Integration of an Ontological Information Security Concept in Risk-Aware Business Process Management

Gernot Goluch*, Andreas Ekelhart*, Stefan Fenz*, Stefan Jakoubi*, Simon Tjoa* and Thomas Mück†
*Secure Business Austria, Vienna, Austria
Email: {ggoluch, aekelhart, sfenz, sjakoubi, stjoa}@securityresearch.at
†Austrian Social Insurance Authority for Business, Vienna, Austria
Email: thomas.mueck@sva.sozvers.at

Abstract— **The ability to prevent risks as well as to appropriately counteract occurring threats has increasingly become a crucial success factor. Traditional business process management provides concepts for the economical optimization of processes, while risk management focuses on the design of robust business processes. While aiming at the same goal, namely the improvement of business, the approaches how to reach this vary, due to a different understanding of improvement. Following this, optimizing recommendations of business process management and risk management may be contradictory. Therefore, we proposed a unified method, integrating both points of views to enable risk-aware business process management and optimization. In this paper, we briefly describe the ROPE (Risk-Oriented Process Evaluation) methodology and the Security Ontology concept, which provides a solid knowledge base for an applicable and holistic company specific IT security approach. This heavy-weight ontology provides structured knowledge regarding the relations between threats, safeguards, and assets, which are crucial for modeling processes in ROPE. We show how the integration of the Security Ontology's knowledge base enhances the applicability of the ROPE methodology leading to improved risk-aware business process management.**

I. Introduction

One of companies' main challenges is the effective and efficient performing of their business processes while simultaneously guaranteeing their maximum robustness and security [1] [2]. The domains covering these tasks are business process management on the one side and risk management as well as business continuity management on the other side. Business process management aims at optimizing a company's processes regarding economical aspects, while risk management's and business continuity's ambitions are to design robust business processes in order to strengthen the resilience of day-to-day business [3] [4] [5]. Both worlds try to advance and mature business, but they achieve their goals with different focuses, which may lead to contradictory improvement recommendations. Wide-accepted methods and practices in the field of business process management [6] [7] [8] and in the area of risk management as well as business continuity management exist [3] [4] [9] [10] [11] [12], but the discovery of an already existing method, which comprehensively combines the domains' capabilities, has been a challenging task.

Although risk management approaches differ in their specific implementation, the majority of the methods consist at least of the following stages. The first step to enable an appropriate risk management is to identify potential risks. In order to develop a strategy to handle these risks, it is of great importance to assess and prioritize them. After implementing the strategy, risks have to be monitored. Monitoring is essential to react on changing risks. The evaluation of the strategy supports the improvement of an organization's risk management. [3] [4] [9] [10] [11] [13]

Business continuity management (BCM) is a management process to improve the resilience of a company including unexpected catastrophes (e.g., earthquakes, fire, or flooding). Within its domain, the Good Practices Guideline [9] of the Business Continuity Institute[1] is widely-accepted and followed by governmental institutions and industry. The underlying life cycle covers six main topics: (1) establishment of a BCM policy and a BCM program management, (2) understanding the organization, (3) determining BC strategies, (4) developing and implementing BCM response, (5) exercising, maintaining and reviewing BCM arrangements, and (6) embedding BCM in the organization's culture.

Methods emerging from the business process world consider risk and business continuity issues rather separated than integrated. Focusing on risk management or business continuity management, business driven optimization and business process simulations are not adequately realized. As a consequence, we propose a methodology which combines the strengths and benefits of both worlds and thus, we antecedent introduced our ROPE (Risk-Oriented Process Evaluation) methodology [14] [15] [16], which enables risk-aware business process management. This integration leads to the simultaneous optimization of efficiency and security of business processes.

Previous research has shown that the ROPE methodology is applicable, however there is still optimization potential regarding real world appliance. The risk management domain

[1] Business Continuity Institute: http://www.thebci.org, last access: 20 August 2007

1530-1605/08 $25.00 © 2008 IEEE

is complex and requires knowledge about assets and their values, vulnerabilities, threats, threat probabilities, and the economic balance between the impact of threats and costs of countermeasures [17]. ROPE's main focus is on risk-aware business process modeling and simulation, but mechanisms for modeling and storing risk management knowledge can be further improved. To make full use of the described optimization potential we combine the ROPE methodology with the Security Ontology [18] [19], an ontology covering major aspects of the risk management domain, including a general classification as well as concrete data on threats, vulnerabilities, assets, countermeasures and threat probabilities.

