Business Impact Analysis and Risk Assessment

Abstract

Driven by the steadily growing number of natural disasters, the threat of terrorist and other criminal attacks as well as changed legislation and regulations, companies are increasingly forced to prepare against threats that endanger the survivability of crucial business activities. As a consequence, management has to pay more attention to business continuity issues including serious management commitment and more appropriate funding. Business impact analysis and risk assessment concepts enable adequate business continuity planning as they deliver essential information about the impact of resources' disruption on business. In this paper we present how these concepts can be enhanced through the application of the ROPE (Risk-Oriented Process Evaluation) methodology enabling risk-aware business process management and simulation. Moreover, we present essential extensions of the ROPE simulation capabilities leading to a more efficient and effective business continuity planning.

Keywords: risk-aware business process simulation, business continuity planning, business impact analysis, risk assessment

1. Introduction

According to [1] "... 80% of businesses affected by a major incident close within 18 month. 90% of businesses that loose data from a disaster are forced to shut down within two years. 58% of UK organizations were disrupted by September 11th. One in eight was seriously affected." Business continuity management and business process management are essential domains within a company and are a prerequisite to efficiently and effectively perform business operations and strengthen the company's resilience against potential threats. [2, 3, 4] Those domains are often not applied in an integrated way, but rather treated as separate operational fields. 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 business continuity management analysis may considerably differ. There are widely accepted and practiced concepts and standards regarding the business continuity management [5, 6, 7, 8, 9, 10] as well as the business process management domains [11, 12, 13]. Nevertheless, a concept is missing to comprehensively combine the advantages of both 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. In order to overcome existing shortcoming, we introduced the ROPE (Risk-Oriented Process Evaluation) methodology [14], which combines the advantages of both domains leading to risk-aware business process modeling and simulation. A core concept of this approach is the process-oriented modeling of threats, counter and recovery measures, which is described in detail within the chapter "Risk-Aware Business Process Modeling and Simulation". Based on this process-oriented modeling of counter and recovery measures we identify significant improvement opportunities regarding the support of business continuity management's business impact analysis and risk assessment.

In this paper, we present key business impact analysis and risk assessment approaches and our ROPE methodology, which enables risk-aware business process modeling and simulation. The major contribution of this paper is to show the application of the ROPE methodology providing significantly enhanced support within the fields of business impact analysis and risk assessment leading to the following benefits:

- Extended business process analysis capabilities through a process-oriented consideration of threats and countermeasures.
- Simulation-based identification of a company's critical

business processes and single points of failure.

- Simulation-based identification of the impact of resources' disruptions on business processes.
- Enhanced cost/benefit analysis regarding alternative business continuity strategies through the risk-aware business process simulation.
- Support regarding the prioritization of threats on business.

In the chapter "Improving Business Impact Analysis and Risk Assessment" we discuss in detail how the application of our ROPE approach leads to the aforementioned benefits.

2. Risk-Aware Business Process Modeling and Simulation

In this section, we describe the ROPE methodology for enabling the risk-aware business process modeling and simulation in order to establish the basis for further discussions on its incident handling extension. More detailed information on our previous work, especially on the method and our developed proof of concept prototype, is provided in [14, 15].

Our approach consists of five iterative processes, which are basically derived from [11, 12] and extended according to [14]. 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.

In the following, we describe those core concepts of our methodology which are essential for further discussions on the incident handling topic: "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 modeling-layers allows a risk-aware process evaluation of business processes." [14] 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. 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 [14]. 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. The formal representations (1) and (2) show the composition of an action element (c ... condition, a ... action, r ... resource, e ... environment). Within the *TIP layer*, the process-oriented modeling of threats, counter and recovery measures takes place.

$$a\{c_1...c_n\} \tag{1}$$

$$c\{r_1...r_n, e_1...e_n, c_1...c_n\} \tag{2}$$

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 impacted element.

