doi:10.2478/acss-2014-0006

2014/15

Applied Computer Systems

DE GRUYTER OPEN

Security Process Capability Model Based on ISO/IEC 15504 Conformant Enterprise SPICE

Antanas Mitasiunas[1], Leonids Novickis[2], Rimas Kalpokas[3]

[1-3]*Vilnius University,* [2]*Riga Technical University*

***Abstract* – In the context of modern information systems, security has become one of the most critical quality attributes. The purpose of this paper is to address the problem of quality of information security. An approach to solve this problem is based on the main assumption that security is a process oriented activity. According to this approach, product quality can be achieved by means of process quality – process capability. Introduced in the paper, SPICE conformant information security process capability model is based on process capability modeling elaborated by world-wide software engineering community during the last 25 years, namely ISO/IEC 15504 that defines the capability dimension and the requirements for process definition and domain independent integrated model for enterprise-wide assessment and Enterprise SPICE improvement.**

***Keywords* – Enterprise SPICE, information security, process capability, Security SPICE.**

I. Introduction

Three decades ago, software developers started to seek for the established and confirmed procedures and solutions to cope with software crisis that was caused by the fact that project costs exceeded the estimated costs and schedules were not met as well as failure of functionality and quality was observed. Inspired by traditional engineers, software engineering community has developed standards and models such as ISO/IEC 15504 and CMMI that have been used by numerous software organizations around the world for guiding tremendous improvements in their ability to improve productivity and quality. The concept of software process capability, which expresses process predictability, has become an efficient working tool for process and product quality management.

The results of software engineering in terms of software process are generalized to any process capability assessment and improvement. In their turn, other "soft" engineers, e.g., innovation, follow a pioneering way of software engineers. Software engineering being an extremely creative activity has been able to express it in process oriented terms. Developed and validated enhanced innovation and technology transfer process capability maturity model [5], [18] is another successful

confirmation of the possibility to express such a creative activity as innovation in process oriented terms.

Software Engineering Institute (SEI) of Carnegie Melon University. These models have evolved into CMMI version 1.3 [7-9] known as CMMI for Development, CMMI for Acquisition and CMMI for Services.

The purpose of this paper is to validate a new approach for capability modeling and to develop ISO/IEC 15504 conformant information security process capability model as a core element of the approach proposed.

The state of the art in process capability maturity modeling and information security process modeling is provided in Sections 2 and 3. Sections 4 and 5 contain authors' contribution to process capability modeling and information security process modeling. The last Section concludes paper results achieved and provides future work to be done to complete the solution of the problem addressed.

The main idea for the modeling approach taken in this paper and the construction of a primary process category is based on a related work done in [17].

II. Motivation and Capability Modeling

Information security process capability model, introduced in the paper, is based on process capability maturity modeling elaborated by a world-wide software engineering community. Software engineering community has considerably contributed to the state of the art of process modeling. The numerous attempts to solve the software crisis applying technological and methodological approaches were not successful. Consequently, software engineers turned to the software development organizational issues aiming to keep software projects within the planned scope, schedule and resources.

This approach is based on the assumption that product quality can be achieved by means of process quality – process capability. High process capability cannot be established at once during the launch of an activity. Process capability can be improved applying iterative procedure of process capability assessment and improvement.

Process capability is related to the predictability of process results. Organizational maturity expresses the way organization activities are performed. The idea of maturity expresses the improvement path of organization activities to achieve better results. Process capability concept enables one to measure the state of performance of organization's activities at a separate process level and to plan individual steps for processes capability improvement.

The research in this area is based on ideas originated from capability maturity models (CMM) developed since 1987 by

In parallel, the international community has developed an international standard for process assessment ISO/IEC 15504: Process assessment framework, also known as project SPICE (Software Process Improvement and Capability dEtermination) initiated by the Ministry of Defence of UK in 1991 [13], [14].

ISO/IEC 15504 represents the third generation of process capability maturity models that refer to an external process reference model. The process capability assessment framework is defined in the normative part of ISO/IEC 15504-2.

In this context, an approach taken by ISO/IEC 15504 [13], [14] referring to the external process reference model is particularly important. It enables to extend the application area of the model outside software engineering. External process reference model must satisfy requirements of process definition in terms of process purpose and outcomes.