Thus, we present in this paper our ROPE methodology and discuss the optimization potential of the existing knowledge representation within ROPE on the one hand and our concrete improvement considerations by integrating the Security Ontology on the other hand. Additionally, the ROPE framework is enriched with a classification of threats, their countermeasures, and the threatened assets provided by the Security Ontology.

II. The need for a conceptual schema about IT security

Nowadays, companies are increasingly interconnected and dependent on IT, which makes IT security a very important field for guaranteeing business continuity [20] [21] [22]. Driven by legislation (e.g., Basel II [23] and Sarbanes-Oxley Act [24]), IT security is no longer considered as only a costly responsibility that generates minor additional business benefit and value for the organization; management is compelled to pay more attention to implement an appropriate IT security approach. We thus need a conceptual schema to clarify the meaning and interdependence of IT security relevant terms which then can be used to improve risk analysis and threat simulation processes [19].

On this account we developed a conceptual schema about IT security, namely the Security Ontology [18], which is based on the security relationship model proposed by the National Institute of Standards and Technology [25] (compare Figure 1). A brief description about the fundamental model should clarify the idea how this concept helps to improve the simulation results of the ROPE methodology. Threats, vulnerabilities and safeguards are the pivotal elements: a threat exploits an existing vulnerability and therefore represents a potential danger to corporate assets and is initiated by a threat agent. To pose a risk to an organization, a threat has to exploit a vulnerability, via a physical, technical or administrative weakness, and cause damage to defined assets. Safeguards have to be installed, and applied respectively, to mitigate an identified vulnerability and to protect the corresponding assets by either preventive, corrective or detective measures.

One shortcoming of the ROPE methodology is that it initially lacks of a proper knowledge base regarding concrete knowledge about threats, threat probabilities, vulnerabilities, assets, and countermeasures. The Security Ontology provides a framework which includes knowledge about threats and their

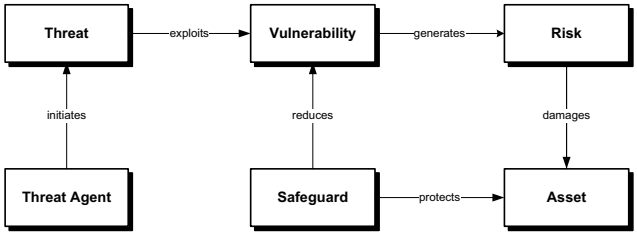

Fig. 1. Security Relationships

side effects on a highly granular level; ROPE benefits from that knowledge as follows:

- Knowledge about threats and the threatened infrastructure elements is provided, which eases the ROPE modeling process significantly.
- A standardized infrastructure element classification, which follows the United Nations Standard Products and Services Code [26] and includes ontological restrictions, ensures that ROPE is provided with a comprehensive infrastructure model to enhance the simulation results (e.g., each computer server has to be assigned to a physical location).
- Within the Security Ontology each infrastructure element contains risk management relevant attributes such as delivery time and asset costs, which are required for the quantitative risk assessment in ROPE.

The reason for describing the IT security domain by an ontology and not by a relational database solution is to share the common domain understanding and the possibility to reuse existing knowledge to make domain assumptions explicit [27]. Furthermore, the usage of a well-defined ontology enables inference engines to infer new knowledge based on existing facts and rules, and reasoner engines to maintain consistency. The Security Ontology represents a ready-to-use but extendable knowledge set, which has to be filled with concrete data about the corporate assets, which will be stored as instances of the already modeled asset classes. As a result corporate assets are related with the corresponding threats, threat probabilities, vulnerabilities, and countermeasures.

The details about how the ROPE methodology benefits from the Security Ontology concept can be found within subsection III-A and III-B. [19] and [18] provide an in-depth description of the ontology.

III. ROPE

Within this section, we briefly describe the ROPE methodology introduced in [14], which enables the risk-aware management and simulation of business processes. Therefore, we give a brief description of the methodology's processes, but concentrate on the modeling and simulation aspects. This focus enables our subsequent discussion concerning the integration of the Security Ontology into ROPE.

The ROPE methodology consists of five iterative processes derived from the BPMS Business Processing Modeling Systems Paradigm [6]. The *strategic decision process* is re-

sponsible for identifying the overall goals, which should be reached by implementing ROPE. This includes at least (1) the determination and prioritization of the business processes which have to be considered, (2) financial and temporal scopes of the project and (3) responsibilities. Furthermore, measurable success criteria have to be defined in order to perform adequate evaluations. Within the *re-engineering process*, the information gathered within the initial process is utilized to design a target model for the identified and prioritized business processes. To be able to create the target model the process itself consists of five stages. As mentioned above, the focus of this introduction is on this process. On this account the five stages are succeeding described in-depth. The *resource allocation process* aims at acquiring, assigning and coordinating required resources to ensure the risk-aware execution of the re-designed business processes. Within the *workflow execution process* the business processes are executed at a workflow level through the application of a workflow management system. The output of the workflow execution is the basis for the *performance evaluation process*, where qualitative and quantitative evaluations are performed to enable further improvements of the business processes.