Within our developed proof of concept 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 exe-

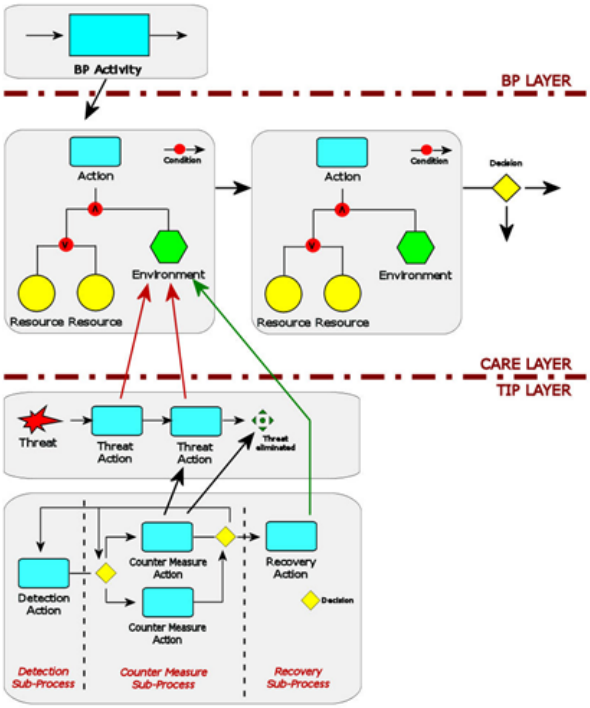

Figure 1. The three layers of ROPE [14]

cuted 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.

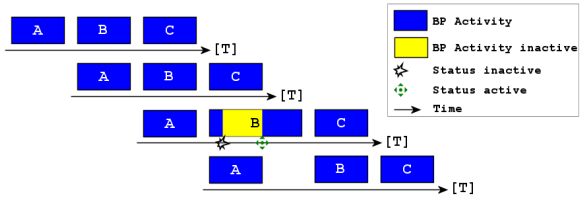

Figure 2. Risk-Aware Business Process Simulation [14]

3. Business Impact Analysis

In this chapter, we reflect approaches of standards and widely accepted good practice guidelines regarding the execution of a business impact analysis (BIA) enabling the discussion on how the ROPE methodology improves conducting a BIA. The British Standard BS25999 [6] defines a BIA as the "process of analysing business functions and the effect that a business disruption might have upon them". This definition is comparable with the definition of the National Fire Protection Agency NFPA1600 [16]: "This analysis measures the effect of resource loss and escalating losses over time in order to provide the entity with reliable data upon which to base decisions concerning hazard mitigation, recovery strategies, and continuity planning."

The *Good Practice Guidelines (GPG) 2007* of the Business Continuity Institute (BCI[1]) [8] are management guidelines for implementing BCM. The GPG approach follows the business continuity management lifecycle of the British standard BS25999 [6], which succeeded the public available specification PAS56 [17], and comprises the following phases: (1) Understanding the organization; (2) Determining BCM options; (3) Developing and implementing BCM response; (4) Exercising, maintaining and reviewing. The organizational implementation aspects are considered through the phases (5) BCM programme management and "embedding BCM in the organization's culture". As BIA is addressed in Understanding the organization we outline the according steps and refer the reader to [6, 8] for detailed information on the other phases. According the GPG, [8] the BIA "...identifies, quantifies and qualifies the business impacts of a loss, interruption or disruption of business processes on an organisation and provides the data from which appropriate continuity strategies can be determined."

The most important BIA process steps are: (1) Identify business activities and their management owners; (2) Identify appropriate staff to best-possible gather information; (3) Identify scenarios leading to severe impacts on the company's reputation, assets or financial position; (4) Identify the time-frame within which disruptions of business activities are unacceptable. Depending on the analyzed company, miscellaneous information gathering techniques such as workshops, questionnaires and interviews can be applied. The two main deliverables of the BIA for each business activity are the maximum tolerable period of disruption (MTPD) and the recovery point objectives (RPO). The MTPD determines the time-frame within a company's survivability is irrevocably threatened by the disruption of certain business activities. The RPO defines the point in time until essential information has to be restored after the business activity has been successfully recovered.

