2008

Deriving Resource Requirements Applying Risk-Aware Business Process Modeling and Simulation

Stefan Jakoubi
Secure Business Austria, sjakoubi@securityresearch.at

Gernot Goluch
Secure Business Austria, ggoluch@securityresearch.at

Simon Tjoa
Secure Business Austria, stjoa@securityresearch.at

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

DERIVING RESOURCE REQUIREMENTS APPLYING RISK-AWARE BUSINESS PROCESS MODELING AND SIMULATION

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

Goluch, Gernot, Secure Business Austria, Favoritenstrasse 16, 1040 Vienna, Austria, ggoluch@securityresearch.at

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

Quirchmayr, Gerald, University of Vienna, Faculty of Computer Science, Liebiggasse 4, 1010 Vienna, Austria, gerald.quirchmayr@univie.ac.at

Abstract

Today, companies face the challenge to effectively and efficiently perform their business processes as well as to guarantee their continuous operation. To meet the economic requirements, companies often consult business process management experts. The robustness and continuity of operations is separately considered in other domains such as business continuity management and risk management. The shortcoming of this separation is that in most cases a common reasoning and information basis is missing. With the risk-aware process modeling and simulation methodology named ROPE we fill this gap and combine the strengths of the aforementioned domains. In this paper, we present new ROPE simulation capabilities focusing on the determination of resource requirements considering the impact of occurring threats on business processes. Furthermore, we introduce an example scenario to clarify how a company can benefit from applying these extensions.

Keywords: risk aware business process modeling and simulation, capacity planning, business process management.

1 INTRODUCTION

In today's global economy, where conditions change often and rapidly, the efficiency and effectiveness of the execution of business processes has become a central issue. As these processes depend on the assigned resources a considerable optimization focus lies on the minimization of the resources' costs and simultaneously on the maximization of their returns. The optimization of business processes is the key objective of the business process management domain. Especially through business process modeling and simulation techniques an exhaustive analysis of a company's processes can be performed leading to an economic business process optimization.

Another critical factor, which influences the ability to compete, is the continuous operation of a company's business processes. The reasons why the execution of business processes may be interrupted are manifold and addressed by several domains, e.g. business continuity management, risk management, disaster recovery or incident handling. "It is very difficult to isolate all the disciplines related to planning for and recovering from an incident which threatens an organisation either from an internal or external source. All the disciplines are closely related and there are areas of cross-over…" (ENISA 2008). Although the individual domain's focuses, approaches and techniques may vary, their common overall objective is to reduce the likelihood and to mitigate the effects of events that may threaten a company's survivability.

All abovementioned domains are essential within a company and are a prerequisite to efficiently and effectively perform business operations and strengthen the company's resilience against potential threats. Nevertheless, those domains are often not applied in an integrated way, but rather treated as separate operational fields and addressed in separate projects. Thus, in many cases a common information and reasoning basis is missing, leading to a quite different understanding of advancing the company's potentials. This is why recommendations resulting from business process management and security domains such as business continuity management analysis may considerably differ. Exemplarily, the need for and benefits of backup facilities (e.g. a redundant electronic data processing center) may be divergently valuated.

There are widely accepted and practiced concepts and standards regarding the business continuity management (BSI 2006; BCI 2008; DRI/DRJ 2007; NFPA 2007; NIST 2002b), the risk management (Alberts et al. 2001; BSI 2007; NIST 2002a) as well as the business process management domains (BOC 2008; Karagiannis et al. 1996; Scheer et al. 1992). Nevertheless, a concept is missing to comprehensively combine these domains. We are convinced that this combination allows a risk-aware business process analysis enabling the optimization of efficiency, robustness and security of business processes at the same time.

Therefore, we have introduced our ROPE (Risk-Oriented Process Evaluation) methodology (Jakoubi et al. 2007), which enables the consideration of risks in business process modeling and simulation. The core concept of this approach is the process-oriented modeling of threats, counter and recovery measures. Threats endanger the operability of resources, which are essential for the continuous execution of a company's business processes. Counter measure and recovery measure processes try to eliminate a threat and re-establish the functionality of disrupted resources. This process-oriented modeling of threats, counter as well as recovery measures and the interconnection to resources enables the risk-aware business process modeling and simulation. Within the course of this paper we focus on a centralized view on a company's resources in order to enable the analysis of resource requirements across the boundaries of separately applied business process management, business continuity management or risk management projects.

This paper is structured as follows: Methods and techniques that influenced the development of our method are described in chapter 2 "underlying and related approaches". In chapter 3 "ROPE – A Methodology Enabling Risk-Aware Business Process Modeling and Simulation" we summarize our developed methodology in order to support further discussions. In chapter 4 "Deriving Resource

Requirements Applying ROPE" we present the major contribution of this paper, which is the extension of the ROPE simulation capabilities in order to derive resource requirements for business processes considering economic and security aspects. This resource requirements simulation comprises a *resource utilization simulation* and an *extended path simulation*. The resource utilization simulation concentrates on the utilization of resources during an incident. The extended path simulation highlights the effects of a resource shift on business processes, which is caused by counter measure activities. An example scenario outlines the potentials and benefits of applying the aforementioned modeling and simulation capabilities of ROPE. In chapter 5 "Conclusion" we close the paper outlining our research results.

