A Model-Driven Engineering approach with Diagnosis of Non-Conformance of Security Objectives in Business Process Models

A.J. Varela-Vaca, Rafael M. Gasca and A. Jimenez-Ramirez
Computer Languages and Systems Department,
Quivir Research Group
ETS. Ingeniería Informática, Avd. Reina Mercedes S/N,
University of Seville, Seville, Spain
{ajvarela, gasca, ajramirez}@us.es

***Abstract*—Several reports indicate that the highest business priorities include: business improvement, security, and IT management. The importance of security and risk management is gaining that even government statements in some cases have imposed the inclusion of security and risk management within business management. Risk assessment has become an essential mechanism for business security analysts, since it allows the identification and evaluation of any threats, vulnerabilities, and risks to which organizations maybe be exposed. In this work, a framework based on the concepts of Model-Driven Development has been proposed. The framework provides different stages which range from a high abstraction level to an executable level. The main contribution lie in the presentation of an extension of a business process meta-model which includes risk information based on standard approaches. The meta-model provides necessary characteristics for the risk assessment of business process models at an abstract level of the approach. The framework has been equipped with specific stages for the automatic validation of business processes using model-based diagnosis which permits the detection of the non-conformance of security objectives specified. The validation stages ensure that business processes are correct with regard to the objectives specified by the customer before they are transformed into executable processes.**

***Index Terms*—business process; risk management; risk assessment; security requirement; conformance**

I. Introduction

Over recent years, a new paradigm has emerged within the scope of business IT: Business Process Management (BPM). BPM is defined as a set of concepts, methods, and techniques to support the modelling, design, administration, configuration, enactment, and analysis of business processes [1]. BPM has turned into an essential tool for organizations. BPM aims at narrowing the gap between business processes that a company performs and the implementation of these processes in Business Process Management Systems (BPMS).

The cost and consequences of security failures and of the materialization of a threat in these systems range from mildly annoying to catastrophic, since they can result in serious injury and lives lost, systems destroyed, security breaches, and so on.

Gartner's CIO report [2] indicates that the most important business priorities include: improving business, security and IT management. Likewise, security and risk management is gaining and ever more role in the government statements, in such a way that certain regulations and laws now impose the inclusion of risk and security management within business management, such as the Spanish National Security Scheme [3] and recommendations of the European Network and Information Security Agency [4]. Risk assessment, (hence referred to as *RA*), has become a crucial mechanism for business security analysts, since risk assessment is a procedure which allows the identification and evaluation of any threats, vulnerabilities, and risks to which organizations may be exposed, therefore it also enables stakeholders to select the treatment or countermeasures in order to mitigate, reduce, control, or transfer the risks identified in the RA.

In this work, a framework is proposed based on the concepts of Model-Driven Development. The framework provides several stages of modelling, ranging from a high abstraction level to an executable level. The main effort is focused on the abstract level where an extension of business process models which includes risk information is presented. Likewise, various diagnosis stages are incorporated into the framework in order to validate the models.

This paper is structured as follows: in Section II a introduction of the framework is given; in Section III a description of the diagnosis stage is presented; in Section IV an extension of business process modes with risk is detailed; Section V introduces an example; in Section VI a comparison of related work is presented and finally in Section VII conclusion are drawn and ongoing work is described.

II. Framework overview

The proposed framework is developed based on Model-Driven Development (MDD) [5] and Model-Driven Architecture (MDA). MDD is a software engineering approach where models become the key elements in software development, while MDA is a particular vision of the concepts MDD provided by the OMG. One of the main goals of MDA is the improvement of the software adaptation to several different technological scenarios, thereby providing a structural separation in the architecture at different abstraction levels of

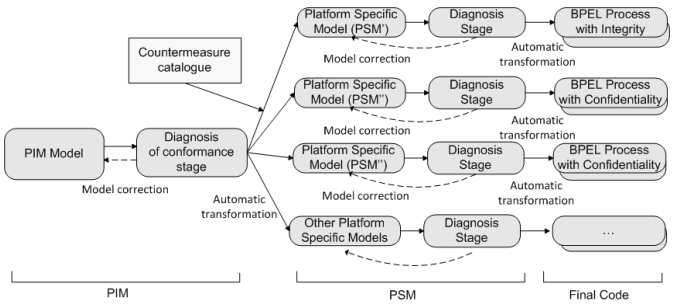

Fig. 1. Framework overview of the different stages of modelling.

