

A Formal Approach Enabling Risk-Aware Business Process Modeling and Simulation

Simon Tjoa, *Member, IEEE*, Stefan Jakoubi, *Member, IEEE*, Gernot Goluch, *Member, IEEE*, Gerhard Kitzler, Sigrun Goluch, and Gerald Quirchmayr

Abstract—The effective, efficient and continuous execution of business processes is crucial for meeting entrepreneurial goals. Business process modeling and simulation are used to enable desired business process optimizations. However, current approaches mainly focus on economic aspects while security aspects are dealt with in separate initiatives. This missing interconnection may lead to significant differences in improvement suggestions, such as the differing valuation of security investments (e.g., redundancy of systems).

The major contribution of this paper is the introduction of a formal model that is capable of expressing the relations between threats, detection mechanisms, safeguards, recovery measures and their effects on business processes. This novel business process simulation capability paves the way for the evaluation of security investments at process design stage by allowing the consideration of stochastic influences of the occurrence of threats on process activities and resources in a unified way. A stylized business case outlines how our method can be applied to real world scenarios.

Index Terms—Business Process Reengineering, Consulting and Strategic Planning, Security Enablement Methods and Tools

1 INTRODUCTION

COMPANIES are increasingly confronted with the challenge of performing their processes efficiently and effectively with regard to economic aspects, while maintaining security, continuity and compliance of processes at the same time.

Business process management is the dominant domain aiming at optimizing the execution of business processes

so that activities are performed efficiently and effectively in economic terms. "The biggest benefit of business process optimization and simulation is that they deliver insight into dynamic processes so that they are designed well and operated effectively as conditions change." [1] However, business processes face threats that endanger the effective and efficient execution of their activities. There exist diverse classifications of these threats [2], [3], [4], ranging from accidents (e.g., unavailability of ICT resources or the absence of strategic personnel) to natural catastrophes (e.g., earthquakes) and to deliberate acts (e.g., sabotage or theft). 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 [5], [6], [7], [8].

The European Network and Information Security Agency (ENISA) states that "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..." [9]. Although the individual domains' 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. Within the last years the business continuity management domain has gained in importance as it attaches value to determining the effects of threats on business processes with the first priority on a company's survival: "the biggest driver for security expenditure, according to the Global State of Security Survey, is business continuity, whereas protecting the company's reputation and customer data take precedence in the ISBS 2008". [10] Therefore, business impact analysis and risk assessment techniques are predominant [11], [12]. An interesting detail in the context of this paper is that temporal aspects are considered within the business impact analysis. There, information such as the financial impact of an activity disruption after a specific duration is taken into account. However, existing methods and techniques from the business process management and related domains are not used to capture the dynamic

- S. Tjoa is with the St. Pölten University of Applied Sciences, Matthias Corvinus-Straße 15, 3100 St. Pölten, Austria. E-mail: simon.tjoa@fhstp.ac.at.
- S. Jakoubi is with the Austrian IT-Security Competence Center, Secure Business Austria, Favoritenstr. 16, 1040 Vienna, Austria. E-mail: sjakoubi@sba-research.org.
- G. Goluch is with the Austrian IT-Security Competence Center, Secure Business Austria, Favoritenstr. 16, 1040 Vienna, Austria. E-mail: ggoluch@sba-research.org.
- G. Kitzler is with the Austrian IT-Security Competence Center, Secure Business Austria, Favoritenstr. 16, 1040 Vienna, Austria. E-mail: gkitzler@sba-research.org.
- S. Goluch is with the Austrian IT-Security Competence Center, Secure Business Austria, Favoritenstr. 16, 1040 Vienna, Austria. E-mail: sgoluch@sba-research.org.
- G. Quirchmayr is with the Faculty of Computer Science, University of Vienna, Liebigg. 4/3-4, 1010 Vienna, Austria. E-mail: Gerald.quirchmayr@univie.ac.at.

characteristics of business processes. Advantages of business process management techniques are not used to enhance current business impact analysis techniques. For example, modeled business processes can be simulated applying path analysis concepts. This provides valuable information, such as the probability of certain business cases (i.e., the probability of the possible business process execution paths) and consequently the expected value of the process iterations weighted with the according paths' probabilities.

In summary, there is a growing need for an integrated approach that combines security and compliance-related disciplines with business process management. Recently conducted surveys and reports such as [13], [14] confirm this by outlining that business process improvement, regulative and legislative changes and business interruptions are major concerns of today's businesses. For appropriately addressing these concerns and maximizing the entrepreneurial success, it is indispensable to implement risk, business process and resource management. As long as the information flow between the abovementioned domains (e.g., business process management or business continuity management) is not appropriately coordinated and harmonized, there is a lack of common information and reasoning basis in many cases, leading to a quite different understanding of how the company's potentials can be advanced. For example, there may be very divergent views on the need for and benefits of backup facilities (e.g., a redundant electronic data processing center). Consequently, building the conceptual bridge between the business process and the security/contingency domains is the overall vision of our current research.

In this paper we introduce our work on risk-aware business process management, which seeks to decrease the gap between economical and security viewpoints within an organization. In the scope of this paper, the term *risk-aware business process management* is used to describe business process management that considers the integration of security and risk aspects. This combination allows a risk-aware business process analysis, enabling the optimization of efficiency, robustness and security of business processes at the same time.

The paper is organized as follows: In section 2 we summarize related research results. At the end of the related work section we provide a short overview on our previous work in the field of business process security. Section 3 introduces the formal model and simulation approach. In section 4 we first present a sample scenario, which is then used to demonstrate how our method can be applied to real-world business cases. Furthermore, section 4 outlines the implementation of our approach in Simulink® [15]. Section 4.3 presents simulation results of our stylized business case. Section 5 concludes the paper and discusses further research aims and challenges.

2 RELATED WORK

In this section, we provide an overview of related work aiming at the best possible support of the planning and implementation of organizational resilience. We therefore start with a selection of standards and good practices and proceed with related scientific research. Due to the limited space, it is not possible to provide full details. Thus, we would refer the reader to the cited work for detailed information.

2.1 Standards and Good Practices

As a representative standard for the risk management domain, we selected the ISO27005[16], and for the business continuity management domain the BS25999[6], [7]. However, we also provide the reader with references to further standards and good practices in these domains. The international standard ISO27005 [16] provides guidelines for information security risk management. It provides an iterative process consisting of the following key phases: (1) Context establishment: gathering of all information relevant for setting management parameters, defining scope and boundaries, as well as setting up and running the information security risk management process; (2) Risk assessment: identification, quantification or qualification as well as prioritization of risks; (3) Risk treatment: selection and implementation of measures for each risk treatment strategy (i.e., risk reduction, risk retention, risk avoidance, and risk transfer); (4) Risk acceptance: formal recording and approval of decisions regarding accepted risks; (5) Risk communication: exchange of all relevant risk information between decision makers and other stakeholders; (6) Risk monitoring and review: continuous monitoring and review of risks considering changes in the risk and in the organizational environment.

The following paragraph outlines further related standards and best practices we want to mention.

OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) [17] is a widely accepted method for protecting a company's assets. OCTAVE is an asset-driven approach that provides information security risk evaluation. An important best practice guide is the Baseline Protection Manual supplied by the German Federal Office for Information Security. In addition to its structured method, it provides an excellent Threat and Safeguards Catalogue. [3] Regarding process-oriented methods, the Failure Modes and Effects Analysis (FMEA) is widely used in the automotive industry. FMEA prioritizes risks of items and tries to minimize them via process iterations ([18], [19]). A further representative standard for risk management is the NIST SP800-30 [2]. Business continuity management (BCM) is a management process to improve the resilience of a company even regarding unexpected catastrophes (e.g., earthquakes, fire, flooding, etc.). To achieve an adequate level, a company-wide BCM strategy has to be implemented. The Good Practice Guidelines (GPG) of the Business

Continuity Institute (BCI) [11] are management guidelines for implementing BCM according to BS25999. The GPG approach follows the business continuity management life cycle of the British standard BS25999 [6], [7], which succeeded the publicly available specification PAS56 [20], and comprises the following phases: (1) Understanding the organization: provide information that enables prioritization of an organization's products and services and the urgency of activities that are required to deliver them. This sets the requirements that will determine the selection of appropriate BCM strategies. (2) Determining BCM options: evaluation of a range of strategies allowing an appropriate response to be chosen for each product or service, such that the organization can continue to deliver those products and services at an acceptable level of operation and within an acceptable time frame during and following a disruption. (3) Developing and implementing a BCM response: creation of a management framework and a structure of incident management, business continuity and business recovery plans that detail the steps to be taken during and after an incident to maintain and restore operations. (4) Exercising, maintaining and reviewing: makes it possible to demonstrate the extent to which a company's strategies and plans are complete, current and accurate and identify opportunities for improvement. (5) BCM program management: application of various (project) managerial, operational, administrative and technical disciplines to ensure the successful implementation of the BCM program. (6) Embedding BCM in the organization's culture: ensuring that the BCM program and the communication of relevant information fit in the organization's environment and culture.