2 UNDERLYING AND RELATED APPROACHES

At the beginning of this section we briefly introduce underlying approaches. However, for more detailed information we kindly refer the reader to the denoted references. Subsequently, we point out and describe several approaches that exist in the research area of process security improvement and risk management linked to business processes.

The British Standard BS25999 (BSI 2006) defines business continuity management as "holistic management process that identifies potential threats to an organization and the impacts to business operations that those threats, if realized, might cause, and which provides a framework for building organizational resilience with the capability for an effective response that safeguards the interests of its key stakeholders, reputation, brand an value-creating activities." The Good Practice Guidelines of the Business Continuity Institute (BCI 2008) provide an overview and guidance on the business continuity management lifecycle as recommended by the British Standards BS25999 and other best practices.

The National Institute of Standards and Technology (NIST) defines risk and risk management as follows: "Risk is the net negative impact of the exercise of a vulnerability, considering both the probability and the impact of occurrence. Risk management is the process of identifying risk, assessing risk, and taking steps to reduce risk to an acceptable level." (NIST 2002a)

Within this paper we understand an incident as "situation that might be, or could lead to, a business disruption, loss, emergency or crisis" (BSI 2006); an threat as "potential cause of an unwanted incident, which may result in harm to individuals, a system or organization, the environment or the community" and risk as "combination of the probability of an event and its consequences" (ISO 2007). For further definitions of frequently used terms, we kindly refer the reader to abovementioned literature.

The aim of the POSeM (Process Oriented Security Model) methodology developed at the University of Zürich by Susanne Röhring (Röhrig 2003) is to secure business processes by calculating and deriving abstract and system specific measures. POSeM follows a five-step approach, where general security objectives of business processes are determined and further refined to a security enhanced process model via the description language SEPL (Security Enhanced Process Language). Furthermore a list of security measures is derived by derivation rules, which are defined in a second rule base and can be configured via the SMDL (Security Measures Description Language). Finally system specific measures are generated.

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.

Zur Muehlen and Rosemann (Zur Muehlen et al. 2005) identified risk as an inherent property of every business process. To counteract the trend of considering risk mainly from a project management perspective they addressed the topic of risk management in the context of business process management. Therefore a taxonomy of process related risks is presented and its possible appliances in the analysis and documentation of business processes are discussed. A taxonomy for business

processes is also introduced, including five clusters (goals, structure, information technology, data and organization) and two distinguished lifecycles (build-time and run-time), enabling the classification of both errors and risk. Furthermore four interrelated model types are presented to capture risk in the context of business processes: (1) Risk Structure model, providing insights into the relationship between risks. (2) Risk Goal model, depicted by a risk/goal matrix. (3) Risk State model, capturing the dynamic aspects of risk and consisting of the object types risk, consequence and connectors (XOR and AND). (4) EPCs (Event-driven Process Chain) extended with risks, enabling the assignment of risks to individual steps in the process.

Both, the described approach and the ROPE methodology aim at modeling risks in the context of business processes. The main difference is that ROPE connects risks and corresponding threats to resources utilized within process activities, while the methodology of zur Muehlen and Rosemann directly links risks to process activities. By using a more granular modeling technique we, on the one hand aim at providing more detailed simulation input, but on the other hand are aware of the additional modeling work, which has to be done to acquire the needed information concerning resources and their relation to process activities.

(Neiger et al. 2006) also address the need for a holistic business view on risk management in the enterprise systems space. Furthermore they present a framework by applying value-focused process engineering principles to risk management models, which enables risk-oriented process management, incorporating a multi-disciplinary view of risk. The presented framework introduces four steps to achieve this integration: Firstly business values and objectives are decomposed to identify relevant process risks, while each business activity is examined in order to identify further relevant risks. Secondly value-focused approaches are used to identify specific risks and to determine the processes and corresponding functions which contribute to these risks. In the following process configurations are proposed to identify the best process structure that meets the business objectives. The comparison of alternative configurations and their corresponding results finally enable the choice of the optimal process configuration that meets the identified risk minimization objectives, with regards to overall business requirements.

This value focused process engineering approach enables more risk-aware process configuration related decisions by introducing a decision model. The ROPE methodology currently does not include a specific decision model but focuses on simulation output, concerning threats regarding resources and related process risks.

An interesting approach to detect existing process anomalies and to check process conformance is the work of van der Aalst and de Medeiros (Van der Aalst et al. 2005), which advocates the use of process mining techniques to analyze audit trails for security violations. By using a specific algorithm security efforts at various levels (from low-level intrusion detection to high-level fraud prevention) are supported. Even though the presented approach differs methodically from our method, similarities in the goal of analyzing processes regarding weaknesses can be found.