[1] http://www.thebci.org, accessed September 2007

The *special publication SP800-34* of the National Institute of Standards and Technology (NIST[2]) [10] provides instructions, recommendations and guidance for contingency planning regarding information technology systems. This special publication proposes a process for contingency planning in order to determine appropriate measures after an emergency or system disruption. The process comprises the following seven phases: (1) Develop the contingency planning policy statement; (2) Conduct the business impact analysis; (3) Identify preventive controls; (4) Develop recovery strategies; (5) Develop an IT contingency plan; (6) Plan, testing, training and exercises; (7) Plan maintenance.

Business continuity management and contingency planning rely on the same decision basis resulting from a conducted BIA. The NIST SP800-34 provides the succeeding three step approach for performing a BIA: (1) Identify critical IT resources; (2) Identify disruption impacts and allowable outage times; (3) Develop recovery priorities. Although the NIST SP800-34 concentrated more on IT than the aforementioned GPG of the BCI, the sub-phases comprise comparable objectives: The identification of (1) critical business processes as well as (2) critical resources, their (3) maximum allowable outage times and the (4) impacts of their disruption on business leading to (5) the development of recovery priorities.

Summarizing, the main goals of performing a BIA are the following:

- The identification of a company's critical business processes and resources.
- The identification of potential single points of failure.
- The identification of the impact of business processes' disruptions on business.
- The identification of business activities' maximum tolerable period of disruption (MTPD).
- The identification of recovery point objectives (RPO) and recovery priorities.

For more detailed information on BIA, we refer the reader to [6, 8, 18, 16, 10].

4. Risk Assessment

In this chapter, we reflect approaches of standards and widely accepted good practice guidelines regarding the execution of a risk assessment enabling the discussion on how the ROPE methodology improves conducting a risk assessment. The British Standard BS25999 [6] defines risk assessment as the "overall process of risk identification, analysis and evaluation" whereas the National Fire Protection Agency standard NFPA1600[16] is more precise: "A comprehensive risk assessment identifies the range of possible hazards, threats, or perils that have or might impact the entity, surrounding area, or critical infrastructure supporting the entity. The potential impact of each hazard, threat, or peril is determined by the severity of each and the vulnerability of people, property, operations, the environment, and the entity to each threat, hazard, or peril."

Like BIA, risk assessment is also addressed within the Good Practice Guidelines (GPG) in the chapter "understanding the organization" [8]. According to the GPG, the aims of risk assessment are the identification of internal and external threats, the prioritization of these threats and the development of an action plan as well as to inform the risk management. The process, which ensures to meet these objectives, comprises at least the succeeding activities: (1) Listing of the threats to selected processes; (2) Estimating the impact of each threat and determination of the occurrence rate; (3) Determination of the likelihood of each threat; (4) Calculating the risk out of the previous activities; (5) Select risk strategy for each threat (risk acceptance, risk transfer, risk avoidance, risk reduction).

The *Risk Management Guide for Information Technology Systems* [19] published by NIST outlines a more detailed approach which contains the following nine steps: (1) *System Characterization*: In this step the scope of the assessment is determined. The techniques of the determination of the system characterization comprise questionnaires, interviews, document reviews and automated scanning tools. (2) *Threat Identification*: In this step threats and essential information related to threats such as the source, motivation and threat actions are collected. (3) *Vulnerability Identification*: Within this phase vulnerabilities that could be exploited by identified threats are listed. The techniques to identify vulnerabilities can among others include penetration testing, audits and vulnerability lists. (4) *Control Analysis*: This step determines the implemented and planned controls and is therefore essential for the next step which estimates the occurrence rate of a threat. (5) *Likelihood Determination*: The output of this phase is a likelihood determination of each identified threat. The factors which must be at least considered according to NIST are: threat-source motivation and capability, nature of the vulnerability and existence and effectiveness of current controls. (6) *Impact Analysis*: This analysis copes with the investigation of impacts that arise from the threats. (7) *Risk Determination*: In this step the level of risk is determined. (8) *Control Recommendations*: Recommendations how the organization can handle the identified risks (including measures that eliminate or mitigate risks) are elaborated. (9) *Results Documentation*: The NIST recommends creating an official report once a risk assessment is completed. This report should be presented to the senior management.