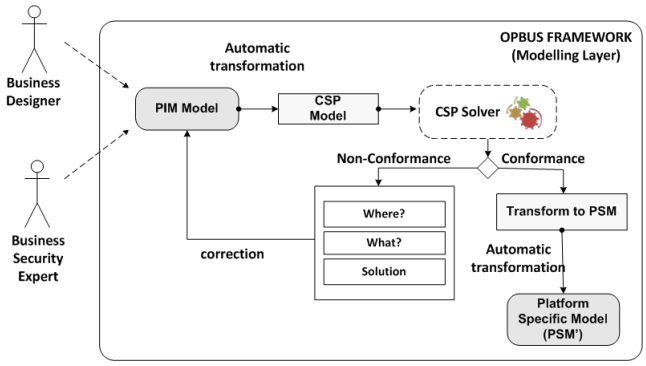

Fig. 2. Diagnosis process of checking conformance.

modelling. This separation enables the specification of models at a very high level through a Platform Independent Meta-Model (PIM) for a particular domain but with only non-specific information about the platform where the model will be deployed. MDA introduces the concept of transformation which allows the conversion of abstract models into models of a more specific nature specified by a Platform Specific Meta-Model (PSM). The main benefit of using MDA comes from the transformation between models at different abstraction levels, which allows executable code to be obtained automatically from abstract models by applying successive transformations. However, transformations are a conflictive point of the architecture since if a model is not validated at one level, when this same model is then transformed into another model, non-conformance properties could be introduced along with the different models. Hence, it is crucial to validate the models before transformations are executed. MDA does not provide any diagnosis stage as an integrated part of the architecture, although this idea has already presented in other studies [6] where the MDA architecture is extended with diagnosis points before model transformations.

The framework is structured in at least three stages, as shown in Figure 1. In the first stage, PIM models are built, then a the first transformation between a PIM model to PSM models is proposed. In this transformation, extra information is introduced in terms of information of a more specific nature information on mechanisms to control or mitigate security problems. Therefore, PSM models are PIM models enriched with specific information. Although other intermediate transformations can be introduced between PSM and other PSM models, as a first approach, a transformation from PSM models to final code is proposed. A particular diagnosis stage is introduced for the validation of models before each transformation.

We propose the utilization of business process models based on BPMN by the OMG [7] as the PIM of the framework. Business process models are only a graphical representation of a set of tasks and control flows that define the structure of a business process. Nowadays, at the design level business process models gather no information for instance about how the tasks are executed or which platform is used. Although, these models are abstract, they still need an evaluation and validation of their security and risks. To this end, an extension of BPMN models the inclusion of risk information is provided in order to focus on security issues so that the risk assessment of business processes can be performed. Moreover, a model-based diagnosis has been incorporated into the different diagnosis stages in order to determine the non-conformance of the security properties of business processes.

Therefore, this paper is focused on presenting the extension of business process models to include risk information, as a PIM Meta-Model, and on introducing the first diagnosis stage.

III. Diagnosis of non-conformance of security objectives

Model-based diagnosis is included in the diagnosis stages in order to perform a the risk assessment of business processes and to identify any non-conformance of security objectives at the acceptable levels. As defined in the ISO/IEC 27002, ”the risk assessment will help to guide and determine the appropriate management action and priorities for managing information security risks, and for implementing controls selected to protect against these risks.” Therefore, a risk assessment process is an obligatory step towards determining whether the risks must be managed.

The diagnosis of non-conformance implies three tasks: detection, identification and isolation. Detection is used to find the existence of the non-conformance of objectives, and the identification and isolation permit the elements involved in the non-conformance to be located. In this way, the application of constraint programming [8] is considered as a solution for the automation of the diagnosis stage. To this end, a transformation is attempted from the business process models enriched with risk information into a Constraint Satisfaction Problem (CSP). This CSP model can be automatically solved using a solver tool (a solver is a engine of constraints that implements some algorithms in order to solve CSPs). The solver can retrieve information on whether the model conform to the acceptable values specified and is also able to provide information to identify and isolate where and what fails to conform to. The complete diagnosis process is depicted in Figure 2. In Section V an example of the detection of non-conformance is detailed.

