs of CPS and its main subsystems.

In the Table 3 in its left part are the fundamental scientific results that have been obtained to date in modern management theory of complex technical objects. In the right part of this figure are those new scientific and applied results that were obtained within the framework of the developed theory of CPS proactive management, based on these fundamental scientific results.

Table 3. Results of a qualitative analysis of proactive management processes of disaster tolerant CPS

№	Contents and ways of implementing results	
	The main results of qualitative analysis of the management of complex technical objects (CTO)	Ways of results implementation
1	Analysis of the solutions existence in control problems of CTO	Checking the adequacy of the description of cyber physical systems (CPS) proactive management
2	Conditions for controllability and attainability in control problems of CTO	Verification of the feasibility of CPS control technology. Identifying the main factors (constraints) affecting the indicators of the target and information technology capabilities of CPS
3	The uniqueness condition for optimal programmed controls in the tasks of planning the operation of CTO	Assessment of the possibility of obtaining optimal plans for CPS use
4	Necessary and sufficient conditions for optimality in control problems of CTO	Preliminary analysis of the structure of optimal program management, obtaining basic relationships for constructing scheduling algorithms of CPS application
5	Stability and sensitivity conditions in control problems	Estimation of stability (sensitivity) of CPS proactive management to disturbing effects, to a change in the composition and structure of the initial data, calculation of management risk indicators

6. Conclusions. The current situation within business indicates the necessity for more complicated and more effective IT risk management system development. In the presented paper the given approach allows to perform IT risk analysis which is based on the unified IT system model specification. In this way the one window approach is realised for both system developers and maintainers and for those responsible for the security policy of a system. The presented DSL and modelling based tool are in design stage. Further work will be performed to improve the Domain specific language. The second group of further activities will be devoted to implementation of an appropriate simulation engine, including generation of experimental frames from available business data and maschine learning approaches for model parameter finetuning. Model repository and tools for storing and processing simulation results will be developed for domain specific decision support.

This approach will be approved on state-wide IT systems and Industry 4.0 solutions.

References

1. Biro M., Mashkoor A., Sametinger J., Seker R. Software Safety and Security Risk Mitigation in Cyber-physical Systems. *IEEE Software*. 2018. vol. 35. no. 1. pp. 24–29.
2. Hu F. Cyber-Physical Systems: Integrated Computing and Engineering Design. New York: CRC Press. 2018. 398 p.
3. Romanovs A. Security in the Era of Industry 4.0. 2017 Open Conference of Electrical, Electronic and Information Sciences (eStream). 2017. 1 p.
4. Klimov R., Reznik A., Solovjova I., Slihte J. The Development of the IT Risk Management Concept. *Computer Science*. 2008. vol. 5. pp. 131–139.
5. Romanovs A., Merkuryev Y., Klimov R., Solovjova I.A Technique for Operational IT Risk Management in Latvian Monetary and Financial Institutions. Proc. of 8th WSEAS International Conference on Applied Computer Science «Recent Advances on Applied Computer Science». 2008. pp. 230–235.
6. Teilans A. et al. Domain Specific Simulation Language for IT Risk Assessment. Proceedings 25th European Conference on Modelling and Simulation (ECMS2011). 2011. pp. 342–347.
7. Lund M.S., Solhaug B., Stølen K. Model-Driven Risk Analysis: The CORAS Approach. Springer. 2010. 460 p.
8. Kleins A., Merkuryev Y., Teilans A., Filonik M. A meta-model based approach to UML modelling and simulation. Proceedings of the 7th International Conference on System Science and Simulation in Engineering. 2008. 6 p.
9. Skorobogatjko A., Romānovs A., Kuņicina N. State of the Art in the Healthcare Cyber-physical Systems. *Information Technology and Management Science*. 2014. vol. 17. pp.126–131.
10. Cyber-Physical Systems. Available at: https://ptolemy.berkeley.edu/projects/cps/ (accessed: 11.02.2018).
11. Patterson D.A., Hennessy J.L. Computer Organization and Design: The Hardware/Software Interface: 5th ed. Morgan Kaufmann. 2013. 800 p.
12. Milenkovic A., Otto C., Jovanov E. Wireless sensor networks for personal health monitoring: issues and an implementation. *Computer Communications*. 2006. vol. 29. no. 13-14. pp. 2521–2533.
13. Buyya R., Broberg J., Goscinski A. Cloud Computing: Principles and Paradigms. John Wiley & Sons 2010. 637 p.
14. Achim D., Brucker J.D. Metamodel-based UML notations for domain-specific languages. Proceeding of 4th International Workshop on Language Engineering (ATEM 2007). 2007. 15 p.
15. Lenz G., Wienands C., Greenfield J., Kozaczynski W. Practical software factories in. NET. New York: Apress. 2006. 214 p.
16. Sindre G., Opdahl A.L. Eliciting Security Requirements by Misuse Cases. *Requirements engineering*. 2005. vol. 10. no. 1. pp. 34–44.
17. Matulevicius R., Mayer N., Heymans P. Alignment of misuse cases with security risk management. Third International Conference on Availability, Reliability and Security (ARES 08). 2008. pp. 1397–1404.
18. Kupriyanovskij V.P., Namiot D.E., Sinyagov S.A. [Cyber-physical systems as the basis of the digital economy]. *International Journal of Open Information Technologies*. 2016. vol. 4. no. 2. pp. 18–24. (In Russ.).
19. Wolf W. Cyber-physical systems. *Computer*. 2009. vol. 3. pp. 88–89.
20. Belenkov V.G., Budzko V.I., Sinicyn I.N. *Katastrofoustojchivost' korporativnyh informacionnyh sistem* [Catastrophic stability of corporate information systems]. Part 1. M.: IPI RAN. 2002. (In Russ.).
21. Belov P.G. *Sistemnyj analiz i modelirovanie opasnyh processov v tekhnosfere: Uchebnoe posobie dlya stud. vyssh. ucheb. zaedenij* [System analysis and modeling of dangerous processes in the technosphere: Textbook for students of higher educational institutions]. M.: Izdatel'skij centr «Akademiya». 2003. 512 p. (In Russ.).

