A Flexible Integration of Security Concern in Rule based Business Process modeling

Khadhir Bekki[1] , Hafida Belbachir[2]

[1] Department of Computer science, Ibn khaldoune University, Tiaret, Algeria

Bekki_kh@Yahoo.fr

[2]Department of Computer science, Mohamed Boudiaf University, Oran, Algeria

H_Belbach@Yahoo.fr

Abstract Today, to stay competitive, organizations are in the quest to execute their business processes correctly and continuously. This need require to apply risk, security and business process management in a more integrated way. At the same time, business processes need to be more flexible and adaptable. Habitually, The business rules represent main driving force for adaptability and competitiveness in organizations. The ECA (Event-condition-action) is a popular way to incorporate flexibility into a process design. As well, separation of concerns becomes one of the cornerstone principle in software engineering, and it supports adaptation in several ways. In this paper, we propose a flexible way to integrate security concern into rule based business process modeling. First, we govern any business activity through our ECATE formalism (Event-Condition-Action-Temporal condition- trigger Event) based on business rules. Then, we integrate the security requirements in a separate concern as EUCATE rules (a variant of ECATE rule). The rules based process will verified before being deployed in the runtime environment

Keywords: Business processes modeling, business rules, flexible modeling, separation of concerns, security.

1 Introduction

Actually, companies are more to more in the quest to execute their business processes correctly and continuously. Within the last years, the private sector has noticed a growing need to improve security to meet tighter regulative and legal requirements[1]. This need forced organizations to integrate the capture of security requirement in the business process modeling.

The early design of security requirements have some benefits [2] (1) use the security knowledge of security business process analysts at high level in modeling step.

(2)reduce potential costs avoiding the additional implementation of business processes security after the implementation of business process. (3) simplify the capturing of the security requirements. As well, flexibility, adaptability and correctness, besides knowledge-intensiveness belong to the most challenging issues of business process[3].
The BPEL language does not provide any support for the specification of either authorization policies or authorization constraints on the execution of activities composing a business process [4]. It is important that such an authorization model be high-level and expressed in terms of entities that are relevant from the organizational perspective [4]. The regulations and policies in organizations are often expressed in terms of business rules that are sometimes defined as high-level structured statements that constrain, control, and influence the business logic [5]. Business rules are defined as[5]: ”the set of policies for regulating the whole business within and out-side an organization”. They represent main driving force for adaptability and competitiveness. The ECA pattern has been widely adopted for business rules [6]. They are an interest way to incorporate flexibility into a process design. And, they are a popular approach to catch unanticipated events and adapt to exceptions [7].
As well, separation of concerns provides a way to separate development of the functionality and the crosscutting concerns (e.g., quality of service, security). This principle has become one of the cornerstone principle in software engineering, and has lead to a wide spread of aspect-oriented programming(AOP) approach [8].
The advantages in addressing each concern separately are transparency, evolution, understandability and scalability. More, it is necessary to bring them together to understand which global system properties emerge at any given activity [9].
In order to incorporate flexibility and adaptability into a business process design, and benefit of the advantages of separation of two concerns: security and functional in business process modeling, we propose, in this paper, a new rule based model that wants to improving the flexibility, adaptability of business process.
First, for the functional concern, we govern any business activity through our ECATE formalism (Event-Condition-Action-Temporal condition- trigger Event) based on business rules. Then, we integrate the security requirements in a separate concern as EUCATE rules (a variant of ECATE rule).
The rest of this paper is organized as follows. In the second section, we present rule based business process modeling as set of ECATE rules. The third section explain how to integrate flexibly the security requirement in the ECATE rules based process. The section 4 gives a related works. Finally, wrapped up by some concluding remarks and further required extensions of this work.

