AI Communications 29 (2016) 233–235
DOI 10.3233/AIC-140651
IOS Press

Thesis

OPBUS: A framework for improving the dependability of risk-aware business processes

Angel Jesus Varela-Vaca
Department of Computer Languages and Information Systems, University of Seville, Sevilla, Spain
E-mail: ajvarela@us.es

Abstract. Business processes and IT infrastructure have become a cornerstone for the management of organizations. Nevertheless, business processes are ever threatened by problems due to the exposure of these processes to external and third parties outside the control of the organizations. Risk management is mostly overlooked or is taken into consideration separately from business process management with a complete lack of formalization and automation. In this work, innovative and relevant contributions based on model-based diagnosis and constraint programming techniques are proposed for enhancement the dependability of business process management from design to run-time.

Keywords: Business process management, risk management, security, dependability, feature model, constraint programming, model-based diagnosis

1. Introduction

There currently exists a growing trend to externalize complex and critical processes of organization services by using business process management systems. These processes are ever threatened by security problems due to the exposure of business processes to external and third parties outside the control of the organizations. Nevertheless, security risk management is mostly overlooked or is taken into consideration separately from Business Process Management (BPM).

BPM [1] provides methods, techniques and tools to support business process development. BPM provides a diagnosis stage where processes are analysed to identify problems (i.e. deadlocks, starvations, etc.) and to find things that can be improved. In general, diagnosis methods have been applied to determine the activity or activities which are the cause of a malfunction when, after the execution of a process instance, the behaviour of the business process does not correspond to the expected.

OPtimization of BUsiness process Security (OPBUS) framework [3] is proposed for the improvement of the dependability of the life-cycle of BPM. OPBUS presents three main contributions: (1) *Diagnosis of non-conformance of risks*, to perform an assessment of business process models by diagnosing the tasks within the model whose risks are non-conformant with regard to expected acceptable risk levels; (2) *Selection of optimal configurations and generation of configurations*, using diagnosed tasks within the model to perform an optimized search of countermeasures that enable configurations that reduce and mitigate risks to be generated according to the needs of the organizations; and (3) *Deployment fault tolerance infrastructure*, to provide a diagnosis and recovery infrastructure at run-time in order to ensure the correct execution in spite of the existence of faults.

2. Contributions

(1) *Diagnosis of non-conformance of risks in business process models*. Our contribution consists on two parts: (1) transformation of business pro-

cesses onto risk-aware business process models by providing a risk model as an extension of these models; and (2) the provisioning of verification methods for the risk assessment of business process models, and for the diagnosis of tasks whose risks are non-conformant with regard to acceptable risk level.

Firstly, we propose a light extension to business process models [2] that enables the risk identification, risk estimation and the establishment of business objectives of the business process tasks and artifacts. Risk assessment strives to compute the risks (risk estimation) in order to evaluate (risk evaluation) whether risks are acceptable in accordance with business objectives. Automatic techniques are provided [5] in order to perform risk estimation and risk evaluation of an entire business process. We propose computing risk estimation based on various control-flow patterns [2]. Thereafter, risk estimation and business processes are diagnosed in order to identify which elements within the model are non-conformant to the expected risk criteria. In order to automate risk estimation and the risk evaluation we provide a verification mechanism that enables the Model-Based Diagnosis (MDB) and Constraint Programming (CP) techniques to automate it. Thus, business process models and their extensions are transformed into constraint programs that are evaluated using a constraint solver. The constraint solver evaluates the model by providing a result of non-conformance or conformance of the business process. If there is any non-conformance, then the elements of the business process model involved in the non-conformance are isolated by means of an exoneration process.

(2) *Generation and selection of optimal configurations* for security controls present a big challenge in business process management systems since there is a vast list of IT controls that must be set up with a large number of configurations. This heterogeneity makes difficult to ensure the effectiveness of the configuration with regard to organizational requirements. This contribution [6] firstly provides a formalization of IT security countermeasures for business processes based on security patterns and feature models for the representation countermeasures. Subsequently, a catalogue of IT security countermeasures have been formalized [4] to enforce confidentiality, integrity, availability and authentication in business processes management systems. Feature-Oriented Domain Analysis (FODA) have been applied [4] over the catalogue of security patterns for the inference, selection, and generation of optimal configurations with regard to single and multiple objectives. In order to automate FODA, CP techniques have been used where two different analyses have been carried out. A first analysis consisted of obtaining the total number of configurations regardless of attributes and extra functionalities; moreover, a model consistency operation has been applied to the models in order to detect possible void feature models. Subsequently, a second analysis consisted of applying optimized searches has been applied to achieve specific configurations with regard to one or multiple objective functions.

(3) *Deployment fault tolerance infrastructure*. Business processes must be deployed after selecting countermeasures. Despite countermeasures, business processes could still have faults (such as zero-day vulnerabilities) during run-time hence these processes could be affected by unexpected faults. The contribution presents a fault tolerance layer [3] (cf. Chapter 6), that may be integrated into a business process management system, composed of two main stages: (1) an error detection mechanism based on business rules and MDB using CP techniques for the detection and isolation of faulty components; (2) definition of various fault tolerance patterns based on replication and redundancy, dynamic binding of services, check-pointing and roll-back, and diversity. Error detection mechanisms compare the results of the business process with the results of the business rules. In the case of any discrepancy, the MDB is applied in order to detect and isolate which components of the business process are responsible. Once faulty components are identified, error detection stage communicates the decision to recovery stage to release a recovery mechanism.

Acknowledgements

This work has been partially funded the Regional Government of Andalusia (under Grant P08-TIC-04095), by the Government of Spanish (under Grant TIN2009-13714).

References

[1] W. Aalst, A. Hofstede and M. Weske, Business process management: A survey, in: *Business Process Management*, W. Aalst and M. Weske, eds, Lecture Notes in Computer Science, Vol. 2678, Springer, Heidelberg, 2003, pp. 1–12.

[2] A. Varela-Vaca, R. Gasca and A. Jimenez-Ramirez, A model-driven engineering approach with diagnosis of non-conformance of security objectives in business process models, in: *2011 Fifth International Conference on Research Challenges in Information Science (RCIS)*, 2011, pp. 1–6.

[3] A.J. Varela-Vaca, OPBUS: A framework for improving the dependability of risk-aware business processes, available at: http://estigia.lsi.us.es/angel/thesis/.

[4] A.J. Varela-Vaca and R.M. Gasca, Towards the automatic and optimal selection of risk treatments for business processes using a constraint programming approach, *Information and Software Technology* **55**(11) (2013), 1948–1973.

[5] A.J. Varela-Vaca, R.M. Gasca and L. Parody, OPBUS: Automating structural fault diagnosis for graphical models in the design of business processes, in: *21th International Workshop in Principles of Diagnosis (DX'10)*, 2010.

[6] A.J. Varela-Vaca, R. Warschofsky, R.M. Gasca, S. Pozo and C. Meinel, A security pattern-driven approach toward the automation of risk treatment in business processes, in: *CISIS'12*, Advances in Intelligent Systems and Computing, Vol. 189, Springer, Berlin/Heidelberg, 2013, pp. 13–23.