Regarding the visualization of our ROPE simulation approach, the work of (Hao et al. 2006) is of high interest. They introduce a new visualization technique, called VisImpact, which turns raw operational business data into valuable information. By analyzing operational data and abstracting the most critical factors influencing business operations, VisImpact is able to reduce data complexity. This impact factors are represented by nodes in a symmetric circular graph and therefore provide insight into core business operations and relationships. Furthermore the method has already been applied to real-world applications, such as fraud analysis.

3 ROPE – A METHODOLOGY ENABLING RISK-AWARE BUSINESS PROCESS MODELING AND SIMULATION

In this section, we briefly introduce our ROPE (Risk-Oriented Process Evaluation) methodology to establish the basis for further discussions. More detailed information on our previous work, especially

on the method, our developed proof of concept prototype and application scenarios is provided in (Goluch et al. 2008; Jakoubi et al. 2007; Tjoa et al. 2008a; Tjoa et al. 2008b).

Our approach consists of five iterative processes, which are basically derived from (BOC 2008; Karagiannis et al. 1996) and extended according (Jakoubi et al. 2007). The *Strategic Decision Process*: Identification and prioritization of the business processes to be analyzed and definition of measurable success factors in order to provide an adequate basis for evaluation of the results. The *Re-Engineering Process*: This process consists of five iterative sub-processes. An AS-IS model is transformed into an improved target model. Furthermore, we apply our modeling concepts within these sub-processes in order to enable the risk-aware modeling and simulation of the business processes. The *Resource Allocation Process*: Identification, assignment and coordination of resources required for the business process execution. The *Workflow Management Process*: Execution of the business processes within a workflow environment. The *Performance Evaluation Process*: Evaluation of the performance of the executed business processes in order to identify on the one hand, if the defined success criteria are met, and on the other hand to continuously improve the processes.

We want to mention that within our concept we do not propose any specific information acquisition technique. We recommend consulting industry-specific standards and best practices in order to be compliant with commonly applied or required approaches.

In the following, we describe those core concepts of our methodology which are essential for further discussions: "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." (Jakoubi et al. 2007) A TIP consists of the succeeding sub-processes. The *Detection sub-process*: Modeling of actions which concern the detection and analysis of the related threat. Depending on the kind and point in time of the detection, the appropriate counter measure sub-process is invoked. The *Counter measure sub-process*: Modeling of actions regarding the counteracting of the threat. The *Recovery sub-process*: Modeling of actions in order to recover the functionality of the CARE element which is affected by the occurred threat.

Figure 1 schematically shows the three modeling layers and the risk-aware business process simulation interactions. The interaction between the three layers enables the risk-aware business process simulation. In the *business process layer* the modeling of the company's business processes is performed. For our approach, the granularity of a business process activity is not appropriate (Jakoubi et al. 2007). Thus, in the *CARE layer* we refine business process activities into actions which are executed by resources within certain environments. Furthermore, relations exist between those elements which represent dependencies between each other. For our proof of concept purposes, we applied the notation for the modeling of (business) processes by ADONIS (BOC 2008) (BP and TIP layer). Regarding the representation of the CARE layer we used a graph representation in order to adequately visualize the interdependencies of CARE elements.

Each realization of a threat is modeled as a TIP and threatens CARE elements. During the risk-aware business process simulation, threat actions decrease the functionality of linked CARE elements until the elements are non-operational and / or the threat is eliminated. Counter measure actions try to eliminate the threat. If the threat cannot be eliminated, a recovery of an affected CARE element is impossible. Otherwise, recovery actions restore the functionality of an affected element.

Regarding the CARE layer, we are aware of the fact that existing tools and techniques also provide resource modeling capabilities. However, the reason why we introduce our own concept is that we require the information regarding the dependencies between resources realized through the logical "OR" and "AND" operators between the CARE elements.