[2] http://www.nist.gov, accessed September 2007

The key objectives of conducting a risk assessment according to [8, 20, 21, 19] are at least the following:

- The identification of threats on business activities.
- The analysis of these threats regarding their occurrence rates and impacts on business enabling...
- ... the prioritization providing essential information for risk management.

5. Contributing to Business Impact Analysis and Risk Assessment

In this chapter, we firstly outline how the application of the ROPE methodology contributes to conduct a BIA as well as a risk assessment based on their key objectives as described in the chapters "Business Impact Analysis" and "Risk Assessment". The basis for performing a BIA and risk assessment is the identification of a company's crucial business activities and business processes. In a further step, the resources that are required for the execution of these processes have to be determined. At this point the requirements for executing a BIA or a risk assessment diverge. Until now there is enough information available to perform the BIA, which comprises the business processes and their resources enabling the determination of the impact of resources' disruption on business activities. Risk assessment builds on the same basis, but requires the additional identification of threats on business processes and resources, their occurrence rates as well as already implemented safeguards. This enables the prioritization of threats, the development of risk strategies and the identification of missing safeguards.

5.1 Enhancing Business Impact Analysis applying the ROPE Methodology

The ROPE methodology provides a structured approach guiding the representation of a company's AS-IS situation leading to according models within the ROPE business process and CARE (Condition, Action, Resource and Environment) modeling layers. In the following, we outline required extensions, benefits and application scenarios of ROPE within the business impact analysis domain.

In order to support the determination of the disruption of resources on business activities, we have extended the ROPE analysis capabilities with respect to the *simulation of disaster scenarios* through the systematic disruption of CARE elements. Therefore, we offer the possibilities to set one or more CARE elements to a non-operational state. This leads to the analysis of the business processes providing fault trees and the determination of temporal and financial losses. Moreover, as the complex company environment has been modeled, the application of ROPE decreases the probability of overlooking dependencies while simultaneously supporting the discovery of new relationships.

The simulation of disaster scenarios still needs manual input to define the non-operational CARE elements. That is the reason why we additionally added automated analysis features to the ROPE methodology. As the environment and infrastructure of a company are often of a high complexity, there is a significant probability that human analysts do not identify crucial resources, which bear the potential to become single points of failure. As a consequence we have developed an automated weaknesses analysis of the companies business processes. On the basis of the identified critical business processes, the *weaknesses analysis of business processes* firstly determines all CARE elements on which the processes (including sub-processes) depend. Secondly, it simulates the breakdown of CARE elements. Therefore, the analyst defines simulation options such as the maximum number of simultaneously disrupted CARE elements. Figure 3 schematically shows the concept of the weaknesses analysis of business processes. Finally, the results of the simulation are visualized for the analyst. This *systematic resource disruption simulation* supports risk analysts and decision makers in prioritizing and focusing on business activities. Applying this simulation from another perspective, it enables the *determination of business activities' degree of interaction* on CARE elements, ranging from buildings to human resources. This allows for instance the identification of the importance of certain employees supporting decisions about the impact of an employee's absence (e.g. illness) justifying the planning of redundancies or fallback strategies.

The aforementioned extended simulation capabilities of ROPE serve as an essential information basis for decisions makers regarding the identification of business activities' maximum tolerable periods of disruption (MTPD) and recovery point objectives (RPO).

Another example application scenario of ROPE for business impact analysis purposes is the determination of the critical quantity in backlogs. The ROPE simulation provides essential information regarding an appropriate resource planing as well as the analysis of according continuity strategies. Through the identification of a threat's impact on CARE elements and thus on business processes' activities backlogs can be derived. As a result adequate resource planning can take place. Furthermore, the planning and cost / benefit analysis of different continuity strategies is supported by ROPE as these strategies can be modeled and simulated in alternative scenarios. Figure 4 (derived from [22]) schematically shows a backlog trap scenario. Initially, the backlog of a business process is within its normal range. The first label on the backlog curve shows the point in time when a threat's impact eliminates the functionality of essential CARE elements. This consequently leads