Further literature substantially addressing the same phases includes e.g., ISO22399 [21], ISO24762 [8], and NIST SP800-34 [22].

In the Business Process Management (BPM) domain, we want to mention the Business Process Modeling Notation (BPMN) [23], the ARIS reference model [24] and the workflow reference model by the Workflow Management Coalition (WfMC) [25]. However, for our purposes we selected the Business Process Management Systems (BPMS) paradigm by [26] as methodological basis. Briefly summarized, the method consists of five iterative phases: (1) Strategic Decision Process: definition of strategic guidelines, success factors and essential criteria for the business processes of a company. (2) Re-Engineering Process: documentation, adaptation, modeling and optimization of business processes and identification of potential for reorganization. (3) Resource Allocation Process: implementation of business processes in IT as well as in the organization, allocation of resources and infrastructure. (4) Workflow Process: execution of the business processes in the operating environment, collecting operative information as a base for continuing analyses. (5) Performance Evaluation Process: aggregation and preparation of process information, extraction of performance indicators and metrics.

2.2 Related Scientific Research

Compared to the research domains of business process management and risk management, the domain of business process security is still a very young research area. Nevertheless, there is a wide range of approaches trying to reduce the gap between the different domains of security, risk management and business process management.

Zur Muehlen and Rosemann identify risk as an inherent property of every business process [27]. Therefore, they propose to counteract the trend of considering risk only from a project management viewpoint and to tackle the topic of risk management in the context of business process management. They consequently introduce a taxonomy including process related risks and their appliances concerning the analysis and documentation of business processes. Additionally, they propose a taxonomy of business processes including five clusters (goals, structure, information technology, data, and organization) and two separate life cycles (build-time and run-time), enabling the classification of both errors and risks. To capture risks in the context of business processes, the authors introduce four interrelated model types: (1) The Risk Structure Model provides information regarding the relationship between risks. (2) The Risk Goal Model represents a risks/goals matrix. (3) The Risk State Model captures the dynamic aspects of risks and consists of the different object types risk, consequence and connectors. (4) Event-driven Process Chains (EPCs) are extended to consider risks, enabling the assignment of risks to individual steps in the specific process.

The need for a holistic business view of risk management is addressed by Neiger et al. [28] In their approach, they utilize value-focused process engineering, which creates links between business processes and business objectives at the operational and strategic levels, is utilized. This value-focused process engineering approach is applied to risk management models, resulting in a risk-oriented process management view. The overall model consists of four steps: (1) To identify relevant process risks, business objectives are decomposed, while each process activity is examined in order to identify further relevant risks. (2) To identify risks and to determine related processes, value-focused approaches are used. (3) To identify the best process structure to meet the business objectives process configurations are suggested. (4) Finally, to enable the selection of an optimal process configuration, alternative configurations and their corresponding results that meet the identified risk minimization objectives are compared.

Focusing on business process availability Milanovic et al. present a framework for modeling availability considering services, underlying ICT infrastructure and human resources [29]. To model these relations, the authors adapt a service-enabled architecture. Moreover, a fault-model with two failure modes (temporal/value) is used, thus allowing an analytical assessment procedure: (1)

Defining the business process following a process modeling language. (2) Refining activities by modeling atomic services. (3) Creating an infrastructure graph. (4) Mapping services to infrastructure components. Transform paths for service executions into Boolean expressions. (5) Mapping business processes to atomic services. The functional dependency between business process, service and ICT-layer availability is the result. (6) Transforming the Boolean expressions into reliability block diagrams/fault trees to calculate steady-state availability. (7) Calculating the availability of business processes and services by solving/simulating the model generated with the abovementioned steps.

To build the bridge between the business and the technical layer, Sackmann et al. extend current risk management methods with a business process-oriented view. To this end, they introduce an IT risk reference model [30], [31] consisting of four interconnected layers: (1) business process layer, (2) IT applications / IT infrastructure layer, (3) vulnerabilities layer, (4) threats layer. This reference model "serves as foundation for formal modeling of the relations between causes of IT risks and their effects on business processes or a company's returns" [30]. A matrix-based description is used to express these relations.

Using process descriptions as a basis and starting point, the POSeM approach by Röhrig [32] facilitates the selection process of security measures. To meet this objective, two concepts are provided: (1) The Security Enhanced Process Language (SEPL), allowing the representation of security requirements within business processes. (2) Rule bases enabling the validation of specific process security definitions regarding consistency and the identification of required safeguards.

Rodríguez et al. [33] also tackle the challenge of modeling security requirements in business processes in their extension of UML 2.0. According to the authors, this is essential since software developers derive necessary requirements for software design and implementation from business processes. The proposed extension makes use of activity diagrams to allow the definition of business processes security requirements.

Ellison et al. [34] developed the SNA (Survivable Network Analysis) method in order to identify and analyze essential services of critical infrastructures. The method comprises four key steps. Within the first two steps, essential services and assets are identified taking failure impacts and company goals into account. Consequently, it is possible to identify essential components that are crucial for guaranteeing the continuous availability of these essential services and assets. Within step three, intrusion scenarios are developed and mapped onto the architecture in order to identify so called compromisable components. Components that are essential and compromisable as well as their underlying infrastructure are further analyzed with respect to key survivability properties (resistance, recognition, and recovery). This analysis is represented in a survivability map which is

used to trigger evaluation and feedback processes.

Neubauer et al. propose an IT-Security Valuation Framework [35]. To determine the external value of security measures, core business processes are used. The valuation itself is based on downtime costs (lost business value) in the case of a system's unavailability. To measure the costs needed for implementing and attaining a specific level of security, IT processes are used. On the basis of the gathered information, valuation models such as ALE (Annual Loss Expectancy) can be used to calculate expected loss and to define the optimal level of security.

To enable the management of uncertainties in the context of business process management, Sienu et al. [36] suggest a multi-layer integration of business process and risk management. They propose a method for the integrated management of process risks, including a life cycle model, a metamodel, a modeling language and a set of usage rules.

Regarding the compliance of business processes, Weber et al. [37] propose an approach to validate whether the states reached by a process are compliant with a set of constraints or not. This enables compliance checking of a new or altered process against a given constraints base and of the process repository against a different or changed constraints base. The authors formalize and utilize a class of compliance rules and annotated process models respectively.

Sadiq et al. [38] also address the problem field of business process compliance and identify the need for systematic approaches to understand the interconnection and dependency between business and control objectives. Accordingly, the authors introduce a modal logic based on normative systems theory, dealing with the effective modeling of control objectives and their propagation onto business process models.

To establish a connection between a company's core business processes, IT processes and security levels, Jallow et al. [39] propose a framework for risk analysis in business processes with a focus on cost, time and performance/quality analyses. The framework consists of the following six steps: (1) Modeling the activities of the business process. (2) Determining the considered dimensions (i.e., cost, time and output) for each activity. As only one dimension can be evaluated within a specific risk analysis, the objective of each analysis has to be defined. (3) Identifying risk factors, probability of occurrence and impact. (4) Assumptions regarding the risk impact should be defined in order to consider uncertainties associated with risks. The authors use a three-point estimate expressed as a triangular distribution. (5) Calculating each identified risk by multiplying the occurrence probability with the impact. "The impact is not a discrete value but a series of values generated by the simulation based on the distribution". (6) Calculating forecasts for each activity and cumulative results for the whole process. A prototypical framework implementation has been performed using Microsoft Excel using the

add-on software Crystal Ball™.

Above, we gave a representative overview of several research approaches that aim to establish an integrated view on security, risk and business process management. Further work can also be found in the related domain of reliability simulations. Reliability analysis has a potentially wide range of application areas, e.g. risk analysis, engineering design [40] etc. Our main BPEs can be regarded as system reliability concepts. There are various methods to model system reliability. Almost all of them use underlying monte carlo simulations e.g. [41]. For a complex system the underlying monte carlo calculations can be very elaborate and therefore time consuming. It is favored to alleviate that numerical effort by modifying the monte carlo simulation, e.g. [42]

Summarizing, existing approaches have achieved the following research results: (1) Rule-based validation of process security and selection of counter measures. (2) Extension of modeling languages (e.g., UML 2.0) by introducing security requirements modeling capabilities. (3) Stronger link of risk and business process management (e.g., via a taxonomy or via a reference model linking threats, vulnerabilities, ICT resources and business processes). (4) Calculation of business process availability. (5) Integration of business and compliance objectives. (6) Determination of risk impacts on the business process activity layer using Monte Carlo simulation (7) Simulation of reliability of systems. The mentioned approaches contributed substantial results in the field of business process security. However, we still miss a concept meeting the following objectives: (1) Concept for modeling: (a) Business process activities, (b) required resources, (c) threats endangering these resources, (d) detection-, counter- and recovery measures, (e) relations between these components. (2) Concept for the simulation-based determination of risk impacts (e.g. time, costs, backlogs, etc.) on resources and/or directly business process activities considering the interaction between threats as well as detection-, counter- and recovery measures.