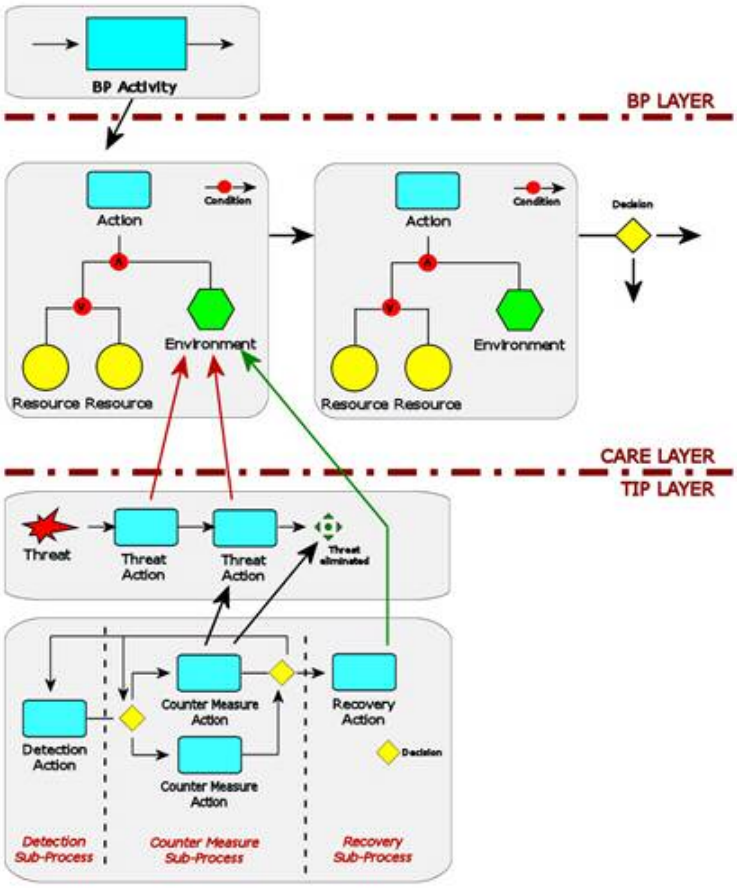

Figure 1: The three layers of the ROPE methodology (Jakoubi et al. 2007)

In order to substantiate our developed ROPE modeling and simulation capabilities we have realized a proof of concept prototype. Within the prototype, the simulation approach consists of two steps. Firstly, the simulation of occurred threats (i.e. the simulation of the affected TIP processes) determines the points in time when CARE elements are not operational. Secondly, the simulation of the business processes is performed considering delays or downtimes of their activities caused by potential non-operational states of the activities' (CARE) elements. Figure 2 shows the scenario, if a business process is executed several times. Two times, the business process performs without interruption while within the third iteration business process activity B is delayed as a consequence of an occurred threat and the resulting suspension for the duration of its downtime. Accordingly, this delay affects the succeeding iterations of the business process. The main benefits of the methodology result from the risk-aware simulation regarding the determination of economic damage and time loss as well as from the illustration of costs that can be caused by security, counter and recovery measures.

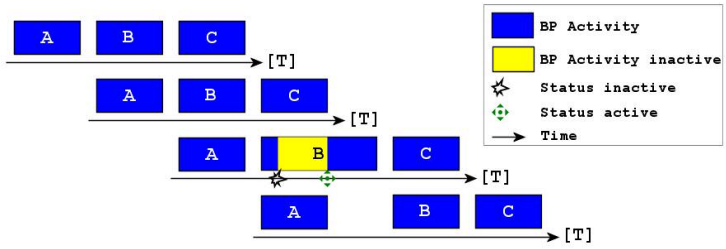

Figure 2 Risk-Aware Business Process Simulation (Jakoubi et al. 2007)

Through the process-oriented representation and linking of business process activities, resources, threats and security measures, we support the business process, business continuity and risk management domains as follows:

- A holistic concept considering the objectives of the abovementioned domains leads to synergy effects, e.g. the usage of the same information basis
- The structured representation of processes (TIP) can be used as emergency procedures during incidents
- Performing of simulation based analysis enables the determination of impacts on business processes and resources caused by threats
- Identification of costs caused by threats and safeguards
- Decision support regarding the selection of counter and recovery measures

4 DERIVING RESOURCE REQUIREMENTS APPLYING ROPE

In this chapter, we introduce our extensions of the ROPE simulation to provide resource requirements analysis capabilities. According to (Jakoubi et al. 2007), the ROPE simulation is based on the path simulation. Summarizing, the ROPE path simulation considers occurring threats (i.e. the simulation of the according TIP processes) and subsequently performs the business processes simulation considering delays or downtimes of their activities caused by non-operational states of the activities' (CARE) elements. This ROPE simulation provides information about the economic damage and time loss as well as the illustration of costs that can be caused by the execution of counter and recovery measures. Furthermore, the simulation shows the impacts caused by an occurred threat on CARE elements and as a consequence on business processes.

The ROPE path simulation provides valuable information about the occurrence rate of all possible (simulation) paths. Nevertheless, the path analysis has some shortcomings when it comes to resource considerations: (1) it does not highlight how the resource utilization changes during an incident scenario. (2) It does not determine the impact of resources' re-allocation on business processes (e.g. backlogs). (3) It is not possible to retrieve the resource requirements needed to minimize the impact of a threat. (4) It does not indicate which resources are needed to eliminate potential backlogs caused by the disruption of a business process. (5) The current ROPE path simulation only considers resources' availability of business processes, but ignores resource requirements of threat impact processes.

As resources are crucial to perform a company's activities, we identified the need to not only consider resources, which are required to execute business process activities, but also those, which are ad-hoc required while counteracting a threat to the continuous operation of business process activities. Furthermore, we believe that it is also absolutely essential to analyze potential re-allocations of resources that support the counteracting of threats in order to enhance preliminary resource planning.

