2007

Rope: A Methodology for Enabling the Risk-Aware Modelling and Simulation of Business Processes

Stefan Jakoubi
Secure Business Austria, sjakoubi@securityresearch.at

Simon Tjoa
Secure Business Austria, stjoa@securityresearch.at

Gerald Quirchmayr
University of Vienna, gerald.quirchmayr@univie.ac.at

ROPE: A METHODOLOGY FOR ENABLING THE RISK-AWARE MODELLING AND SIMULATION OF BUSINESS PROCESSES

Jakoubi, Stefan, Secure Business Austria, Favoritenstraße 16, 1040 Vienna, Austria, sjakoubi@securityresearch.at

Tjoa, Simon, Secure Business Austria, Favoritenstraße 16, 1040 Vienna, Austria, stjoa@securityresearch.at

Quirchmayr, Gerald, University of Vienna, Department of Distributed and Multimedia Systems, Liebiggasse 4/3-1, 1010 Vienna, Austria, gerald.quirchmayr@univie.ac.at
University of South Australia, School of Computer and Information Science, Mawson Lakes Campus, Mawson Lakes SA 5095, Australia, gerald.quirchmayr@unisa.edu.au

Abstract

Risk management is essential regarding the maintenance of a company's business processes. The ability of companies to prevent risks as well as to respond quickly and appropriately to emerging threats is increasingly becoming a crucial success factor. In order to cope with these challenges, companies constitute business process and risk management approaches. Traditional business process management focuses on the economical optimization of processes. Apart from that, risk management provides the design of robust business processes to strengthen the resilience of daily business. Both domains aim at improving business performance, but they approach this goal from a different view on the understanding of improvement. Due to the fact that optimizing recommendations of business process management and risk management may be contradictory, we propose one unified method which integrates both points of views to enable risk-aware business process management and optimization. In this paper, we introduce the ROPE (Risk-Oriented Process Evaluation) methodology which combines capabilities of business process management, risk management and business continuity management to support the holistic evaluation of business processes not only regarding their economic efficiency but also their robustness and security. The basis for this combination is the refinement of business process activities into four atomic elements (Conditions, Actions, Resources and Environments) and a process-oriented way of modeling threats, preventive and reactive counter measures as well as recovery measures. In this paper we demonstrate how risk-aware business process management and simulation can be enabled through the application of the ROPE methodology.

Keywords: risk management, risk-aware business process modeling, risk-aware business process management, risk-aware business process simulation, secure business processes, threat modeling

1 INTRODUCTION

Companies face the challenges to perform their business processes efficiently in economic terms as well as to guarantee their continuous operation at the same time. Traditional business process optimization concentrates on the economic improvement of day-to-day business, especially on the reduction of financial overheads whereas risk management and business continuity management focus on the resilience of daily business. (Alberts et al. 2001, CERT OCTAVE 2005, BCI NaCTSO London First 2003)

It is undeniable that companies highly depend on the efficient and moreover continuous operation of their critical business processes. (Bank of Japan 2003a, Bank of Japan 2003b) Wide-practised and accepted concepts and methods exist in the field of business process management (Karagiannis et al. 1996, BOC 1996-2004, Scheer et al. 1992) on the one hand and in the domains of risk and business continuity management on the other hand (Alberts et al. 2001, BCI 2005, BSI 2004, CERT OCTAVE 2005, ISO/IEC 17799:2005). Though, it was a challenging research task to find a concept that combines the capabilities of the business process, risk management and business continuity worlds in a holistic way. We are convinced that exactly this combination, or more specific the integrated and process-oriented management of risks within business processes, enables a risk-aware business process optimization. This integration allows the optimization of efficiency and security of business processes at the same time.

In this paper we present the ROPE (Risk-Oriented Process Evaluation) methodology, which has been developed at the University of Vienna (Jakoubi 2006, Tjoa 2006). Our method delivers a consistent combination of business process modelling, risk management and business continuity concepts. Thus, we firstly present why we identified a need for our methodology. Secondly, we describe how ROPE supports the integrated and process-oriented management of risks within business processes. Thirdly, we show how ROPE provides the simulation of business processes in a risk-aware sound manner.

1.1 Related Work

Several approaches and studies exist in the research area of process security improvement and risk management linked to business processes.