22. Budzko V.I., Belenkov V.G., Kejer P.A. [Problems of Creation of Disaster-Tolerant Automated Systems of Banking Settlements]. *Sistemy i sredstva informatiki — Systems and Means of Informatics*. 2002. vol. 12. pp. 48–57. (In Russ.).
23. Yusupov R.M. et al. [New scientific direction in creating technologies for situational management in emergency situations]. *Trudy Mezhdunarodnaoj Nauchnaoj SHkoly «Modelirovanie i Analiz Bezopasnosti i Riska v Slozhnyh Sistemah (MA BR-2007)»* [Proceedings of the International Scientific School "Modeling and Analysis of Security and Risk in Complex Systems (MA BR-2007)"]. 2007. pp. 94–99. (In Russ.).
24. Ohtilev M.Ju., Sokolov B.V., Jusupov R.M. *Intellektual'nye tehnologii monitoringa i upravlenija strukturnoj dinamikoj slozhnyh tehnicheskih ob'ektov* [Intellectual technologies of monitoring and management of complex technical objects structural dynamics] M.: Nauka. 2006. 410 p. (In Russ.).

Teilans Artis Andreevich — Ph.D., Dr. Sci., professor, head of information and communications technologyresearch centre, Rezekne Academy of Technologies. Research interests: software engineering, discrete event computer simulation, design of domain specific languages. The number of publications — 25. artis.teilans@rta.lv; 115, Atbrivosanas aleja, LV-5001, Latvia; office phone: +37126529669.

Romanovs Andrejs Vasil'evich — Ph.D., Dr. Sci., associate professor, deputy head of the modelling and simulation department of Institute of information technology, Riga Technical University. Research interests: modeling and design of management and industrial information systems, cybersecurity, IT governance and IT risk management, information systems for health care, e-commerce, integrated information technologies in business of logistics, as well as education in these areas.. The number of publications — 79. andrejs.romanovs@rtu.lv; 1, Kalku street, LV-1658, Riga, Latvia; office phone: +37167089514, Fax: +37167089513.