In order to overcome the abovementioned shortcomings we introduce the integration of a resource requirements simulation into ROPE. The resource requirement analysis of ROPE, which bases on the additional resource requirements simulation capabilities, performs the following simulation steps:

- Simulation of selected threat scenarios (i.e. simulation of the according TIP) focusing on resource utilization aspects. The results of this simulation outline the overload of resources caused by additional tasks for performing a TIP.
- Simulation of selected threat scenarios (i.e. simulation of the according TIP) focusing on the impacts of a resource's re-allocation from a business process to a TIP. The results of this simulation outline the additionally required resources to perform a TIP without disrupting a business process through the re-allocation of resources.

We present the succeeding example scenario as basis for further discussions. The key business process of the travel agency "ROPE travel" is dealing with customer booking orders. The agency's internal booking system depends on a single server providing essential services for the employees. A second ongoing business process of the agency is the first level support, which is performed by the agency's incident manager.

The travel agency plans to analyze the high prioritized booking order business process, especially the impacts of a potential non-availability of the single server. Following the ROPE methodology, a business analyst initially models the business processes and their required resources (CARE diagrams). In a second step, a security analyst performs a risk assessment on the agency's current situation. The identified threats, counter and recovery measures are modeled within according TIP diagrams and assigned to the corresponding endangered resources. The initial establishment of all required TIP diagrams is quite time-consuming. Thus, we plan to develop a TIP template pool on the basis of (BSI 2004), which can be customized to the company's needs.

Figure 3 schematically shows this example scenario focusing on a virus threat, which endangers the server. In the figure, we only depict the relevant actions and resources in order to ensure an adequate clarity of the example. Thus, we outline the three typical actions of the business process (BP) "booking order". The action "query information systems" requires the resources "server" and "travel agent" to be appropriately performed. The business process "first level support" also consists of three actions. The action "handle support request" requires the resources "incident manager" and "ticketing system" to be adequately executed.

The TIP "virus" comprises threat actions that negatively affect the resources, which are assigned to the TIP (within the example this is the server). Furthermore, the TIP shows the counter measure actions "eliminate virus" and "determine virus source" as well as the recovery action "re-integrate resource". The counter measure actions try to eliminate the virus and the recovery action tries to re-establish the functionality of the affected server. Moreover, the TIP counter and recovery actions require the resource "incident manager", which is primarily needed by the action "handle support request" of the business process "first level support".

For more information about our example TIP virus and its graphical representation we kindly refer to the ROPE homepage[1]. This representation bases on the IT-Grundschutz Manual[2], more precisely on the "Procedures in the event of computer virus infection". (BSI 2004)

Applying the ROPE path simulation capabilities, the following information is derived: (1) Given that the threat virus affects the CARE element server before it has been detected, we determine the points in time when the server enters a non-operational state. After counter measure actions have been able to eliminate the threat, recovery measures try to re-establish the functionality of the server. This enables the risk-aware business process simulation of ROPE considering downtimes of CARE elements (see also figure 1). (2) The additional costs of performing TIP actions are determined. For a more concise description of the ROPE path simulation capabilities and benefits (e.g. cost/benefit decision support for alternative risk treatment strategies), we refer the reader to (Jakoubi et al. 2007; Tjoa et al. 2008a).

[1] http://rope.securityresearch.at
[2] Formerly known as IT-Baseline Protection Manual of the German Federal Office for Information Security