The first methodology to mention is POSeM (Process Oriented Security Model), developed at the University of Zürich by Susanne Röhring. (Röhring 2003) The aim of this methodology is to provide "… a set of working methods to analyse and derive appropriate security measures." (Röhring 2003) POSeM follows a five-step approach. Firstly, it determines general security objectives of business processes. In a second step these objectives are refined to a security enhanced process model via the description language SEPL (Security Enhanced Process Language). Within the next step the consistency of the SEPL specification is checked by a rule base using the SCRL (Security Consistency Rule Language). Hereafter a list of security measures is derived in the fourth step. The derivation rules are defined in a second rule base and can be configured via the SMDL (Security Measures Description Language). Outcomes of the fourth phase are measures on a generic and abstract level. To generate system specific measures systems information are added in the fifth step. This methodology aims at securing business processes by calculating and deriving which measures can be taken to secure a business process.

Both, POSeM and ROPE aim at securing business processes. The main difference between the POSeM approach and the ROPE methodology is their totally different intent. While POSeM aims on the rule-based suggestion of security measure implementations, ROPE provides a simulation-based determination of the impact of threats and counter measures on business process executions.

The second approach known in the literature is the extension of the UML language called UMLsec by Jan Jürjens (Jürjens 2002) which was developed at the University of Munich. The UMLsec enriches the UML language with security extensions that enable a security evaluation of UML diagrams. Although the concepts of our methodology and UMLsec are different, basic similarities can be found: both approaches try to enrich a modelling language to take security issues into account.

Relevant work which has influenced ROPE originates from the fields of risk and business continuity management (Alberts et al. 2001, Brühwiler 2003, BSI 2004, BCI 2005, Department of Defense 1980, Wallmüller 2004).

2 THE ROPE METHODOLOGY

The ROPE (Risk-Oriented Process Evaluation) methodology aims at securing business processes by incorporating risk and business continuity management as an integral part. ROPE combines the advantages of business process modelling, risk management and business continuity concepts. Business process modelling enables the optimization of a company's processes regarding financial and workflow aspects. However, the management of risks is considered in-depth separately. Whereas concepts of risk management and business continuity provide effectively the management of risks in a holistic way, they hardly support the *simulation of risks* in a business process-oriented manner. With our approach we "fill the gap" between these concepts in order to enable risk-aware business process modelling and simulation.

The ROPE methodology consists of five iterative processes, which are derived from the BPMS business process modelling paradigm (Karagiannis et al. 1996, BOC 1996-2004), enriched with risk-oriented aspects. In the following we give a brief overview of essential information of these processes, especially on ROPE-specific extensions, but concentrate on the Re-Engineering process where we introduce our developed concepts, which enable risk-aware business process modelling and simulations.

2.1 The Strategic Decision Process

The establishment of a risk-aware process evaluation always has to be initially triggered by the support and backing of the (senior) management. (Alberts et al. 2001, BCI NaCTSO London First 2003)

In this phase senior management defines and prioritizes all business processes that are crucial for the performance of the company. We propose the application of a rating system, which classifies the relevance of business processes (i.e. low, medium, high and critical) in order to determine adequate prioritizations. This classification forces management to carefully reflect on the company's business process landscape. Management must be fully aware of the company's most important business processes to ensure that further analysis will be considered accurately.

It is also during this process that the financial and temporal scope of establishing ROPE needs to be defined. Furthermore, a team has to be assigned which is responsible for the implementation of the ROPE Process.

It is essential that management identifies critical success factors in order to evaluate results. The measurement against defined success factors enables a continuous improvement of securing the business processes.

2.2 The Re-Engineering Process

In this phase, the criteria obtained from the strategic decision process are used as a basis to develop a target model for the selected business processes. The re-engineering process consists of five stages

(selection, acquisition, analysis, design and evaluation criteria) derived from the BPMS paradigm (Karagiannis et al. 1996, BOC 1996-2004). The re-engineering process is a sequential process and can be iterated several times. Especially the evaluation sub-process can initiate a new iteration, the analysis and design sub-process use the results of the evaluation sub-process.

The aim of the *criteria selection stage* is to determine the main characteristics of securing the identified business processes. Therefore, the results of the Strategic Decision Process serve as input for defining understandable and measurable criteria which can be evaluated within the evaluation stage. The level of modelling granularity and the minimal functional level of an activity are two exemplary criteria.

The *acquisition stage* concentrates on business process activities. An activity is defined by Dubray (2002) as follows: "An activity represents a unit of work performed by a user, system or partner. An activity may have some input and output and some associated actions (pre and post activity)". In our approach, activities are refined into four atomic CARE elements: **C**onditions, **A**ctions, **R**esources and **E**nvironments. An activity consists of actions which are executed by resources within certain environments. The relation between Actions, Resources and Environments is expressed by Conditions.