The third main source in process capability maturity arena is iCMM v2.0 (integrated Capability Maturity Model), addressing the issues of model integration and architecture representation, developed by the US Federal Aviation Administration in 2001. It influenced a lot the current state of the area of CMMs [11] and is along the same lines as ISO/IEC 15504 (SPICE) and CMMI models. Based on an external process reference model approach, the convergence of SPICE and iCMM models is possible and, in fact, it is completed as Enterprise SPICE initiative, i.e., the model FAA iCMM plays the role of baseline in the development of SPICE based Enterprise Process Reference Model and Process Assessment Model. Enterprise SPICE model consists of a Process Reference Model supplemented by a Process Assessment Model. Enterprise SPICE has been developed by a joint effort of more than one hundred experts representing 31 countries from all continents. Enterprise SPICE has been the most challenging process capability assessment and improvement initiative for the last several years. The first stage of Enterprise SPICE [10] project is completed, and the draft of the future standard is publicly available.

Hundreds of various generic and specific organizational maturity models have been developed. These models mainly provide the characteristics of maturity levels. However, very few of them provide the decomposition of an activity modelled as a collection of processes defined in minimal terms, namely, a process name, a process purpose and the process outcomes.

III. Security Process Modelling Related Work

Security is a quality attribute of a system that is often implied because of the technical difficulty to prove or demonstrate otherwise. Because of that, security engineering aspect of system development often starts in the requirement specification as a sort of a set of preemptive technical and non-technical measures that are felt to increase security and ends with the implementation of the mentioned measures. When actual security issues occur, however, the measures are taken individually and often the systematic causes of the vulnerabilities exploited are overlooked. To avoid such a situation, a way to continuously monitor and improve security measures is needed. To achieve this, dedicated security-focused processes must be defined and institutionalized. Given the process-based view of security, related process capability should be continuously evaluated (assessed) and improved. Objective assessment is deemed impossible without a reference model, which, in this case, is an information security process reference model. Once the information security process reference model is developed, process capability assessment and improvement, and, therefore, systematic increase in security become manageable tasks. Moreover, the need for systematic assessment and improvement of security is growing with the development of complex information systems, cloud computing being the primary example. Cloud computing relies on trust between a cloud service provider and a consumer. It is believed that trust must be based on something provable, i.e., certification. Certification of various important aspects of cloud computing providers is foreseen to be required and it is already under development [20]. Certification usually has a reference, to which the system evaluated can be qualitatively or even quantitatively compared. The security certification can be based on process capability assessment using the Information Security Process Capability Model presented in this paper.

Enterprise SPICE can be seen as a universal tool for modeling various process-oriented activities that comprise an organization’s information processing system (the term “information processing system” is understood as including every element of an organization that produces, transfers or uses information manipulated by its processes, including hardware, software, people and infrastructure). For the case of the model being universal and domain-independent, its process categories cannot include application-specific processes. On the other hand, specific quality attributes such as security and safety are very important in every information-processing system. Therefore, foreseeing that security and safety might not be unique in this respect, “Special Applications” area was conceived introducing an additional process covering the specific area, namely *SAP.1. Safety and Security* [10], [12]. It defines Application Practices as goals to be achieved by implementing process areas in a way of intentionally applying security and safety to base practices without naming them specifically. The knowledge of the concrete methodology of how these application practices are performed is implied rather than specified and, therefore, strongly relies on an implementer. Therefore, we can state that Enterprise SPICE defines security and safety as attributes applied to the existing processes but not a process-based activity. The same, with some reservations, can also be said about the safety extensions to the ISO/IEC 15504 (Part 10) [15], +SAFE safety extensions to the CMMI-DEV [19] and the work done on security extensions to the ISO/IEC 15504 [16].

The US Federal Aviation Administration has viewed the iCMM as being insufficient in providing a framework for assessing and improving safety and security of a system, and, therefore, it has created and published Safety and Security Extensions for Integrated Capability Maturity Models [12]. It must be noted that the evolutionary close relationship between the iCMM and Enterprise SPICE allows, with minor corrections, the application of these extensions to the Enterprise SPICE. These extensions provide the relationship between Application Practices and Base Practices and additional implementation guidance.

BSI publications [3], [4] on information security management systems provide comprehensive information security body of knowledge that can be used as a source for the codifying of information security knowledge in process oriented terms.