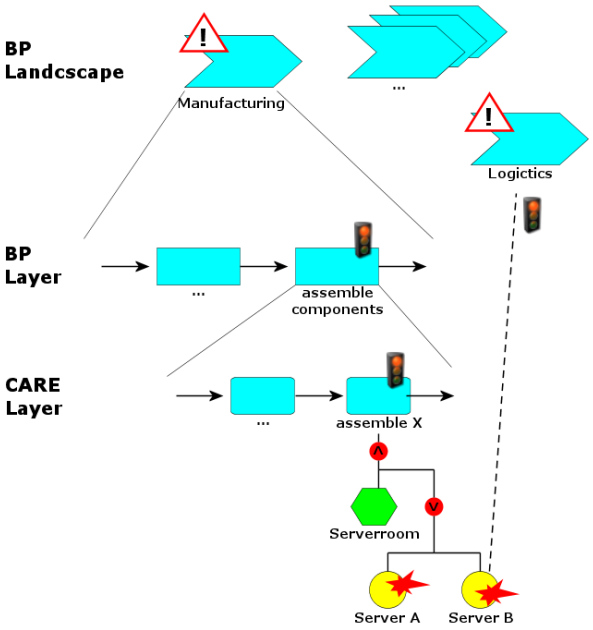

Figure 3. ROPE Weaknesses Analysis of Business Processes

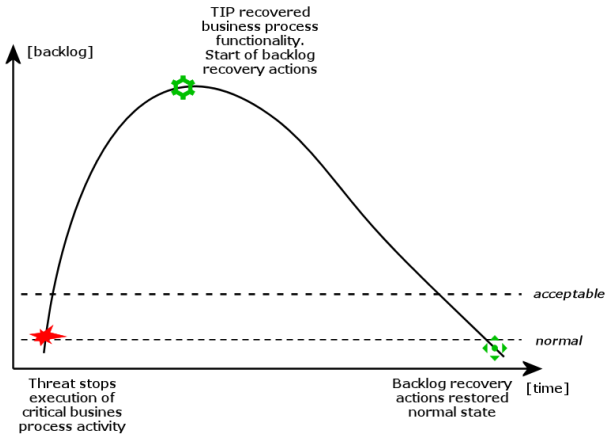

Figure 4. ROPE Backlog Trap Simulation in a Pictorial Form

to the breakdown of business process activities that depend on these CARE elements. The inability to perform the business process results in an increase of the quantity in backlogs. The second label represents the point in time when the threat is eliminated by the according TIP. Although the TIP also restored the functionality of the affected CARE elements, the quantity in backlogs will not decrease until adequate backlog recovery actions take place. These actions are executed until the quantity in backlogs reaches the defined (normal) state. Thus, the ROPE simulation not only determines the additional costs, which are caused by TIP counter measures and recovery measures, but also the additional costs resulting from the required resources and actions to restore the target quantity in backlog. We will conduct future research in the field of resource allocation optimization in order to use the aforementioned simulation results for improving the assignment of resources minimizing potential backlog traps.

The output of conducting a ROPE-supported BIA forms valuable input for executing a succeeding risk assessment and comprises the following key deliverables:

- Process-oriented representation of the company's business activities.
- Refined business process activities represented by CARE diagrams.
- Simulation-based identification of critical business processes and potential single point of failures.
- Simulation-based determination of the impact of business processes' disruption on business.
- Prioritization of the business processes providing essential information for the determination of MTPD and RPO.

5.2 Enhancing Risk Assessment applying the ROPE Methodology

As mentioned before, if a risk assessment is conducted after a BIA, the BIA's output serves as valuable input for further risk considerations.

Threats and threat scenarios are determined on the basis of the already prioritized CARE elements and business activities. ROPE supports this task by the process-oriented modeling of threats within TIP (Threat Impact Process) diagrams, which are assigned to the according threatened CARE elements. Within the TIP diagrams not only the threats are represented in a process-oriented way but also the existing counter measures and recovery measures of the company. The modeling of threats, counter measures and recovery measures enables the risk-aware business process simulation of various threat scenarios. This further allows (1) the evaluation of determined occurrence rates of threats, (2) the risk-aware view on the analyzed business process regarding the determination of financial and temporal losses with respect to threats occurrence probabilities as well as (3) the identification of additional costs resulting from the execution of the counter measures and recovery measures modeled within the TIP diagrams.

