ISSN 2278-5612

Model-based Framework for Change Management and Integrated Development of Information Security

Anna Medve
Department of Electrical Engineering and Information Systems, University of Pannonia, Veszprém, Hungary
medve@almos.uni-pannon.hu

ABSTRACT

This paper introduces a business process-based goal-oriented framework which consists of generic and specific model repositories, and of methodology for integrated change management of business and IT evolutions. Sets of generic models of ISO/IEC 27001 and 27002 standards for information security support developers and decision makers in MDE process. The techniques and tools used are from the User Requirements Notation technologies for model compositions and traceability assessments of goal-oriented and scenario-based models. An example is given from the instantiation of framework for B2B change management with empirical validation within a commercial SME. The framework supports MDE process of enterprise architecture re-engineering integrating the development of information security.

Indexing terms/Keywords

Business and IT alignment, Change Management, Standard-based Information Security Engineering, End-user Development, User Requirements Notation, Business Process Modeling, Model Driven Engineering.

Academic Discipline and Sub-Disciplines

Computer Science; Business Management;

SUBJECT CLASSIFICATION

Computer Science Software Engineering Classification

TYPE (METHOD/APPROACH)

Experimental Research

Council for Innovative Research
Peer Review Research Publishing System
Journal: International Journal of Management & Information Technology
Vol. 5, No. 3
editor@cirworld.com
www.cirworld.com, member.cirworld.com

1. INTRODUCTION

This paper introduces the BUSITEV framework for model-based integration of BUSiness and IT EVolutions. This work is an evolution of our previous proposals for re-engineering of business systems [1-4].

The business information system's evolutions need to be integrated in technological and business plans with accentuate impact analysis and security policy [5].

The goal of BUSITEV framework is to support developers and decision makers in evolutionary modeling of changes. This framework contains a collection of templates for ISO/IEC 27001/27002 standards-based information security engineering integrated in business change management with MDE technologies. It contains a versioning-based cooperative work environment for business analysts to generate strategy decisions and simulations, themselves. The BUSITEV framework acts as an MDE multi-model approach, which combines components of models, technologies, and standards to create a customized solution to a business problem or goal.

The rest of the paper is organized as follows: Section 2 presents URN technologies and introduces our approach on change management and model driven engineering. Section 3 introduces the BUSITEV framework of multi-model approach for integrated view of business goals, problems, and generic solutions. Section 4 presents examples from an instantiation of the framework for B2B evolutions. Related works are discussed in Section 5 followed by Conclusions.

2. BACKGROUND

2.1 User Requirements Notation Technologies

User Requirements Notations is a first standardization effort for user requirements engineering language that combines in one unified language goal models and scenarios from Goal-oriented Requirement Language (GRL) and Use Case Maps (UCM). URN is viewed as complementary to notations of UML2.0 OMG methodologies. The URN supporting tool is the Eclipse-based jUCMNav tool, which contains simulation engine for implementing traceability relationships between functional and quality requirements [6-10].

URN has concepts for the specification of stakeholders, goals, non-functional requirements, rationales, behavior, structure, and scenarios in use case maps. Use case maps form the functional model which scenarios can be exported in UML interaction diagrams. The unique combination of goals and scenarios found in URN enables not only to describe and analyze What, When, Who, Where, Why, and How aspects of business processes as relations to business objectives. The URN allows reasoning about alternatives from intentional ambiguity and abstraction levels for scenario interactions, performance, and architecture [10-11].

GRL goal model. A Goal-oriented Requirements Language (GRL) [6] model and its abstraction capability are shown in Figure 5. The elements of the goal tree can be connected to each other via contribution, correlation and decomposition types of relationships. URN standard supports three sample GRL evaluation mechanisms: quantitative, qualitative, as well as a mixed analysis.

UCM functional model. A Use Case Maps (UCM) [6] model is shown at Figure 4 that shows UCM model components, the processing paths with responsibilities as events in a scenario with start point and end points. The colors of the structural elements can be selected and fixed for the internal standard of an organization, as visual information of a business context. UCM allows visualizing structural and operational aspects in one functional model. For more semantics see at [ucm-jucmnav].

jUCMNav tool. The jUCMNav [7] is an open-source Eclipse plug-in that can handle URN’s concepts for integrating functional with quality requirements. jUCMNav provides integrated supports for model transformations. It can generate reports and can export diagrams in various formats.

For more details of URN, GRL, UCM, jUCMNav see at [8] the publications and reports available at the URN Virtual Library.

2.2. The Role of Business Process Modeling and Model Driven Engineering (MDE) in our Approach for Change Management Methods

Traditionally, software runs on a platform and the components are created by programming. When creating a software system this work does not mean significant costs. Problems and big costs arise when the business process and/or the IT services change due certain circumstances [12]. In order to manage the changes, determine the place of the requirements and changes and manage the dependence of the elements of the system an enhanced traceability is required between the requirements and their execution.

MDE enables the scaling of change management by modeling and simulations for optimization in order to make decisions. All this requires automation with knowledge-based human support. Scalability of MDE provides the tool-problem/tool-solution pairs with which the different experts can be involved in the processes who explore/verify the real root of the problem and validate the solutions. For example, at the modeling of the business processes on user level the shortages of process organization which cause inconsistency in the work processes among the organizational units are revealed. These are typically caused by the manually executed problem solving in the sphere of administration due to the low integrity of the enterprise application system. This way the modeling of the business processes results in the optimization of the processes and the changes of the organization at the same time as well as the required software maintenance for the problem generating change management. Business process specifications make a bridge between the problem and the solution and with them the software process can be scaled together with the technologies rendered to them [4].

MDE technologies support the embedding of traceability in the elements of the model and the methods of model management by model transformations. The modeling tools provide so called repository-based common work with mechanisms similar to the program version managing systems in the hierarchical legal system of authority.

Based on the above we generalize the redesign of business models in order to involve the decision makers and strategy development. For this the development works elements are distributed on the technology line and are supported by several languages in order to harmonies the view points and involve the decision makers in the strategy design of change management. Namely, tools and techniques are provided for business experts with URN technologies for the goal-oriented change management of business processes. When the change in the system means a new aspect, the multi-language approach is an appropriate tool for the distributed management of the viewpoints in order to coordinate the development work and integrate the results. When the change takes place because it is required that the system should follow the strategies of the business networks, it is feasible to involve the business analysts in the change of the system and adjust the changed function of the system to the new indicators in the system configuration process.