ISO/IEC 15504 conformant capability modeling of the information security management process is addressed by research conducted at the Public Research Centre Henri Tudor in Luxembourg [1], [2] with an aim to facilitate the adoption of security management systems for SMEs based on the development of a process reference model and a process implementation model.

IV. Validation of a New Method for Process Capability Modeling

The main idea of this research is to integrate an application dependent SPICE conformant process modeling with the application independent capability dimension and process dimension components. The goal of such integration is to keep the application dependent component as simple as possible and to maximize domain independent reusable part of process capability assessment model for the improvement of a process-oriented activity.

ISO/IEC 15504 introduces the concepts of a capability measurement framework and requirements for external process model. This enables to minimize the efforts for creation of a process capability assessment model only by forming a SPICE conformant external process model. ISO/IEC 15504 capability dimension can be reused.

In addition, Enterprise SPICE as a generic SPICE conformant and domain independent external process model can be applied. It consists of Life Cycle, Organizational and Support Process categories.

Enterprise SPICE is defined at a quite abstract and low granularity level. In order to express domain dependent issues, the processes of Application category should be defined to address the body of knowledge of a particular application area that is not represented at a sufficient level by the Enterprise SPICE process model.

Therefore, the development of SPICE conformant process capability model for a particular application domain can be restricted by the development of description of the Application category processes only.

Enterprise SPICE model applies almost the same but not identical concept of Application area introduced in [10] that consists of application practices. An application practice is implemented by a set of base practices that belong to one or more Enterprise SPICE processes. To assess the capability of an application area and application practices, the associated base practices shall be assessed in the context of their performance for application practices. In this case, the body of knowledge of an application area should implicitly define the performance context of base practice to be assessed.

The purpose of Application process category concept introduced in the present paper is to reflect directly the body of knowledge in terms of essential processes and base practices of application that are not represented by the Enterprise SPICE model at the extent needed by the improvement task.

The application of provided methodology enables to develop an application dependent process capability model which is a SPICE conformant model that reuses the ISO/IEC 15504 capability framework. It also reuses the Life Cycle, Organizational and Support Process categories from the Enterprise SPICE process dimension and provides the Application category's processes, which satisfy the requirements to process a definition established by ISO/IEC 15504. The Application category can consist of processes that further extend or detail the Life Cycle, Organizational and Support Process categories.

Organizational and Support Process categories are less application domain dependent compared to the Life Cycle Process category. In this paper, the Application Process category, called here Primary Process category, is composed of Life Cycle Process category supplemented by domain dependent processes.

The goal of the development of Information Security Process Capability Model is to build a framework that describes security as a process-oriented activity and is sufficiently detailed as a tool for any organization that wishes to assess and increase the capability of the security quality attribute of its processes in the context of enterprise-wide process improvement.

The supplementation of Enterprise SPICE with application area specific knowledge transforms it from a domain-independent model to a domain-dependent model. Focusing on information security potentially narrows its applicability; the model does not enforce any processes that would limit a set of organizations to Information Technology or related domains aside from having an information system, the security of which is the main focus of the model.

Next section implements the methodology for effort minimization of domain dependent process capability modeling outlined in the present paper for information security assurance area to validate the approach provided and to create a new information security process capability assessment model.

V. Information Security Process Capability Model

Information security process capability assessment and improvement are based on a process capability assessment model as a core tool for quality management. An idea is to build a new SPICE conformant process capability model called Information Security Process Capability Model as an external Process Assessment Model according to requirements [13] using the Enterprise SPICE capability model that refers to the capability framework defined in the normative part ISO/IEC 15504-2.

The Process Reference Model of Information Security Process Capability Model consists of Primary, Organizational and Support Process categories (see Fig. 1 below).