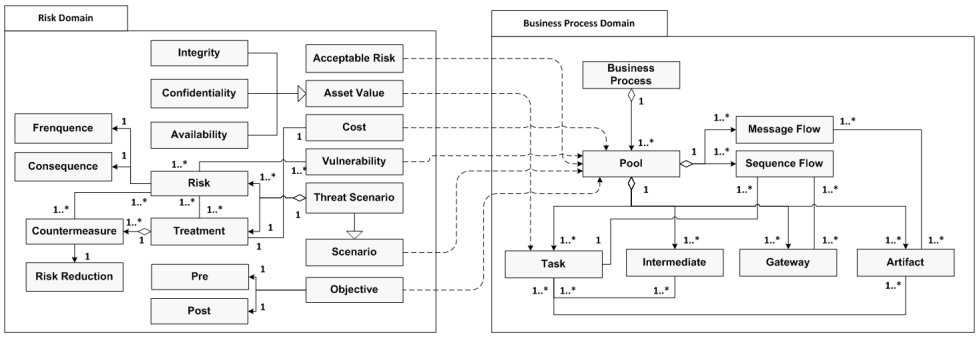

Fig. 3. Business process meta-model extension with risk information.

IV. Extending business process models with risk information

An extension of the BPMN meta-model is defined, see Figure 3. The extension is mainly based on the UML profile of Quality of Service (QoS) and Fault Tolerance (FT) Characteristics and Mechanisms Specification, [9]. This profile defines a generic catalogue of QoS characteristics and categories. These characteristics and categories are the constructors for the description of non-functional aspects such as latency, security, and integrity. Our approach is contained within the QoS category of Security that covers various subjects, such as the protection of entities and access to resources. The profile also provides a set of generic concepts in order to develop risk assessment capabilities within IT systems.

Before continuing, an introduction is required of the set of concepts from the UML profile which are used to in the definition of the extension of the meta-model:

- *Assets* are the elements (participants, tasks, business processes, etc.) that contribute value to the organization.
- *Vulnerabilities* can be defined as those faults linked to an asset that could compromise the correct operation of the asset or compromise the information that is used for the asset. In our context, faults are considered as the non-conformance with regard to the specification.
- *Threats* are situations or actions that can occur to the assets which may cause damage to the organization.
- *Countermeasures* are the appropriate measures which help towards a reduction of the impact of a threat to the organization.
- *Treatment* is a specific countermeasures that the organization uses to reduce the effects of a threat

A. Modelling the evaluation of assets

Assets could be considered as the pools, tasks, resources and data that use the business processes. We have assumed that a pool is an individual business process which gathers information relative to the participants, tasks, data objects, and flows. Therefore, a business process is the main asset to be assessed.

The profile [9] introduces the concept of *Asset Value* to the qualification of assets. This attribute indicates an estimation about the importance of a business process. Furthermore, the asset value is separated into three sub-categories in accordance with ISO/IEC 27004, and related to security issues: Value integrity, Value confidentiality, and Value availability. The qualification of the individual tasks is also permitted within the business process. In the asset assessment task two types of measurement are usually applied: qualitative (verbal scale of values) and quantitative (interval of numerical values). A qualification based on an interval of values from 1 (worst value) to 5 (best value) is adopted in our approach. This interval of values is the same as that used by the CRAMM methodology, although other intervals of values can be used, since the profile restricts none of these attributes. An example where activities are qualified can be observed in Figure 4 .

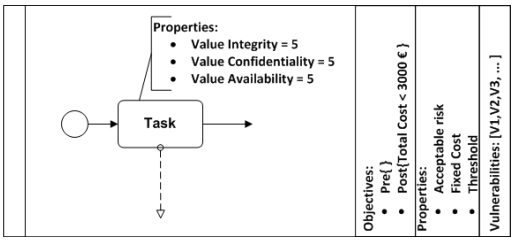

Fig. 4. Business process extended with new parameters.

$$AssetValue = Value\_Integrity + Value\_Confidentiality + Value\_Availability;$$

Information relative to the goals of the business process is considered. In this way, the Objective concept defined by the Business Motivation Model [10] is adopted. Objectives permit the constraints to express what the customer needs with respect to the business process. Objectives are modelled by two parameters *Pre* and *Post*, and are indicative of what the process requires (Pre), and of what the process should ensure (Post). An example of objectives is shown in Figure 4 where *Post* indicates that the total cost associated to the business process cannot exceed 3000 euros.