As outlined before the focus of this section is the risk-aware business process modeling and simulation, which takes place within the re-engineering process. This process itself consists of five iterative stages, which result in the target model. The tasks of the *criteria selection stage* include the determination of the key characteristics for securing the selected business processes, where essential information is obtained from the output of the strategic decision process. The *acquisition stage* focuses on business process activities, which are examined in detail by ROPE in order to enable adequate risk-aware considerations. Therefore, a business process activity is refined into four atomic element types: *Conditions*, *Actions*, *Resources* and *Environments* (CARE). As stated in [14] an activity consists of actions which are executed by resources within certain environments; the relation between *Actions*, *Resources* and *Environments* is expressed by *Conditions*. The refinement of an activity is modeled by means of CARE diagrams. As a business process activity is directly dependent on the functionality of its CARE elements, it is essential to investigate the impacts of threats on CARE elements and how to counteract those. Thus, CARE elements have to be analyzed within this stage to identify existing threats and countermeasures. This information serves as basis for the process-oriented representation of the determined threats, countermeasures and recovery measures. This representation later on enables the risk-aware business process simulation. The information concerning the behavior of threats, countermeasures and recovery measures is modeled in so called TIP (Threat Impact Process) diagrams. A challenging but all the more essential task in the context of the acquisition stage is the most accurate identification of threat occurrence rates. The determination of threat incidence rates is absolutely important for valid simulations, thus they have to be carefully determined and estimated. Figure 2 shows schematically the refinement of the business process activity; the CARE and TIP diagrams are discussed in detail within sub-sections III-A and III-B.

Within the *analysis stage*, the outcome of the previous stage is investigated in order to identify new potential threats and as a consequence required countermeasures. The output of the risk-aware business process simulation delivers the fundamentals for improving the selected business processes. The gathered information is evaluated to determine the impact of threats on CARE elements. The evaluation process yields information required for the target model. The aim of the design stage is the improvement of an as-is model towards the target model and consists of following steps [14]:

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

In the *evaluation stage* it is analyzed if the target model meets criteria defined within the criteria selection stage. If necessary the process returns to previous stages.

Our approach, as it is a generic concept, is applicable for every type of business process and security threat as long as it can be represented in a process-oriented way. In practice, the feasible level of granularity and accordant cost / benefit considerations defines the appropriate modeling scope. From a business process modeling point of view, one definitely will model the server landscape of your company as well as associated security threats, but will hardly model the components and assemblies (e.g., wiring or resistors) of each server. The modeling complexity would significantly increase while it is doubtful, if the simulation results would substantially benefit from this higher technical level of detail.

At the current state of research the ROPE simulation covers two approaches: (1) through a *path analysis* during the TIP simulation all possible paths and their occurrence rates can be identified. This leads to the determination of the execution time and cost of each TIP path. (2) the *simulation of threat impacts* enables the determination and visualization of an occurred impact on the execution of a business process and the corresponding countermeasures. Business process activities consist of multiple CARE elements which face threats. Occurred threats decrease the functionality of assigned CARE elements until they reach their non-functional stadium or countermeasures successfully terminate the threats. Once a threat is eliminated, recovery measures may restore the functionality of affected CARE elements.

Figure 3 shows four iterations of an example business process. The first two process iterations can perform under normal conditions, while within the third iteration, an occurred threat impacts the CARE elements of activity B. As a consequence, the execution of this activity is suspended for the downtime of the affected elements. This directly influences the succeeding iterations, as schematically shown in the figure.