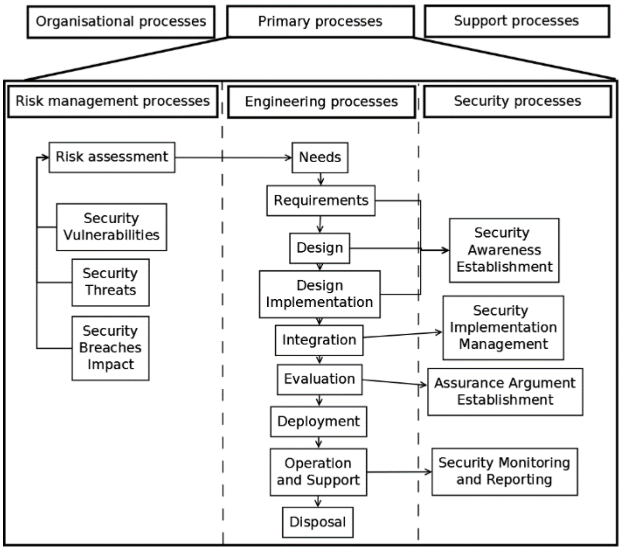

Fig. 1. Information Security Process Capability Model: relationship of the Primary Process category processes.

Organizational and Support Process categories are reused from [10]. Primary Process category is composed of three subcategories: Security Risk Management Process subcategory, Engineering Process subcategory and Security Process subcategory.

The Security Risk Management and Security Process subcategories are based on corresponding security practices from [6], [12]. They contain the processes that represent the security domain-specific knowledge. The Engineering Process subcategory comprises processes that are based on the Life Cycle Process category from the Enterprise SPICE.

According to ISO/IEC 15504-2, requirements for the process description of the Process Reference Model (PRM) must be done in minimal terms of process purpose and outcomes that are achieved as a result of process successful implementation. In addition to PRM, the Process Assessment Model of Information Security Process Capability Model contains a set of indicators that explicitly addresses the purpose and outcomes, as defined in the PRM, and that demonstrates the achievement of the process attributes. Description of Information Security Process Capability Model processes that belong to Primary Process category, excluding the Engineering Process subcategory that is reused from the Enterprise SPICE, is provided in Table I.

TABLE I.

INFORMATION SECURITY PROCESS CAPABILITY ASSESSMENT MODEL: SECURITY RISK MANAGEMENT AND SECURITY PROCESS SUBCATEGORIES

PRIM.RISK.1. Security Vulnerabilities	
Purpose	**Outcomes**
To identify, analyze and report information security vulnerabilities of an artifact to be protected	1) Information security vulnerability analysis strategy is developed and maintained; 2) Vulnerabilities are identified; 3) Vulnerabilities are analyzed; 4) Dependent vulnerabilities are derived; 5) Information security vulnerabilities are reported.
Base Practices	
PRIM.RISK.1.BP.1: Develop and maintain information security vulnerability analysis strategy. [Outcome: 1] PRIM.RISK.1.BP.2: Identify vulnerabilities. [Outcome: 2] PRIM.RISK.1.BP.3: Analyze vulnerabilities. [Outcome: 3] PRIM.RISK.1.BP.4: Derive vulnerabilities. [Outcome: 4] PRIM.RISK.1.BP.5: Report information security vulnerabilities of an artifact. [Outcome: 5]	
PRIM.RISK.2. Security Threats	
Purpose	**Outcomes**
To identify, analyze and report information security threats for an artifact to be protected	1) Analysis strategy of information security threats is developed and maintained; 2) Natural threats are identified; 3) Man-made threats are identified; 4) Threats are analyzed; 5) Likelihood of threats is assessed; 6) Information security threats are reported.
Base Practices	
PRIM.RISK.2.BP.1: Develop and maintain the analysis strategy of information security threats. [Outcome: 1] PRIM.RISK.2.BP.2: Identify natural threats. [Outcome: 2] PRIM.RISK.2.BP.3: Identify man-made threats. [Outcome: 3] PRIM.RISK.2.BP.4: Analyze threats in the operation environment of an artifact. [Outcome: 4] PRIM.RISK.2.BP.5: Assess likelihood of threats. [Outcome: 5] PRIM.RISK.2.BP.6: Report information security threats of an artifact. [Outcome: 6]	
PRIM.RISK.3. Impact of Security Breaches	
Purpose	**Outcomes**
To identify, analyze and report the impact of information security breaches on an artifact to be protected	1) Analysis strategy of the impact of information security breaches is developed and maintained; 2) Assets to be protected are identified; 3) Impacts are identified; 4) Impacts are analyzed; 5) Impacts are reported.
Base Practices	
PRIM.RISK.3.BP.1: Develop and maintain the analysis strategy of the impact of information security breaches. [Outcome: 1] PRIM.RISK.3.BP.2: Identify and categorize assets potentially affected by information security breaches. [Outcome: 2] PRIM.RISK.3.BP.3: Identify impacts. [Outcome: 3] PRIM.RISK.3.BP.4: Analyze impacts. [Outcome: 4] PRIM.RISK.3.BP.5: Categorize impacts. [Outcome: 4] PRIM.RISK.3.BP.6: Report impacts. [Outcome: 5]	
PRIM.RISK.4. Security Risk Assessment	
Purpose	**Outcomes**
To identify, assess and report information security risks of an artifact operated in a defined environment	1) Information security risk assessment strategy is developed and maintained; 2) Risk factors are identified; 3) Risk factors are assessed and categorized; 4) Risks are prioritized; 5) 6) Risks are monitored and reported.