These objectives serve as a basis for the identification of open research challenges and led us to the development of a methodology enabling risk-aware business process modeling and simulation [43], [44].

In this work, we present an extension of our method comprising the introduction of a novel formal model and simulation approach.

2.3 Previous Work

Following, we present our overall vision of risk-aware business process management [45], [46], [44], [43] in order to both provide the reader with an adequate overview and to clarify our contribution in sections 3 to 5.

In our vision, risk-aware business process management can be performed when appropriate bridges between business process management and the relevant security domains (e.g., risk or business continuity management)

are built. Risk-aware business process modeling enables according simulations as the logical next step. These two techniques are the cornerstones of business process planning and reengineering where our current research focus lies. In a nutshell, in our conceptual approach

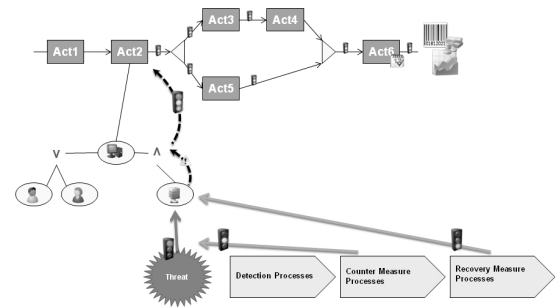


Fig. 1. Conceptual Approach towards Risk-Aware Business Process Modeling and Simulation

(see Fig. 1) business process elements, such as activities and resources, are endangered by threats. If a threat is successful, one of the possible impacts may be the unavailability of a resource, leading to delays in the execution time of connected activities. In order to represent the current security situation detection-, counter- and recovery measures are modeled. If sufficient information is available, these measures are modeled as business processes that require resources and are endangered by threats. Detection measures invoke counter- and/or recovery measures. The quality of the measure affects the point in time when detection or invoking respectively, takes place. Counter measures try to eliminate an occurred threat and recovery measures try to re-establish the functionality of potentially affected business process elements. Basically, detection measures are the first step and thus can influence counter and recovery measures, whereas the efficiency and effectiveness of counter measures only influences following (or overlapping acting) recovery measures. Fig. 1 shows the conceptual approach described above. In our opinion, a real strength of our approach is that results of typical projects, such as business process analyses, risk assessments or business impact analyses do not end up as dusty reports in cabinets but can be modeled and continuously used for simulation purposes. Following, we motivate our vision of building the bridge between the business process management and risk as well as contingency domains. To exemplify our vision, Fig. 2 schematically depicts core activities of the Business Continuity Management (BCM) Life Cycle (left side) according to [6], [7] and core activities of the Business Process Modeling paradigm BPMS (right side) according to [26]. In between our bridging concept is sketched that is described below Fig. 2. The following items describe the steps how the mentioned domains may be applied in a more integrated way: (1) The interconnection of business process modeling and simulation techniques with business impact analysis and risk assessment techniques enables the risk-

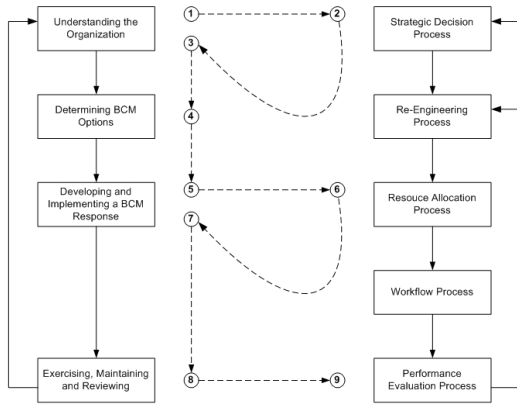


Fig. 2. Introduction of Risks into Business Process Management

aware business process analysis. (2) Processes can be better understood not only focusing on economic factors but also taking risks and business process activity disruptions into consideration. Exemplarily, financial and reputational impacts of a process interruption are taken into account when defining strategic guidelines, success factors and essential criteria (e.g. availability requirements) for the business processes of a company. (3) This broadened view on business delivers added value when (re-) engineering and optimizing the business processes. Subsequently, business processes are available which have been designed under consideration of economic, continuity and risk information. (4) This delivers added value for determining BCM options as the evaluation of potential strategies (e.g. alternate data center) can be tightly aligned to the available business process information (e.g. product/service value, processes' prioritization or availability/recovery requirements). (5) Selecting the most appropriate option is the basis for developing and implementing the BCM response. Accordingly, plans can be developed considering process characteristic such as minimal resource requirements after an incident. (6) The risk-aware designed business processes and the related continuity plans build the fundament for determining appropriate resources. This comprises not only resource utilization considerations to perform the business process activities under normal conditions. When a threat occurs, it endangers the activities' execution and causes the invocation of plans that detail the steps to be taken during and after an incident to maintain and restore operations. (7) This further leads to a sufficient implementation of both, the business process execution in the operation environment and the institution of the business continuity and business recovery plans. (8) The aggregation and preparation of process information, extraction of performance indicators and metrics serves as valuable input for iterations in the BCM life cycle. (9) Vice versa, lessons learned and metrics from plans' rehearsal or even invoked plans is the start for continuously improve the understanding of a company's

business and its processes.

3 THE FORMAL MODEL

In this section, we introduce our novel formal description for modeling threats, detection-, counter-, and recovery measures, their interdependencies, as well as the impact on the attributes of affected resources. For demonstration purposes we will focus on the security attributes confidentiality, integrity and availability. Subsequently, we will use a sample scenario to show how our formal model can be used to support an evaluation initiative of a company.

3.1 A Formal Description of Business Process Elements

To simulate the continuous execution of business process elements (BPE) [47], we first introduce the set of resources $\mathcal{R} = \{R_1, \dots, R_n\}$, the set of activities $\mathcal{Act} = \{Act_1, \dots, Act_l\}$ and the set of attributes $\mathcal{A} = \{A_1, \dots, A_m\}$. Every single resource and activity have their own attributes out of the set \mathcal{A} . Within our formal model, the interaction between activities and resources is realized as Resource requirements RR_i , where i stands for the corresponding activity. These elements hold information about the attributes of certain resources needed to execute successfully. This can be graphically expressed as seen in Fig.1. This could also be formally expressed, using the tuples (R_j, A_j, ν) where R_j is the needed resource, A_j its specific needed attribute and ν represents a threshold defining the minimum attribute condition that is necessary to execute the activity. Using the logical operators \vee/\wedge , it is possible to create a whole resource tree needed for execution of a certain activity (including the possibility to represent redundancies of resources).

For clarity, we provide an example, referring to Fig. 1. The mentioned activity is named Act_2 . Our set of attributes consists of 2 elements: A_1 is the availability of a certain BPE and A_2 the integrity of a BPE. To execute this activity successfully, it is necessary to have Server R_1 access (availability 80%, integrity 100%), an available client PC R_2 (availability 100%) and, as can be seen in the figure, one of the two employees R_3, R_4 (availability 80%). In our model we would express this as follows:

$$RR_2 = (R_1, A_1, 0.8, A_2, 1.0) \wedge (R_2, A_1, 1.0) \wedge [(R_3, A_1, 0.8) \vee (R_4, A_1, 0.8)] \quad (1)$$

3.2 A Formal Description of the Behavior and Effects of Threats and Safeguards

In order to simulate threats, it is indispensable to formally describe the impacts of threats on business processes and the effects of counter- and recovery measures. In this section we therefore introduce our formal model, which achieves the abovementioned objective.

As our approach focuses on business process management, we assume that threats can affect specific attributes

of business process elements (BPE), such as the availability of a resource or the execution of an activity.

In order to formally describe a threat, we introduce an impact function $\omega(t)$ that holds information about a threat's characteristics, such as its behavior or speed.

Let $\mathcal{T} = \{T_1, \dots, T_n\}$ be the set of possible threats. Every T_n possesses the following four parameters, which express the threats outcome: (1) p_n indicates the probability of occurrence in (2) a given interval $[t_0; t_1]$; (3) the impact function $\omega_n(t)$; and (4) the corresponding attribute.