As an activity consists of CARE elements, it directly depends on the level of functionality of its elements. In ROPE we therefore focus consequently on threats to CARE elements, especially how an occurred threat impacts an element. Due to that, existing threats and counter measures have to be identified within this stage. On the basis of this identification it is possible to design Threat Impact Processes (TIP). For each identified threat, a TIP diagram describes the behaviour of a threat and its specific counter measures in a process-oriented way.

The adequate identification of threats – especially within a dynamic business process environment – is an important task of the acquisition stage. Furthermore, it is essential to pay special attention to obtain precise occurrence probabilities of potential threats. Insufficient information causes the necessity to estimate these probabilities. Experts agree that this is difficult because of the unpredictable nature of risks and the potential lack of experience. As threats may occur in combinations, the relations between threats and their corresponding TIP have to be modelled. Thus, it is very important to consider interactions of threats, for instance when estimating the occurrence rate of related threats. Exemplarily, a DDoS (Distributed Denial of Service) attack is often followed by further attacks. Therefore, an occurred DDoS attack raises the occurrence rate of related threats.

Figure 1 of section 3 schematically shows the refinement of a business process as described above. A detailed discussion of diagrams and concepts which support the ROPE methodology follow in the chapter "The ROPE Diagrams".

The main goals of the *analysis phase* are the evaluation of existing preventive and reactive counter measures as well as the identification of new threats. Subsequent to this analysis, it is possible to determine the impact of threats on CARE elements. The results of this stage also enable the detection of weaknesses and vulnerabilities which can then serve as postulation of potential solutions.

Moreover, the refinement of business processes via the CARE and TIP concepts enables a risk-aware business process simulation. The simulation results deliver the basis for improving the security of the examined business processes. The ROPE simulation is described in-depth in section 4 "ROPE Simulation". Currently, we consider within the simulation only availability aspects, but we plan extensions in order to take confidentiality, integrity, reliability, accountability and authenticity into account as it is proposed in the Austrian Security Manual (BKA 2004).

The aim of the *design stage* is the development of a target model with respect to the results of the analysis phase. Weaknesses and opportunities analysed within the analysis process are considered to enable the development of the AS-IS-Model towards an improved target model.

This stage consists of the following steps:

- Modelling of new or changed CARE elements

- Modelling of new or changed threats and relations between threats
- Modelling of new or changed counter and recovery measures
- Assigning TIP to CARE elements in order to enable the risk-aware business process simulation

The *evaluation stage* determines whether the resulting target model matches the success criteria identified in the criteria selection stage. Iterations back to the analysis stage as well as to the design stage are possible.

2.3 The Resource Allocation, Workflow Management and Performance Evaluation Processes

The aim of the *resource allocation process* is the identification, assignment and coordination of resources to guarantee the risk-aware execution of the business processes. Therefore the target model of the ROPE Re-engineering process is used to derive requirements and additional resources to execute the business processes in the real environment.

Within the *workflow management process*, the modelled business processes are executed. Workflow management systems provide the adequate functionality to manage and administrate the business process execution.

The output of the execution serves as an essential input for the evaluation that is performed within the succeeding *performance evaluation process*. It carries out the qualitative and quantitative information evaluation of the executed risk-aware business processes. This information is used to achieve a continuous improvement of the business processes.

3 ROPE DIAGRAMS

In the following, we introduce two new diagram types which enable a risk-aware view on business processes: the CARE (Condition, Action, Resource and Environment) diagram and the TIP (Threat Impact Process) diagram. The CARE diagram offers the opportunity to refine business process activities. This refinement, which leads to element breakdown, is essential for all further risk-aware considerations via ROPE. The second diagram type (TIP diagram) is used to describe the effects of a specific threat and how counter and recovery measures operate. The refinement of business processes within the CARE and TIP diagrams as well as the interaction between the three modelling-layers allow a risk-aware process evaluation of business processes.

The ROPE Methodology consists of three modelling-layers:

- Business process modelling layer: Representation of the company's business processes – business process activities serve as linkage to the next modelling-level.
- CARE (Condition, Action, Resource and Environment) modelling layer: Identification of a business process activity's elements (Action, Resource and Environment) and their coherences (Condition).
- TIP (Threat Impact Process) modelling layer: Identification of potential threats as well as their management- and recovery strategy.