We claim that MDE in change management has the advantage to support that in a framework we generate starting with parametric solutions object and process classes, we compile parametric forms for the simulations, and we give samples for the reuse to coordinate the viewpoints of the analysts and the concerned parties. With enough practice the change phenomena in a field yield the technology and know-how property which, in the created models, contain business intelligence and knowledge, i.e., the specified business model created by the experts. The model-driven framework of change management based on, supported by URN technologies, provides the integration of the changes in existing implementation models and/or rapid development with component technologies.

2.3. Motivations for Application of URN Technologies in the business domain

In the business domain, unlike telecommunication, enterprise standards do not make up a comprehensive system regarding business processes. Generally, the particular objects are connected to the system functions through data management and according to the regulation of the organizational structures. In the activity and role centered events the data flow aspect is generally accepted for cooperation and there are elaborated tools for verification. However, for the management of system level tasks the process centered aspect is more efficient—e.g., production management, logistics, maintenance of IT systems. For the maintainers of IT systems communication in the data centered aspect is especially difficult as the execution of enterprise demands always results in changes on procedure level. Interests may emerge to manage their own efficiency among the fields and then the relations of the concerned parties may result in the clash of technocratic and bureaucratic viewpoints and generate organizational and management changes in the enterprise [13].

In enterprise systems business processes are dynamic while the services of the integrated management system (ERP) are fixed and static with a certain level of flexibility. Opposed to the procedure based work of IT processes in the field of business the management and control-monitor functions apply data and data group flow aspects for management on the level of activities. However, it has been proved that for managers the process centered aspect is more efficient as soon as they understand it e.g., when documenting work processes or when they try to improve these processes [14].

For change management an important aspect in the application of URN is with what modeling techniques and process organization the advantages of URN can be utilized to specify the problem, the solution and the alternatives for the concerned parties to make decisions. Our recommendation is the management of the outputs of business modeling and requirements development by pairing problem-solution with URN technologies. By restricting UCM paths with components and by embedding them in scenarios we answer the questions such as Where, What, With what, With whom, When, and Who does what. To the question Why we answer with the help of GRL goal trees. Ideally, change management is required with regards to the changes of business circumstances among which we can provide a relative continuity with URN goal-oriented models and traceable functional models.

2.4. Application of Use Case Maps Elements onto Process Specification Categories

Start point and end points and path ramifications shows a workflow style of UCM notations, as well as And/Or, Fork, Join points are to compose-decompose path of process variations. UCM has notations for expression of time and of organizational hierarchy. Colored components are actors and organizational elements, lines are path of the flow which contains the actions of responsibilities within a process in consecutive relative time’s units. By restricting UCM paths with components and by embedding them in scenarios we answer the questions such as Where, What, With what, With whom, When, and Who does what. To the question Why we answer with the help of GRL goal trees.

Figure 1 shows the usual basic workflow signs and the elements required to structure the business process model with regards to information passing and modularity in root-map and sub-map diagrams. The route of the process takes place along Path in which the activities receive a partial order with indication of consecutive sequence. Loops and circles are allowed in the path direction. We can provide their consistency with structure division by Static and Dynamic stubs, and/or with Conditions during validation. The textual requirements which cannot be built in functions, activities or conditions are collected by categories and are shown as notes with reference to Dynamic stubs. The hiding of the details and the hierarchy of the functions are given with static or dynamic stubs. The textual requirements which cannot be built in functions, activities or conditions are collected by categories and are shown as notes with reference to Dynamic stub. For quality expectations we can give idioms for timing, pairing, constraints, limits and asynchrony-synchronic functions whose Timer, Or-Fork, Or-Join, And-Fork, And-Join idioms are shown in Figure 2.

The checking of the wellness of the processes and the concrete cases of their execution take place with simulations in the form of scenarios, which is indicated with red color. Figure 3 shows the example of the role of the scenarios and the method of execution of their management and of execution in the development tool.

Color coding indicates the organizational units given with components and the abstract objects which mean the software solutions of the functions and with regards to the object or tools of the activities the place and mood adverbials.

Figure 4 shows an example of a validation result this and part of a scenario which answers the questions Where, What, With what and With whom.

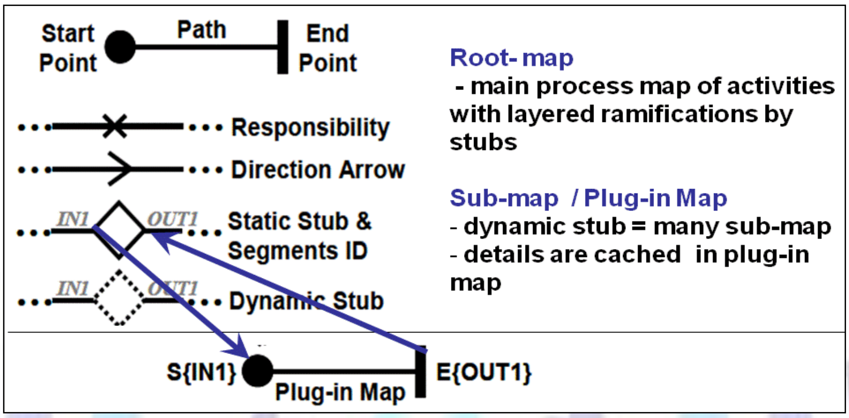

Start Point
Path
End Point
Responsibility
Direction Arrow
IN1
OUT1
Static Stub & Segments ID
IN1
OUT1
Dynamic Stub
Root- map
- main process map of activities with layered ramifications by stubs
Sub-map / Plug-in Map
- dynamic stub = many sub-map
- details are cached in plug-in map
S{IN1}
Plug-in Map
E{OUT1}