For example, a threat T_1 (e.g., virus) that attacks the attribute A_4 (e.g., availability) with the occurrence probability p_1 (e.g., 70%) within the time interval 2 and 5.5 and the impact function $\omega_1(t)$ (e.g. linear function) can be formally expressed as:

$$[T_1; 0.7; [2, 5.5]; \omega_1(t); A_4]. \quad (2)$$

A threat can be eliminated by safeguards. We group safeguards according to their behavior into preventive, blocking and reactive measures. The comprehensive differentiation between these types is described in the following paragraphs.

Preventive measures: A preventive action influences a threat's probability of occurrence. An example of preventive measures against the threat "fire" would be the usage of fireproof materials in a building or the introduction of a non-smoking policy in a company. Let $\mathcal{PA} = \{PA_1, \dots, PA_m\}$ be the set of all preventive actions. One specific action can be described as a set of tuples

$$PA_m := \{(T_k, \rho_k), \dots\} \quad (3)$$

where T_k is the applicable threat and ρ_k the linked probability. A threats occurrence probability p_n is decreased by ρ_n leading to the new occurrence probability $\tilde{p}_n : \tilde{p}_n = p_n - \rho_n$.

Blocking measures: Blocking measures are defined in our model as safeguards that immediately destroy a threat on detection. Therefore, no further consequences arise for the business processes. An example of a blocking measure would be the live scanning of e-mails. If a virus is detected in the e-mail traffic by the scanner it is immediately quarantined or deleted.

Let $\mathcal{BA} = \{BA_1, \dots, BA_l\}$ be the set of blocking actions, then every BA_l can be described as a set of tuples

$$BA_l := \{(T_k, \beta_k), \dots\} \quad (4)$$

where T_k is the applicable threat and β_k is the probability of its detection. The difference between those two probabilities is obvious. While the \tilde{p}_n stands for the probability of a threat occurring, the probability β_k decides whether a threat is detected and immediately destroyed.

Reactive measures: A reactive measure can be defined as a safeguard that counteracts threats during an attack. Examples of reactive measures would be the manual removal of a virus.

As threats invoking a reactive measure may already have caused damage, it consists of following three parts: (a)

detection measures, (b) counter measures and (c) recovery measures. These three measures are modeled in processes and therefore have similar characteristics as BPEs, such as certain resource requirements. An active threat is necessary for a successful detection. The detection also decides which counter measure is appropriate for a given threat. The counter measure then decides which recovery measure is needed. A simplified representation would be:

Detection \rightarrow Counter Measures \rightarrow Recovery. While the counter measure starts immediately after the detection period is over, the recovery measure can overlap with the counter measure and begin while the counter measure is still active.

To realize this we state: The detection measure has no direct or indirect influence on the threat itself. The detection is active in every time step. The predefined detection period starts as soon as there is a recognizable change in the attribute's condition function. We specify a specific detection measure as follows:

$$DM_k := \{T_j, A_i, dm_k(t), (CM_m, \dots)\} \quad (5)$$

where T_j is the threat, which may by definition be detected by the specific detection measure DM_k , A_i the specific attribute, $dm_k(t)$ the function that describes the probability of recognizing the threat T_j at a given "attribute's condition" and the required counter measures CM_m , which can also be a multidimensional vector. The definition of the function dm_k enables us to define a threat that should be detected once the damage is x%.

The counter measures affect a threat's state and therefore have an influence on the impact function $\omega_n(t)$ of a linked threat T_n . A certain counter measure CM_m is further expressed as

$$CM_m := \{cm_m(t), (RM_n, \dots), (tc_n, \dots)\} \quad (6)$$

where $cm_m(t)$ is the function that describes the effect on the threat's impact function, RM_n are the required recovery measures and tc_n is the threshold, which holds information on when the recovery can start. The influence on the threat's impact can be realized by a new impact function:

$$\tilde{\omega}_n(t) := \omega_n(t) \cdot (1 - cm_m(t)) \quad (7)$$

To know at which time step t_r the recovery measure RM_n is started, we require two assumptions:

- 1) $\tilde{\omega}_n(t_r) = tc_n$
- 2) $\tilde{\omega}'_n(t_k) \leq 0$

The counter measure is stopped once $\tilde{\omega}_n(t) = 0$.

The recovery measure has a direct influence on the attribute's condition function $z_i(t)$. It is further specified through a recovery function $rm_i(t)$. The influence on the condition of an attribute can be seen as a new condition function

$$\tilde{z}_i(t) := z_i(t) + rm_i(t) \quad (8)$$

The recovery ends once the condition $\tilde{z}_i(t) = 1$.

In the following we outline how our method can be applied to model an activity's attributes "availability" and "integrity".

3.3 Modeling the Activity's Attribute Availability

We assume that every activity has a "degree of completion" attribute $G : \mathbb{R} \rightarrow [0, 1]$ (continuous). The activity is considered completed once $G = 1$. Finite activities have the following characteristic properties:

$$\exists \tilde{t} \in \mathbb{R} \text{ with } G(\tilde{t}) = 1 \quad (9)$$

$$\exists g, \text{ integrable, with } G(t) = \int_0^t g(u)du \quad (10)$$

Hence, the execution time of a process activity is the solution of the following integral equation:

$$G(\tilde{t}) = \int_0^{\tilde{t}} g(u)du \quad (11)$$

To measure the effect of a threat attacking the availability attribute of an activity, function (11) has to be enhanced with the threat's impact function $\omega(t)$:

$$G(\tilde{t}) = \int_0^{\tilde{t}} g(u) - \omega(u)du \quad (12)$$

3.4 Modeling the Activity's Attribute Integrity

Certain activities exhibit the attribute "integrity". To measure integrity loss we use a similar approach as described in section 3.3. We assume the integrity of a certain activity to be a real function $i : \mathbb{R} \rightarrow [0, 1]$. While no threat is active, we set $i(t) = 1$. The loss of integrity is defined as follows:

$$IL(t) = \int_{t_0}^t (1 - i(u))du \quad (13)$$

While no threat is active, the "loss of integrity" is constant equal 0, $IL(t) = 0$. Regarding the impact of a certain threat on the activities' integrity, we enhance the above function (13) with the threat's impact function $\omega(u)$:

$$IL(t) = \int_{t_0}^t (1 - (i(u) - \omega(u)))du \quad (14)$$

with $\omega(u)$ being the integrity impact of a certain threat and t_0 standing for the starting time of the activity. The enhanced function enables us to measure the resulting loss of integrity.

3.5 Relation between Resources' and Activities' Attributes

When a threat attacks any of a resource's attributes to a significant extent, the resulting impact has an indirect influence on the corresponding activity's attribute. We assume that this interrelation is proportional to the difference emerging from the actual resource's attribute condition and the needed attribute condition. The

needed state of an attribute ν can be obtained from the corresponding resource requirements (see section 3.1, equation (1)).

Let N_{t_m} be the actual condition of a resource's attribute $A_i(t)$ at time unit t_m , $0 < N_{t_m} < 1$. If the condition N_{t_m} reaches the threshold ν , then the condition's alteration has an influence on the linked activity's attribute. To realize this we define a help function:

$$\varphi(t) = f(\nu - N_t) \quad (15)$$

$$f(0) = 0 \quad (16)$$

The help function $\varphi(t)$ can be seen as function of threat impact on the activity's attribute, which depends only on the resource's condition and is independent of the original threat's impact function. Fig. 3 illustrates the

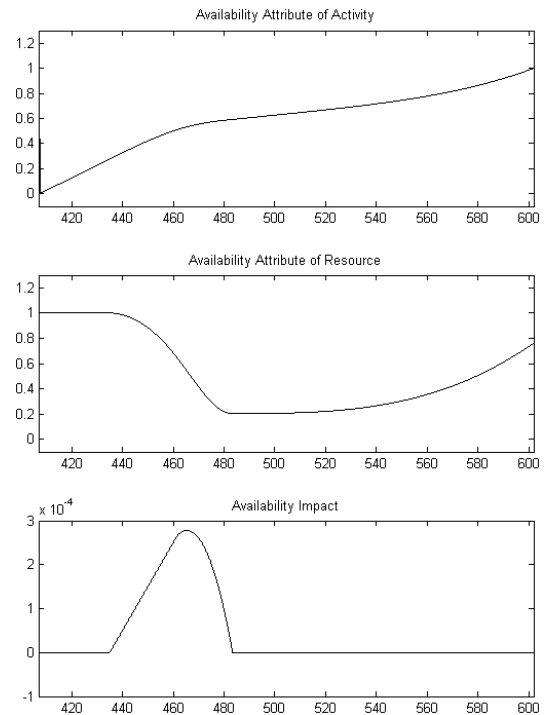


Fig. 3. Influence of a Threat and its Consequences on the Availability Condition Function. In Ascending Order: Impact Function, Resource Attribute Condition and Activity Attribute Condition

influence of a threat impact on the linked resource's availability condition. Additionally, it shows that an attacked resource's availability has an indirect influence on the activity's completion function. The lower chart depicts the threat's impact over time, while the middle chart shows the according impact of the threat on the availability of the affected resource over time. The upper chart shows the resulting impact on the continuous completion function of the assigned activity (leading to an increase in the execution time). In this section we outlined how relations between activity attributes and resource attributes can be described using the example of the attribute "availability". This example applies analogously to all similar cases (e.g., integrity attribute).