Base Practices
PRIM.RISK.4.BP.1: Develop and maintain information security risk assessment strategy. [Outcome: 1]
PRIM.RISK.4.BP.2: Identify risk factors. [Outcome: 2]
PRIM.RISK.4.BP.3: Assess and categorize risk factors. [Outcome: 3]
PRIM.RISK.4.BP.4: Prioritize risks. [Outcome: 4]
PRIM.RISK.4.BP.5: Monitor and report risks. [Outcome: 5]

PRIM.SEC.1. Security Awareness Establishment	
Purpose	**Outcomes**
To provide knowledge needed for information security task definition, solution implementation and usage	1) Information security awareness establishment strategy is developed and maintained; 2) Information security needs and requirements are known and communicated; 3) Information security requirements are understood for the design and implementation of an artifact; 4) Information security constraints are understood for the operation of an artifact.
Base Practices	
PRIM.SEC.1.BP.1: Develop and maintain information security awareness establishment strategy. [Outcome: 1] PRIM.SEC.1.BP.2: Communicate information security needs and requirements. [Outcome: 2] PRIM.SEC.1.BP.3: Understand information security needs and requirements for the implementation of an artifact. [Outcome: 3] PRIM.SEC.1.BP.4: Communicate information security constraints to users. [Outcome: 4] PRIM.SEC.1.BP.5: Understand information security constraints for the operation of an artifact. [Outcome: 4]	

PRIM.SEC.2. Security Implementation Management	
Purpose	**Outcomes**
The required information security is provided in the operation of an artifact	1) Information security implementation management strategy is developed and maintained; 2) Information security responsibilities for the whole life cycle are established; 3) Information security awareness is managed; 4) Information security control mechanisms are established and managed.
Base Practices	
PRIM.SEC.2.BP.1: Develop and maintain information security implementation management strategy. [Outcome: 1] Establish security responsibilities. [Outcome: 1] PRIM.SEC.2.BP.2: Establish information security responsibilities for the whole life cycle of an artifact. [Outcome: 2] PRIM.SEC.2.BP.3: Manage information security awareness of all stakeholders. [Outcome: 3] PRIM.SEC.2.BP.4: Establish and manage information security control mechanisms. [Outcome: 4]	

PRIM.SEC.3. Assurance Argument Establishment	
Purpose	**Outcomes**
To establish and maintain security assurance arguments and support evidence throughout the life cycle.	1) Strategy of information security assurance argument establishment is developed and maintained; 2) Information security assurance objectives are identified; 3) Information security assurance evidences are analyzed; 4) Information security assurance arguments are provided.
Base Practices	
PRIM.SEC.3.BP.1: Develop and maintain the strategy of an information security assurance argument establishment. [Outcome: 1] PRIM.SEC.3.BP.2: Identify information security assurance objectives. [Outcome: 2] PRIM.SEC.3.BP.3: Analyze information security assurance evidences. [Outcome: 3] PRIM.SEC.3.BP.4: Provide information security assurance argument. [Outcome: 4]	

PRIM.SEC.4. Security Monitoring and Reporting	
Purpose	**Outcomes**
To establish and maintain independent monitoring and reporting of information security status and issues	1) Information security monitoring and reporting strategy is developed and maintained; 2) Event records are analyzed; 3) Information security incidents are identified; 4) Information security incidents are analyzed; 5) Information security incidents are reported.
Base Practices	
PRIM.SEC.4.BP.1: Develop and maintain information security monitoring and reporting strategy. [Outcome: 1] PRIM.SEC.4.BP.2: Analyze event records. [Outcome:2] PRIM.SEC.4.BP.3: Identify security incidents. [Outcome: 3] PRIM.SEC.4.BP.4: Analyze security incidents. [Outcome: 4] PRIM.SEC.4.BP.5: Report security incidents. [Outcome: 5]	

VI. Conclusion and Further Research

The paper provides the following new results in process capability modeling and information security process capability assessment and improvement:

1) A validated method for SPICE conformant process capability modeling based on ISO/IEC 15504 capability framework and Enterprise SPICE domain independent external process model is proposed;
2) Based on the proposed methodology, a SPICE conformant Process Assessment Model called an Information Security Process Capability Model is developed.