Fig 1: Structure of process model with UCM notations

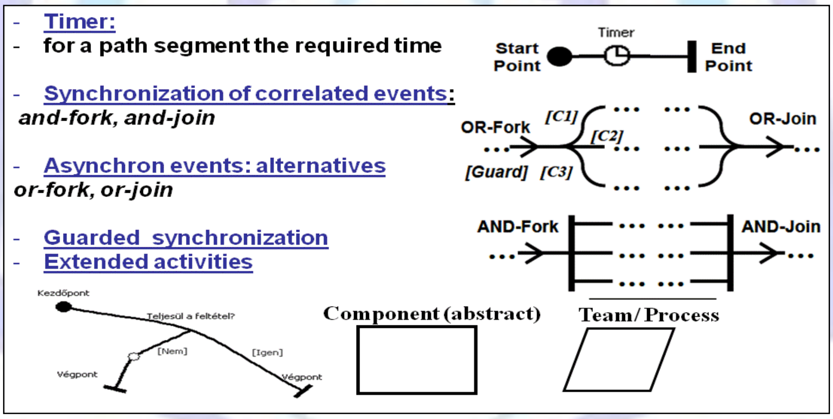


Fig 2: UCM notations form process model elements to meet quality expectations

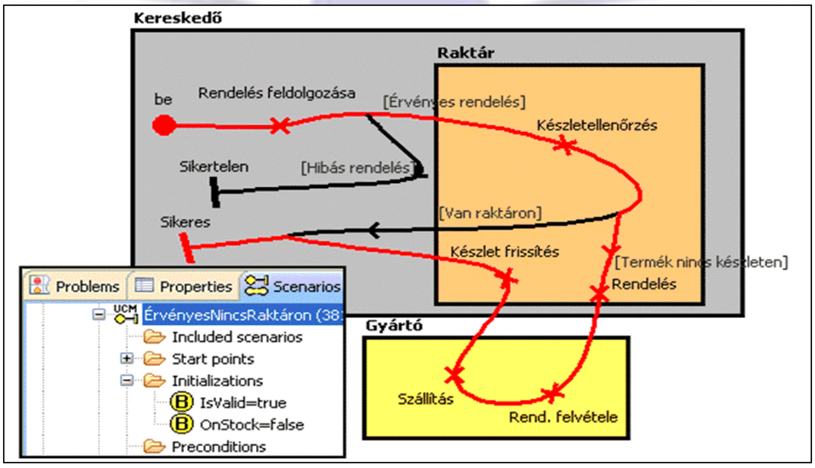


Fig 3: UCM scenario example to questions Where, What, When, With whom, Who

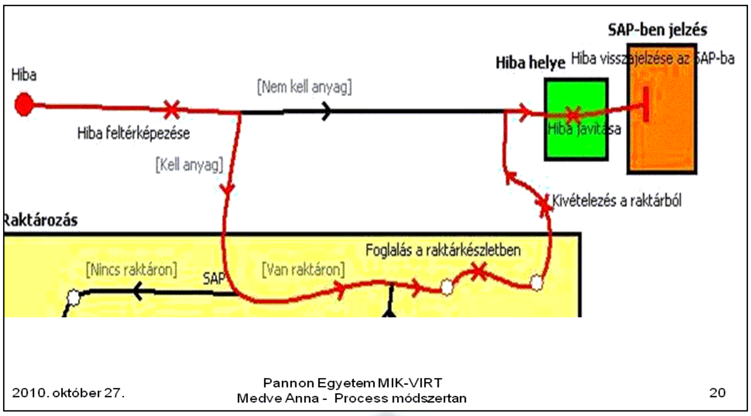


Fig 4: UCM scenario examples to questions Where, What, With what, With whom

2.5. Application of GRL Modeling for Business Strategies

With GRL modeling goal trees used by business analysts can be built to assess the strategies and connect them to the business process executing it with the application of URN Link. Figure 5 shows the elementary GRL signs: the oval is the goal and the cloud is the soft goal. The difference is in the state of execution: the goal can be executed with resources and activities but the soft goal cannot be fully executed. For this reason, along the partial goals and effects, the state of execution is observed with strategies which are followed by the decision. The task of the activities is the hexagon and the task of the resources is the square. The effect of the resources is indicated as dependency if it is indispensable for the execution. In the case of complex business goals the model is divided into actors in an ellipsis which can place a role in a distant reference. The assessments take place with the simulations of the strategies on a color scale and the scale of [-100,+100] whole numbers. It is feasible to follow the leveling of the goal tree quality technique and organize the partial goals into roles in the hierarchy of goals, soft goals, activities and resources.

For business analysts it is advantageous if they manage themselves with URN technologies to build and assess the strategies .For business analysts it is advantageous if they manage the building and assessment of the strategies themselves with URN technologies.

2.6. Visual Supports for Business Analysts and Process Managers: jUCMNav Tools

Part of URN technologies required for modeling is jUCMNav tool which is Eclipse plug-in. Further indicators are available in URN virtual directory and jUCMNav project page at http://jucmnav.softwareengineering.ca/ucm/bin/view/ProjetSEG/HelpOnLine. The visual support of jUCMNav helps business analysts and process managers and provides further possibilities for the developers [15] for the observation of efficiency and the development of designs and test models. The documentation of the results can be obtained in picture, html, rtf, and pdf formats. jUCMNav tool provide the traceability between goals and its realization in functional models.

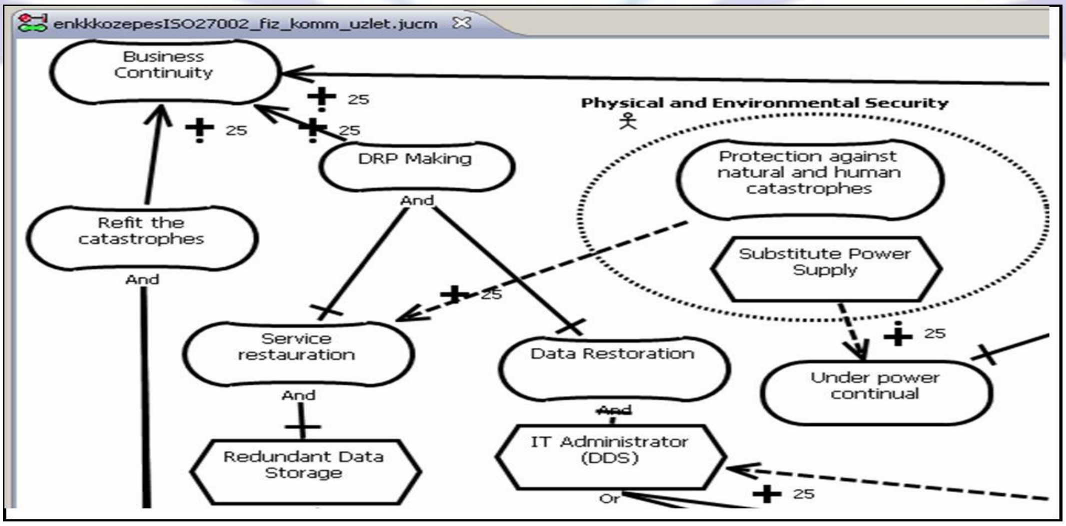


Fig 5: Generic model of security recommendations for Business Continuity information security of the ISO/IEC 27002.

