University of Tartu

Faculty of Mathematics and Computer Sciences

Computer Sciences Institute

Information Technology

Olga Altuhhova

Developing System Security through Business Process Modelling

Bachelor thesis

Supervisor: Raimundas Matulevičius

Author: .... "......" June 2011

Supervisor: .... "......" June 2011

Allow to defence

Professor: .... "......" June 2011

Tartu 2011

Abstract

Business process understanding and modelling is one of the major aspects in the modern information system (IS) development. Thus, there exist several modelling approaches to support this activity, and one on them is the business process modelling notations (BPMN). Although BPMN is a good approach to understand business processes, there is a limited work to understand how this language could deal with business security and security risk management for IS. This is a problem, since both business processes and security concerns should be understood in parallel to support a development of the secure IS. In this paper we analyse BPMN with respect to the domain model of the IS security risk management (ISSRM). We apply a structured approach to understand key aspects of BPMN and how modeller could express secured assets, risks and risk treatment using BPMN. Thus we align the main constructs of the BPMN language with the key concepts of the ISSRM domain model. We show applicability of our approach on a running example related to the Internet store. We believe that our proposal would allow system analysts to understand both business processes and security concerns using the same modelling language (thus, removing the necessity of learning several modelling languages). In addition we open a possibility for the business and security model interoperability and the model transformation between several modelling approaches (if these both are aligned to the ISSRM domain model).

Content

Content of Figures

Content of Tables

Chapter 1. Introduction

1.1 Motivation

Security is a major aspect of Information System development that affects each component of the system very closely. We can claim that the process of security integration into the information systems is not completely and appropriately understood, otherwise there won't exist a necessity in analysing and designing new methodologies and tools. The concept of security itself refers to the capability of a product, information system in our case, to protect information and data in order to avoid the accessibility of it by unauthorized persons or systems that are able to read or modify it. One of the important component of IS development is Business process understanding and modelling. It helps us effectively analysing the needs of providing software and services that become considerable and practical for the demands of any kind of business nowadays. So the actual challenge remains to create business processes with respect to security of the system being described.

1.2 Scope

The great variety of business process modelling approaches was developed in order to optimize business processes and to meet its business goals. Some of them are EPC, YAWL, and UML activity diagrams. The short description of each is presented below.

An Event-driven Process Chain (EPC) is a type of flowchart that is used for business process improvement and also for laying out business process work flows, originally in conjunction with SAP R/3 modelling. The EPC is a base of the ARIS-framework and combines the different views towards the description of enterprises and information systems in the control view on the conceptual level (Seel et.al, 2005).

Another representative of the business process modelling tools is YAWL, Yet Another Workflow Language, which is java-based open-source workflow system. Funded on a concise and powerful modelling language, YAWL is able to support complex data, integration with organizational resources and external applications, process verification and process configuration. It has open interfaces based on Web standards that enable to plug-in existing applications and to extend the system. It also provides a graphical editor with built-in verification functionality that helps to detect errors automatically on early stages (Aalst et.al, 2005).

The most common and typical tool for business process modelling is UML activity diagrams. The standardized general-purpose modelling language, UML, uses activity diagrams to model the workflow behind the system being designed. An activity diagram is a flowchart which shows the flow of control between the sequential activities of a process (Börger et.al, 2000).

For this analytical work we choose quite young modelling notation BPMN, which is becoming a standard that has been developed by Business Process Management Initiative in year 2004 (White, 2004). Although the BPMN, which stands for Business Process Modelling Notation, is a comparatively new methodology, it gained a respectable place among the business process modelling languages. Because BPMN is a standard and thanks to it's similarity to flowcharting notations, it is friendly and familiar to business users. Each shape has a defined meaning, confined with rules that precisely dictate what can be connected to what. That means diagrams that you create will be completely understandable to other users from any business companies. Moreover, BPMN specifies the technical details that can be attached to any shape, details that make the model executive as an automated workflow. Nowadays BPMN provides language that describes process behaviour, shareable by business and IT; "We've never had that before" (Silver, 2009).

1.3 Problem description

Although BPMN is a good approach to understand business processes, there is a limited work to understand how this language could deal with business security and security risk management for IS. This is a problem, since both business processes and security concerns should be understood in parallel to support a development of the secure IS. There exist several attempts (e.g. (Rodriguez et.al, 2007)) to understand how security could be modelled, but the means to express security with BPMN is not yet understood.

1.4 Purpose and research question

In our thesis we investigate how BPMN could be used to determine the security risks. More specifically we analyse this approach with respect to the domain model of the information systems security risk management (ISSRM). Our analysis allows us to determine the BPMN constructs which could be used to express secure business and IS assets, their risks and security requirements to mitigate these risks.

1.5 Short overview of contribution

During the analysis we apply a structures approach to understand key aspects of BPMN and how modeller could express secured assets, risks and risk treatment using BPMN. Thus in this way we align the main constructs of the BPMN language with the key concepts of the ISSRM domain model. In addition we extend BPMN with the principles to model and manage security risks. We show applicability of our approach on few illustrate examples (e.g., Internet store). We believe that our proposal will allow system analysts to understand both business processes and security concerns using the same modelling language (thus removing the necessity of learning several modelling languages). In addition we open the possibility for the business and security model interoperability and the model transformation between several modelling approaches (if these are also considered using the ISSRM domain model).

1.6 Structure of the thesis

Current work consists of five logical parts, divided into 10 chapters. Chapter 1 is introductive, it makes a short overview of a thesis, scope of our work, problem domain. Chapters 2 and 3 is a background of a thesis; it consist of description of Information System Security Risk Management, or ISSRM, and the second is dedicated to Business process modelling notation or BPMN, which is taken as a base for current work. In Chapter 4 we make an analysis of adopting the BPMN to ISSRM, using the running example. Chapter 5 is mapping and summarizing of the result in one Table for better view. Chapter 6 represents problems that we faced with during the modelling of the example with a focus to security, and some improvements' proposals.

Chapter 2. Information System Security Risk Management

Information System Security Risk Management (ISSRM) is practitioner-oriented methodological tool that helps organizations make decisions related to the security of Information Systems (Dubois et al., 2010). Today there exists hundreds of ISSRM methods and standards, which mainly consist of process guidelines to identify vulnerable assets, determine security objects, risks, define and implement security requirements for risk treatment.

2.1 Scope and basic definitions

The ISSRM approach used in this work focuses on security risk management. The goal of using the ISSRM approach is to protect organization's assets. *Asset* is defined as anything that has value to the organization, and has a need in protection. Assets, related to the organization information system, such as people, machines, processes, data, software and similar will be taken into account as well. All the risks that threaten to above-mentioned subjects have to be evaluated with respect to three main properties: *confidentiality* – means that information can't be or become available to any unauthorized individuals or processes, *integrity* – the property of protection the accuracy and completeness of secure assets, *availability* – corresponds for accessibility in usage upon demand of authorized individual or entity. Other criteria like accountability, authenticity can be added according to the context requirements.

2.2 Domain model

The domain model shown in Figure 1 consists of a conceptual model that puts together main ISSRM concepts, their relationships, and corresponding definitions. The model characterizes three principal groups of concepts: *asset-related* concepts, *risk-related* concepts and *risk treatment-related* concepts: marked correspondingly as blue, orange and green (Matulevičius et al., 2008a).