Acceptable Risk is another parameter incorporated into the extension. This parameter indicates how acceptable the risk is in order to conform with the expected risk of the organization. Acceptable risk is not included within the profile, but its inclusion is considered since it permits the specification of a requirement which indicates that the overall risk of the business process cannot exceed certain limits. As defined in the ISO/IEC 31000: ”the risk assessment is a process which helps to determine if the risks are acceptable”. In the case when the

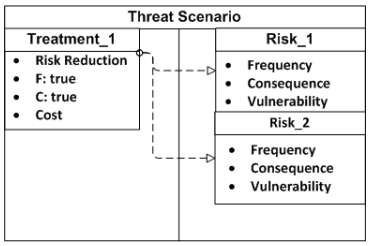

Fig. 5. Example of a threat scenario.

risk of a business process exceeds the limits, business experts have to decide whether to transfer, avoid, mitigate, or accept this risk. Therefore, this parameter can play a crucial role in the risk assessment process.

Other parameters are included into the business process with regard to monetary value. The inclusion of cost parameters is considered as a means to carry out a more realistic analysis. Only two parameters are included in the extension with respect to the business process: *Fixed* cost, and *Threshold* which indicate the cost and the interval of allowed monetary values respectively.

B. Modelling vulnerabilities

Vulnerabilities are possible causes of non-conformance which could compromise the correct operation of the assets or the information that is used for the assets. A list of vulnerabilities is included in extension, as shown in Figure 4. Vulnerabilities can also be linked to specific tasks or flows inside the process, although, for the sake of simplicity only those vulnerabilities that affect the entire business process are taken into account. Vulnerabilities could be selected from some of the available catalogues such as the NIST catalogue [11] and ISO/IEC 27005 - Annex C.

Vulnerabilities are associated with a set of risks concerned with the likelihood, given a specific situation, of the business process being compromised or damaged. Risks are attached into the threat scenarios which are given detailed below section. Risk must be linked with a specific vulnerability previously attached to the business process. This is represented as a relation between Vulnerability and Risk in the meta-model in the Figure 3.

C. Modelling risks, treatments and threat scenarios

The UML profile [9], introduces the concept of scenarios attached to assets. These scenarios describe, identify and document unwanted incidents concerned with exploring the threats and vulnerabilities of the asset under assessment. In our case, threat scenarios can be attached to business processes. Threat scenarios are composed of two sets, the first for risks, and the second set to specify the countermeasures, as shown in Figure 5.

A *risk* represents a factor that indicates the combination of the probability of an event and its consequence:

- *Frequency* indicates how often a risk occurs.
- *Consequence* indicates the possible extent of the risk incurred by the threat.

Countermeasures is a set of treatments applied in order to reduce the risks. Each treatment has an associated property called *Risk Reduction* which indicates the value of reduction if the treatment were applied to a specific risk. In addition, a new property *Cost* is added to take into account the cost of implementation of treatment.

It is assumed that treatment could reduce the effects of risk by the same percentage (frequency and consequence), however this is false in the majority of cases. For this reason, three types of treatments are considered one that reduces the *frequency*; another that reduces the *consequence*; and a third that reduces both these factors. Therefore, two Boolean parameters *F* and *C* are included into the treatments in order to indicate whether the risk reduction affects *frequency* or *consequence*. Hence, the casuistic is larger, since the selection of treatment could multiply due to the wide range of solutions available, which could reduce the frequency, the consequence or both.

V. Example of an application

In this section, an example of the problem of risk assessment and of the verification of non-conformance is presented using the extension proposed. The example depicted in Figure 6 represents a business process of patients who try to be admitted into a medical centre for a medical evaluation. The business process is evaluated with regard to security issues. Business security experts have identified a threat scenario with two risks: Deny of Service (DoS) and Unexpected manipulation of personal data; and have identified one treatment for Data Integrity Systems in the form of a Message Authentication Code (MAC).