3. THE BUSITEV FRAMEWORK

We built a generic goal-based framework with User Requirements Notation (URN) technologies [6-8]. Technically, URN is which offers the integration possibility of business strategies and business processes. Methodologically, the framework realization consists on instantiation of a set of customizable problems and solutions in the form of generic and specific models of domains managed within jUCMNav tool and a revision control system for model releases.

3.1 The Generic Model of the Framework

Our research context fixes the solution space as generic models from an initial development for a problem space. We obtain generic models by applying goal-orientation and classifying requirements on functional, non-functional, and extra-functional with traceability links between them. Generic goal models serve to identify the strategies for a problem space from selecting a set of possible solutions.

The identified strategies and the built goal graph help to architect functional requirements into business process model [16]. Thereby, we captured the behavioral and structural details of a strategy between problem space and solution space.

Goal-orientation helps to capture goal graphs thus identify common problems and potential solution choices, as well as the forces that have to be considered. Documenting common solutions to the identified problem should be made with adequate tools forming reusable assets.

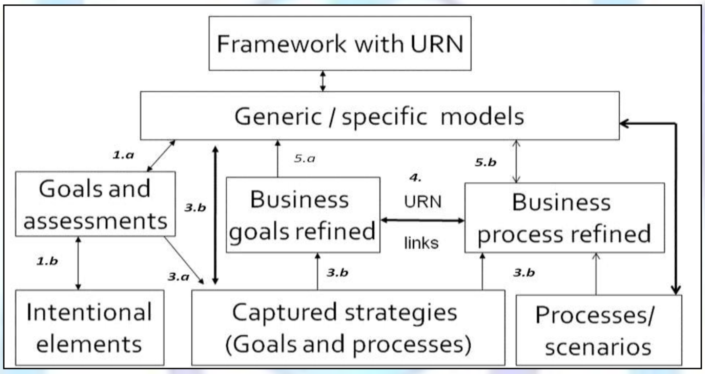


Fig 6: Generic model of BUSITEV framework.

See Figure 6 to follow how the framework creation and usage is made. The generic models form an input (1) to iteration for goal-based engineering of intentions. The generic models give also the elements of a business process/scenarios intended to be built or actualized (5.a), (5.b). Given the generic models, goals and assessments are identified from intentions and analysis of problem space (3.a). These results in captured strategies, which forms realizations as business processes or scenarios (3.b). Linking goals to realizations i.e. e. forming URN links from goal models to process models (4.), decision makers give nodes between problem space and solution space.

A repeated analysis is done during change management. URN links give traceability links for multi-model approach and for validation and simulation automation. Business goals and processes redefined can be added (3.b), (5.a), (5.b) as specific models into models repository of the framework.

The framework supports model-transformations by jUCMNav tool capabilities. These help to formalize business mechanisms as goals and scenarios, and to simulate and validate them with variations by involving business decision makers. This give an advanced conceptional design process with inclusion of business decision makers.

This framework conception supports business analysts in multi-model usage process and decision making. Business analysts can use the framework themselves: selecting generic/specific models, assessing and defining strategies, and refinements for changed models, or defining of specific models.

3.1. Implementing and Reuse of the Framework

During the implementation of the framework the experts/model developers create the model collection of the goals and scenarios typical for the domain (Figure 6, steps 1, 2, 3a, 3b) which constitutes the starting generic models for change management and the specific models for the quality and technology alternatives for standard based change management. With a framework implemented onto a domain even beginner decision makers can manage changes by reusing the business models created for the domain by the experts. By using MDE technologies the decision of the experts becomes available for change management.

Generic models implemented in BUSITEV framework:

• **Support for business analysis** with Guide of the Business Analysis Body of Knowledge (BABOK Guide) [17] with the generic models of the recommendations of the standard. A Guide to the Business Analysis Body of Knowledge® (BABOK ® Guide) is a recognized standard for the practice of business analysis. The BABOK® Guide defines a Requirements Classification Scheme stated as classes of Business Requirements, Stakeholder Requirements, Solution Requirements and Transition Requirements, which support the dynamics of system's evolution.

For business analysis the standard classifies the requirements schemes, tasks and connections, determines the control points and recommends methods. It gives a detailed description of the development in textual, table and system depiction forms. It matches the development of requirements with business analysis. By articulating the recommendations of the standard into main phases we provide a visual documentation for the process organization of change management in a reusable generic model collection. This visual documentation of business analysis standard supports aligning business analysis with requirements engineering.

• **Support for the integrated development of IT security** with generic and specific models. We map the recommendations of ISO/IEC 27001 and 27002 [18] standards into goal-tree models for the chapters and sub chapters of the standards with the recommendations of goals and security requirements. In the structure of the models we follow the structure of the standards as the security audits can occur in practice. The models provide visual documentation about the recommendations of the standards and generic security goals and business aspects about the composition of the protection measurements. The adaptation of the models is highlighted as strategy decision during change management

ISO/IEC 27001 and 27002 standards provide business aspects for the structures of security estimations, provide for modeling the generic security requirements list about IT security, provide a model of the partial system managing IT security and for the harmonization of the assessment of IT security with other standards like ISO 9004 [19].

Generic security goal models form a basis for strategy creation and for creating the set of specific security models. The framework instantiation, which is introduced in Section 4 has specialized templates for e-trading assessments and for typology assessments of security levels as human, software, hardware and objects resources.

•S**upport for the integration of mobile tools into the business process** for developers with generic models of mobile application development

•**Support of repository-based collaborative work** with SVN [20] subversion manager to manage the concurrent access rights and team communications for developers scattered by geography to function as a single team. In a teamwork context to avoid confusion, the word version is almost never used. Versions in the first sense we call revisions, and in the second sense releases. This opportunity allows business analysts and stakeholders separated in space and/or time to collaborate, synchronize and negotiate conflicting changes. Revision Control Systems (RCS) manages multiple revisions of files [21]. RCS automates the storing, retrieval, logging, identification, and merging of revisions.