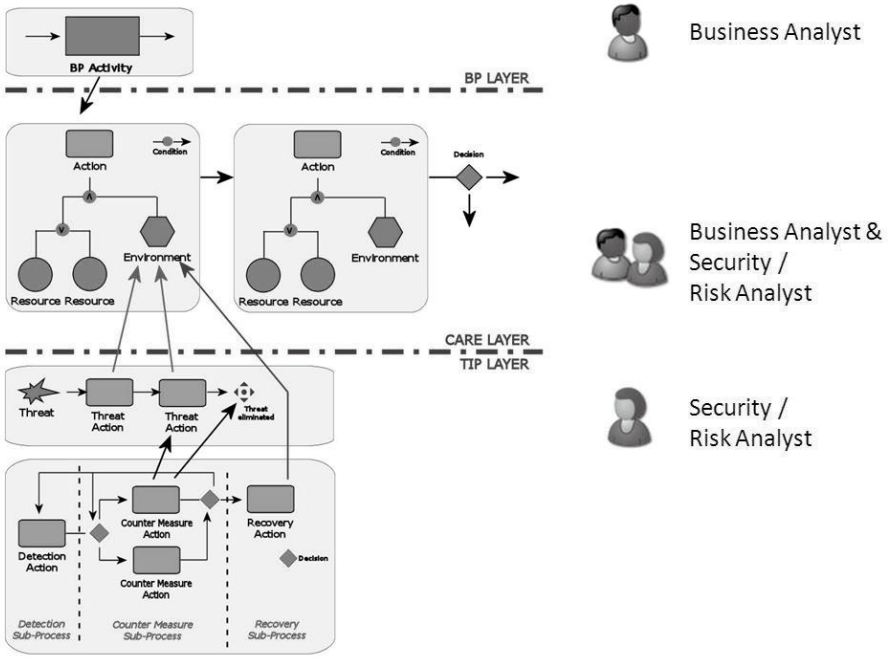

Fig. 2. ROPE Overview

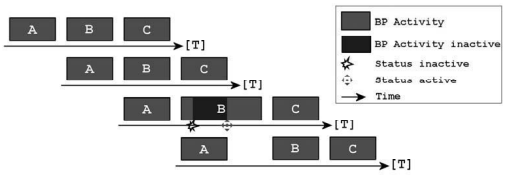

Fig. 3. Business Process Activity Temporal Shifts

A. CARE Layer

To refine business process activities we use the CARE (Condition, Action, Resource and Environment) diagram (compare Figure 2). An activity consists of *Actions* which are executed by *Resources* within specific *Environments*. Constraints and relationships between *Actions*, *Resources* and *Environments* are modeled as *Conditions* within the CARE diagram. Those relations describe the dependency between elements (logical relations), which are represented by edges. Due to the fact that CARE elements are temporarily dependent on each other, delays that are caused by the unavailability of one or more elements have to be added to the execution time.

Utilizing the Security Ontology's infrastructure classification: The infrastructure section of the Security Ontology contains a wide range of physical elements which are utilized within an organization. Parts of the categorization such as the IT and telecommunication branch follow established standards like the United Nations Standard Products and Services Code [26] to ensure a standardized structure. To guarantee that the entire organization can be mapped to the ontology, the *Infrastructure* sub-ontology also provides structural elements which enable the mapping of the physical environment elements, such as buildings, floors, rooms, windows or doors.

These elements perfectly fit on the one hand to the *Resource* and on the other hand to the *Environment* elements within the CARE concept. Relation 1 and 2 in Figure 4 schematically represent the mapping of the Security Ontology's elements *company1:PhoneServer* and *company1:ExchangeServer* to the corresponding *Resource* elements in the CARE diagram. Concerning *Environment* elements, several ontology elements, such as instances of the ontology classes *ent:Building* or *ent:Room*, provide the required company data for the modeling phase in ROPE (see Relation 4 in Figure 4). Furthermore, classes and corresponding instances located in the *ent:Role* tree of the Security Ontology provide the basis for human CARE resources.

Listing 1 shows a code snippet from the Security Ontology regarding the ontological representation of concrete corporate assets. The snippet shows an instance of the *ent:ComputerServer* class, namely the exchange server of the company. The physical location (room R0101), the delivery time (5 days), and the asset costs (3000$) are stored within the ontology and can be used by ROPE for the quantitative risk assessment.

```
<ent:ComputerServer
 rdf:about="http://www.company1.com#ExchangeServer">
```

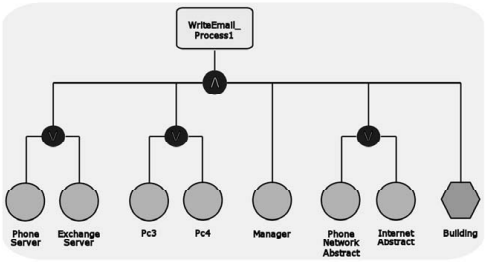

Fig. 5. CARE Example Element

```
<ent:infrastructureLocatedInRoom>
  <ent:Room rdf:about="http://www.company1.com#R0101">
  </ent:Room>
</ent:infrastructureLocatedInRoom>
<ent:deliveryTime rdf:datatype="xsd:int"
>5</ent:deliveryTime>
<ent:assetCost rdf:datatype="xsd:int"
>3000</ent:assetCost>
</ent:ComputerServer>
```

Listing 1. OWL representation of computer server instance *company1:ExchangeServer*

CARE *Action* elements are represented within the *bdpsi* namespace of the *Security Ontology*. The root class of this namespace is the *bdpsi:Action* class, from which all succeeding classes and instances are derived. In Figure 4 the action *WriteEMail_Process1* is mapped to the CARE *Action* element via the schematically represented Relation 3.