There are several ways to calculate these risks, where each methodology applies its own criteria. An example of the criteria adopted in this paper is shown in the formula below, which permits the calculation of the risk value for the *Fill out Admin Request (FoR)* task:

$$Risk_{FoR} = \sum_{r \in risk} AssetValue_{FoR} * \sum_{t \in treatment} \{[Frequency_r - RR_t * Frequency_r/100)] * [Consequence_r - (RR_t * Consequence_r/100)]\}$$

In general, this formula can be used for the calculation of the risk value of any single task. This calculation is a tedious and time-consuming task for several reasons, one of which is the possibility of having to support interval values for the different parameter of the model. In Figure 6 shows some parameters that are specified as an interval of values: RR=[10%-40%], Frequency=[1-3], Consequence=[2-5], and so on. In this case, the calculation of the risk has to be carried out while taking into account all possible combination of values for each parameter. For instance, the FoR risk value can be calculated as shown below, according the following set of values: the MAC has a risk reduction of 10%, DoS risk has (Freq=1 and Conseq=2), and Unexpected theft has (Freq = 3 and Conseq=4).

$$Risk_{FoR} = [9*(1-(1*10/100))*(2-(2*10/100))] + [9*(3-(3*10/100))*(4-(4*10/100))] = 126$$

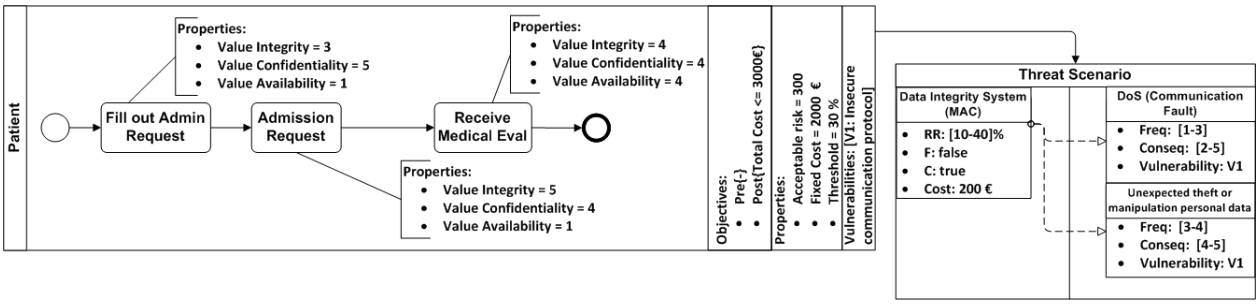

Fig. 6. Example of scenario of a business process extended with risk capabilities.

Considering another case, for instance, an increase of the risk reduction to 30%, the risk value is less than before.

$$Risk_{FoR} = [9*(1-(1*30/100))*(2-(2*30/100))]+ \\ [9*(3-(3*30/100))*(4-(4*30/100))] = 63$$

Considering another case, for instance, where the DoS frequency is 3, the risk estimation is even higher than the first estimation.

$$Risk_{FoR} = [9*(3-(3*10/100))*(2-(2*10/100))]+ \\ [9*(3-(3*10/100))*(4-(4*10/100))] = 162$$

Previous risk values are only three examples of risk calculation for the same task, although there exist more than 100 casuistics that must be considered. Clearly, the problem could become an exponential problem.

Assuming that the risk values for each task are fixed as follows:

$Risk_{FoR} = 140$
$Risk_{AR} = 160$
$Risk_{RME} = 192$

Then, the risk value for the Patient business process is obtained as follows:

$$Risk_{BP_{Patient}} = 140 + 160 + 192 = 492$$

Once the risk value is determined, the conformance can be checked with regard to the acceptable risk (Acceptable Risk). A business process that exceeds the specified level of acceptable risk implies the existence of non-conformance.

$$\forall p \in BP \rightarrow Risk_p < AcceptableRisk_p$$

In the case above, the Patient business process display non-conformance since its risk value exceed the acceptable levels specified. The result of the diagnosis (detection) of non-conformance could be shown as follows.