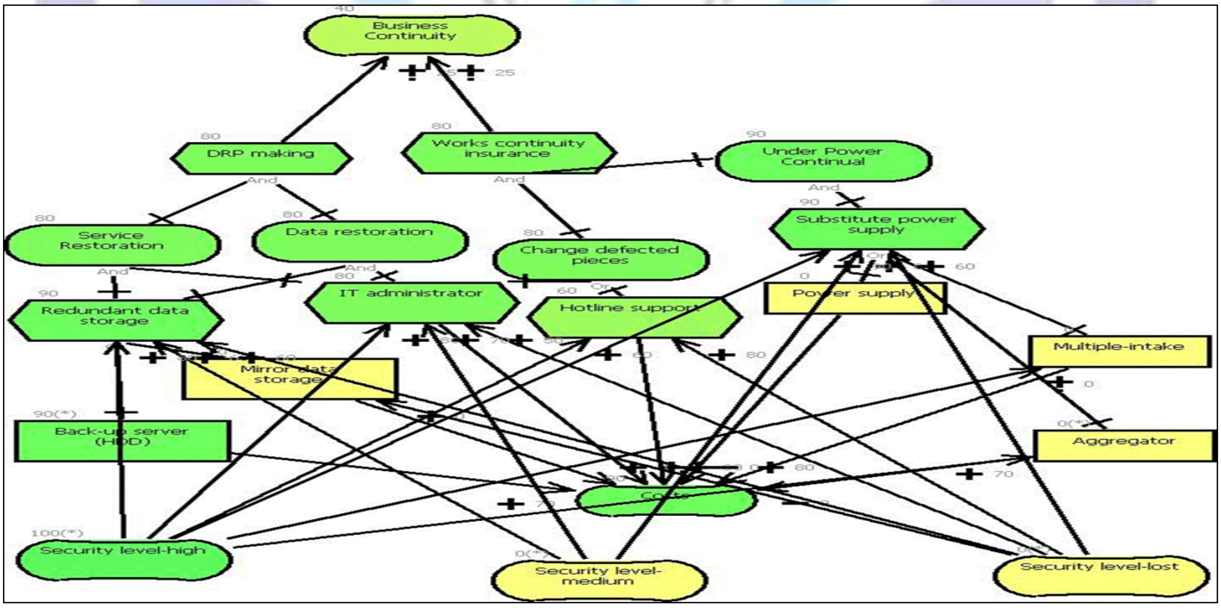


Fig 7: Strategy creation and its evaluation starting from generic model of security recommendations for Business Continuity information security of the ISO/IEC 27002.

4. FRAMEWORK INSTANTIATED FOR B2B EVOLUTIONS WITH INTEGRATED SECURITY ENGINEERING

Instantiation of BUSITEV framework for a domain it consists to follow the methodology for evolutionary modeling (4) to create the generic goal and functional models for the domain, i.e. trading systems, followed by specific models obtained by creating business strategies and by refining generic models. We named BUSITEV-SMIWEP framework the instantiated BUSITEV framework for B2B type of evolutions.

The validation of BUSITEV framework is rooted in a business change management SMIWEP project with B2B evolution purposes (the acronym of the project title in Hungarian) realized within Sonepar Magyarország Kft. commercial SME. The firm has a chain of branches for electro-technical products in each region of Hungary. This project it consists the frame for empirical validation of analysis templates and generic models. It has involving undergraduate students resulting in over twenty theses for BSC and MSC students.

4.1. Examples for Strategy Creation and Integration into Functional Model

Figure 5 shows a part of a GRL model. In this model are used notations for intentional elements and relationships. Here, the intentional elements are goals, soft goals and their realizations by tasks and resources, which realize security assessments. Relationships used are contributions, decompositions, and/or logical operators. The content of this graph is captured from the ISO/IEC 27002 standard recommendations.

4.2. Strategy Creation from Generic/Specific Models

Figure 7 illustrates one of the model templates for strategy creation and evaluation. The tasks and resources rendered to the security recommendations contribute to the security of the system to varying extents therefore various levels of security can be attributed to them. This ensures that the particular company, having determined the level of the security risk of information can set the features of one or two elements to see which tools to purchase to defend against the risks related to the given security level. The security levels are determined together with the levels of risks therefore 3 groups can be identified—low, medium and high colorings at the bottom of Figure 7. The simulation results show an evaluation for high-level security strategy assessment.

Figure 8 presents an example where the aim is the information security for business continuity of e-commerce and where the level of security is set to medium.

We can see what tools are needed to reach this level and the related costs—indicated by green in the simulation. Also, the costs can be set and then the necessary tools will be colored accordingly, -90% red, -50% pink, -20% orange, 0% yellow, 50% light green, 90% dark green. By setting the determined cost it becomes possible to see the type of defense related to the particular security levels and, vice versa, what costs a solution related to a given security level requires.