4 EVALUATION

This section provides information on how our formal description can serve as input for conducting risk-aware business process simulations. We therefore introduce a sample scenario and demonstrate how we simulate effects of threats and safeguards using the professional toolkit Simulink®.

4.1 Sample Scenario

In order to demonstrate the capabilities of our formal model, we introduce a sample scenario, which is later on used to show how our approach can be applied to real world scenarios. For sake of clarity this is a stylized business case.

For our sample scenario we assume that the company ACME has business processes and that the employees assigned to several of these business process activities require computer client resources to perform their work. An audit was conducted and one of its findings was that improvements should be made in client protection - from an organizational perspective through appropriate policies and procedures and on the technical side through the implementation of an adequate anti-malware solution. Thus, ACME decided in the course of an improvement initiative to assess different organizational and technical solutions. ACME analysts identified the following actions that should be considered and evaluated: (1) preventive policies, procedures and awareness trainings in order to reduce the probability of successful malware attacks and spreading; (2) an intrusion detection system at the network layer; (3) an anti-malware tool on client side for which different options should be evaluated from a cost/benefit perspective; (4) clear procedures regarding how to react to a malware incident; (5) clear procedures regarding how to recover from a malware-incident.

After an exhaustive analysis workshop, ACME identified 15 incidents with a major impact on the availability of clients that had been reported within the last year. According to British Telecom, an average business suffers 11 virus attacks per day [48] - ACME takes this value as feasible input data for further considerations. Furthermore, the Information Security Breaches Survey 2008 [10] indicated that the median number of breaches of large businesses is three significant infections per year. Thus, the management of ACME decided that a strategic major goal would be to reach this median. Appropriate analyses and evaluations regarding organizational and technical actions should be performed to justify security investments and to gain the management approval for implementation projects.

The initial solution planning workshop resulted in the following proposals for further (scenario) evaluations. Two anti-virus toolkits should be evaluated. The products vary in acquisition costs and detection rate.

4.2 Implementation

The **main layer** (Fig. 4) of the model represents our internal setting, which is composed of 2 activities (*1st Level Support* and *2nd Level Support*) and 2 resources (*PCs* and *Server*) for each activity. Fig. 4 shows the main layer of the built Simulink model.

On the left side of this layer the blocks *simin* and *Chart* construct incoming "calls" for the activity *1st Level Support*. This signal, represented by a Boolean, gets forwarded to the activity block itself and is there used to determine whether the activity has to be executed or not (0 stands for no execution, 1 represents a "need of execution"). The outcome variables of this block are the signals *Backlog*, *Resourceneeds*, *Next Needs*, *Integrities* and *Degrees*. *Resourceneeds* is used to determine whether the server and PCs are needed. *Backlog* counts the piled up calls. *Integrities* and *Degrees* are the two attributes "Loss of Integrity" (LI) and "Degree of Completion" (DC), both introduced in sections 3.3 and 3.4. They record the state of the attributes' conditions. *Next Needs* is of Boolean type. This signal is usually set to 0. Whenever *1st Level Support* has finished an execution, the signal is set to 1. The *2nd Level* block represents a decision. Whenever the input signal (*In1*) is 1, the block decides whether *2nd Level Support* is needed or not. The block *2nd Level Support* is built in the same way as *1st Level Support*, with the only difference being that there is no output signal *Next Needs*.

The *PCs* and *Server* blocks represent the implemented resources. Both activities need PC availability, server availability and server integrity for successful execution. The input signals (*Needsact1*, *Needsact2*) hold information on the extent of availability/integrity that is needed by the activities. The output signals (*Availabilities*, *Availabilities1* and *Integrity*, *Integrity1*) contain information on the possible degree of availability or integrity the resources are able to provide. This information serves as an input signal for both activities *1st Level Support* and *2nd Level Support*.

The **activity layer** (Fig. 5) is the subsystem of the two

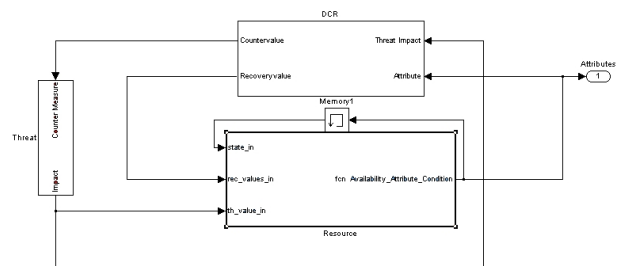


Fig. 6. Simulation Model: **Resource Layer**

activity blocks *1st Level Support* and *2nd Level Support*. It has three input signals: *Initialize*, *Resourcegets Availability* and *Resourcegets Integrity*. The input signal *Initialize* is forwarded to the state flow chart *on/off* which switches the activity on or off. If it is switched on the output signal *on_off* is set to 1. This indicator is forwarded to the out

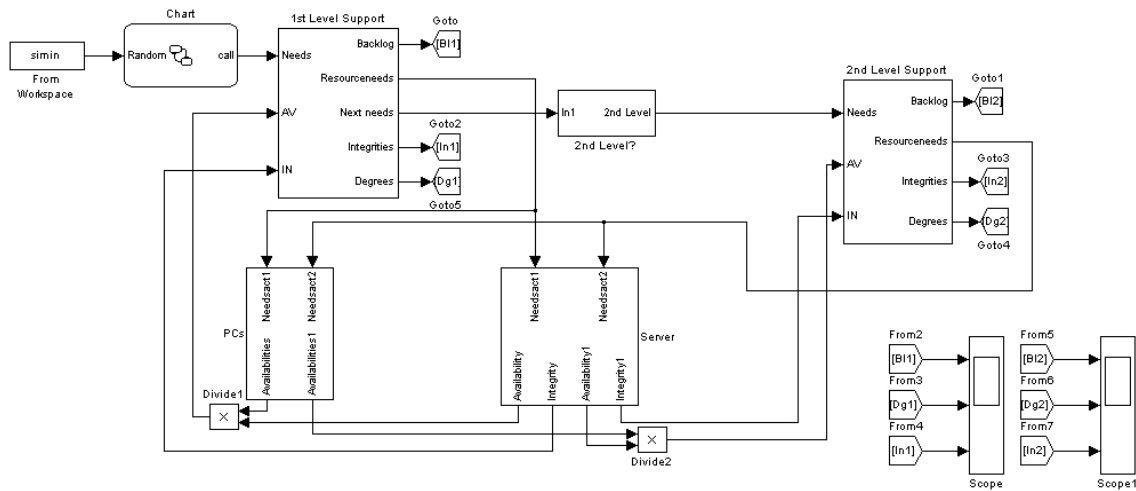


Fig. 4. Simulation Model: **Main Layer**

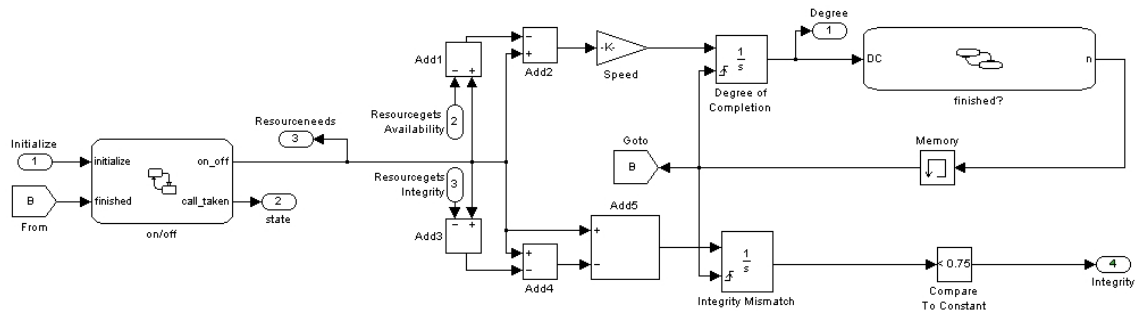


Fig. 5. Simulation Model: **Activity Layer**

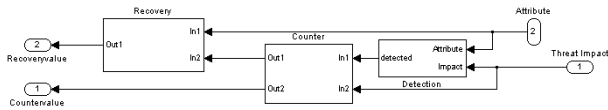


Fig. 7. Simulation Model: **Detection - Counter - Recovery Measure Layer**

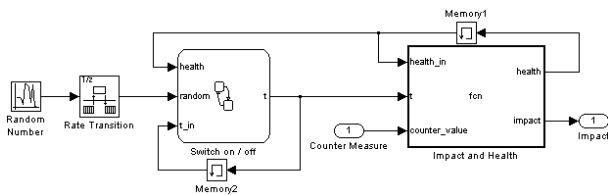


Fig. 8. Simulation Model: **Threat Layer**

port *Resourceneeds* and further used for calculation of DC and LI.