The **asset-related** concepts describe the important assets that need to be protected. The asset generalizes two more concepts: the *business asset, which is defined* as information, process, skill inherent to the business of the organization that has value to it, in terms of it business model and is necessary for achieving its objectives, and *IS asset* that has value to the organization and necessary for achieving its objectives and supporting business assets. The security needs of business assets characterized with the help of *security criterion*, such as *confidentiality, integrity* and *availability.*

The second group is **risk-related** concept. *Risk* is a combination of a *threat* with one or more *vulnerabilities* leading to a negative *impact* that harms one or more *assets*. In this definition *impact* means a potential negative consequence of a risk that harms assets of an organization, when a *threat*, *potential attack* that can lead to harm, is accomplished. *Threat* exploits the *vulnerabilities* that characterize the weakness of the *IS asset*. A combination of a *threat* and one or more *vulnerabilities* leads to *impact*. A *threat agent* is an agent who has means to harm intentionally IS assets. An *attack method* is a standard means by which a threat agent executes *threat*.

The third group is **risk-treatment** related concepts. *Risk treatment* is a decision to treat the identified risks. It satisfies a security need. Categories of risk treatment decision include: *risk avoidance* – decision not to become involved in, or to withdraw from, a risk; *risk reduction* – action to lessen the probability or/and negative consequences, associated with a risk; *risk transfer* – decision to share the burden of loss from a risk with another party; *risk retention* – accepting the burden of loss from a risk. The condition over the phenomena of the environment that we wish to make true by installing the IS, in order to mitigate risks is called *security requirement*. This is implemented by a designed means to improve security, specified by a security requirement, and implemented to comply with it. A *control* designates a means to improve the security by implementing the security requirements.

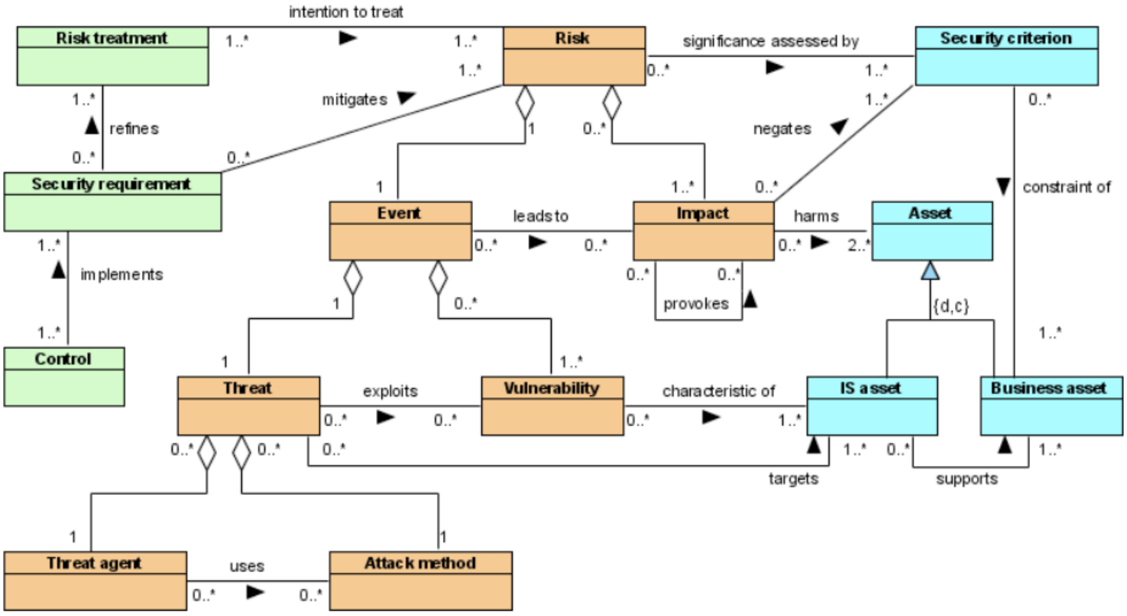


Figure 1. The ISSRM domain model; adapted from (Dubois et al., 2010)

2.3 The ISSRM process

The ISSRM process (see Figure 2) describes the activities needed to identify, monitor and control security risk. Within the process, a risk is defined as any future events that may prevent one meet the team’s goals. A process allows you to identify risk, quantify the impact and take actions to prevent it from occurring or reducing the eventual impact. The first step is dedicated to *context and asset identification*, it starts with analysis of the organization, its environment and assets that need protection. Then it goes the *determination of security objectives* (e.g., *integrity*, *confidentiality* or *availability).* Third step is *risk analysis and assessment*. The purpose is to identify and estimate risks qualitatively or quantitatively.

Risk treatment is an activity of selecting and implementing measures to modify the risk. *Risk treatment* includes as its major element, risk control/mitigation, but also extends further to, for example, risk avoidance, risk transfer, risk financing, etc. The next step is to *define* *security requirements*, i.e. the security solutions to mitigate the risks. Finally, it is necessary to select and implement the countermeasures/controls within the organization.

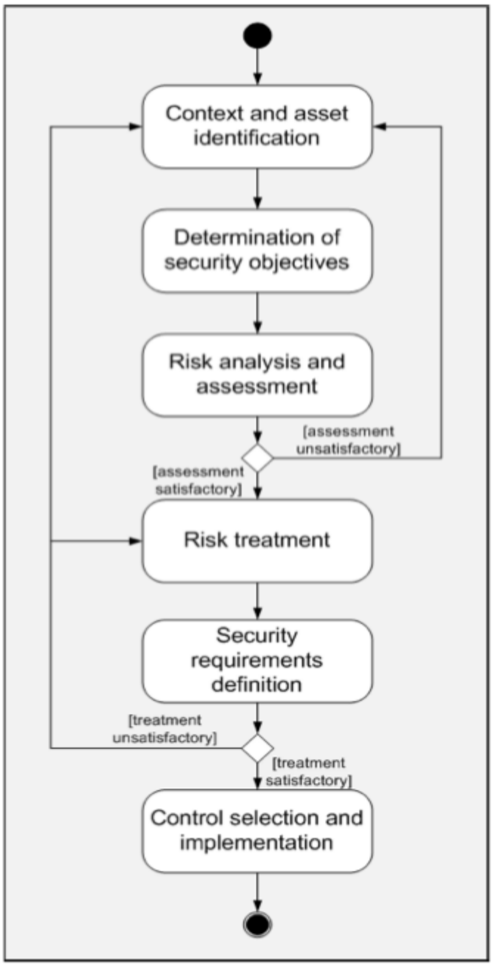

Context and asset identification
Determination of security objectives
Risk analysis and assessment
[assessment unsatisfactory]
[assessment satisfactory]
Risk treatment
Security requirements definition
[treatment unsatisfactory]
[treatment satisfactory]
Control selection and implementation

Figure 2. ISSRM process, adapted from (Matulevičius et al., 2008a)

2.4 Summary

In this chapter we presented basic definitions of the ISSRM approach, its domain model and the process of risk management. We also defined the scope of ISSRM application, where we are focusing only on security risk management. With the help of conceptual model we present three principal groups of concepts of ISSRM: *asset-related* concepts, *risk-related* concepts and *risk-treatment related* concepts. The ISSRM process represents steps to be taken to manage the security risks. This process includes context and asset identification, determination of security objectives, risk analysis and assessment, risk treatment, security requirements engineering and implementation of selected control measures.