2 A Rule based business process modeling

2.1 Definition

The process modeling aims to provide high-level specification independent from implementation of such a specification. To support verification, validation, simulation of the automated process, the process modeling language provides the appropriate syntax

and semantics to specify the precise requirements of business processes and reflect the logic of the underlying process
As given in[10], two formalisms on which the most predominant process modeling languages are developed, are graph-based formalism and rule based formalism.
Rule-based approach proposes to model the logic of the process with a set of business rules. Each rule specifies properties of one or more business activity, such as the pre and post conditions of execution. In comparison with graph based approaches, the rule based approaches are more expressive and flexible [10]. They are able to express the temporal requirements. They take advantage in adaptation to ad hoc modification at runtime and exception.
Business rules are considered as policies, laws and know-how for doing business in any cross-organizations. The ECA pattern has been widely adopted for business rules[6]. It is an interest way to incorporate flexibility into a process design. The E-C-A paradigm has been the foundation for many rule-based processes modeling approaches. A survey of rule based approaches is given in [10].

To cope with flexibility, adaptability and temporal requirements of business process, we propose an ECA based formalism ECATE to govern business rules as follows:

ON	**E**vent
IF	**C**ondition
DO	**A**ction
TIME	Constraint of execution **T**ime
Trigger	Post **E**vent

Its semantics is: for each concern (C) when the event (E) occurs, the activated rule evaluates the condition(C). The condition is either a Boolean expression or a SQL query on the database. If the condition is satisfied, the action (A) is executed. The Time (T) is a condition on the execution time. It captures the constraints of time. This condition is of type “before t”, “after t”, “during t” or a combination of three types. before t means that the action A should be performed before the time t, “after t” means that the action A should be performed after the time t. “during t” means that the execution time of the action A should not exceed the time t. If the time constraint is violated then the process will be interrupted and a compensating action will be launched. The event triggered E design the set of events raised after the execution of the action.

2.2 Example

In order to give an intuitive idea about our formalism, let us consider the following scenario, inspired from [11]. Upon receipt of customer order, the calculation of the

initial price of the order and shipper selection is done simultaneously. When both tasks are complete, a purchase order is sent to the costumer. In case of acceptance, a bill is sent back to the customer. Finally, the bill is registered. A Functional constraint exists in this scenario: the bill payments must be made 15 days before the delivery date. The security constraints in this scenario are: 1) the client must be authenticated in the company system to control purchases. 2) The client must be authenticated in bank system to do banking. 3) If the amount of the bill exceeds some value m, the client must have an authorization between 08h00 and 19h00 to pay bill. The figure 1 shows the modeling of the functional concern of this example.