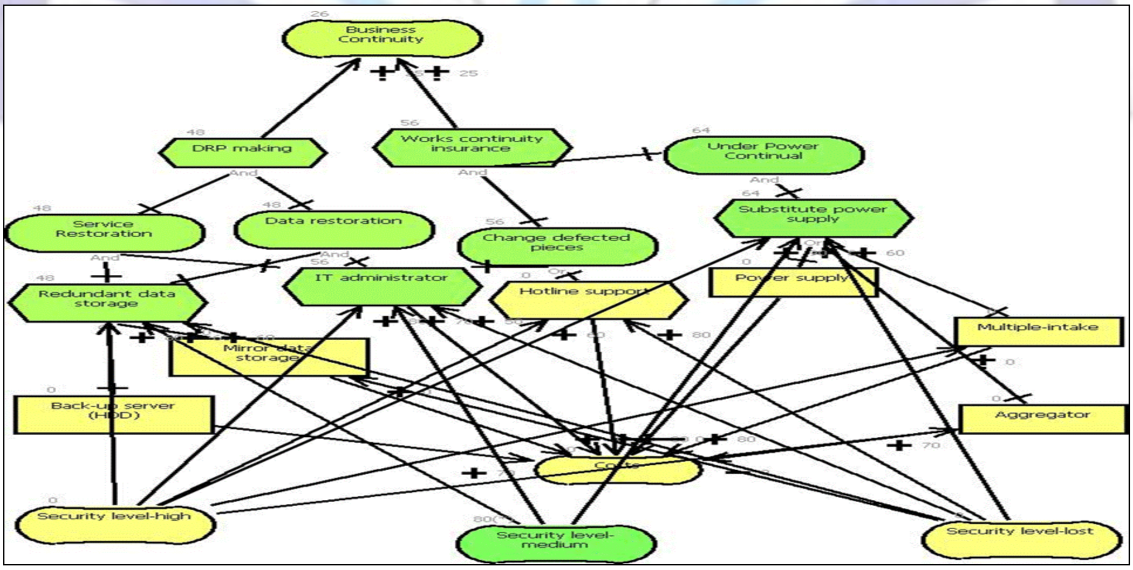
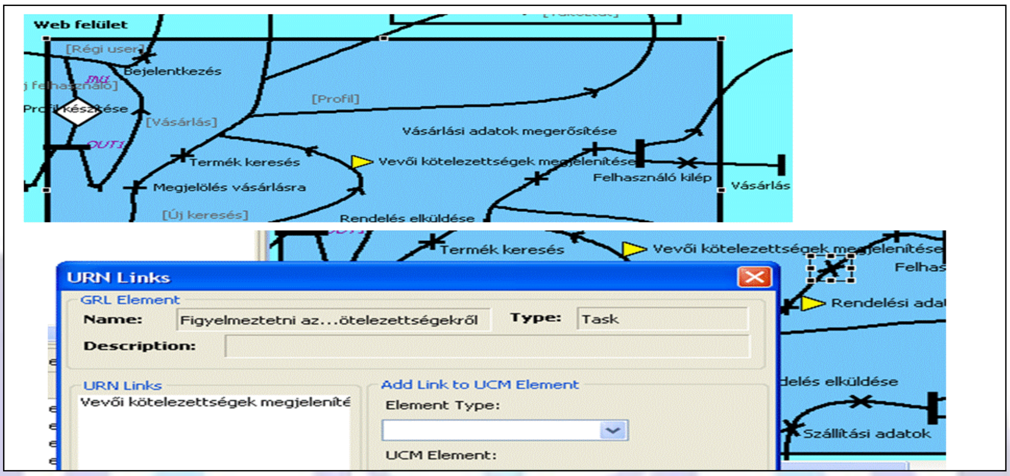


Fig 8: Specific model of security recommendations from ISO/IEC 27002 evaluated for medium level of Business Continuity information security.

Figure 8 shows the results of a simulation for evaluating the strategy for medium level of security goal fixed at 100. With the initial choices this alternative results in 26 units for Business Continuity security in rapport with the desired 80 unit of medium level of security, because as you can observe initial values for majority of resources are fixed at 0 to achieve low level of costs. It is the responsibility of system and business analysts to chose simulate and validate solution assessments.

4.3. Integration of Strategies into Functional Model

The resulted functional model after the integration of strategies into business processes is shown in Figure 10. It shows new components, use case paths and responsibilities marked with yellow triangle which are added with URN-links for integrating requirements realizations from goal-strategy models. This step illustrated with Figure 9 it consists of linking goals to functional model elements. Yellow triangles serve as traceability points between elements of a strategy model and its realizations. They highlight how many components and process elements can appear in functional model for satisfying security requirements. The strategy goal model used for refining the functional model in this example is from previous strategy models captured by simulation.



Name: Figyelmeztetni az…ötelezettségekről Type: Task

Description:

URN Links: Vevői kötelezettségek megjelenité

Element Type:

UCM Element:

Fig 9: URN Link: linking goals to functional model elements. Yellow triangles serve as traceability points between elements of a strategy model and its realizations

An illustration of the resulted functional model after the integration of strategies to observe how many of new components, use case paths and responsibilities are added for integrating security requirements into the functional model.

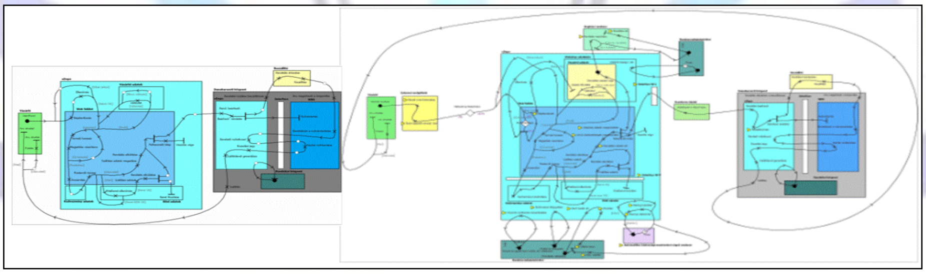


Fig 10: An illustration view of e-trading system's functional model: before (*left*) and after (*right*) the integration of security requirements (*Illustration view*)

5. RELATED WORK AND DISCUSSION

van Lamsweerde in [22] argues on the role of modeling notations that help to raise the level of abstraction in requirements descriptions. Goals have been used as an important mechanism for connecting requirements to design. A goal-oriented approach would allow the requirements to be refined and clarified through an incremental process. The well-known GORE method and tool have many applications in requirements engineering. We constructed the validation steps for specific templates deriving from generic models using the refinement method of KAOS [23]. Akoka et al. in [24] present their results on methods engineering research based on systemic view of decisions and processes, and a mechanism of guidance by quality supported by risk analysis and cost evaluation models and tools.

Eric Yu et al. in [25] show that each high-level goal can be associated with a set of concerns, in response to which, alternative refinements of the goal can be introducing, and a high-variability goal model constructing. Some of these methods engineering research results are applying by CSERG researchers [7] to realize the knowledge-based analysis support of the jUCMNav tools.

Pourshahid et al. [26] research results in metamodeling with URN profile and structuring pattern-based framework it support goal-based elicitation and validation of functional models. Our framework complements their work with integrating changes management strategies into functional models based on generic model repository with possibility of involving decision makers. These strategies, resulting from quality and extra-functional requirements simulations, drive change realizations for business processes and IT features included in business units. Other work as [2] integrate goal analysis for information security and customers loyalty correlations during e-business design.