Chapter 3. Business Process Modelling Notation

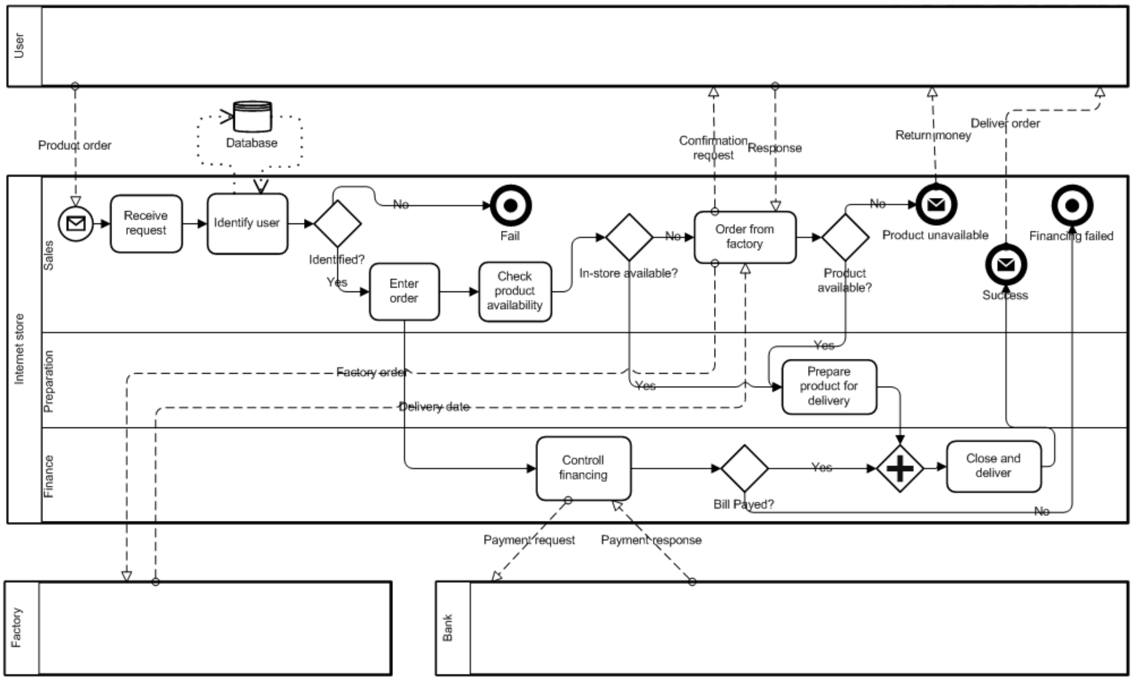
Business Process Modelling Notation (BPMN) is a language for constructing business process models (White, 2004). It considered to be business-friendly, because it is based on notions familiar from traditional flowcharting. At the same time, the notations are linked to a semantic model, which means that each shape used in the notation has a specific meaning, with defined rules and connections between objects. The key element of BPMN application is the Business Process Diagram. It is constructed of a set of graphical elements that were chosen to be distinguishable from each other and to utilize shapes that are familiar to most modellers. It describes a typical order of activities and what role or organizational unit performs or is responsible for the process.

As a part of pedagogical approach the use of BPMN is classified to three levels, based on how the model is used (Silver, 2009). *Descriptive modelling* describes the typical order of activities and what role or organizational unit each one performs, or responsible for. *Analytical modelling* describes the activity flow precisely, including the exception paths significant to key performance indicators. *Executable modelling* targeted to the system developing, not business architecture or analysis. The scope of this work is *Descriptive modelling*, which is the first level of BPMN. It basically concentrates on business-oriented process mapping by simply documenting what the flow is.

3.1 Introduction to BPMN through example

Figure 4 represents an order making, execution, and product delivery process in the Internet store. This process begins with order making by user that means choosing the product and paying the bill. To clear the situation this two actions are included in the meaning of Product order.

There are four participants involved in the communication, they are represented with a help of *lanes*: User, Internet store, Factory and Bank. We can also notice that the Internet Store, a *pool*, which is the main container of a process, is divided into three *lanes*: it is done in order to organize flow elements belonging to different store departments. The process begins with a message, which triggers a *start event* Request for product and the first *task* Receive request. The next *task* is identification of a user (see the BPMN *task* Identify user), which requires the connection with the Database, checking the necessary information: if the user is not identified, the process is leaded to the *end event* with a sign of *terminal signal* inside, which doesn't mean the end of *parent process*, but the end of *sub-process*. The second path is the *sequence flow* with the confirmation of User's successful identification (see the BPMN *gateway* Identified?), continues with the order entering into the system (see *task* Enter order), and it is the point where main process flow forks into two parallel going sub-processes: checking the product availability and the finance control. The system checks the product availability in-store (see *task* Check product availability), if it is not available (see *gateway* In-store available?), it offers User to order needed product from factory (see *task* Order from factory), sending a request for confirmation. This activity uses a *message flow* (see Confirmation request and Response), which helps to organize the communication between participants. If the product is not in the store (see the BPMN *gateway* In-store available?), it is ordered from the factory (*task* Order from factory); otherwise the product is prepared for delivery (*task* Prepare product for delivery). In the second parallel the payment for the product is checked with the Bank. Both parallels are joined with a *gateway*, after which the order is closed and delivered (*task* Close and deliver) to the user. The process finishes with an *end event* (Success), which sends a message to the User (see BPMN *data flow* Deliver order).



Legend:

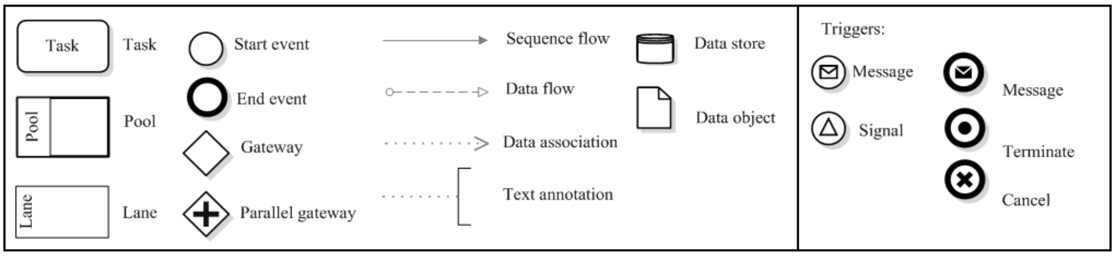


Figure 3. The BPMN example: the internet store

3.2 Major constructs and concepts

The four basic categories of objects are *flow objects*, *containers*, *flows* and *artefacts*. The *flow objects,* used to describe the atomic units of a process, are *events*, *tasks* and *gateways*. An *event* indicates *start* or *end* of a process path; it can be *triggered* or *non-triggered* (it means an activity that executes or finishes the event; e.g. message, timer, error etc). A *task* is an atomic activity that has no internal sub-parts defined by the model. In some cases, task can also represent the *sub-process*, a compound activity with sub-parts then the task figure is labelled with a small plus on the bottom, which identifies collapsed process. The control of the divergence and convergence of sequence flow is realised by the *gateways*. The *gateway* determines traditional decisions, as well as forking, merging, and joining of paths. We can define some types of *gateways*. An *exclusive gateway* or *XOR gateway* represents an exclusive decision, which means only one of the output *sequence flows* to be followed, based on some condition; *parallel gateway* signifies a parallel split or AND-split, means that all of the outgoing *sequence flows* are to be followed in parallel, unconditionally.