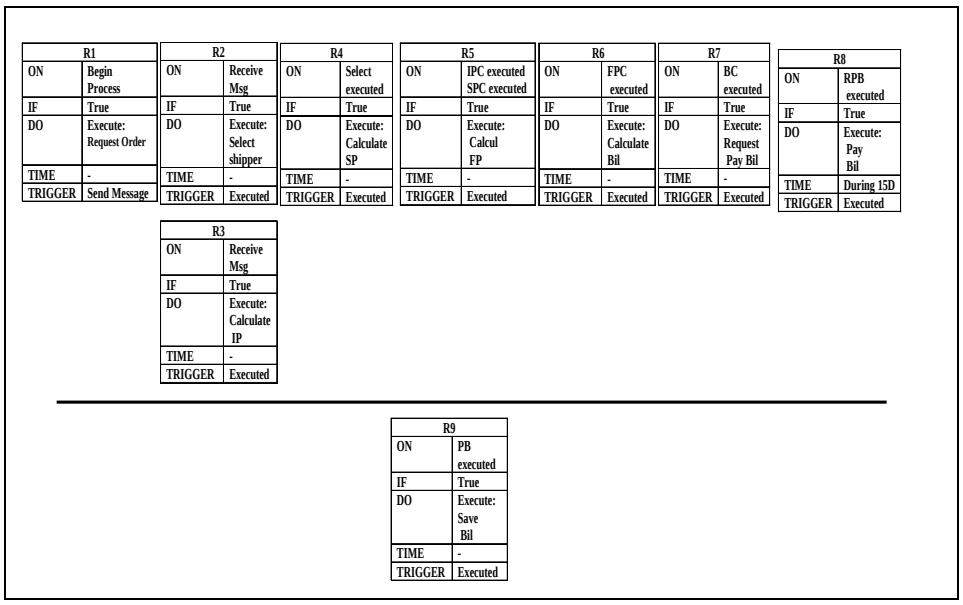

Fig. 1. ECATE rules based Business process

This model represents the business process of the purchase order process as set of ECATE Rules. So, The business rules are governed as ECATE rules. The event “begin process” activates the business process. It represents customer order (it may be, for example, clicking on the button "Place an order"). The two rules R2 (policy of initial price calculation), R3 (policy of shipper selection) have the same event to be activated. They represent two Parts of business process which will be executed in parallel. The constraint " the bill payments must be made 15 days before the delivery date " is specified in the time condition of the rule R8. The attribute time contains the value "during 15D" which means that if the execution of the action pay bill exceed 15 day after the activating event "request pay bill executed", so the order will be rejected, and a compensation action, to compensate the executed action part effects, will

Be launched. The successful execution of the rules R2 ,R3 actions will activate the rule R4. In turn, the execution of this rule action actives another rules. And so on, until the end of process rules set.
So, the business process of the purchase order, in this example, is governed in a flexible way as a set of ECATE rules. A flexibility way mean that we can implement changes in some rules (parts of a business process) without affecting the rest of rules (other parts).
But, this ECATE rule based model take only the functional concern of the process.

3 Flexible integration of security concern

Separation of concerns provides a way to separate development of the functionality and the crosscutting concerns (e.g., quality of service, security). This principle has become one of the cornerstone principle in software engineering, and has lead to a wide spread of aspect-oriented programming(AOP) approach [8]. The advantages in addressing each concern separately are transparency, evolution, understandability and scalability. More, it is necessary to bring them together to understand which global system properties emerge at any given activity [9]. Some scientific research efforts have interested to integrate the capture of security requirements in business process modeling. A survey of these works is given in [3]. But, they haven't used an ECA based formalism to capture the security requirement. Governing the business rules as ECA rules with separation of concerns have many benefits including[9] (1) the inherent ability of adapting any concern rules before imposing them on running services or components; (2) the promotion of understandability of each concern in isolation and then the study of the coherent composition.
In order to integrate the security concern flexibly into a business process design, and benefit of the advantages of separation of two concerns: functional and security in business process modeling, we use, in this section, EUCATE rule, which is a variant of ECATE, to govern the security requirement.
Our formalism EUCATE is defined as fellow:

ON	**E**vent
USER	Activity **U**ser
IF	**C**ondition
DO	**A**ction
TIME	Constraint of execution **T**ime
Trigger	Post **E**vent

It have the same semantic of ECATE. The added attribute user specifies the activity user. The figure 2 shows the integration of security requirements in the previous model, using EUCATE rule in separate concern.