Future research directions: validation of an application dependent process capability modeling approach versus application area implementation by referencing to base practices of domain independent process model; development of an approach to assessment and improvement of organization’s security process based on the information security process capability assessment model presented in this paper.

VII. Acknowledgements

The research has been partly supported by the project eINTERASIA "ICT Transfer Concept for Adaptation, Dissemination and Local Exploitation of European Research Results in Central Asia's Countries", grant agreement No. 600680 of Seventh Framework Program Theme ICT-9.10.3: International Partnership Building and Support to Dialogues for Specific International Cooperation Actions – CP-SICA-INFSO.

References

[1] Mangin, O., Barafort, B., Heymans, P., Dubois, E.: Designing a Process Reference Model for Information Security Management Systems. In: Mas, A., Mesquida, A., Rout, T., O'Connor, R.V., Dorling, A (Eds.) SPICE 2012, CCIS, vol. 290, Heidelberg, Springer (2012), p. 129-140.

[2] Barafort, B., Humbert, J.P., Poggi, S.: Information security management and ISO/IEC 15504: the link opportunity between security and quality. In Proceedings of the 6th International SPICE Conference on Process Assessment and Improvement (SPICE 2006), Luxembourg, (2006): http://alpha.nyit.edu/som/faculty/khoo/spring2012/mist757/others/wp13_spice.pdf

[3] Information Security Management Systems (ISMS), BSI-Standard 100-1, Version 1.5. May, 2008, www.bsi.bund.de

[4] IT-Grundschutz Methodology, BSI-Standard 100-2, Version 2.0. May 2008, www.bsi.bund.de

[5] Boronowsky, M., Woronowicz, T., Mitasiunas, A. BONITA – Improve Transfer from Universities for Regional Development. The Proceedings of the 3rd ISPIM Innovation Symposium held in Quebec City, 2010: http://www.ispim.org/members/proceedings/Quebec10/commonfiles/files/26728727_Paper.pdf

[6] Cloud Computing. Benefits, risks and recommendations for information security. European Network and Information Security Agency (ENISA), 2009: https://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment

[7] CMMI-ACQ, 2010. CMMI for Acquisition, Version 1.3. Software Engineering Institute: www.sei.cmu.edu/reports/10tr032.pdf

[8] CMMI-DEV, 2010. CMMI for Development, Version 1.3. Software Engineering Institute: www.sei.cmu.edu/reports/10tr033.pdf

[9] CMMI-SVC, 2010. CMMI for Services, Version 1.3. Software Engineering Institute: www.sei.cmu.edu/reports/10tr034.pdf

[10] Enterprise SPICE An Integrated Model for Enterprise-wide Assessment and Improvement. Technical Report - Issue 1. The Enterprise SPICE Project Team, September 2010, p. 184, www.enterprisespice.com/page/publication-1

[11] Ibrahim, L., Bradford, B., Cole, D., LaBruyere, L., Leinneweber, H., Piszczek, D., Reed, N., Rymond, M., Smith, D., Virga, M., Wells, C. FAA-iCMM. The Federal Aviation Administration Integrated Capability Maturity Model for Enterprise-wide Improvement. U.S. Federal Aviation Administration, published by FAA (2001), p. 480.