- Business process tasks:
  - $Risk_{FoR} = 140$
  - $Risk_{AR} = 160$
  - $Risk_{RME} = 192$
- Risks:
  - DoS (Communication fault):
    - Frequency = 4
    - Consequence = 5
  - Unexpected theft or manipulation of personal data:
    - Frequency = 2
    - Consequence = 5
- Treatments:
  - Data Integrity System (MAC):
    - Risk Reduction = 30%
- Non-Conformance:
  - $Risk_{BP_{Patient}} = 492 \not< 300$

On the other hand, the risk value Patient business process can also lie within the acceptable limits as defined other casuistic examples, for example:

- Business process tasks:
  - $Risk_{FoR} = 63$
  - $Risk_{AR} = 70$
  - $Risk_{RME} = 84$
- Risks:
  - DoS (Communication fault):
    - Frequency = 1
    - Consequence = 2
  - Unexpected theft or manipulation personal data:
    - Frequency = 3
    - Consequence = 4
- Treatments:
  - Data Integrity System (MAC):
    - Risk Reduction = 30%
- Non-Conformance:
  - $Risk_{BP_{Patient}} = 217 \not< 300$

An exhaustive search for solutions is impossible due to the enormity of the search space. Therefore, it is necessary for other mechanisms to determine the set of values for the parameters that conform to specified levels of acceptable risk. For this reason, CSP is proposed as the mechanism to solve this problem since it permits specified variables with open domains (interval of values) and a function objective (non-conformance criteria). The CSP solver attempt to find an assignment of values for the variables in order to satisfy the objective function whenever is to be possible.

VI. Related work

A comparative study of several approaches is developed following the survey presented by [22] as shown in Table I. The comparison is carried out in accordance with the following categories: (1) Modelling: indicates which modelling languages are supported; (2) Security issues: indicates whether the qualification is carried out with regard to security parameters; (3) Cost: indicates whether costs are considered for the risk assessment; (4) Objectives: indicates whether the approach supports the specification of requirements; (5) Vulnerabilities: indicates whether the approach supports the specification of vulnerabilities; (6) Countermeasures: indicates whether the approach supports the specification of Countermeasures; (6) Diagnosis conformance: indicates whether the

TABLE I
COMPARISON OF BUSINESS PROCESS SECURITY APPROACHES.

	Security issues	Cost	Objectives	Vulnerability/Threat	Diagnosis non-conformance	Countermeasure	Modelling
Our approach	✓	✓	✓	✓	✓	✓	BPMN
Korherr [12]	X	✓	✓(Partial)	X	X	X	EPC and BPMN
Menzel [13]	✓	X	X	X	X	X	BPMN
Cope [14]	✓(Partial)	✓	X	✓	X	✓	BPMN
Muehelen [15]	X	✓(Partial)	X	✓(Partial)	X	✓(Partial)	EPC
Lambert [16]	X	X	X	X	X	X	IDEF
Rodriguez [17]	✓	X	✓	X	X	X	UML
Neiger [18]	X	✓	✓	X	X	X	EPC
Sackman [19]	✓	✓	Possible	?	X	Possible	Independent
Jakoubi [20]	✓	✓	Possible	✓	X	Possible	Independent
Neubauer [21]	X	✓	Possible	?	X	✓	Independent

approach supports the diagnosis (detection, identification and isolation) of the conformance of requirements as specified.

It should be come in mind that the majority of approaches support some characteristics, however not all of these characteristics are supported together in such a way as we propose in our extension. Furthermore, no approach supports or fosters a process for the analysis of the conformance of the requirements specified with regard to the risk or security issues as identified in the model.

VII. CONCLUSION

In this work, we have proposed a framework separated into various modelling stages based on the MDD ideas. We have focused on the PIM stage. The main contribution lies in the presentation of a meta-model which is an extension of business process models by including risk information based on standard approaches. This extension is necessary in order to carry out a risk assessment of the business process. Furthermore, the proposed framework is equipped with several diagnosis stages for the automatic diagnosis of models. In the first diagnosis stage, we have proposed the application of a model-based diagnosis using constraint programming techniques for the automatic verification of conformance by business processes with security to specified objectives. To the best of our knowledge, this paper is the first approach which provides a mechanism to carry out the risk assessment, and proposes an automatic checking of the conformance of acceptable risk based on diagnosis techniques. In future work, we propose extending the framework capabilities to include new properties in the PIM Meta-Model. Furthermore, we are also considering the completion of diagnosis by means of providing identification and isolation mechanisms through the use of the constraint programming approach.