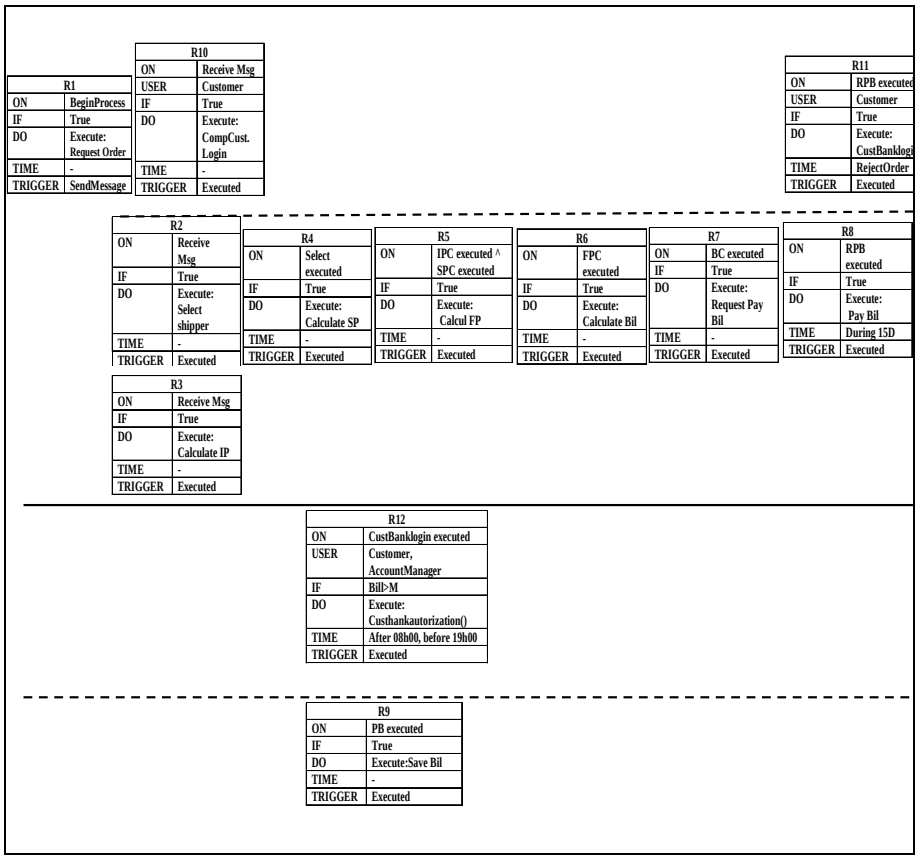

Fig. 2. Integration of security concern

The security requirements are modeled separately as set of EUCATE Rules. The separation of concerns promotes the understandability of each concern in isolation. For example, The rules R10, R11, R12 are of security concern that govern a security constraints. These rules may be modeled and handled by a security expert designer, independently of other concerns. The three rules R10 (policy of Company customer login) R2 (policy of initial price calculation), R3 (policy of shipper selection) have the same event to be activated. It is “begin process” event that represents customer order (it may be, for example, clicking on the button "Place an order"). However, they can't be activated at the same time, because they are of two different concerns. To avoid conflict between concerns, the security concern has more priority. In result, the rule R10 is activated before the rules R2 and R3. More, the rules R2 and R3 can not be activated if the R10 is not activated successfully. In other words, the condition and the time condition of R10 must be satisfied. If not, the order will be rejected. So, it will be

useless to activate the rules R2 and R3. In a positive case, R2 and R3 will be activated in the same time, because they are of the same concern. In turn, the execution of these rules actions actives another rules. And so on, until the end of process rules set.

So, the business process of the purchase order is governed now in a flexible way as a set of rules divided on two concerns: security concern and functional concern. A flexibility way mean that we can implement changes in some rules (parts of a business process) without affecting the rest of rules (other parts).

4 Verification of rules based process

It is important that a process model is correctly defined, analyzed, refined and verified before being deployed in the runtime environment[10].

The exceptions healing of the business process means that detecting the functional errors on the process and the risks on changing rules. These risks may be exceptions raised at run time like infinite loop and process non-termination, services deny.

The verify of functioning of the business process by analyzing the graph of rules based process is not scope of this paper . We are interested here by the formal verification of the rules based process. Our verification consists of two steps : the transformation of ECATE/EUCATE rules into a Petri net, and verification of such Petri net

The steps of such verification are summarized in the following diagram:

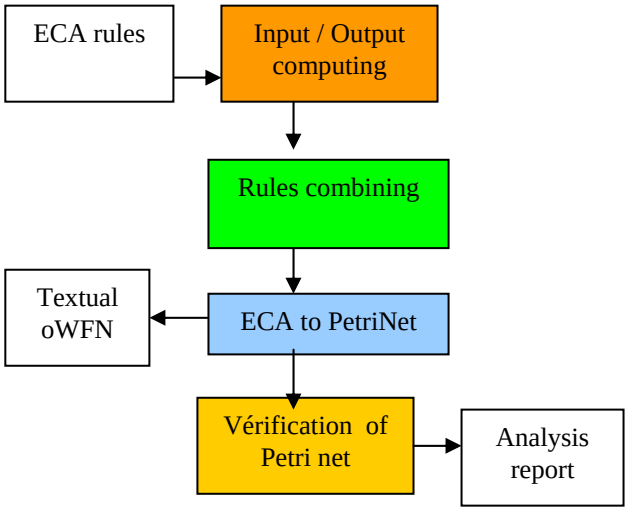

Fig. 3. Verification Environment

The oWFN (open WorkFlow) is a kind of Petri nets in order to verify the controllability property. The transformation of ECA rules to Petri Net allows to verify rules based business process and to exploit technical verification of Petri nets in the framework of business processes.

The transformation steps are as follows:

a. Structuring the used ECA rules
   In our case, the used rules must simples: the two sides must contain only one variable, in order to have reducing during the following steps. The complex rules can be represented by simple sub-rules.
b. Research inputs and outputs
   The input are variables with non beginning and not having predecessors,The outputs are variables non final and have no successors.
c. Combining rules
   This step consist to reduce simple rules number applying the following principles:
   Each left side of the rule must contain one input variable and one variable or one input and several variables.
   Each right side of the rule must contain one output and one variable or one output and several variables.
   A rule doesn't contain an input and output in the same time. All the rules must respect the previous principles and are able te be combined.
d. Rules from ECA to Petri Net
   Each rule becomes transition. The event and action becomes places.
e. Verification of Petri net
   We verify the properties of Deadlock, Live lock, Boundness and controllability on the produced Petri net using tools of Petri net verification as Lola[12] and Fiona[13]. The detail of the verification is not given in this paper.

5 Related work

The authors in [6] believe that it is important to couple WS-BPEL with a model for expressing authorization policies and constraints, and a mechanism to enforce them. They see that it is important that such an authorization model be high-level and expressed in terms of entities that are relevant from the organizational perspective. They propose an extension of WS-BPEL syntax with an authorization model that also supports the specification of a large number of different types of constraints. But, BPEL is not flexible.

[14] propose a flexible access control policies through the use of three classes of restraint rules in active cooperation: authorization rules, assignment rules and activation rules. A restraint rule consists of prerequisite conditions and a consequence. Each condition is in form of one or more weighted atomic conditions combined through logic operation connectors.

To enable a dynamic business process management, the authorization policies in [15] are expressed in an SQL-like language which can be rewritten into query sentences for execution. The framework proposed supports dynamic integration and execution of multiple access control polices from disparate enterprise resources.

In order to support the authorization policy development, [16] introduce a simple and readable authorization rules language implemented in a Ruby on Rails [17] authorization plug-in that is employed in workflow application. Ruby on Rails is a Web development framework that supports agile development and draws from the metaprogramming features of the programming language Ruby.

Authors in [18] propose active role-based access control model to assign permissions to users in real time and automatically. They combine the role-based access control model with the active database. They exploit the characteristics of the active database to assign roles to users based on the event trigger, user and environmental conditions, and to assign permissions to roles using the RBAC model.

6 Conclusions and future work

In this paper, we present a flexible integration of security concern in a rules based business process modeling. We are proposed a new ECA based rules to govern the functional and security business rules in multi-concerns view. The approach is thoroughly illustrated using an order purchase example.

How to manage this flexibility? What are the relationships between the rules of different concerns? How to recognize and heal the functional exceptions in rules based process? How to verify this rules based business process? Some answers for these questions will be subjects of future works.