The blocks *Add1* and *Add2* realize $\varphi(t)$, defined in equation (16). According to our formal model (see subsection 3.3), this signal gets integrated into the *Degree of Completion* block. The second input port of this block is only of a technical nature. It is a so-called trigger signal (Boolean) that resets the integral value back to its initial value 0. The *finished?* block determines if the *Degree of Completion* equals 1. If so, an indicator for a finished execution of the activity switches the *on_off* signal in the block *on/off* back to 0.

The same subsystem calculates the LI attribute condition. The blocks *Add3*, *Add4* and *Add5* realize $\varphi(t)$. This function gets integrated into the *Integrity Mismatch* block, according to our formal model (see subsection 3.4). The second input port of the integrator is again a resetting trigger, as described above. This value gets further compared to a changeable constant that determines whether there is enough integrity for a successful execution. This is a result of the fact that integrity is either 1 or 0.

Fig. 6 shows the **resource layer**. This subsystem stands for the two resources *PCs* and *Server*. We chose to describe only one of the two resource layer. It contains two further subsystems: the **threat layer** (Fig. 8) and the **Counter mechanisms layer** (Fig. 7).

For the prototypical simulation we exemplarily simulated two threats on different attributes. The first threat attacks the availability attribute of a resource, the second threat its integrity attribute. This is again implemented in two different subsystems working in the same way. For explanation we focus on the server’s availability.

The **resource layer** contains the *Resource* block, the counter measure mechanisms block *DCR* and a corresponding *Threat* block. The *Resource* block is realized as an embedded Matlab[®] function block. This means that within the block we created a Matlab[®] function that calculates the resource’s condition (*state_in*) at each time step of the simulation. Depending on the input

signals - th_value_in , rec_values_in - the condition is decreasing or increasing respectively. Therefore, the output signal of that block is the attribute's condition (*Availability_Attribute_Condition*). This signal is forwarded to the corresponding DCR block, which is described below. The output signals of the DCR block are: *Countervalue* and *Recoveryvalue*. The counter value serves as input signals for the corresponding *Threat* block, while the recovery value is directly connected to the *Resource* block. The *Threat* block represents the threat's impact value. The input signal *Counter Measure* decreases the threat's health and therefore its impact value, which is sent on to the *Resource* block.

The **detection - counter - recovery measure layer** can be seen in Fig. 7. It contains three blocks, one for each measure. This subsystem has two input signals, *Attribute* and *Threat Impact*, and two output signals, *Countervalue* and *Recoveryvalue*. The input signal *Attribute* is used for the *Recovery* and *Detection* blocks. By the same token, the *Threat Impact* signal serves as input for the *Detection* and *Counter* blocks. The two output signals *Countervalue* and *Recoveryvalue* represent the values of the counter and recovery measure at each time step, which are further used as input signals for the *Threat* block and the *Resource* block from the **resource layer**.

The *Detection* block has two input signals, *Attribute* and *Impact*, which come directly from the **resource layer**. The first one is used to calculate a pointwise detection probability, depending on the attribute's condition function $dm_1(t)$ in our formal model (see section 3.2, equation (5)). The time dependency is only a formal representation. Whenever this value is larger than a certain threshold (determined by random numbers), the threat is said to be detected. In this case, the output signal *detected* is set true, and calls the corresponding counter measure (*Counter* block). The second input signal *Impact* is only used to re-enable the detection measure, as it gets inactive after detecting the threat.

The *Counter* block has two input parameters. The first *In1* comes directly from the *Detection* and is of Boolean nature, the second signal *In2* represents the threat's health resp. impact and comes directly from the *Threat* block in the **resource layer**. Within the block there is an *on/off switch* which is turned "on" once the Boolean signal *In1* is true, which is when the threat is successfully detected. Once the block is activated the block calculates a counter value on the basis of the counter measure function $cm_1(t)$ (see section 3.2, equation (6)) from our formal model. This value is the output signal *Out2*. As long as the threat remains undetected, the counter value is set to 0. The second output signal *Out1* is used as an indicator value for the start of the recovery measure. It is set to 1 once the counter measure has been successful. The *Recovery* block works in a very similar way to the *Counter* block. It has two input signals. *In1* comes directly from the *Resource* block in the **resource layer**, and *In2*, which is the indicator value of the abovementioned *Counter* block. Once the recovery starts, which is when

the indicator is set to 1, the block calculates a recovery value on the basis of the recovery function $rm_1(t)$ defined in the formal model (see section 3.2, equation (8)). This value also serves as the only output signal of the *Recovery* block, and is 0 as long as the counter measure does not activate the recovery measure.

The **threat layer** (Fig. 8) has only one input signal, *Counter Measure*, representing $cm_1(t)$. To decide whether a threat is going to be active, we draw a random number in each time step. Once the block *Random Number* draws a number larger than a certain threshold, the threat occurs. This is realized in *Switch on/off*. Once there is an active threat in a certain time step, *Switch on/off* switches to on and the signal t starts to run at 0, representing the time the threat is active. It is used as an input signal for the *Impact and Health* block. This block calculates the actual *Health* depending on the *Counter Measure* signal. Additionally it determines the *impact* value, depending on the threat's health. This is realized as an embedded Matlab[®] function, which consists of the impact function $\omega_1(t)$. As described in our formal model the basic impact function $\omega_1(t)$ is enhanced with a factor that represents the counter measure value. The enhanced impact function would be $\tilde{\omega}_1(t)$ (see equation 7). This function is used within the *Impact and Health* block to determine the threat's *health* and *impact*. The only output signal *Impact* serves as an input signal for the *Resource* block in the **resource layer** and for the corresponding DCR block.

4.3 Simulation Results

This section discusses the initial results gained from our proof-of-concept simulation of the sample scenario. We compare two different settings where the introduced approach was used and demonstrate how changes in the scenario impact backlogs and revenues of activities.

We simulated two scenarios differing in the quality of the blocking measure of the availability threats. Fig. 9 depicts scenario 1. The implemented blocking measure has a detection rate of 75% for the availability threat and 84% for the implemented integrity threat. The purchase cost of the availability threat blocking measure is set to 12,000\$ and the cost of the integrity threat blocking measure is 7,000\$. As there are no running costs, this would be the only expense for these particular measures. Fig. 9 consists of eight corresponding subplots. **Subplots (f)-(h)** one can see the Integrity impact (h), the condition function of the integrity attribute (g) of the implemented resource and the linked integrity attribute (h) of the overlying activity. We see one successful attack by the threat. It has only a minor influence on the resource's integrity attribute due to its small and short impact. The sudden decrease of the threat's impact function is due to the strong counter measures. This leads to a loss of the activity's integrity attribute. This happens around the simulation time 150-250. The gap in the activity's integrity around the time 50-80 is due to the lack of an activity itself. Regarding the impacts of an integrity loss

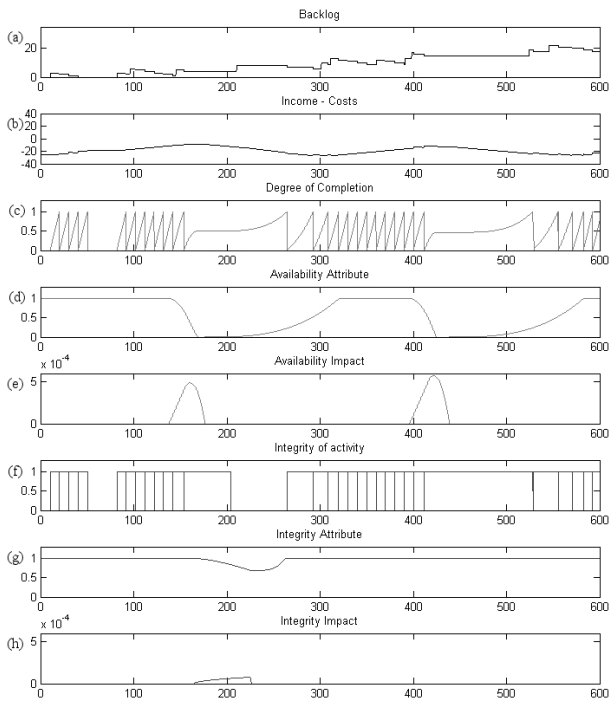


Fig. 9. Simulation Results of Scenario 1. Availability Blocking Measure: 75%

we assume a negative income (i.e. additional costs).