Based on [6] our framework enables variability from intentional ambiguity and abstraction levels involving stakeholders in decision making. We constructed the jUCMNav-based validation steps to derive specific templates from generic models. For these steps we inspired from the refinement method of van Lamsweerde's [27], and Akoka's et al. [24] mechanisms for guidance by quality supported risk analysis and cost evaluation models. Well-suited techniques are elaborated at [16] for goal and scenario modeling, analysis, and transformation with jUCMNav.

Authors of [28] it established model-based fault detection for strategy creation and integration into functional model starting from process mining. Our framework provides a methodology to provide recommendations and relations from standards in visual form enabling reasoning about assessments.

Other frameworks are in special editions [29-30] to engender a “security culture” within an organization. Several approach meant to elicit security requirements according to system-theoretic considerations with the help of investigations in the business environment, workshops with stakeholders and risk analysis.

There are also languages, techniques and methods that address security requirements engineering. Authors of [31] provide the results of a systematic literature review of existing languages, techniques, artifacts, diagrams, resumed as models in general used in order to represent the elicitation of security requirements from the early phases of the development. They state that most of models are not standard compliant or have been developed following a particular standard, which leads to the problems that some security requirements are able to be specified by the models and others are not. In our case the models are based on ISO/IEC 27001/27002 standards and the CIA triad of confidentiality, integrity, and availability, as well as the SQUARE security requirements, is covered.

Research on methods for checking security conform to standards are presenting by Karaback et al. in [32] related on the ISO/IEC 17799 supporting tools and software for checking organization's standard compliance. Some standards COBIT, ITIL, ISO/IEC 17799 co-exist as reference frameworks for information security governance. Our framework provide methodology to provide recommendations and of relations from standards in visual form enabling reasoning about assessments and integrating into scenarios of functional views.

UMLsec[33] and SecureUML [34] extend UML with the focus on the recommended design for security for evolving systems to meet changing business needs, new regulations and policies and novel technologies. Their high-level approach uses formal verification and tool-supported refactoring techniques for traceability.

Some works deal with modeling of security of the software as an unexpected ability of a system termed with vulnerabilities, preventions and detection of defects. Other works deal with the identifying of the malicious users who reduce the degree of technology determinism. A review of existing methods and creation of new formal models and tools can be finding at SHIELDS Project Consortium [35]. Their tools for detect, inspect, test, design models for vulnerabilities are conforms to MDD/MDE methods today’s but not follows intend to use security standards in analysis phase.

In [36, 37] Massacci et al. presented the extending RE modeling and formal analysis methodologies to cope with security requirements by the informal and formal approaches. The SI* tool and Secure TROPOS methodology extends the TROPOS methods with security related concepts and formal analysis techniques capturing security requirements from the organizational point of view and ISO 17799 assessments. Our framework enable variability from intentional ambiguity and abstraction levels involving stakeholders in decision making, further can be a base for pre- and post audit processes.

Despite the many techniques and methods available for security in the early phases of software development, these is no other technique or method that reuse information security standards for reasoning about security levels, assets, costs and links security requirements to functional map.

Our framework contributes with generic models as bases for instantiation of a framework for supporting teamwork releases of business analysis, and integration of strategy realizations into functional models.

6. CONCLUSIONS

This paper introduces the BUSITEV framework for integrated engineering of business and IT evolutions. The framework based on User Requirements Notation standard (URN) and URN-supporting tools [6-7] provide methods and techniques for traceability and variability management. The framework contains generic models as reusable visual documents of information security standards and of business analysis standard. It has already been validated empirically for e-commerce security conforming to the corporate social responsibility at Sonepar Magyarország Ltd. SME.

BUSITEV framework is goal-oriented. Its inputs are goal and functional models from business-related generic standards where only some of the intentions and high-level goals need to be identified for generating specific models for a specific domain. The main output of the method is a more complete goal model combined with a business process model that is aligned with the identified goals, as well as additional traceability links between the two complementary views, see Figure 1. This framework has a set of methods to reuse and refine models from repository and to follow the collaborative work of stakeholders to do decisions for change management.

Our work is novelty at the moment from the point of view of the integrated development of information security within business strategies with the support for CEOs. The main contribution of our research is the methodology that enables CEOs to decide on the strategies rather than CIOs. Our frameworks support the involvement of business decision makers.

Strong points are from linking business goals and requirements to functional models; it reuses information security standards for reasoning about security levels, assets, costs and risks; the framework supports releases between internal stakeholders for cooperating and further reasoning; portability by Eclipse and some transformation engines of jUCMNav tool. Weak points are the manual assessment of risk and cost estimation in the case of a greater goal-tree. For improving the framework we intend to introduce some generic methods in form of template collections to support communications between stakeholders and services on demand in the case of outsourcing security management.

ACKNOWLEDGEMENTS

The author is grateful to Atilla Steszli CIO for industrial experimentation at Sonepar Magyarország Ltd. SME.
This research work was supported by TÁMOP-4.2.1/B-09/1/KMR-2010-0003.

REFERENCES

[1] Medve, A. 2008 Advanced steps with standardized languages in the re-engineering process, Journal of Computer Standards & Interfaces, Elsevier, 30 (5):315-322.

[2] Medve, A.2008 Advanced steps with standardized languages in the re-engineering process, Journal of Computer Standards & Interfaces, Elsevier, 30 (5):315-322.

[3] Medve, A., Kövesi, K. 2009 Modeling and Analysis of Information Security Starting from ISO/IEC 27001 Standard and Customer Loyalty Relationships. In: IFIP CONFENIS'2009, Győr, Hungary, p. 128-137.

[4] Medve, A. 2011 Standards-based Framework for Functionally Integrated Engineering of Information Systems. In T.Szmuc, M.Biró (Eds.) 5th IFIP TC2 Central and Eastern European Conf. on Software Engineering Techniques (CEE-SET 2011), Debrecen, Hungary, p.52-58.

[5] Medve, A. 2012 Model-based Framework for Integrated Evolution of Business and IT Changes. In: S.Hammoudi, M.Sinderen, J.Cordeiro (Eds.) ICSOFT 2012. Proc. of the 7th Int. Conf. on Software Paradigm Trends, 24 - 27 July 2012, Rome, Italy, SciTePress, p.255-260.