Merkuryev Yuri Anatolievich — Dr. Habil., professor, Academician of the Latvian Academy of Sciences, head of the modelling and simulation department of Institute of information technology, Riga Technical University. Research interests: modelling and simulation of complex systems, methodology of discrete-event simulation, supply chain simulation and management. The number of publications — 357. jurijs.merkurjevs@rtu.lv, http://www.itl.rtu.lv/mik/ymerk.html; 1, Kalku street, LV-1658, Riga, Latvia; office phone: +37129454253, Fax: +37167089513.

Dorogovs Pjotrs Petrovich — chief of information centre, Ministry of Interior of Republic of Latvia. Research interests: architecture modeling of integrated information systems, governance of IT, cybersecurity. The number of publications — 20. Pjotrs.dorogovs@inbox.lv; 1, Kalku str., LV-1658, Riga, Latvia; office phone: +37167089514.

Kleins Arnis Yanovich — software developer, Computer Hardware Design Ltd. Research interests: software engineering, discrete event computer simulation, design and development of domain specific languages. The number of publications — 12. arnis12321@gmail.com; 17, Draudzibas iela, LV-5001, Ogre, Latvia; office phone: +37129491955.

Potryasaev Semen Alekseevich — Ph.D., senior researcher of laboratory for information technologies in systems analysis and modeling, St. Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences (SPIIRAS). Research interests: system analysis and operations research, theory of managing the structural dynamics of complex organizational and technical systems. The number of publications — 90. spotryasaev@gmail.com, http://litsam.ru; 39, 14-th Line V.O., St. Petersburg, 199178, Russia; office phone: +7(812)328-0103, Fax: +7(812)328-4450.

Acknowledgements. The research described in Section 5 supported by the state research #0073–2018–0003 (# of state registr. AAAA-A16-116030250074–1).

УДК 004 **DOI** 10.15622/sp.59.5

А.А. Тейланс, А.В. Романов, Ю.А. Меркурьев, П. Дорогов,
А.Я. Клейнс, С.А. Потрясаев

ОЦЕНКА РИСКОВ КИБЕРФИЗИЧЕСКИХ СИСТЕМ С ИСПОЛЬЗОВАНИЕМ МОДЕЛИРОВАНИЯ ДОМЕНОВ И ИМИТАЦИОННОГО МОДЕЛИРОВАНИЯ

Тейланс А.А., Романов А.В., Меркурьев Ю.А., Дорогов П.П., Клейнс А.Я., Потрясаев С.А.
Оценка рисков киберфизических систем с использованием моделирования доменов и имитационного моделирования.

Аннотация. В настоящее время системы, разрабатываемые для интеграции реальных физических процессов и виртуальных вычислительных процессов — киберфизических систем (КФС), используются во многих областях промышленности и национальной инфраструктуры, таких как производство, медицина, управление транспортом и безопасность, автомобилестроение, управление промышленными процессами, энергосбережение, экологический менеджмент, промышленные роботы, управление технической инфраструктурой, распределенные роботизированные системы, целевые системы защиты, технологии нанотехнологий и биологических систем. При широком использовании подобных систем уровень ИТ-рисков и киберрисков резко возрастает, в результате чего атаки против КФС могут привести к неуправляемым и непредсказуемым последствиям. Таким образом, существует необходимость в хорошо продуманной системе оценки рисков КФС, что обеспечит общее представление о состоянии безопасности КФС, а также эффективное распределение защищаемых ресурсов. Характер КФС отличается от ИТ-систем главным образом потребностью в операциях реального времени, поэтому традиционный метод оценки рисков для ИТ-систем может быть адаптирован для условий работы КФС. Разработка языка моделирования доменов (“domain specific language”, DSL), основанного на унифицированном языке моделирования UML и описанного в данной статье, обеспечивает синергизм широко используемой в ИТ-индустрии методики с используемыми в конкретных областях подходами к управлению рисками. В отличие от традиционного использования UML для целей имитационного моделирования, описанный в статье язык моделирования DSL обогащен набором стохастических атрибутов моделируемых процессов. Подобные стохастические атрибуты можно использовать для дальнейшей реализации дискретно-событийных симуляторов.