The BPMN *containers* are *pools* and *lanes*. They both play roles of object holders. However, the *pool* shows the message flow between the process and external participants. The *lane* is a subdivision of a process, used to organize flow elements belonging to different categories, also represent performer roles or organizational units.

Relationships between different BPMN constructs are defined with *flows,* which include *sequence flow*, *message flow* and *associations*. The *sequence flow* links *activities*, *gateways*, and *events* within a single *pool*; it is represented by a solid line connector. The *message flow* is a dashed connector representing a signal sent between two *pools*. *Association* is used to associate *data*, *text,* and other *artefacts* with *flow objects*, represented with the help of dotted line connector.

The last group of graphical objects in BP diagrams is *artefacts*. The BPMN *artefacts* contain concepts of *data objects*, which are defined as mechanism to show how data is required or produced by *activities*, data stores and *annotations*. *Data stores* describe the way data could be stored. *Annotations* suggest mechanism to provide additional text information for the user of a *BP Diagram*.

3.3 BPMN Meta-model

Figures 3 and 4 represent the BPMN conceptual meta-model. Current model is realised with the help of UML class diagram. It brings together major BPMN concepts, relations and classification, according to previous paragraph. Figure 4 defines four groups of graphical objects. The construction of BP Diagram begins with defining process participants, it influence on decision of how many *pools* should be used. The *pool* can be divided into *lanes* or not, if decided to classify the process part accordingly to some rules, *pool* becomes filled with *lanes*, if not – then pool is the only container of a process. The model shows that every *lane* itself can be divided into more *lanes*, if necessary. *Containers* are a group represented by *pools* and *lanes*; group contains *flow objects*: *tasks*; defined as sub-process or not, *gateways*; of any data type and also labelled or not, and *events*; start, end or intermediate and triggered or not. The *flow objects* and *artefacts* has different type of connection within the groups and between each other, these relations are represented in Figure 5. It shows that *flow objects* are connected with *sequence flow*. Connection between *artefact* and *tasks* is realised with *data association flow*. *Tasks* and *events* can be connected to *pools* with *data flow*. We can notice that some connection lines are marked with 'to' and 'from' pointers, which mean that flows go into and from the object. It is also marked how many connections different elements can have.

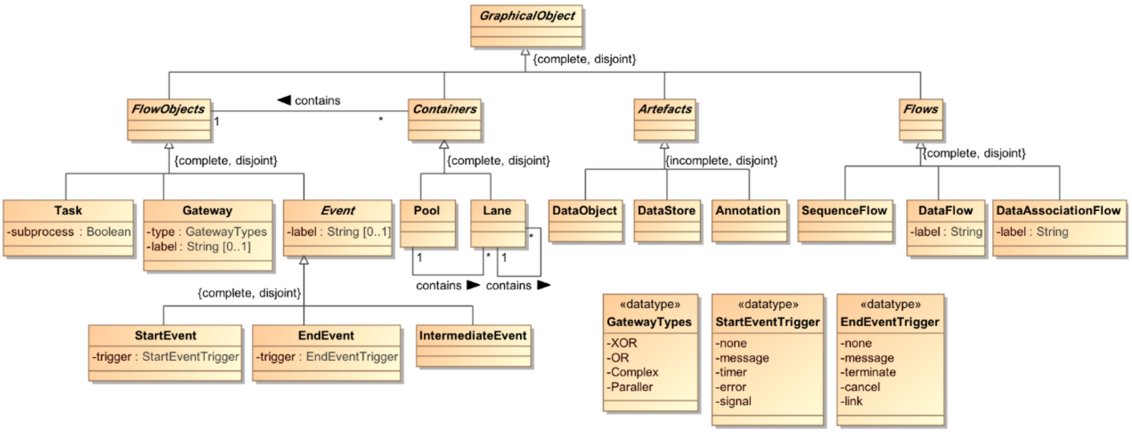


Figure 4. Extract of BPMN Meta-model: Concept classification

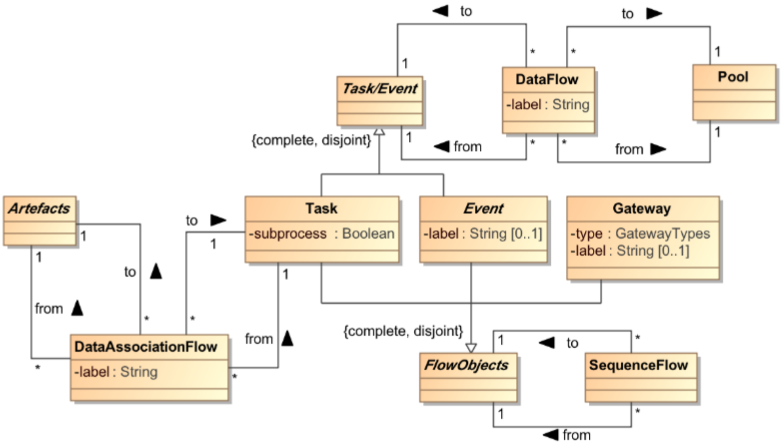


Figure 5. Extract of BPMN Meta-model: Relationships

3.4 Summary

This chapter is dedicated to Business Process Modelling Notation, language for constructing business process models. We defined the scope of analysis, concentrating on *Descriptive models*, the first level of BPMN modelling. We made the short introduction to BPMN using example, created with BPMN version 2.0, which represents the main activities in the Internet store: order making, order execution, product delivery. In paragraph 3.2 we collected together major BPMN concepts and constructs. The connections and relationships between them are represented in the Figures 4 and 5, in BPMN meta-model.

Chapter 4. Analysis

In this section we will consider how the BPMN language could be applied according to the ISSRM process. More specifically we will follow the six steps of the ISSRM process to investigate security risks in the online registration process at the Internet store.

4.1 Context and asset identification.

Let's consider the following situation where the potential *user* (presented as the BPMN *pool* User) wishes to start using the Internet store *system* (see the BPMN *pool* System). In order to get details of the registration, user sends a message with an inquiry to the system administrator. The process of the message handling is presented in Figure 6. Here the *system* accepts the message (see *task* Accept message), the message is read by the system administrator (see *task* Read message) and the explanations (see *data flow* Demand for registration) are sent (see *task* Send answer) back to the *user*.