[12] Ibrahim, L., Jarzombek, J., Ashford, M., Bate, R., Croll, P., Horn, M., LaBruyere, L., Wells, C., 2004. Safety and Security Extensions for Integrated Capability Maturity Models. U.S. Federal Aviation Administration: https://buildsecurityin.us-cert.gov/sites/default/files/SafetyandSecurityExt-Sep2004.pdf

[13] ISO/IEC 15504-2, 2003. Information Technology – Process Assessment – Part 2: Performing an Assessment. ISO, Geneva (2003), p. 26

[14] ISO/IEC 15504-5, 2006. Information Technology – Process Assessment – Part 5: An Exemplar Process Assessment Model. ISO, Geneva (2006), p.172

[15] ISO/IEC 15504-10, 2011. Information Technology – Process Assessment – Part 10: Safety Extension. Technical specification. ISO, Geneva (2011). p.32

[16] Mesquida, A. L., Mas, A., Amengual, E. An ISO/IEC 15504 Security Extension. In: Rout, t., O'Connor, R.V., Rout, T., MaCaffery, F., Dorling, A (Eds.) SPICE 2011, CCIS, vol. 155, Heidelberg, Springer (2011), p.64-72

[17] Mitašiūnas, A., Novickis, L. Enterprise SPICE based education capability maturity model. In: Niedrite, L., Strazdina, R., Wangler, B. (eds.) BIR 2011 Workshops. LNBIP, vol. 102-116, Heidelberg, Springer (2012), p. 106-116

[18] Novickis, L., Lesovskis, A., Mitasiunas, A. Technology Transfer Model and Web-based Solution for Transport Logistics Service Providers. Proceedings of the European Computing Conference (ECC'11), Wisconsin, USA , WSEAS, Stevens Point (2011), p. 65-74

[19] +SAFE. A Safety Extension to CMMI-DEV, version 1.2. Software Engineering Institute, 2007: http://www.sei.cmu.edu/reports/07tn006.pdf

[20] Sunyaev, A., Schneider, S. Cloud Services Certification. Communications of the ACM. Volume 56, issue 2 (2013), p. 33-36. http://dx.doi.org/10.1145/2408776.2408789

Antanas Mitasiunas is an Associate Professor at the Computer Science Department of Vilnius University and Founder and Managing Director of the software development company MitSoft Ltd. He obtained his doctoral degree in 1981 from Moscow University. He is the author of 70 scientific publications. He has been a Lithuanian national expert of EU FP7 ICT Committee, 2007-2010. He has been involved in EU-funded projects: SQUARE - INCO COPERNICUS Joint Research project, 1995-1997, MitSoft coordinator; BONITA - Baltic Sea Region INTERREG project, 2008-2012, VU coordinator and he is involved in eINTERASIA – FP7 International cooperation project, 2013-2015 as WP leader. He is the elected board member of the world-wide project Enterprise SPICE and also architecture team member, key developer, editorial team member and reviewer of Enterprise process capability model. He has been an associated editor of international journal "The Tamkang Journal of Science and Engineering (TKJSE)" since 2000. His research fields include process capability assessment and improvement, innovation and technology transfer process capability modeling, solutions for electronic document specification, creation and verification.
E-mail: antanas.mitasiunas@maf.vu.lt

Leonids Novickis is the Head of Division of Applied Systems Software. He obtained Dr.sc.ing. degree in 1980 and Dr.habil.sc.ing. degree in 1990 from the Latvian Academy of Sciences. He is the author of 180 publications. Since 1994 he has been regularly involved in different EU-funded projects: AMCAI (INCO COPERNICUS, 1995-1997) – WP leader; DAMAC-HP (INCO2, 1998-2000), BALTPORTS-IT (FP5, 2001-2003), eLOGMAR-M (FP6, 2004-2006) – scientific coordinator; IST4Balt (FP6, 2004-2007), UNITE (FP6, 2006-2008) and BONITA (INTERREG, 2008-2012) – RTU coordinator; LOGIS, LOGIS-Mobile and SocSimNet (Leonardo da Vinci) – partner. He was an independent expert of IST and Research for SMEs in FP6 and FP7. He is a corresponding member of the Latvian Academy of Sciences and an elected expert of the Latvian Council of Science. His research fields include web-based applied software system development, business process modeling, e-learning and e-logistics.
E-mail: leonids.novickis@rtu.lv

Rimas Kalpokas is a Software Developer and a Researcher at MIT-SOFT, Ltd. Since 2011 he has been regularly involved in EU funded research programs INTELEKTAS LT and INTELEKTAS LT 2 as a researcher and developer. He obtained BSc (2009) and MSc (2011) degrees in Computer Science from Vilnius University. His research areas include information security process, process modeling and cloud computing platforms.
E-mail: rimas.kalpokas@gmail.com