Ключевые слова: киберфизические системы, информационные технологии, риски, оценка рисков, язык моделирования доменов, моделирование, UML, CORAS, катастрофоустойчивые киберфизические системы, структурная динамика.

Тейланс Артис Андреевич — д-р техн. наук, профессор, руководитель научно-исследовательского центра информационных и коммуникационных технологий, Резекненская технологическая академия. Область научных интересов: программная инженерия, имитационное моделирование дискретно-событийных систем, разработка доменно-специфичных языков программирования. Число научных публикаций — 25. artis.teilans@rta.lv; аллея Освобождения, 115, LV-4601, Резекне, Латвия; р.т.: +37126529669.

Романов Андрей Васильевич — д-р техн. наук, доцент, заместитель заведующего кафедрой имитационного моделирования института информационных технологий, Рижский технический университет. Область научных интересов: моделирование и проектирование управленческих и индустриальных информационных систем,

кибербезопасность, управление ИТ и рисками, информационные системы для здравоохранения, электронная коммерция, интегрированные ИТ в логистике и цепях поставок, а также образование в этих областях. Число научных публикаций — 79. andrejs.romanovs@rtu.lv; ул. Калкю, 1, LV-1658, Рига, Латвия; р.т.: +37167089514, Факс: +37167089513.

Меркурьев Юрий Анатольевич — Dr. Habil., профессор, академик Латвийской академии наук, заведующий кафедрой имитационного моделирования института информационных технологий, Рижский технический университет. Область научных интересов: имитационное моделирование сложных систем, методология дискретно-событийного имитационного моделирования, моделирование логистических систем и цепей поставок и управление ими. Число научных публикаций — 357. jurijs.merkurjevs@rtu.lv, http://www.itl.rtu.lv/mik/ymerk.html; ул. Калкю, 1, LV-1658, Рига, Латвия; р.т.: +37129454253, Факс: +37167089513.

Дорогов Пётр Петрович — начальник информационного центра, Министерство внутренних дел Республики Латвия. Область научных интересов: моделирование архитектур интегрированных информационных систем, управление ИТ, кибербезопасность. Число научных публикаций — 20. Pjotrs.dorogovs@inbox.lv; ул. Калкю, 1, LV-1658, Рига, Латвия; р.т.: +37167089514.

Клейнс Арнис Янович — разработчик программного обеспечения, Computer Hardware Design Ltd. Область научных интересов: программная инженерия, имитационное моделирование дискретно-событийных систем, разработка доменно-специфичных языков программирования. Число научных публикаций — 12. arnis12321@gmail.com; ул. Драудзибас, 17, LV-5001, Огре, Латвия; р.т.: +37129491955.

Потрясаев Семен Алексеевич — к-т техн. наук, старший научный сотрудник лаборатории информационных технологий в системном анализе и моделировании, Федеральное государственное бюджетное учреждение науки Санкт-Петербургского института информатики и автоматизации Российской академии наук (СПИИРАН). Область научных интересов: системный анализ и исследование операций, теория управления структурной динамикой сложных организационно-технических систем. Число научных публикаций — 90. spotryasaev@gmail.com, http://litsam.ru; 14-я линия В.О., 39, Санкт-Петербург, 199178; р.т.: +7(812)328-0103, Факс: +7(812)328-4450.

Поддержка исследований. Результаты исследований, представленные в разделе 5, осуществлялись при финансовой поддержки госбюджетной темы №0073–2018–0003 (№ гос. регистр. АААА-А16-116030250074–1).

Литература

1. *Biro M., Mashkoor A., Sametinger J., Seker R.* Software Safety and Security Risk Mitigation in Cyber-physical Systems // IEEE Software. 2018. vol. 35. no. 1. pp. 24–29.
2. *Hu F.* Cyber-Physical Systems: Integrated Computing and Engineering Design // New York: CRC Press. 2018. 398 p.
3. *Romanovs A.* Security in the Era of Industry 4.0 // 2017 Open Conference of Electrical, Electronic and Information Sciences (eStream). 2017. 1 p.
4. *Klimov R., Reznik A., Solovjova I., Slihte J.* The Development of the IT Risk Management Concept // Computer Science. 2008. vol. 5. pp. 131–139.
5. *Romanovs A., Merkuryev Y., Klimov R., Solovjova I.A* Technique for Operational IT Risk Management in Latvian Monetary and Financial Institutions // Proc. of 8th WSEAS International Conference on Applied Computer Science «Recent Advances on Applied Computer Science». 2008. pp. 230–235.