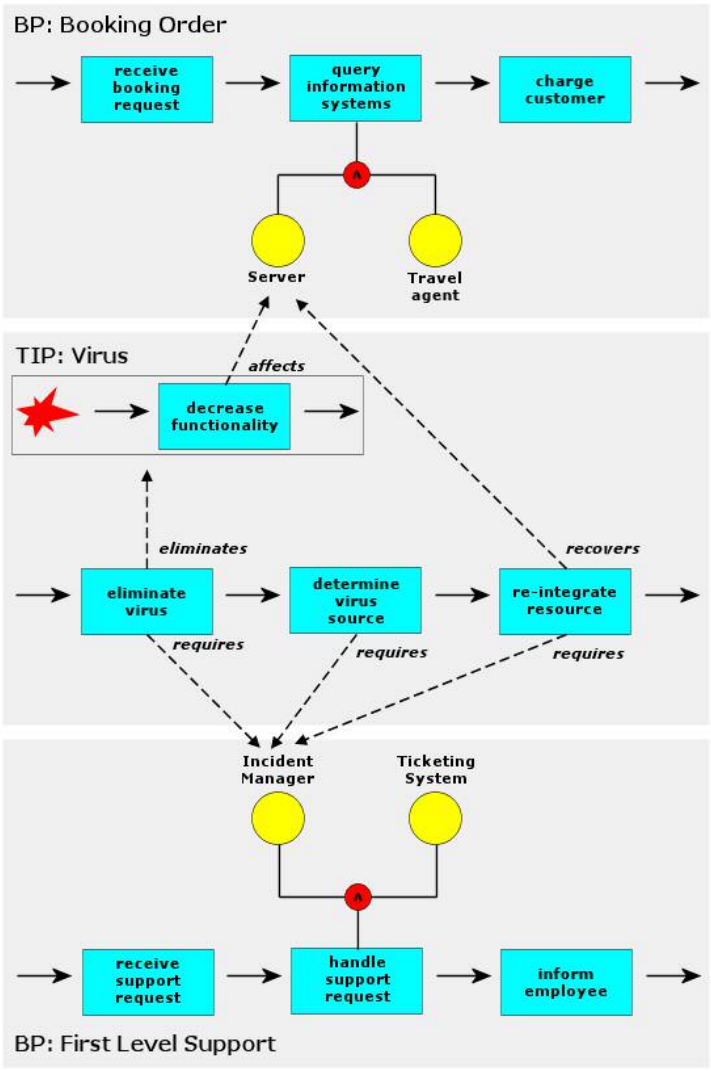

Figure 3: The travel agency scenario

In the following, we introduce our extensions of the ROPE simulation in order to enable resource requirement analysis. The extensions comprise two simulation procedures: (1) the *resource utilization simulation*, which analyses the working capacity of a resource (e.g. the resource is working 60 percent over its planned capacity); (2) the *extended path simulation*, which shows the impacts, if a resource is re-allocated from business processes to threat impact processes under the assumption that the resource's working capacity must not exceed 100 percent.

4.1 Resource Utilization Simulation

The *resource utilization simulation* comprises the succeeding steps in case that a TIP has been invoked to counteract an occurred threat.

- Determine if all resources required for performing the TIP are operational.
- As long as a required resource is operational its working capacity is increased for the additional workload caused by executing assigned TIP actions. Thus, a resource's working capacity exceeding 100 percent is possible.

To follow up the example scenario of "ROPE travel", we assume that the travel agency optimized their resource allocation. Consequently, all resources operate at full capacity (i.e. 100 percent) within

their business processes. Through the simulation of the threat scenario virus, it is possible to determine the resource requirements during a virus incident. In our example, the incident manager would not only be working to full capacity within its business process but is also needed for executing the TIP actions "eliminate virus", "determine virus source" and "re-integrate resource". As a consequence, his working capacity will exceed 100 percent. Information resulting from this simulation serves as valuable input for resource / capacity management decisions. As a consequence, the responsible decision maker has to decide, if this overloaded resource is acceptable (e.g. if the occurrence rate of the threat virus is negligible) or if additional resources have to be allocated for performing the TIP (e.g. contract with other companies or additional employees).

Figure 4 shows example result of resource utilization simulation. The incident manager is working over its full capacity between 10 and 14 o'clock (140 percent). Within this time frame he has been additionally required by the TIP for counteracting the virus and recovering the server.

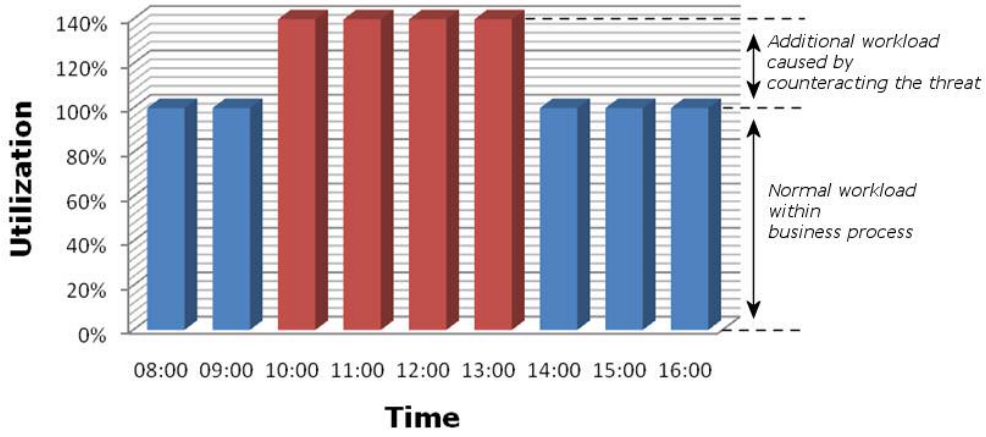

Figure 4: Simulation results presented in a bar chart. The chart indicates that the observed resource is overloaded over a period of four hours (10:00 – 14:00)

The main result of the resource utilization analysis is the determination of resources' workload capabilities (in percent), if threats endanger the continuous execution of business processes. Thus, the results serve as essential input for identifying bottlenecks and provide decision makers valuable information for capacity planning. However, the resource utilization analysis does not consider the circumstance that in practice certain tasks cannot be simultaneously performed. It exclusively focuses on the resource's working capacity to guarantee the continuous execution of the threatened business processes. The incident manager cannot simultaneously handle a support request and eliminate the virus. Nevertheless it is essential to know the required amount (percentage) of additional resources to avoid the incident manager's overloading.