Subplots (c)-(e) show two attacks on the availability attribute of a certain resource, where (e) shows the availability impact, (d) the resource's availability attribute condition and (c) the resulting influence on the activity's completion. We assume an activity to be finished once the completion function is 1; this function can be seen in subplot (c). Due to the less efficient blocking measure (75%), two threats are able to attack successfully. They have a significant effect on the resource's availability, as can be seen in subplot (d). For a short period of time the resource is even completely unavailable. This results in a deceleration of the activity's completion. The counter measure period is rather short in comparison to its recovery period, which takes a particularly long time (d). One can see that even more than one activity experiences a deceleration in completion due to the long recovery period of the needed resource.

In **subplots (a)-(b)** we can now see the overall benefit (b) and the arising backlog (a). Due to the cheap but weak blocking measure and the resulting threats, there is almost no benefit. The counter and recovery periods of the attacked resource cost more than the activity is able to produce, hence the decrease and increase in the benefit function in subplot (b). The backlog is initially good, but in the periods of availability loss the backlog cannot be processed. Fig. 10 shows the simulation results of scenario 2. As mentioned above, the difference lies in the availability threat blocking measure. It now has a detection percentage of 95%, while the integrity threat blocking measure stays the same (84%). Due to the higher quality of the availability threat blocking measure

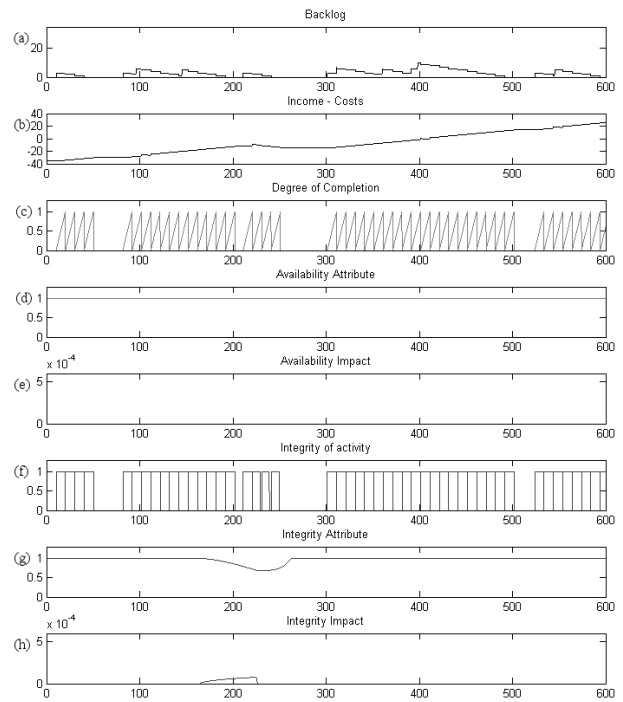


Fig. 10. Simulation Results of Scenario 2. Availability Blocking Measure: 95%

the purchase costs are 22,000\$, 7,000\$ respectively.

Subplots (f)-(h) are exactly the same as in scenario 1. Due to the better availability threat blocking measure, no availability threat is able to attack successfully. This results in a constant impact curve $\equiv 0$, which is represented in chart (e). Therefore, the availability attribute of the resource is constant $\equiv 1$ (d). In this case every activity can be processed in the same predefined time period. The results of this simulation show that the lack of successful threats yields a significant lower backlog (a) and an almost constant increase in benefit (b). The slight dip in the benefit function (b) is due to the successful attack of an integrity threat ((f)-(h)), resulting in negative income for a brief period of time.

When comparing the two scenarios, scenario 2 is clearly the better choice. Despite the higher purchase costs, the benefit of the better availability threat blocking measure is significant, as can be seen in both the subplots (a) and (b).

5 CONCLUSION

The management of processes and the calculation of risks that threaten the meeting of organizational objectives have been performed for decades. However, in recent years, it can be observed that regulative bodies increasingly force companies to take more stringent measures regarding risk and business continuity aspects when economically optimizing their business processes. This new challenge has also been addressed by the scientific community, leading to substantial research results concerning the integration of security and risk aspects into business process analysis and design. Nevertheless,

few research efforts can be found in the simulation-based evaluation of risk impacts on the execution of business processes.

In this paper we presented our current research results in the field of risk-aware business process management. The major contribution of this paper is the introduction of a novel formal model and simulation approach enabling the simultaneous consideration of economic, risk and contingency aspects when analyzing and designing business processes. We introduced a formal model enabling the expression of business process elements as well as relations to and between threats and safeguarding measures. We described our formal model and a prototypical implementation with the professional toolkit Simulink[®] on the basis of a demonstrative sample scenario. We built a formal model consisting of the succeeding key elements: Threats affect attributes of business process elements, such as availability, confidentiality or (indirectly) execution times. Threat preventing or threat defeating measures are grouped into preventive, blocking and reactive measures. Preventive measures affect the occurrence probability of a threat (e.g., no-smoking policy). Blocking measures immediately eliminate a threat once recognized (e.g., anti-virus scanner) giving the threat no chance to harm anything. Reactive measures consist of the three parts Detection, Counter, and Recovery measures: Detection measures can recognize a threat with a defined effectiveness and accordingly invoke appropriate counter and/or recovery Measures. Counter measures try to eliminate an occurred threat, and recovery measures re-establish the intended functionality of attacked attributes. Reactive measures are modeled as processes that, like business processes have a specific process flow and resource requirements. Our novel formal model allows us to map real world scenarios with professional tools like Simulink[®] in order to perform risk-aware business process simulations. The simulation results have been very promising, showing the negative impacts of threats and the positive effects of safeguarding measures on the execution of business processes.

The tailoring of our approach to different situations than presented in the stylized scenario is possible as the introduced formal model provides sufficient flexibility. The required modeling effort depends on the wanted level of granularity. Exemplarily, in the case of a high-level business impact analysis in order to determine the order of impacts' magnitude and the greater overview about dependencies between processes and resources the required effort is rather low. However, one must not forget the effort for the information gathering phase. Business specialists have to be questioned in order to determine process activities, connections to resources (e.g. required services) and potential risk scenarios. Subsequently, technical specialists have to enrich the model with details of the underlying infrastructure (e.g. server cluster) and assessment of related information and communication technology risks.

The application of our proposed method is expected to render the following benefits: (1) Integrated modeling of business processes, risks as well as detection, counter, and recovery measure information. Consequently, this allows the simulation of threats and safeguard measures on attributes of business process elements, such as the availability or integrity of a resource. Subsequently, impacts on business process executions can be derived in a simulation-based way. (2) Identification of single points of failure or substantial weaknesses in resource planning and allocation. Simulation-based determination of resource requirements of business processes with regard to numerous threat scenarios. (3) Provision of valuable information concerning the justification of security/contingency investments when simulating different threatening and mitigation scenarios. Metrics such as the maximum tolerable period of disruption (MTPD) or mean time between failures (MTBF) can easily be determined. These may again serve as valuable input, e.g., for reviewing service level agreements. (4) Simulation-based support of target-performance evaluations enhancing continuous process improvement cycles.

Currently, we focus on two further research challenges that extend our formal model and simulation approach: (1) Extension of the formal model to consider service level management aspects (e.g., planning service level agreements from a requester's view or analyzing impacts of resource disruption regarding agreement breaches from a provider's view), and (2) dynamic resource re-allocation taking into consideration resource requirements of counter and recovery measures and priorities of business processes affecting this re-allocation.

We are convinced that our approach has the potential to find its way into business process analyzing and planning domains where it would provide substantial support in the integrated consideration of economic as well as risk and continuity aspects.