6. *Teilans A. et al.* Domain Specific Simulation Language for IT Risk Assessment // Proceedings 25th European Conference on Modelling and Simulation (ECMS2011). 2011. pp. 342–347.
7. *Lund M.S., Solhaug B., Stølen K.* Model-Driven Risk Analysis: The CORAS Approach // Springer. 2010. 460 p.
8. *Kleins A., Merkuryev Y., Teilans A., Filonik M.* A meta-model based approach to UML modelling and simulation // Proceedings of the 7th International Conference on System Science and Simulation in Engineering. 2008. 6 p.
9. *Skorobogatjko A., Romānovs A., Kuņicina N.* State of the Art in the Healthcare Cyber-physical Systems // Information Technology and Management Science. 2014. vol. 17. pp. 126–131.
10. Cyber-Physical Systems. URL: https://ptolemy.berkeley.edu/projects/cps/ (дата обращения: 11.02.2018).
11. *Patterson D.A., Hennessy J.L.* Computer Organization and Design: The Hardware/Software Interface: 5th ed. // Morgan Kaufmann. 2013. 800 p.
12. *Milenkovic A., Otto C., Jovanov E.* Wireless sensor networks for personal health monitoring: issues and an implementation // Computer Communications. 2006. vol. 29. no. 13-14. pp. 2521–2533.
13. *Buyya R., Broberg J., Goscinski A.* Cloud Computing: Principles and Paradigms // John Wiley & Sons. 2010. 637 p.
14. *Achim D., Brucker J.D.* Metamodel-based UML notations for domain-specific languages // Proceeding of 4th International Workshop on Language Engineering (ATEM 2007). 2007. 15 p.
15. *Lenz G., Wienands C., Greenfield J., Kozaczynski W.* Practical software factories in. NET // New York: Apress. 2006. 214 p.
16. *Sindre G., Opdahl A.L.* Eliciting Security Requirements by Misuse Cases // Requirements engineering. 2005. vol. 10. no. 1. pp. 34–44.
17. *Matulevicius R., Mayer N., Heymans P.* Alignment of misuse cases with security risk management // Third International Conference on Availability, Reliability and Security (ARES 08). 2008. pp. 1397–1404.
18. *Куприяновский В.П., Намиот Д.Е., Синягов С.А.* Кибер-физические системы как основа цифровой экономики // International Journal of Open Information Technologies. 2016. vol. 4. no. 2. pp. 18–24.
19. *Wolf W.* Cyber-physical systems // Computer. 2009. vol. 3. pp. 88–89.
20. *Беленков В.Г., Будзко В.И., Синицын И.Н.* Катастрофоустойчивость корпоративных информационных систем. Часть 1 // М.: ИПИ РАН. 2002.
21. *Белов П.Г.* Системный анализ и моделирование опасных процессов в техносфере: учебное пособие для студ. высш. учеб. заведений // М.: Издательский центр «Академия». 2003. 512 с.
22. *Будзко В.И., Беленков В.Г., Кейер П.А.* Проблемы создания катастрофоустойчивых автоматизированных систем банковских расчетов // Системы и средства информатики. 2002. Вып. 12. С. 48–57.
23. *Юсупов Р.М. и др.* Новое научное направление в создании технологий ситуационного управления в чрезвычайных ситуациях // Труды Международной Научной Школы «Моделирование и Анализ Безопасности и Риска в Сложных Системах (МА БР-2007)». 2007. С. 94–99.
24. *Охтилев М.Ю., Соколов Б.В., Юсупов Р.М.* Интеллектуальные технологии мониторинга и управления структурной динамикой сложных технических объектов // М.: Наука. 2006. 410 с.