4.2 Extended Path Simulation

In contrast, the *extended path simulation* considers the maximum working capacities of a resource and shows the impacts, which are caused through the resource's re-allocation from business processes to TIP. Thus, it comprises the following simulation steps:

- Determine if all resources required for performing the TIP are operational.
- Re-allocate the resource to execute counter measure and recovery measure actions of the TIP. As a consequence, this resource is not available to execute its tasks of its "origin" business process.
- Determine the impacts of the re-allocation, e.g. increased amount in backlogs or waiting times of resources that are not able to work to normal capacity.

In our example, the capacity manager wants to identify the impact, if the incident manager would be re-allocated for performing TIP actions. The capacity manger is especially interested in the amount in backlogs resulting from the sudden unavailability of the incident manager for the first level support business process. Furthermore, he is highly interested in the consequences of this business process disruption on the working capacities of further human resources of this process (e.g. costs caused by the waiting time of succeeding resources). Thus, in comparison to the resource utilization simulation, the status of the resource incident manager is set non-operational within the first level support business process in order to perform TIP actions to guarantee the operability of the booking order business process. As a consequence, backlogs emerge (and increase) at the interrupted business process action. Moreover, all resources that are allocated after this action are underemployed, if they are not re-allocated.

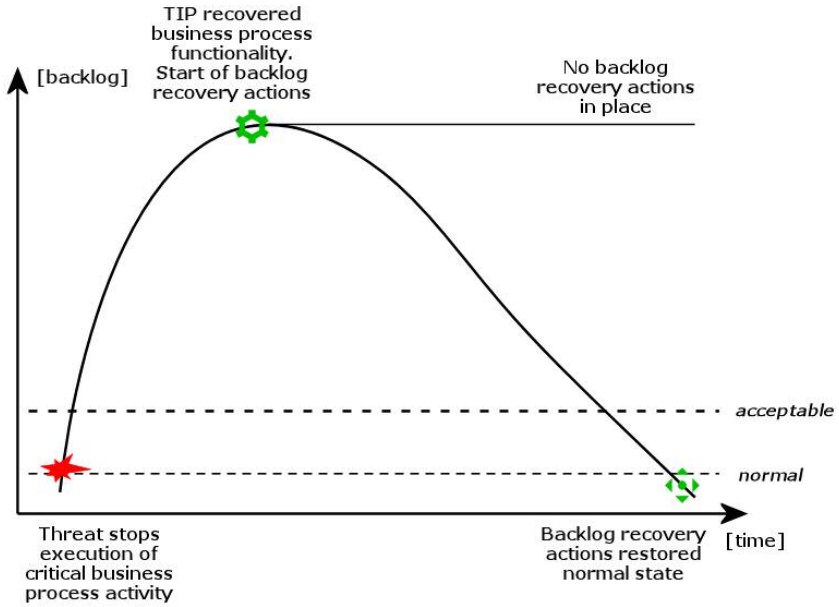

Figure 5: Graphical representation of a backlog incorporating interfaces to ROPE

Figure 5 shows an example backlog curve. Before the virus occurs, the backlogs of the first level support business process are within their normal range. After the threat has caused the disruption of the single server (and thus the critical "query information systems" action), the backlogs significantly increase until the TIP has been able to eliminate the virus and recovered the required server. If there would be actions in place to eliminate potential backlogs, the normal amount in backlogs would be reached with additional temporal and financial expenses.

The main result of the extended path simulation is the determination of the impacts of a resource re-allocation on the originally assigned business process. The outcome of the simulation delivers valuable information about resulting amounts in backlogs, losses caused by the disruption of the business process and by the underemployment of further resources.

Summarizing, we identify the following benefits of applying the extended ROPE simulation capabilities:

- Simulation-based determination of resources working capacities (in percent) in case of re-allocation between processes, for example a resource is required for 100 percent by its dependent business process and simultaneously for 40 percent by a threat impact process. Thus, its theoretically required working capacity is 140 percent.
- Simulation-based determination of the changing resource utilization during threat scenarios, for example the re-allocation of personnel from a business process in order to counteract an occurred threat affecting the operability of another (e.g. higher prioritized) business process.

- Simulation-based determination of additional costs, which are caused by this changing resource utilization. For instance, personnel have to be re-allocated to guarantee the operability of a higher prioritized business process. As a consequence, the execution of the lower prioritized business process is disrupted leading to resources not working to full capacity.
- Simulation-based determination of resource requirements to minimize the impact of an occurred threat considering the shortage of resources resulting from downtimes of resources or insufficient resource capacities.
- Simulation-based identification of essential resources, which would cause severe backlogs of their dependent processes in case of re-allocations.
- Simulation-based determination of additional resource requirements to eliminate backlogs caused by occurred threats.