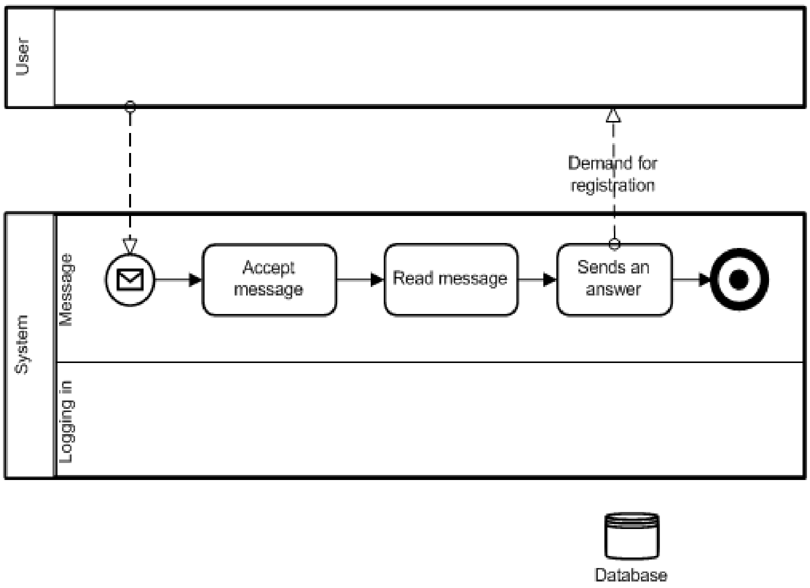


Figure 6. Message handling process

In Figure 7 we present the user registration process. Here, after receiving the instructions, the user registers to the Internet store *system* by submitting his data (see *data flow* User info). The *system*, then, accepts registration information (which includes user data on the preferred Username and Password) and includes it into the database (see task Insert data to DB). After having the valid *username* and *password*, the *user* is able to login to Internet store *system* as illustrated in Figure 8. Hence the *system*, first, checks the *username* existence, and, then, the *password* (see *task* Checks password). If these data matches, the *user* gets the "*Success*" signal and is able to use the Internet store *system.* Otherwise he gets a notification about the failure (see *data flow* No such user or password).

After having the valid username and password, the *user* is able to login to Internet store *system* as illustrated in Figure 8. Hence the *system*, first, checks the *username* existence, and, then, the *password* (see *task* Checks password). If these data matches, the *user* gets the

"*Success*" signal and is able to use the Internet store *system.* Otherwise he gets a notification about the failure (see *data flow* No such user or password).

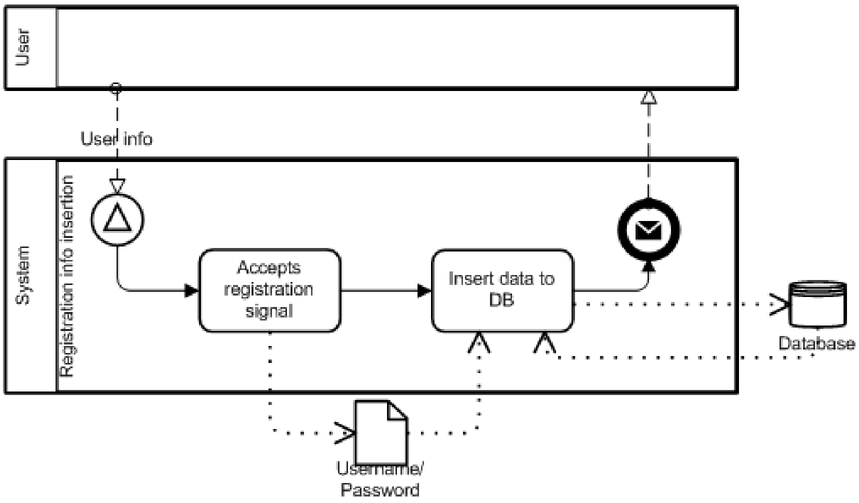


Figure 7. User registration process

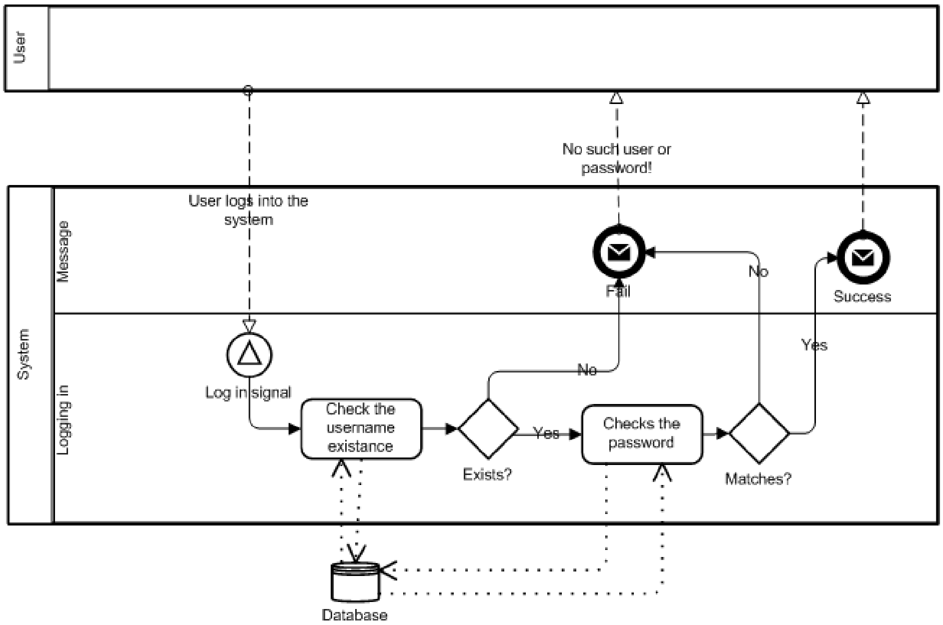


Figure 8. User login process

4.2 Determination of security objectives

In this scenario we can identify few major assets that need protection against security risks. Firstly, we need to ensure confidentiality of *username* and *password*. If confidentiality is revealed the system violators could use the user's personal data for not intended goals. In addition we need to ensure *integrity* of all the business processes (e.g., including the ones described in Figures 6, 7 and 8) needs to be ensured. If integrity is broken the system might be used not according to its purpose.