Looking at the modelling-layers from a user's viewpoint, the business process modelling layer is owned by a business analyst while the CARE and TIP layers are rather scope of security and risk analysts which need an organizational and technical understanding.

Figure 1 provides a schematic overview of the three modelling layers which are described in more detail within the following chapters. A business process activity (BP Layer) is refined via a CARE diagram (CARE Layer) into its atomic elements Conditions, Actions, Resources and Environments. A CARE element which itself faces certain threats, is protected by adequate preventive and reactive counter measures as well as restored to its former condition by recovery measures. This aspect is modelled via TIP diagrams (TIP Layer).

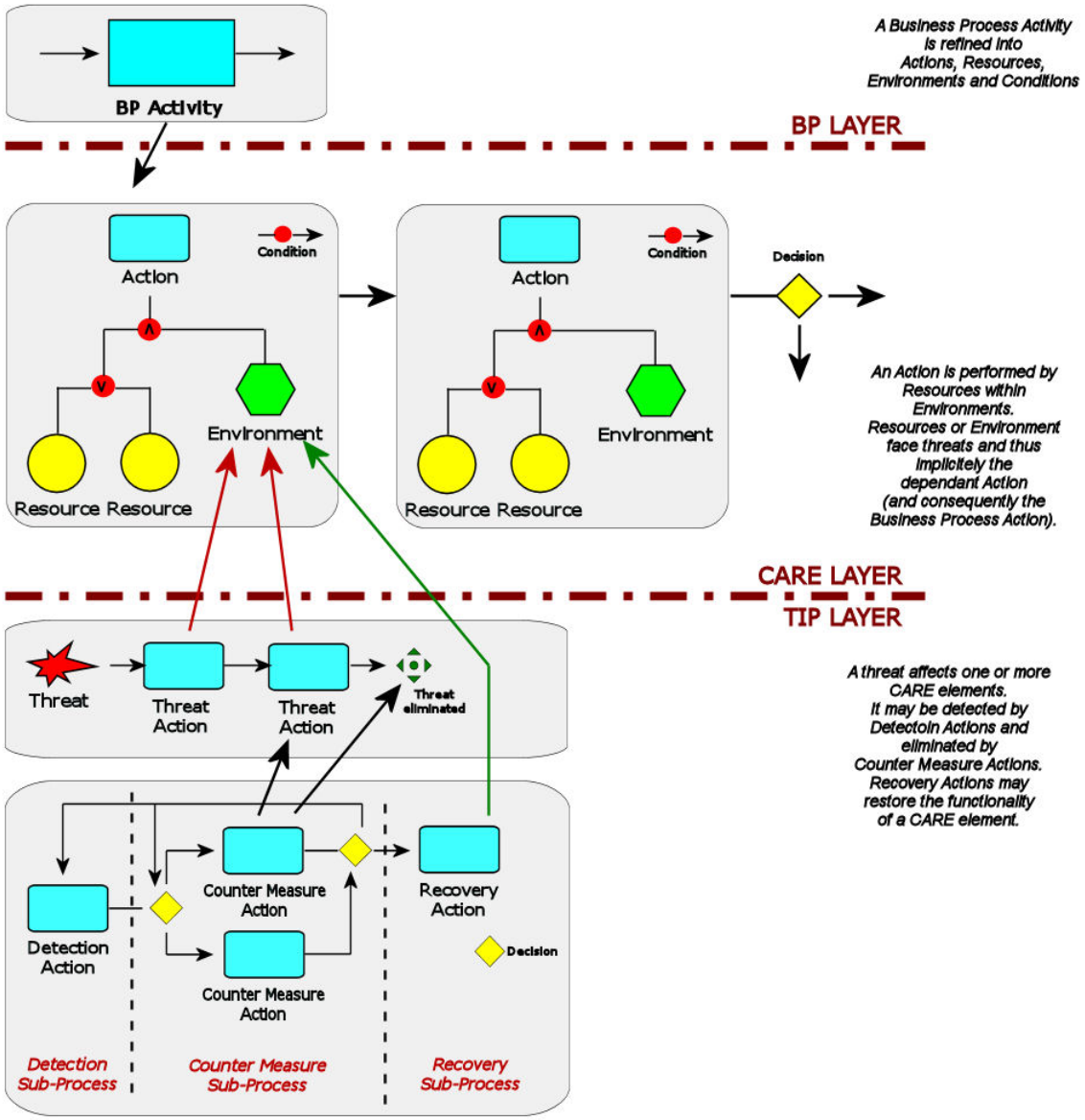

Fig 1 The three layers of ROPE

3.1 CARE Diagram

The CARE (Condition, Action, Resource and Environment) diagram is used to refine business process activities based on the ROPE concept as briefly introduced in the previous chapter. An activity consists of *Actions* which are executed by *Resources* within specific *Environments*. Within the CARE diagram, constraints and relationships between Actions, Resources and Environments are modelled as Conditions. The relations between CARE elements are expressed by edges which describe the path of the dependability between elements.