7 REFERENCES

1. Jakoubi S., Tjoa S., Goluch G., Quirchmayr G., A Survey of Scientific Approaches Considering the Integration of Security and Risk Aspects into Business Process Management, in DEXA '09 Proceedings of the 20th International Workshop on Database and Expert Systems Application, IEEE Computer Society Washington, DC, USA ©2009.
2. Rodríguez A., Fernández-Medina E., Piattini M., Towards a UML 2.0 Extension for the Modeling of Security Requirements in Business Processes, In: Proceedings of Trust and Privacy in Digital Business (TrustBus 2006), Springer, 2006
3. Papazoglou M.P., Traverso P., Dustdar S., and Leymann F, Service-Oriented Computing: a Research Roadmap. Int. J. Cooperativ Inf. Syst., 17(2):223–255, 2008
4. Bertino E., Crampton J., Paci F., Access Control and Authorization Constraints for WS-BPEL, icws, pp.275-284, IEEE International Conference on Web Services (ICWS'06),2006.
5. Business Rules Group. Defining Business Rules - What Are They Really? www.businessrulesgroup.org, 2005.
6. Wan-Kadir W.M.N. and Loucopoulos P., Relating Evolving Business Rules to Software Design. Journal of Systems Architecture, 2003.

7. Ahn G.-J., Sandhu, R., Kang M., and Park J., , Injecting RBAC to secure a web-based workflow system. In Proceedings of the 5th ACM Workshop on Role-Based Access Control, pages 1–10, 2000.
8. Kazhamiakin R., Benbernou S., Baresi L., Plebani P., Uhlig M. and Barai O., Adaptation of Service-Based Systems Service Research Challenges and Solutions for the Future Internet, Lecture Notes in Computer Science, Springer-Verlag, 2010.
9. Aoumeur N., Barkaoui K., Saake G., , A multi-dimensional architectural approach to behavior-intensive adaptive pervasive applications, in ISWPC'09 Proceedings of the 4th international conference on Wireless pervasive computing, IEEE Press Piscataway, NJ, USA. 2009.
10. Ruopeng L., Sadiq S., a Survey of Comparative Business Process Modeling Approaches, in BIS'07 Proceedings of the 10th international conference on Business information systems Springer-Verlag Berlin, Heidelberg ©2007.
11. Boukhebouze M., Amghar Y., Benharkat A., Maamar Z., Rule-based Approach to Model and Verify Flexible Business Processes,International Journal of Business Process Integration and Management: IJBPIM, 2011.
12. Massuthe P., Weinberg D., Fiona: A Tool to Analyze Interacting Open Nets. AWPN 2008: 99-104
13. Schmidt K, LoLA: A Low Level Analyser, Application and Theory of Petri Nets 2000: 21st International Conference, ICATPN 2000, Aarhus, Denmark, June 2000. Proceedings, volume 1825 of Lecture Notes in Computer Science, pages 465–474, June 2000. Springer-Verlag
14. Yuqing Sun , Bin Gong , Xiangxu Meng , Zongkai Lin , Bertino E., , Specification and enforcement of flexible security policy for active cooperation, Information Sciences: an International Journal, July , v.179 n.15, p.2629-2642,2009.
15. Cao J., Chen J., Zhao H., Minglu Li, A policy-based authorization model for workflow-enabled dynamic process management, Journal of Network and Computer Applications, March, v.32 n.2, p.412-422, 2009.
16. Bartsch S., Sohr K., Bormann C., , Supporting Agile Development of Authorization Rules for SME Applications, Collaborative Computing: Networking, Applications and Worksharing, 4th International Conference, CollaborateCom November 13-16, Orlando, FL, USA, 2008.
17. Ruby on rails, website: http://rubyonrails.org/
18. Mei-Yu Wu, Chih-Kun Ke, Jung-Shin Liu, "Active Role-based Access Control Model with Event-Condition-Action Rule and Case-Based Reasoning", JCIT: Journal of Convergence Information Technology, Vol. 6, No. 4, pp. 328 - 339, 2011