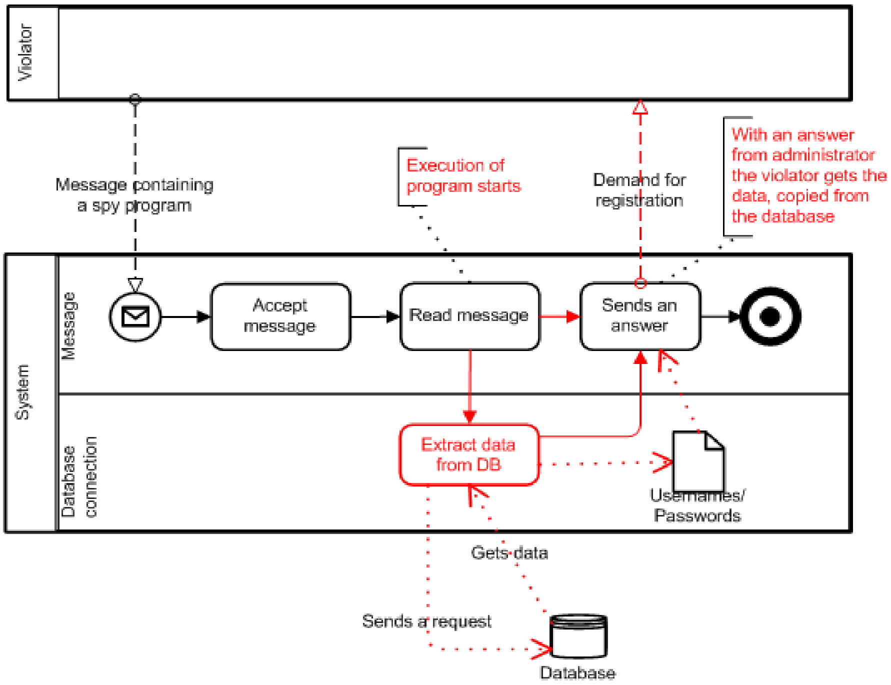


Figure 9. Message handling process including security risk attack

4.3 Risk analysis and assessment

In Figure 9 we model a potential security risk scenario. Let's say, that there exists a violator (presented as the BPMN *pool* Violator) who would like to login to the system without registering the personal user account. Similarly as illustrated in Figure 6, the violator sends a message to the system. However this time, the message includes a spy program (see the *data flow* Message containing a spy program in Figure 9), which is started after the message is accepted (see *task* Accept message) and read (see *task* Read message). The spy program starts a new task (see *task* Extract data from DB), which sends an inquiry to the database and extracts the username and password. These data are then attached to a reply message, which is sent to the violator (e.g., see *task* Sends an answer, and *data flow* Demand for registration). In this analysis we are able to identify the ISSRM *threat agent* (e.g., Violator) and the ISSRM *attack method* (e.g., Message containing a spy program and Extraction of data from the database). Combination of these elements forms a *security threat*. The direct *impact* of this *threat* is that the confidentiality of the username and password is broken. On the other, this *impact* provokes other *impact*, which negates the integrity of the business processes; i.e., the Violator is able to access the *system* without registering to it, and, thus, change the business processes according to his needs.

4.4 Risk treatment

Risk treatment involves deciding how the identified security flow is mitigated. In our example we will take a risk *reduction* – i.e., actions to lessen the probability of the negative consequences – decision.

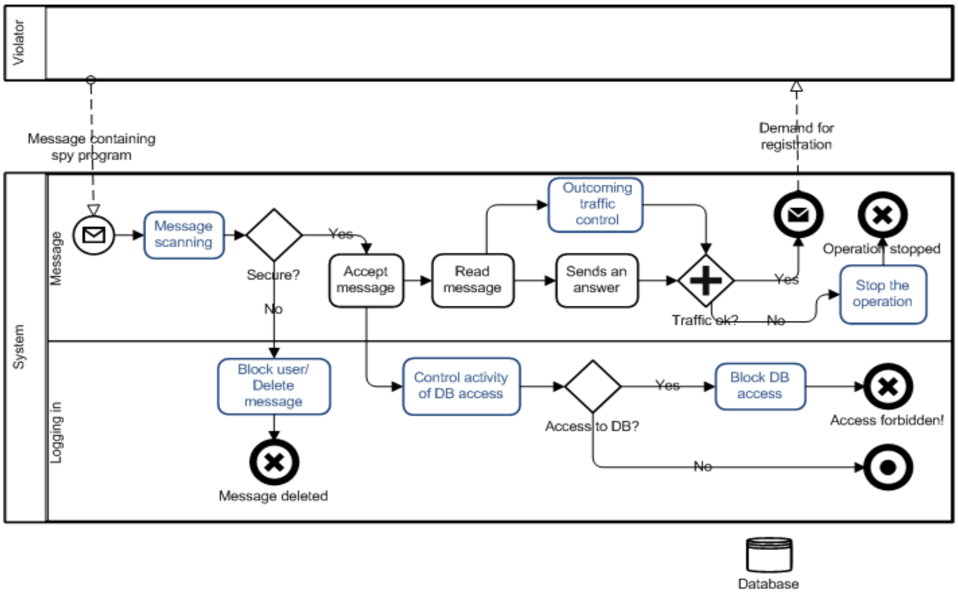


Figure 10. Message handling process including security requirements

4.5 Security requirements definition

To reduce the probability of accepting the message, which contains a spy program, firstly, we introduce a task for Message scanning, as defined in Figure 10. If this message is not secure, it deleted and the sender is blocked (see *task* Block user/Delete message). Secondly, we introduce the *task* to Control activity of DB access. If during the message handling process there exist a try to access the Database, this should be blocked (see *task* Block DB access). Finally the last countermeasure is introduced with a *task* Outcoming traffic control. This *task* controls if the response message is of the same length as it was prepared by the administrator. If this control fails, the *system* stops the message sending (see task Stop the operation).

4.6 Control implementation

Application of the BPMN is typically performed at the analysis stages. Thus implementation of the security requirements remains postponed. On the other hand the iteration of the ISSRM process is needed where the current processes, such as one presented in Figure 10 would be considered for the new security risks.

4.7 Summary

In this Chapter we have performed an analysis of how BPMN can be applied to ISSRM process according to its six steps. We identified context and assets that has any value to the system described in running example, determinate security objectives. We also analysed and made an assessment of risk with the help of created potential security risk scenario. Moreover, we made decision about risk treatment method and according to that we defined the security requirements and opportunity of control implementation.

Chapter 5. Mapping

The analysis of adaption the BPMN language to ISSRM is realised with the semantic alignment between this two approaches. In examples, which are illustrated in Figures 6 to 10, we represent the use of BPMN with respect to possible attack scenarios, implemented controls and security requirements to protect the system from these attacks. The results of the analysis are summarized in Table 1, which gives us an overview of opportunity to match ISSRM concepts, listed in the first column, with BPMN elements, adduced in the second column, providing decisions with required examples.

Table 1. Alignment between the ISSRM and BPMN

The ISSRM domain model		**BPMN constructs**	**Example**
Asset-related concepts	Asset	-	-
	Business asset	*Data object*; *Task*, *Gateway*, *Event*, *Sequence flow*	Username and Password; Processes described in Figures 6, 7, and 8
	IS asset	*Data store* *Pool*, *Lane*	Database; System, Database connection, Message
	Security criterion	-	Confidentiality of Usernames and Password; *Integrity* of processes described in Figures 6, 7, and 8
Risk-related concepts	Risk	-	-
	Impact		Confidentiality of Usernames and Password is broken; Integrity of processes (e.g., Figures 6, 7, and 8) is negated
	Event	-	-
	Threat	-	A violator sends a message containing a spy program, which extract info from database and sends it back to the violator.
	Vulnerability	-	Message is being handled without any scanning; The outgoing traffic is not monitored; The access to database is not controlled
	Threat agent	*Pool*	Violator
	Attack method	*Task*; *Flows (e.g., Data flow* with the label describing attack method; *Data association flow* with the label describing attack method);	Extract info from database; *Data flow* Message containing a spy program; *Data association flows* Sends a request and Gets data
Risk treatment related concepts	Risk treatment	-	Reduction (but other decision are also possible)
	Security requirement	*Task*, *Gateway*, *Event*, *Sequence flow*	*Tasks* Message scanning; Block user/Delete message; Control activity of DB access; Block DB access; Stop operation; Outgoing traffic control *Gateways* Safe?; Access to DB?; Traffic ok? *Events* Message deleted; Access forbidden; Operation stopped
	Control	-	-