The concept of the CARE Condition is a key element of the CARE diagram. It outlines the dependencies between the CARE elements Action, Resource and Environment. Due to the fact that CARE elements are temporarily dependent on each other, delays that are caused by the unavailability of one or more elements have as aconsequence to be added to the execution time.

It is possible to link CARE elements via logical operators to enable complex connections. Figure 2 shows the use of the logical OR-operator to model redundancies within the ROPE refinement of the

example business process activity “processing an order”. The activity of this example is refined into the CARE Action “Process order”, the CARE Resources “PC 1” and “PC 2”, the CARE Environment “Office” and three CARE Conditions. The Conditions state that “Process order” depends on the Resource “PC 1” or on the Resource “PC 2” that are themselves dependent on the Environment “Office”. In this exemplarily case the CARE Action “Process order” could still be executed if one of the CARE Resources “PC 1” or “PC 2” fails.

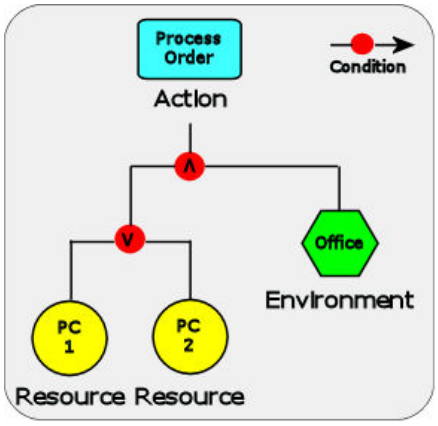

Fig 2 Example CARE Diagram

Based on the example above the following calculation of the execution time can be derived as follows:

$$T = T_{\text{Process order}} + \min \begin{pmatrix} T_{\text{delay PC1}} + T_{\text{delay Office}} \\ T_{\text{delay PC2}} + T_{\text{delay Office}} \end{pmatrix}$$

3.2 TIP Diagram

The TIP (Threat Impact Process) diagram describes the effects of threats and counter measures on CARE Elements. A preventive counter measure is an action which directly influences the incidence rate of a threat. By contrast a reactive counter measure counteracts already occurred threats.

The TIP diagram features three main application areas:

- Supporting the identification of potential risks
- Documentation and visualization of risks
- Determination of risk impacts via simulation

A TIP is considered as an iterative process which consists of detection, counter measures and recovery sub-processes.

- The detection sub-process: Within this sub-process the threat is detected. The impacts of a threat are strongly related to the detection time. The “when” and the “how” of the detection determines the invoked counter measures.
- The counter measures sub-process: Counter measures directly influence threats. If counter measures are not able to terminate the threat, the full impact of a threat affects the concerned CARE element.
- The recovery sub-process: The recovery sub-process provides processes to rebuild the functionality of an affected CARE element.

The sub-processes as well as the TIP itself may run through various iterations. Each sub-process runs at least through one iteration of the sequence assessment and reaction. The execution of the processes may cause state changes of threats or modifications of the functionality of CARE Elements.

The Detection Sub-Process

The detection of a threat is the basis for an adequate reaction. A crucial factor is the reaction time between the recognition of a threat and the invocation of counter measures. The longer the time period between recognition and invocation lasts, the higher the effect of the threat will be. In case of no detection the maximum impact might occur.

The detection sub-process is an iterative process and consists of the following stages:

- The assessment stage: Identification of threats as the basis for initiating a certain set of reactions. The type of detection determines the invoked counter measure.
- The counter measure invocation stage: Activates the selected counter measure sub-process.

Exemplarily, if a virus scanner is installed on a computer, it will detect an occurring virus (assessment), notify the user and start the removal process (counter measure invocation). A human being would probably detect a virus attack later and react in a different way. An automated system will likely react faster and be more effective.