[6] European Network and Information Security Agency - Risk Management - Emerging and Future Risks. ENISA, 2013.

[7] ITU-T Recommendation 2011 Z.151: User requirements notation (URN) - Language definition.

[8] JUCMNav 5.4 the URN tool, http://jucmnav.softwareengineering.ca/ucm/bin/view/UCM/UcmNav, http://jucmnav.softwareengineering.ca/ucm/bin/view/ProjetSEG/HelpOnLine 2013.

[9] URN Virtual Library, http://www.UseCaseMaps.org/pub 2013.

[10] OMG Specifications – http://www.omg.org/technology/documents/spec_catalog.htm; – UML – Unified Modeling Language, v2.4.1. 2013.

[11] Weiss, M., Amyot, D. 2005 Business Process Modeling with URN. International Journal of E-Business Research, 1(3):63-90.

[12] Amyot, D., Mussbacher, G. 2011 User Requirements Notation: The First Ten Years, The Next Ten Years (Invited paper), Journal of Software, Academy Publisher, 6(5):747-768.

[13] Humprey, W. S. 1989 Managing the Software Process, Addison-Wesley.

[14] Mintzberg, H. 1998 Structure et dynamique des organizations (The structuring of organizations). Edition d'Organisation, Paris.

[15] McKinsey Business Technology 2009 How CIO should think about business value?, Innovation in IT Management, 15:28-37.

[16] Mussbacher, G., Amyot, D., Weiss, M. 2007 Visualizing Early Aspects with Use Case Maps. LNCS Journal on Transactions on Aspect-Oriented Software Development, LNCS 4620, Springer, p.105–143.

[17] Mussbacher, G., Amyot, D. 2009 Goal and Scenario Modeling, Analysis, and Transformation with jUCMNav, In: 31st Int. Conf. on Software Engineering (ICSE-Companion), ACM, Canada, p.431–432.

[18] BABOK Guide 2.0: A Guide to the Business Analysis Body of Knowledge . International Institute of Business Analysis. IIBA.2012.

[19] ISO/IEC 27000:2012 Information technology -- Security techniques -- Information security management systems, http://standards.iso.org/ittf/PubliclyAvailableStandards/index.html, http://www.27000.org

[20] ISO Related Standards -ISO 9001:2008, SO 9001:2008 Quality management systems.

[21] SVN: VisualSVN Server Enterprise Edition. http://subversion.apache.org/docs/community-guide/ 2013.

[22] CSV: Concurrent Software Version. https://savannah.nongnu.org/projects/cvs/ 2013.

[23] van Lamsweerde, A. 2009 Requirements Engineering – From System Goals to UML Models to Software Specifications. Wiley.

[24] van Lamsweerde, A., Willemet, L. 1998 Inferring Declarative Requirements Specifications from Operational Scenarios. 1998/12. IEEE Transactions on Software Engineering, Special Issue on Scenario Management.

[25] Akoka, J. Comyn-Wattiau, I., Cherfi, S. S. 2008 Quality of Conceptual Schemas An Experimental Comparison. In RCIS'08 IEEE Int. Conf. on Research Challenges in Information Science, p. 197–208, IEEE Press, New York.

[26] Yu, E. 1995 Modeling strategic relationships for process reengineering. Ph.D. thesis, Dept. of Computer Science, University of Toronto, Canada.

[27] Pourshahid, A., Chen, P., Amyot, D., Forster, A. J., Ghanavati, S., Peyton, L., Weiss, M. 2009 Business Process Management with the User Requirements Notation. Electronic Commerce Research, Springer, 9(4):269–316.

[28] Letier. E., van Lamsweerde, A.2004 Reasoning about Partial Goal Satisfaction for Requirements and Design Engineering, Proceedings of FSE'04, 12th ACM International Symp. on the Foundations of Software Engineering, Newport Beach (CA), Nov. 2004, 53-62 (Best Research Paper Award).

[29] Stark-Werner, Á. 2011 Model-Based Fault Detection and Isolation using Process Mining. Engineering and Technology, 7(73):851–856.

[30] Fernández-Medina, E., Yagüe del Valle, M.I., 2008 State of standards in the information systems security area, Computer Standards & Interfaces, Volume 30, Issue 6, August 2008, Pages 339-340.

[31] Patel, A. 2008 Frameworks for secure, forensically safe and auditable applications, Computer Standards & Interfaces, Volume 30, Issue 4, May 2008, Pages 213-215

[32] Fornaris, E.A., Fernandez-Medina, E. 2010 Security Requirements Models: A survey and Comparison. In: Proc. SEC-MDA'2010 Seconf, pp. 7-13. Paris.

[33] Karabacak, B. Sogukpinar, I. 2006 A quantitative method for ISO 17799 gap analysis. In: Elsevier J. Computers&Security. 25 (6), 413-419.

[34] Juerjens, J. 2002 UMLsec: Extending UML for Secure Systems Development. In: UML 2002. LNCS 2460, pp. 412-425, Springer, Heidelberg.

[35] Jürjens, J., Livshits, B., Scandariato, R. (Eds.)2013 Engineering Secure Software and Systems - 5th International Symposium, ESSoS 2013, Paris, France, February 27 - March 1, 2013. LNCS 7781, Springer.

[36] SHIELDS Project Consortium http://www.shields-project.eu/ 2012.

[37] Tran, L.M.S., Massacci, F. 2013 UNICORN: A Tool for Modeling and Reasoning on the Uncertainty of Requirements Evolutions. In: CAiSE 2013 – Forum.

[38] Massacci, F., Zannone, N. 2011 Detecting Conflicts between Functional and Security Requirements with Secure Tropos: John Rusnak and the Allied Irish Bank. In Social Modeling for Requirements Engineering. MIT Press.

Authors Biography

Anna Medve is Research Assistant at the Department of Electrical Engineering and Information Systems of University of Pannonia at Veszprém (Hungary). She has a Master degree in Computer Science and Mathematics from Transylvania University at Brasov (Romaine) and she submitted doctoral dissertation in software engineering topic in July 2013 to obtain her PhD degree at Eötvös Lóránd University at Budapest (Hungary). She has research interest in formal methods for reengineering of information systems, incremental verification, and integrated information security engineering with novel technologies and methods enginenring for model driven processes.

http://virt.uni-pannon.hu/index.php/in-english/people/1080-medve-anna