5.2 Asset-related concepts

Asset-related concepts concentrate on *assets*, that need to be protected and *security criteria*, describing asset security. We defined that in BPMN the role of *asset* can be played by *data object*, *data association flow*, also *tasks*, which are used to model *business assets*. The *IS* *asset* is a BPMN *data store;* it contains information valuable for the system. From the Figure 6 we can define the example of IS asset – it is a Database, the business assets are username/password that Database contains. *Association* between *tasks* Accept registration signal, Insert data to Database and *Data object* Username/Password in Figure 7 also represent the valuable *assets* of the system with respect to ISSRM domain model. The *business asset* is defined as information or process that has value to organisation. Accordingly, we can make a parallel in definitions of an ISSRM *business asset* and the concept of BPMN *association*; the *association* represents the process flow that associates data with other *flow objects.*

We defined two *security criteria*, which characterize security needs of *assets* in our example: *confidentiality* of usernames and passwords, stored in the database. And from other point we can also talk about *integrity* of business process diagrams.

5.3 Risk-related concepts

Risk related concepts define the risk itself and the major risk assessments. The result of mapping shows that it can be realised only partially, so we can't define risks or event with respect to basic BPMN constructs and concepts. The security criteria, defined earlier, leads to identification of a threat; data confidentiality can be injured, and also the integrity of figures can be harmed. The vulnerabilities of the system are the following; message is being handled without any scanning and the work with it starts immediately after receiving, the outcome traffic of the system is not checked, and check of database access is not performed.

The *threat agent* is defined with the help of a *pool* element in Figure 9, called Violator. The *pool* represents any kind of communication between process participants, so it is the only element that can identify person or participant. The *attacker* carries an *attack method,* a combination of BPMN *task, data flow* and *data association flow*: from our example we can define *task* Extract info from database with *data association flow* to Database element. The impact negates the *security criteria* and compromises the confidentiality of above mentioned *assets*. Using stolen username and password violator illegally gets to the system and can use system services with the rights of a normal user.

5.4 Risk treatment-related concepts

The *risk treatment* describes the decisions that should be taken and controls to be implemented in order to mitigate risks, described earlier. For risk treatment decision we choose risk avoidance; it means that it is more valuable to implement controls that will help to keep system secure and to evade the *impact*. *Security requirements* are represented as a combination of BPMN *tasks, gateways, sequence flows* and *event*. One of the examples of security requirements is a process of message scanning in Figure 10; it starts with task Message scanning, followed by the conditional control realised by the *gateway* Secure?, and then it assumes making of decision to Block user/Delete message, the *event* Message deleted shows the result of the security requirement implementation. All these elements are connected with a *sequence flow*.

5.5 Summary

This chapter makes an overview of mapping the BPMN to ISSRM with respect to security risk analysis. We analysed how BPMN can be applied in order to follow the risk management process. The Table 1 brings the result of our analysis; it introduces the major ISSRM concepts, the synonyms of these concepts in BPMN approach and provides the examples of BMN language use. The analysis shows that mapping can be realised partially; great part of elements can be represented in BPMN, but they can be described according to the problem context.

Chapter 6. Discussion and Conclusion

In this work we have performed an analysis of the BPMN approach following the ISSRM domain model. Our major contribution is the semantic alignment of the BPMN constructs to the ISSRM concepts. In this chapter we discuss the validity threats, conclude the study with the potential extensions and improvements of the BPMN approach towards security risk management and also present the related and future work.

6.1 Threats to validity

The following threats to the validity of this study have been identified. Firstly, our results contain a certain degree of subjectivity. On the one hand, only two researchers have performed this study. Thus, it might mean that some aspects of the BPMN approach or its application could be interpreted and aligned to the ISSRM concepts differently. On the other hand, the running example also involves the subjective decisions on how to model the selected problem. For instance, in Figure 10 we have selected to take the risk reduction decision. However, the security requirements would be different if one would take the risk avoidance (or other) decision. Secondly, the scope of the current work is limited to the BPMN descriptive modelling. We acknowledge the importance to investigate the analytical and executable modelling, but this remains for the future research. Finally, in this work we analyse only a simple example of the Internet store. Although this example is realistic, we have not applied it in the practical settings. Thus, our analysis remains based on the selected BPMN literature (Remco et al., 2007; Seel et.al, 2005; White, 2004).

6.2 Potential improvements

During the example modelling process we faced some difficulties in using BPMN with a focus to security. The contribution of our analysis suggests improvements for BPMN in the context of security risk management activities:

Only part of ISSRM concepts can be realized with the help of BPMN; for example the major part of risk-related concepts of ISSRM cannot be represented with the help of BPMN structures. Some elements for BPMN are also missing in risk-treatment related concepts' group, such as *Risk treatment* or *Control,* and asset-related concepts' group, concepts like S*ecurity criteria.* The only opportunity to describe these concepts is to add extra information textually with the help of *text annotations* for example. Solution for this problem is to provide the BPMN language with new additional constructs to cover all the concepts described by ISSRM. That means to extend the abstract and concrete syntax, and semantics of the language.

The same constructs used for different ISSRM concepts. For example in Table 1 we can notice that the BPMN *task* is used to describe a *business asset*, an *attack method* and also *security criteria*, which can create conflicts in understanding and reading figures. However, the BPMN approach encourage using labels, this problem can be solved in this way: we can label *tasks* describing different types of ISSRM concepts with different labels, to mark if *task* is used to determine *attack method* or *security requirement*. Nowadays there exist a great variety of BPMN modelling tools, and most of them allowed using different colours while drawing models, so *risk-related* concepts can be marked with red colour for example, *risk-treatment* related – with blue (see Figures 8 and 9). Extended language structures will solve this problem too.

The guidelines of how exactly to use BPMN elements for different purposes are not defined; in the process of analysis we faced with a problem when one ISSRM concept can be represented with many BPMN constructs; for example security requirements in Figure 9 can be modelled with *tasks*, *gateways*, and *events*. These constructs can be used in group or separately; for example *gateway* Secure? Can be used without *task* Message scanning, it brings the same point – the control of a process flow. This makes a mess around the modelling process, because no strict rules exist about using one or another element. It can be helpful to define the rules that distinguish how to use different element while modelling system security. It will make understanding of business diagrams easier and modelling - more specified.