The Counter Measure Sub-Process

The counter measure sub-process represents the activities of the particular reactive counter measures. As long as the threat exists there may be iterations within the counter measure sub-process as well as back to the detection sub-process. The exit conditions of this sub-process are at least:

- The threat is eliminated
- No further counter measure exists

The counter measure sub-process consists of the following stages:

- Assessment stage: The situation is rated regarding to the status of the threat and the degree of functionality of the affected CARE Element.
- Counter measure stage: Execution of threat-minimizing actions.
- Recovery invocation stage: Activates the recovery sub-process.

The Recovery Sub-Process

The primary target of the recovery sub-process is the restoration of a CARE element's functionality. This process is divided into short and long term recovery measures. Short term measures provide the minimal functionality of a CARE element. Long term measures are responsible for the establishment of the complete functionality of the CARE element.

The recovery sub-process consists of the following two stages:

- Assessment stage: Identification of the caused effects on an affected CARE element. Selection of the required recovery measures regarding the degree of functionality of the CARE element.
- Recovery stage: Execution of the selected short term as well as long term recovery actions.

4 ROPE SIMULATION

At the current state of research, ROPE supports two simulation approaches: Firstly, the path analysis of a TIP and secondly, the simulation of a threat's impact on the status of CARE elements.

The use of a *path analysis* during the simulation of a TIP enables the determination of the TIP's possible paths. Furthermore, the occurrence rate of each path and its elements can be identified. Due to these occurrence rates it is possible to determine the execution times and (caused) costs for each TIP.

The *simulation of a threat's impact* aims at the determination and visualization of the impact of threats and counter measures on the continuous execution of a business process. CARE elements, which represent a business process activity's components, face threats that decrease their functionality. The simulation of TIP enables the illustration of a threat's impact on CARE elements and their

functionality. Attention should be paid to the fact that the TIP and the occurred threat are parallel processes which influence each other mutually. The TIP tries both to eliminate the threat and to recover the status of the CARE element (positive impact) while the threat process impacts continuously the status of the CARE element negatively.

After the simulation, the following four states can occur:

- Threat eliminated & CARE status functional
- Threat eliminated & CARE status non-functional
- Threat not eliminated & CARE status non-functional
- Threat not eliminated & CARE status functional

The fourth state "threat not eliminated & CARE status functional" only occurs as a temporal state within the simulation because of our assumption that a threat always impacts the status of a CARE element.

Summarizing, the simulation of a threat's impact enables firstly the identification of an affected CARE element's status changes and secondly, the determination of additional times and costs that occur through the execution of those TIP that are assigned to the affected CARE element.

4.1 Proof of Concept Prototype

In order to gain results how the ROPE methodology could be applied in practise, especially its models and the simulation approach, we realized a proof of concept prototype.

Within the scope of the prototype, we implemented the ROPE simulation approach step-wise:

- Pre-simulation of CARE elements and their assigned TIP
- Simulation of CARE Elements
- Risk-aware simulation of the business process

Pre-Simulation of CARE Elements and their assigned TIP

The goal of the pre-simulation is the determination of the status-changes of all affected CARE elements and the points in time of these changes. The pre-simulation is carried out in three steps which are described in the following.

The *identification of affected CARE elements* results from the occurred threat. As one specific TIP is responsible for one specific threat, those CARE elements are selected which are connected to the threat's corresponding TIP.

The occurrence rate of a TIP determines the frequency of the TIP's incidence, respectively the frequency of the threat's incidence, within a certain time slice. A random generator appoints the *entry times of a TIP* within the time slice.

Within the prototype implementation, we use the concept of JAVA threads to simulate the concurrent exertion of influence of threats and counter measures on CARE Elements.

Figure 3 visualizes schematically the simulation's process of the status changes. The horizontal arrows show the timelines of the JAVA threads of the threats as well as the counter and recovery measures. A JAVA mutex object (mutual exclusion) is the synchronizing component which holds the status of the CARE element and the threat. The sloped arrows represent the positive or negative status-changes of the CARE element. The first vertical, dotted line flags the failure of the CARE Element, the second one the termination of the threat and the third one, the recovery of the minimal functionality of the CARE Element. The highlighted area between the first and the third dotted line indicates the time where the CARE element is down, i.e. its idle time.