ACKNOWLEDGEMENT

This work has been partially funded by Consejería de Economía, Innovación y Ciencia of the Regional Government of Andalusia project under grant P08-TIC-04095, and by Spanish Ministerio de Ciencia e Innovación project under grant TIN2009-13714, and by FEDER (under ERDF Program).

REFERENCES

[1] M. Weske, *Business Process Management: Concepts, Languages, Architectures*. Springer, 2007.

[2] Gartner Inc., "Gartner CIO report," http://www.gartner.com/it/page.jsp?id=1283413, 2010.

[3] Spanish Goverment - Presidency Ministry, "Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el mbito de la Administracin Electrnica," 2010.

[4] "Integration of Risk Management with Business processes," "http://www.enisa.europa.eu/act/rm/cr/business-process-integration", 2010.

[5] T. Stahl and M. Völter, *Model-Driven Software Development: Technology, Engineering, Management*. Chichester, UK: Wiley, 2006.

[6] S. Pozo, R. Ceballos, and R. Gasca, "Model-based development of firewall rule sets: Diagnosing model inconsistencies," *Information and Software Technology*, vol. 51, no. 5, pp. 894 – 915, 2009.

[7] "Business process model and notation," "http://www.omg.org/spec/BPMN/1.2", 2009.

[8] P. Hentenryck, "Constraint programming," in *Proceedings of the 5th International Conference on Evolutionary Multi-Criterion Optimization*, ser. EMO '09. Berlin, Heidelberg: Springer-Verlag, 2009, pp. 3–3.

[9] "UML Profile for Modeling QoS and Fault Tolerance Characteristics and Mechanisms," "http://www.omg.org/spec/QFTP/1.1", 2009.

[10] T. B. R. Group, "Business motivation model (bmm) 1.1," Object Management Group (OMG), Tech. Rep., 2007.

[11] A. G. Gary Stoneburner and A. Feringa, "Risk Management Guide for Information Technology Systems," National Institute of Standards and Technology (NIST) - U.S. DEPARTMENT OF COMMERCE, Tech. Rep., 2002.

[12] B. Korherr and B. List, "Extending the epc and the bpmn with business process goals and performance measures," in *ICEIS (3)*, 2007, pp. 287–294.

[13] M. Menzel, I. Thomas, and C. Meinel, "Security requirements specification in service-oriented business process management," *Availability, Reliability and Security, International Conference on*, vol. 0, pp. 41–48, 2009.

[14] E. W. Cope, J. M. Kuster, D. Etzweiler, L. A. Deleris, and B. Ray, "Incorporating risk into business process models," *IBM Journal of Research and Development*, vol. 54, no. 3, pp. 4:1 –4:13, 2010.

[15] M. zur Muehlen and M. Rosemann, "Integrating risks in business process models," in *ACIS 2005 Proceedings*, 2005.

[16] J. H. Lambert, R. K. Jennings, and N. N. Joshi, "Integration of risk identification with business process models," *Syst. Eng.*, vol. 9, no. 3, pp. 187–198, 2006.

[17] A. Rodrguez, E. Fernndez-Medina, and M. Piattini, "Towards a uml 2.0 extension for the modeling of security requirements in business processes," pp. 51–61, 2006.

[18] L. Churliov, D. Neiger, M. Rosemann, and M. Z. Muehlen, "Integrating risks in business process models with value focused process engineering," in *Proceedings of the 14th European Conference on Information Systems*, 2006.

[19] S. Sackmann, *A Reference Model for Process-Oriented IT Risk Management*, 2008. [Online]. Available: is2.lse.ac.uk/asp/aspecis/20080114.pdf

[20] S. Jakoubi and S. Tjoa, "A reference model for risk-aware business process management," *4th International Conference on Risks and Security of Internet and Systems (CRiSIS)*, pp. 82 –89, 2009.

[21] T. Neubauer, M. D. Klemen, and S. Biffl, "Business process-based valuation of it-security," *ACM SIGSOFT Software Engineering Notes*, vol. 30, no. 4, pp. 1–5, 2005.

[22] S. Jakoubi, S. Tjoa, G. Goluch, and G. Quirchmayr, "A survey of scientific approaches considering the integration of security and risk aspects into business process management," in *DEXA Workshops*, 2009, pp. 127–132.