6.3 Related work

In the literature we found few studies on the extension of the business process modelling languages towards security. For instance Sindre introduces an extension of the UML activity diagrams, called mal-activities (Sindre, 2007). Gaaloul *et al.* present a model to ensure integrity, confidentiality and availability when tasks are delegated among business actors (Gaaloul et al., 2008). In the work of Backes et al. security requirements (expressed through the cryptographic primitives) are incorporated in the development of the business processes. The limitations of these works are that they focus either on a coarse-grained level, or target only some specific security aspects (e.g., security requirements) in business processes (Backes et al., 2003)

Rodriguez *et al*. propose the BPMN extensions for modelling secure business processes through understanding the *security requirements*. Firstly, their proposal illustrates the extension of the BPMN abstract syntax with the security-related concepts such as *non-reputation*, *attack harm detection*, *integrity*, *privacy*, *access control*, *security role* and *security permission*. Secondly, the concrete BPMN syntax is extended through the stereotypes introduced to the ordinary constructs of BPMN. The study does not include any consideration of the extension semantics. In comparison to the work of Rodriguez *et al*. in this work we do not propose any concrete extensions of the BPMN. However, we present a semantically grounded analysis based on the well-established domain model for the IS security risk management (Dubois et al., 2010; Mayer, 2009). This allows us (*i*) to understand current BPMN means to deal with security-related problems; (*ii*) to identify the potential BPMN extensions towards security analysis both at the (concrete and abstract) syntax level and at the security-oriented semantics level.

6.4 Future work

The major task of our future work remains the performance of validity test. One opportunity to validate our analysis results is to create an illustrative example with proposed improvements in BPMN – to realise a performance test. That will show if proposed improvements allow using language in earlier mentioned directions with respect to security and risk management. On the other hand, to achieve more objective view, more people can be involved in validation process to conduct usability testing; providing participants with ability for using improved syntax and language semantics, ask them to create an example. That practise will discover if the language mapping and proposed improvements are available and understandable for users and are easy to use in practise. For efficiency testing, we can compare BPMN with other approaches in order to find out if it proposes a reasonable and worth method to model business process security. By reason of scope limitations, we addressed our analysis only for the first level of BPMN modelling – descriptive modelling. But we also acknowledge the importance to investigate two other level - the analytical and executable modelling, so this remains for the future research. On the other hand, our contribution should be also understood in a broader sense. For instance, in some cases application of the BPMN security extensions would not be applicable because of the language nature to model organisation's business processes, i.e., leading to the weak expressive power to address security concerns. This would result in translation of the BPMN model to the security modelling languages, such as Secure Tropos (Matulevičius et al., 2008b) or misuse case (Matulevičius et al., 2008a). Such a model translation would be supported by transformation rules, developed on the semantic alignment of the (business and security) modelling approaches to the common base, i.e., the ISSRM domain model. However, definition of the transformation rules remains a future work.

Süsteemide turvalisuse arendamine kasutades äriprotsesside modelleerimist

Resümee

Äriprotsesside arusaam ja modeleerimine on üks olulisematest aspektidest iga tänapäevase süsteemi arendamisel. Infosüsteemide modeleerimise jaoks on loodud erinevad käsitlused ning üks nendest on äriprotsesside modeleerimisnotatsioon. BPMN aitab äriprotsesse kirjeldama, modelleerima ja optimeerima, kuid väiksemal määral aitab arusaama kuidas saab selle käsitluse raames juhtida äriprotsesside turvalisust ning analüüüsida infosüsteemi turvariske. See aspekt muutub kaasaegsetes infosüsteemides veel komplitseeritumaks kuna turvatud süsteemi loomiseks peavad nii äriprotsessid kui ka turvalisuse küsimused olema vaadeldud parallellselt - koostoimes. Selle uurimistöö eesmärgiks on analüüsida BPMN ja infosüsteemi turvariskide juhtimise vastastikus kaasmõju. BPMN'i võtmeaspektide väljaselgitamiseks ja antud modelleri turvanäitajate, riskide ja riskide juhtimise aru saamiseks antud töös on rakendatud struktureeritud lähenemine. Töös uuritakse kuidas modeller saab BPMN'i abil väljundada turvatud süsteemi komponente, riske või riskide juhtimist. Töös ühtlustatakse BPMN keele põhikonstruktsioonid ISSRM mudeli kontseptiga. Antud uurimistöös BPMN-i käsitluse rakendatavus on vaadeldatud interneti kaupluse näitel.

Meie uurimistöö pakkub infosüsteemi analüütikule või arhitektile võimalust mõistma äriprotsesse ja turvakomponente ühe modeleerimiskeele abil, ja analüüs on tehtud ainult esimesel keele tasemel vaadeldes *Descriptive modelling*. Sellega avatakse ka uurijal võimalus tulevikus tuua paralelle erinevate modeleerimise keelte vahel et uurida ISSRM perekonda kuuluvate mudelite loomises patterne.

References

1. van der Aalst, W.M.P., ter Hofstede, A.H.M. (2005) : YAWL: Yet Another Workflow Language. Information Systems, 30(4), pp 245–275

2. Backes, M., Pfitzmann, B., Waidner, M. (2003): Security in Business Process Engineering. In: van der Aalst W. M. P. (eds.) BPM 2003, pp 168-183. Springer Heidelberg

3. Börger, E., Cavarra, A., Riccobene, E. (2000): An ASM Semantics for UML Activity Diagrams. In: Proceedings of the 8th AMAST 2000, pp. 293-308. Springer, Heidelberg

4. Dubois, E., Heymans, P., Mayer, N., Matulevičius, R (2010).: A Systematic Approach to Define the Domain of Information System Security Risk Management. In: Intentional Perspectives on Information Systems Engineering. pp. 289-306. Springer

5. Matulevičius, R., Mayer, N., Heymans, P. (2008a): Alignment of Misuse Cases with Security Risk Management. In: Proceedings of ARES'08, pp. 1397-1404. IEEE Computer Society

6. Matulevičius, R., Mayer, N., Mouratidis, H., Dubois, E., Heymans, P., Genon, N. (2008b): Adapting Secure Tropos for Security Risk Management during Early Phases of the Information Systems Development. In Proceedings of CAiSE'08, pp. 541-555. Springer Heidelberg

7. Mayer, N. (2009): Model-based Management of Information System Security Risk. Doctoral Thesis, University of Namur

8. Remco, M., Dijkman, R.M., Dumas, M., Ouyang, C. (2007): Formal Semantics and Analysis of BPMN Process Models using Petri Nets. Queensland University of Technology, Tech. Rep.,

9. Rodriguez, A., Fernandez-Medina, E., Piattini, M. (2007): A BPMN Extension for the Modeling of Security Requirements in Business Processes. IEICE – Transactions on Information and Systems, vol E90-D (4), pp. 745-752

10. Seel, C., Vanderhaeghen, D. (2005): Meta-Model Based Extensions of the EPC for Inter-Organisational Process Modelling. In: Proceedings of the 4th GI-Workshop EPK 2005 – Geschaftsprozessmanagement

11. Silver, B. (2009): BPMN Method and Style: A Levels-based Methodology for BPMN Process Modeling and Improvement using BPMN 2.0, Cody-Cassidy Press

12. Sindre, G. (2007): Mal-activity Diagrams for Capturing Attacks on Business Processes. In Proceedings of REFSQ 2007, pp. 355-366, Springer Heidelberg

13. Stephen A. White. (2004): Introduction to BPMN, article, BP Trends, IBM Corporation

14. White, S.A.: Introduction to BPMN, IBM, (2004), http://www.bpmn.org/Documents/Introduction_to_BPMN.pdf

Appendix

Altuhhova O., Matulevičius R., (2011): Security Risk Management using Business Process Modelling Notations, submitted to the 10th International Conference on Perspectives in Business Informatics Research (BIR 2011)