5 CONCLUSION

In this paper, we have presented extensions of our ROPE simulation capabilities enabling a simulation-based determination of resource requirements considering the impact of occurred threats on business processes. These extensions comprise the incorporation of (1) a *resource utilization simulation*, which analysis the working capacity of resources in case of an occurred threat and (2) an *extended path simulation*, which analyses the impacts, if resources are re-allocated from business processes to threat impact processes (TIP). Summarizing, we identify the following main benefits of extending the ROPE simulation capabilities:

- Simulation-based workload capacity analysis of resources in case of occurred threats (overload of resources and impact of a resources' re-allocation).
- Simulation-based determination of resource requirements and resulting additional costs to minimize the impacts of a resource re-allocation (e.g. minimizing backlogs and resources' idle times).
- Simulation-based cost / benefit analysis of resource allocation alternatives enabling the selection of the most appropriate allocation to guarantee the continuous operation of business processes while simultaneously minimizing negative "side-effects".

We are convinced that the strong integration of threat considerations in the business process management domain can become a competitive advantage for companies. In our opinion the shared knowledge of business continuity, risk and business process management enhances the determination of resource requirements, which are needed to perform a company's business processes. Furthermore, this contributes in providing a common information and reasoning basis within the entire company. With ROPE we propose a methodology, which meets the objective to combine the strength of these domains.

References

Alberts, C. J. and Dorofee, A. J. (2001) OCTAVE Method Implementation Guideline Version 2.0.

BOC (2008) Business Process Management Systems (BPMS) Paradigm, http://www.boc-eu.com/jumpto.jsp?goto=BPMS&lg=en, Accessed March 2008.

British Standards Institution (BSI) (2006) BS 25999 – Business Continuity Management.

Business Continuity Institute (BCI) (2008) Good Practice Guidelines 2008.

Distaster Recovery Institute / Disaster Recovery Journal (DRI/DRJ) (2007) Generally Accepted Business Continuity Practises.

European Network and Information Security Agency (ENISA) (2008) Business and IT Continuity: Overview and Implementation Principles.

German Federal Office for Information Security (BSI) (2004) IT-Grundschutz Manual (english version).
German Federal Office for Information Security (BSI) (2007) BSI Standards 100-x (english version).
Goluch, G., Ekelhart, A., Fenz, S., Jakoubi, S., Tjoa, S. and Mück, T. (2008) Integration of an Ontological Information Security Concept in Risk Aware Business Process Management, HICSS 2008 IEEE, January.
Hao, M. C., Keim, D. A., Dayal, U. and Schneidewind, J. (2006) Business Process Impact Visualization and Anomaly Detection, Information Visualization, Volume 5, Issue 1.
International Standards Organization (ISO) (2007) ISO/PAS 22399 – Societal security – Guideline for incident preparedness and operational continuity management.
Jakoubi, S., Tjoa, S. and Quirchmayr, G. (2007) ROPE: A Methodology for Enabling the Risk-Aware Modelling and Simulation of Business Processes, ECIS 2007.
Karagiannis, D., Junginger, S. and Strobl, R. (1996) Business Process Modelling, (Eds, Scholz, R., Bernd, Stickel and Eberhard) Springer, Berlin, pp. 81-106.
National Fire Protection Association (NFPA) (2007) NFPA 1600:2007 - Standard on Disaster/Emergency Management and Business Continuity Programs.
Neiger, D., Churilov, L., zur Muehlen, M. and Rosemann, M. (2006) Integrating Risks in Business Process Models with Value Focused Process Engineering, ECIS 2006.
National Institute of Standards and Technology (NIST) (2002a) NIST SP800-30: Risk Management Guide for Information Technology Systems.
National Institute of Standards and Technology (NIST) (2002b) NIST SP800-34: Contingency Planning Guide for Information Technology Systems.
National Institute of Standards and Technology (NIST) (2004) NIST SP800-61: Computer Security Incident Handling Guide.
National Institute of Standards and Technology (NIST) (2005) NIST SP800-83: A Guide to Malware Incident Prevention and Handling.
Röhrig, S. (2003) Using Process Models to Analyse IT Security Requirements, University of Zurich.
Scheer, A. W., Keller, G. and Nüttgens, M. (1992) Semantische Prozeßmodellierung auf der Grundlage Ereignisgesteuerter Prozeßketten (EPK), Veröffentlichungen des Instituts für Wirtschaftsinformatik, Heft 89, Saarbrücken.
Tjoa, S., Jakoubi, S., Goluch, G. and Quirchmayr, G. (2008a) Extension of a Methodology for Risk-Aware Business Process Modeling and Simulation Enabling Process-Oriented Incident Handling Support, Advanced Information Networking and Applications (AINA).
Tjoa, S., Jakoubi, S. and Quirchmayr, G. (2008b) Enhancing Business Impact Analysis and Risk Assessment applying a Risk-Aware Business Process Modeling and Simulation Methodology, International Conference on Availability, Reliability and Security (ARES).
Van der Aalst, W. M. P. and de Medeiros, A. K. A. (2005) Process Mining and Security: Detecting Anomalous Process Executions and Checking Process Conformance, International Workshop on Security Issues with Petri Nets and Other Computational Models (WISP).
Zur Muehlen, M. and Rosemann, M. (2005) Integrating Risks in Business Process Models, Australiasian Conference on Information Systems (ACIS) 2005, Sydney, Australia.