REFERENCES

- [1] G. Inc., "Misconceptions on process optimization and simulation." Gartner Blog, 2009.
- [2] *NIST Special Publication 800-30, Risk Management Guide for Information Technology Systems*, National Institute of Standards and Technology (NIST) Std., 2002.
- [3] BSI (German Federal Office for Information Security), "IT-Grundschutz Manual (english version)," 2004.
- [4] *ISO/IEC 13335-1:2004, Information technology - Security techniques - Management of information and communications technology security - Part 1: Concepts and models for information and communications technology security management*, ISO/IEC Std., 2004.
- [5] *NIST SP800-61: Computer security incident handling guide*, National Institute of Standards and Technology Std., 2004.
- [6] *British Standard BS25999-1:2006: Business Continuity Management - Part 1: Code of practice*, British Standard Institute (BSI) Std., 2006.
- [7] *British Standard BS25999-2:2007: Business Continuity Management - Part 2: Specification*, British Standard Institute (BSI) Std., 2007.
- [8] *ISO/IEC 24762:2008 Information technology - Security techniques - Guidelines for information and communications technology disaster recovery services*, ISO/IEC Std., 2008.
- [9] European Network and Information Security Agency (ENISA), "Business and it continuity overview and implementation principles," 2008.
- [10] Department for Business, Enterprise & Regulatory Reform (BERR), "2008 information security breaches survey," 2008.
- [11] Business Continuity Institute, "Good Practice Guidelines," 2008. [Online]. Available: <http://www.thebci.org/gpgdownloadpage.htm>

- [12] J. Burtles, *Principles and practice of business continuity*. Rothstein Associates Inc, 2007.
- [13] Gartner Inc, "Gartner exp worldwide survey of more than 1.500 cios shows it spending to be flat in 2009," 2009. [Online]. Available: <http://www.gartner.com/it/page.jsp?id=855612>
- [14] AON, "Global risk management survey '09," 2009. [Online]. Available: <http://www.aon.com/2009risksurvey>
- [15] The MathWorks, "Simulink - simulation and model-based design." [Online]. Available: <http://www.mathworks.com/products/simulink>
- [16] ISO/IEC 27005:2008 *Information technology - Security techniques - Information security risk management*, ISO/IEC Std., 2008.
- [17] CERT. (2009) OCTAVE. [Online]. Available: <http://www.cert.org/octave>
- [18] MIL-STD-1629: *A Military standard - Procedures for performing a failure mode effects and critically analysis*, Department of Defense Std., 1980.
- [19] S. Kmenta and K. Ishii, "Scenario-based fmea: A life cycle cost perspective."
- [20] British Standards Institution, "Pas56," 2003.
- [21] ISO/PAS 22399:2007: *Societal security - Guideline for incident preparedness and operational continuity management*, ISO/PAS Std., 2007.
- [22] National Institute of Standards and Technology, "Nist sp800-34: Contingency planning guide for information technology systems," 2002.
- [23] *Business Process Modeling Notation (BPMN) 1.2*, Object Management Group (OMG) Std.
- [24] A. W. Scheer and M. Nüttgens, "Aris architecture and reference models for business process management," in *BPM*, 2000.
- [25] *Workflow Management Coalition Specification The Workflow Reference Model*, Workflow Management Coalition Std.
- [26] D. Karagiannis, S. Junginger, and R. Strobl, *Business Process Modelling*. Springer, Berlin, 1996, ch. Introduction to Business Process Management Systems Concepts, pp. 81–106.
- [27] M. zur Muehlen and M. Rosemann, "Integrating risks in business process models," in *Australasian Conference on Information Systems (ACIS 2005)*, 2005.
- [28] D. Neiger, L. Churilov, M. zur Muehlen, and M. Rosemann, "Integrating risks in business process models with value focused process engineering," in *European Conference on Information Systems (ECIS 2006)*, 2006.
- [29] N. Milanovic, B. Milic, and M. Malek, "Modeling business process availability," in *IEEE International Conference on Services Computing (SCC 2008)*, 2008.
- [30] S. Sackmann, "A reference model for process-oriented it risk management," in *16th European Conference on Information Systems*, 2008.
- [31] S. Sackmann, L. Lewis, and K. Kittel, "Selecting services in business process execution - a risk-based approach," in *Business Services: Konzepte, Technologien, Anwendungen, Tagung Wirtschaftsinformatik (WI09)*, 2009.
- [32] S. Röhrig, "Using process models to analyse it security requirements," Ph.D. dissertation, University of Zurich, 2003.
- [33] A. Rodriguez, E. Fernández-Medina, and M. Piattini, "Towards a uml 2.0 extension for the modeling of security requirements in business processes," in *International Conference on Trust and Privacy in Digital Business (TrustBus 2006)*, 2006.
- [34] R. J. Ellison, R. C. Linger, T. Longstaff, and N. R. Mead, "Survivable network system analysis: A case study," *IEEE Software*, vol. 16, pp. 70–77, 1999.
- [35] T. Neubauer, M. Klemen, and S. Biffl, "Business process-based valuation of it-security," in *Economics-driven software engineering research (EDSER 2005)*, 2005.
- [36] A. Sienu, E. Lamine, and H. Pingaud, "A method for integrated management of process-risk," in *1st International Workshop on Governance, Risk and Compliance - Applications in Information Systems (GRCIS'08)*, 2008.
- [37] I. Weber, G. Governatori, and J. Hoffmann, "Approximate compliance checking for annotated process models," in *1st International Workshop on Governance, Risk and Compliance - Applications in Information Systems (GRCIS'08)*, 2008.
- [38] S. Sadiq, G. Governatori, and K. Namiri, "Modelling control objectives for business process compliance," in *5th International Conference on Business Process Management (BPM2007)*, 2007.
- [39] A. Jallow, B. Majeed, K. Vergidis, A. Tiwari, and R. Roy, "Operational risk analysis in business processes," *BT Technology Journal*, vol. 25, 2007.
- [40] M. Modarres, M. Kaminskiy, and V. Krivtsov, *Reliability Engineering and Risk Analysis: A Practical Guide*, 2nd ed. CRC Press, 2009.
- [41] H. Wang and H. Pham, *Reliability and Optimal Maintenance*, ser. Springer Series in Reliability Engineering. Springer London, 2006, ch. Monte Carlo Reliability Simulation of Complex Systems, pp. 275–294.
- [42] B. L. A. Naessa and O. Batsevych, "System reliability analysis by enhanced monte carlo simulation," *Structural safety*, vol. 31, no. 5, pp. 349–355, September 2009.
- [43] S. Jakoubi, G. Goluch, S. Tjoa, and G. Quirchmayr, "Deriving resource requirements applying risk-aware business process modeling and simulation," in *16th European Conference on Information Systems*, 2008, pp. 1542–1554.
- [44] S. Tjoa, S. Jakoubi, and G. Quirchmayr, "Enhancing business impact analysis and risk assessment applying a risk-aware business process modeling and simulation methodology," in *International Conference on Availability, Reliability and Security*, 2008, pp. 179–186.
- [45] S. Jakoubi, S. Tjoa, and G. Quirchmayr, "Rope: A methodology for enabling the risk-aware modelling and simulation of business processes," in *Fifteenth European Conference on Information Systems*, 2007, pp. 1596–1607.
- [46] S. Tjoa, S. Jakoubi, G. Goluch, and G. Quirchmayr, "Extension of a methodology for risk-aware business process modeling and simulation enabling process-oriented incident handling support," in *Advanced Information Networking and Applications*, 2008, pp. 48–55.
- [47] S. Jakoubi and S. Tjoa, "A reference model for risk-aware business process management," in *International Conference on Risks and Security of Internet and Systems*. IEEE, 2009.
- [48] British Telecom, "Business continuity - bt data centre services," accessed July 2009. [Online]. Available: <http://business.bt.com/it-solutions/it-services/data-centre-services/business-continuity>

Simon Tjoa received a master's degree in business informatics from the University of Vienna. He is a research scientist at the St. Pölten University of Applied Sciences. His current research interests include business continuity management and business process security. He is a member of the IEEE and IEEE SMC.

Stefan Jakoubi received a master's degree in business informatics from the University of Vienna. He is a researcher at the IT-Security competence center Secure Business Austria. He is a member of the IEEE, ISACA, and associate member of the BCI. His research interests focus on business continuity management, business process management and aspects of organizational security.

Gernot Goluch received the BSc and MSc degrees from Vienna University of Technology. He is researcher at teh competence center Secure Business Austria. He is a member of the IEEE and his work focuses on the research area of risk with a focus on simulation approaches and formal modeling.

Gerhard Kitzler is currently working as researcher at the IT-Security competence center Secure Business Austria. His research interests include numerics of differential equations, modeling and simulation.

Sigrun Goluch is researcher at the IT-Security competence center Secure Business Austria. Her research focuses on graph theory, modeling and simulation.

Gerald Quirchmayr holds doctors degrees in computer science and law from Johannes Kepler University in Linz and currently is Professor at the Department of Distributed and Multimedia Systems at the University of Vienna. His research focus is on information systems in business and government with a special interest in security, applications, formal representations of decision making and legal issues. In 2002 he was appointed as Adjunct Professor at the School of Computer and Information Science of the University of South Australia.