Regarding the domain of risk assessment, the ROPE methodology does not claim to improve the initial determination of threat's occurrence rates, but the method's strength

and added value lies in the evaluation of gathered information through the risk-aware business process modeling and simulation approach as well as in the visualization of threats and their impacts on business activities and processes. The risk-aware simulation results enable an enhanced analysis of the company's situation providing essential information for decision makers regarding the determination of risk strategies. Based on the possibility to simulate different threat scenarios, ROPE provides the ability of simulation-based cost/benefit analysis regarding the selection of alternative counter measures and recovery measures alternatives. Figure 5 exemplarily shows the simulation of three scenarios. Scenario B seems to be optimal while scenarios A and C are inappropriate regarding cost/benefit considerations (outage costs versus recovery costs).

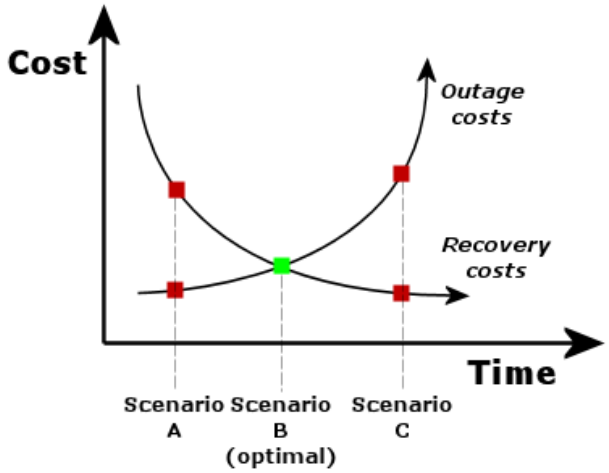

Figure 5. ROPE Scenario Simulation

This leads to improved and justifiable decisions about which risks are to be addressed and which are to be accepted or even out of scope of risk management considerations. Moreover, the ROPE methodology provides *guidance regarding the development of target models* including the development of appropriate risk strategies, counter and recovery measures as introduced in the chapter "Risk-Aware Business Process Modeling and Simulation" and further discussed in [14, 15].

6. Conclusion

In this paper, we have initially presented our ROPE methodology, which enables risk-aware business process modeling and simulation. Applying ROPE, not only business process activities but also their refinement into CARE elements as well as threats, counter measures and recovery measures are modeled in a process-oriented way. Extending the ROPE approach with business impact analysis and risk assessment requirements, ROPE provides valuable support for conducting these two analysis concepts. The main advantages are outlined within the following concluding paragraphs.

The application of the ROPE methodology supporting a business impact analysis leads to succeeding benefits:

- The simulation of disaster scenarios through the systematic disruption of CARE elements.
- This simulation enables the visualization of a dependency tree between the business processes and the required CARE elements. As the complex company environment has been modeled stepwise, ROPE decreases the probability of ignoring dependencies while simultaneously supporting the discovery of new dependency relationships.
- This simulation further enables the weaknesses analysis of business processes regarding the identification of potential single points of failure.
- The simulation-based determination of the impact of one or more disrupted CARE elements on the dependent business processes leading to the identification of temporal and financial losses.
- The simulation results provide essential information for decisions regarding the identification of business activities maximum tolerable periods of disruption (MTPD) and recovery point objectives (RPO).

The application of the ROPE methodology supporting a risk assessment leads to the succeeding benefits:

- Simulation-based analysis of current counter measures and recovery measures.
- Support for the development and cost/benefit analysis of risk strategy and safeguard options.
- Incorporated documentation capabilities through the process-oriented acquisition and modeling of business process (business process layer), resource (CARE layer), threat and safeguard information (TIP layer), which can be easily and structured exported as reports valuable for (corporate) risk management.
- Identification of additional financial and temporal losses caused by the execution of counter and recovery measures.

The future research objectives comprise the improvement of the prototype and conducting a case study for evaluation purposes.