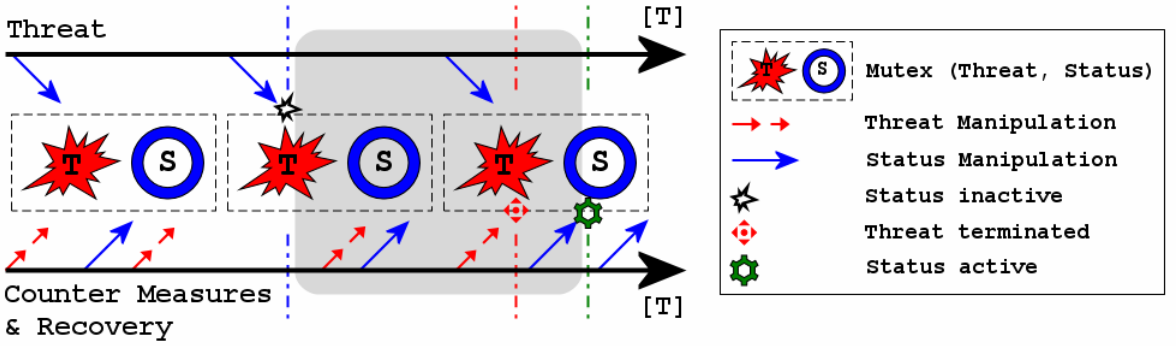

Fig 3 TIP simulation (Jakoubi 2006, Tjoa 2006)

Simulation of CARE Elements

The simulation of a CARE element's functionality is performed through the examination of its dependencies, which are represented by CARE Condition elements. If a CARE element A is dependent on the functionality of a CARE element B, then A fails if B fails. Consequently, the execution time of A and B is delayed until B is recovered.

Simulation of the Business Process

The simulation of the business process is performed within a defined time slice, which is determined by a specific start and end time. The possible paths during the simulation are determined at runtime. Business process activities are examined by the simulation of their CARE elements.

If the status of a CARE element decreases below the minimal level of functionality, the further execution of the current business process activity is delayed until the point in time, where the CARE element is recovered.

Figure 4 shows schematically this case. Within the first two process executions, the business process activities can perform without a delay. Within the third execution, activity B is interrupted by the occurred threat. Consequently, activity B can only be performed with a temporal shift and is suspended for its downtime.

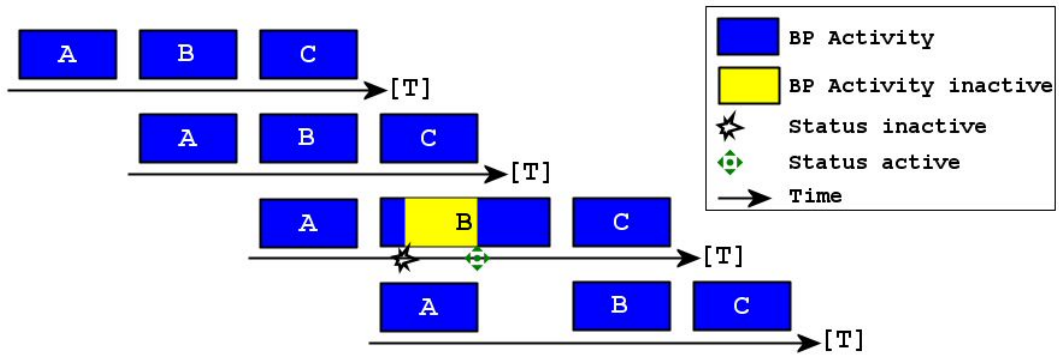

Fig 4 Risk-aware business process simulation (Jakoubi 2006, Tjoa 2006)

5 CONCLUSION

A shortcoming of traditional business process modelling is that risk and business continuity management are addressed separately although risks impact the continuous execution of business processes directly. The concept of ROPE (Risk-Oriented Business Process Evaluation) offers a practical approach for a new kind of risk-aware business process management which enables the

integral incorporation of risk and business continuity management. Through the combination of traditional business process modelling and the process-oriented management of risks, threats, counter and recovery measures ROPE provides the ability to outline the overall impact on the execution of business processes.

A proof of concept prototype substantiates our ROPE methodology and shows that the method's strength not only lies in the risk-aware simulation regarding the determination of economical damage and time loss, but also in the illustration of costs that are caused by security, counter and recovery measures.

6 FUTURE WORK

Within our future research, we plan to investigate succeeding topics in detail.

We intend to develop and model a *set of reference TIP* for the most common threats of a specific field of application. The feasibility of the set of reference TIP within one domain would be followed by our efforts to extend the set of TIP to various other fields.

Since currently we only consider availability aspects, we will concentrate our future research on the development of adequate extensions in order to integrate confidentiality, integrity, accountability, authenticity and reliability into the ROPE methodology. As a consequence, we need to define proper threat and counter measure classifications.

Our proof of concept prototype showed that the concepts offer high potentialities for the practical implementation of the ROPE methodology. *Integrating the ROPE methodology into professional business process management tools* is in progress and part of the future work.

Subsequently to the integration onto a professional tool, we plan a *feasibility study* and an *evaluation of the ROPE methodology* towards other approaches. Another important open issue is the adequate visualization of simulation results.

A well-known problem, not only of ROPE, but also of nearly every single methodology in the field of risk management, is the *estimation of occurrence rates of threats*. In order to examine this exhaustive problem, we conduct further research concerning an information basis on threats.

7 REFERENCES

Alberts, C.J., Dorofee, A.J. (2001) "OCTAVE Method Implementation Guideline Version 2.0 - Volume 1: Introduction", CERT/CC - Software Engineering Institute Carnegie Mellon

Bank of Japan (2003a) Business Continuity Planning at Financial Institutions, July

Bank of Japan (2003b) Business Continuity Planning at the Bank of Japan, September

BCI, NaCTSO, London First (2003) Expecting the unexpected – Business continuity in an uncertain world.

BCI (2005) Good practice Guidelines, 2005. URL http://www.thebci.org, Accessed October 2005

BKA (Federal Chancellery Austria)(2004) Österreichisches IT-Sicherheits Handbuch. URL http://www.cio.gv.at/securenetworks/sihb, Accessed December 2006

BOC (1996-2004) The BPMS®-Paradigm, URL http://www.boc-eu.com/bochp.jsp?file=WP_582571cc1ed802de.b05236.f598e2482c.-7f48, Accessed 25 May 2006

Brühwiler, B. (2003) Risk Management als Führungsaufgabe – Methoden und Prozesse der Riskobewältigung für Unternehmen, Organisationen, Produkte und Projekte. Haupt Verlag, Bern, Stuttgart, Wien

BSI (Federal Office for Information Security) (2004) IT-Grundschutz Manual, 2004. URL http://www.bsi.de/english/gshb/manual/download/index.html, Accessed May 2006

CERT OCTAVE (2005) URL http://www.cert.org/octave, Accessed October 2005

Department of Defense (1980) MIL-STD-1629 A Military standard – Procedures for performing a failure mode effects and critically analysis.
Dubray, J., J. (2002) A Novel Approach for Modeling Business Process Definitions, URL http://www.ebpml.org/ebpml2.2.doc, Accessed 23 March 2006
ISO/IEC 17799:2005 Information technology -- Security techniques -- Code of practice for information security management, URL http://www.iso.org
Jakoubi, S. (2006) A Methodology for the Visualisation of Risks in Business Processes as an Enabler for a Holistic Documentation and Risk Evaluation by means of Simulation for Software Projects (in German), Thesis, University of Vienna
Jürjens, J. (2002). UMLsec: Extending UML for Secure Systems Development. UML 2002, Dresden, Sept. 30 - Oct. 4, 2002, LNCS, Springer-Verlag, URL http://www4.in.tum.de/~umlsec/
Karagiannis, D., Junginger, S., Strobl, R. (1996) Introduction to Business Process Management Systems Concepts, Appeared in: Scholz-Reiter, Bernd; Stickel, Eberhard (Eds.): Business Process Modelling. Springer, Berlin et al. 1996. pp. 81-106
Röhrig, S. (2003) Using Process Models to Analyse IT Security Requirements. PhD Thesis, University of Zurich, URL http://www.ifi.unizh.ch/archive/diss/Jahr_2003/index_diss_2003.html#Susanne
Scheer, A. W., Keller, G., Nüttgens, M. (1992) Semantische Prozeßmodellierung auf der Grundlage "Ereignisgesteuerter Prozeßketten (EPK)", in: Scheer, A. W. (Eds.): Veröffentlichungen des Instituts für Wirtschaftsinformatik, Heft 89, Saarbrücken 1992, URL http://www.iwi.uni-sb.de/nuettgens/Veroef/Artikel/heft089/heft089.pdf
Tjoa, S. (2006) A Methodology for the Enhancement of Business Process Modelling by means of Process-oriented Modelling, Evaluation, and Simulation of IT-Infrastructure (in German), Thesis, University of Vienna
Wallmüller, E. (2004) Risikomanagement für IT- und Software-Projekte. Carl Hanser Verlag, München Wien

8 ACKNOWLEDGEMENT

This work was performed at the Research Center Secure Business Austria funded by the Federal Ministry of Economics and Labor of the Republic of Austria (BMWA) and the federal province of Vienna.