As described before, within the ROPE methodology it is possible to link CARE elements via logical operators to enable complex connections. Table I shows these logical links in the ontology representation. An *Action* element in the Security Ontology has several different relations to other ontology elements (e.g., action *WriteEMail_Process1* has a relation to element *ent:ComputerServer*). This set of *n* relations represents *n AND-linked* operators between CARE elements. Figure 5 illustrates the exemplary CARE element.

Within one relation, *n* instances of the related class are provided (e.g., the relation *bdpsi:writeEMailRequiresComputerServer* links to either the instance *company1:PhoneServer* or *company1:ExchangeServer*). This set of *n* instances represents *n OR-linked* relations between CARE elements.

The above described mapping of the relevant Security Ontology elements to CARE elements provides the required basis for the further appliance of the TIP concept (see subsection III-B).

B. TIP Layer

The TIP (Threat Impact Process) diagram (compare Figure 2) describes the impact of threats and countermeasures on CARE elements and their behavior. An action, which directly influences the occurrence probability of a threat, is a *preventive countermeasure*. By contrast a *reactive countermeasure* counteracts already occurred threats. The TIP diagram provides four main application areas: (1) support for identifying potential risks, (2) documentation and visualization of risks, (3) guidance in case of emergency through process oriented representation of counter and recovery measures, and (4) risk impact determination through simulation.

The iterative TIP process consists of the detection, countermeasure and recovery sub-processes. Within the *detection* sub-process the specific threat is detected; the way of the detection influences the determination of selected countermeasures. The *countermeasure* sub-process directly influences threats. If countermeasures cannot eliminate the threat, the corresponding CARE element(s) are affected with full impact. Furthermore, the *recovery* sub-process provides actions to rebuild the affected CARE element's functionality. Each sub-process runs at least through one iteration of the sequence assessment and reaction. State changes of threats or modifications of the functionality of CARE elements may be caused by the execution of the processes. [14] provides more details on the TIP concept and simulation.

Utilization of the Security Ontology for TIP modeling: Due to the usage of the Security Ontology concepts during the CARE modeling phase, each CARE element is represented by an instance coming from the Security Ontology. Because each threat impact process is modeled for a certain threat we can extract the threatened infrastructure from the Security Ontology by a simple web service query which results in a dataset of the threatened infrastructure as shown in Listing 2:

```
<sec:Fire rdf:about="http://www.abs.com#Fire">
  <sec:threatThreatens rdf:resource=
   "http://www.company1.com#Pc4"/>
  <sec:threatThreatens rdf:resource=
   "http://www.company1.com#Pc1"/>
  <sec:threatThreatens rdf:resource=
   "http://www.company1.com#Pc5"/>
  <sec:threatThreatens rdf:resource=
   "http://www.company1.com#DevelopmentServer"/>
  <sec:threatThreatens rdf:resource=
   "http://www.company1.com#PhoneServer"/>
  <sec:threatThreatens rdf:resource=
   "http://www.company1.com#Pc2"/>
  <sec:threatThreatens rdf:resource=
   "http://www.company1.com#FileServer"/>
  <sec:threatThreatens rdf:resource=
   "http://www.company1.com#Pc6"/>
  <sec:threatThreatens rdf:resource=
   "http://www.company1.com#Pc3"/>
  <sec:threatThreatens rdf:resource=
   "http://www.company1.com#Pc7"/>
  <sec:threatThreatens rdf:resource=
   "http://www.company1.com#ExchangeServer"/>
</sec:Fire>
```

Listing 2. Infrastructure elements, threatened by the threat *Fire*

The *Threat* sub-ontology built upon Peltier's threat classification presented in [28] comprises natural, accidental and intentional threats at the highest level, followed by a detailed sub-classification. An in-depth threat description, as well as endangered security objectives (availability, reliability, safety, confidentiality, integrity, maintainability), following the security- and dependability taxonomy referring to [29] are

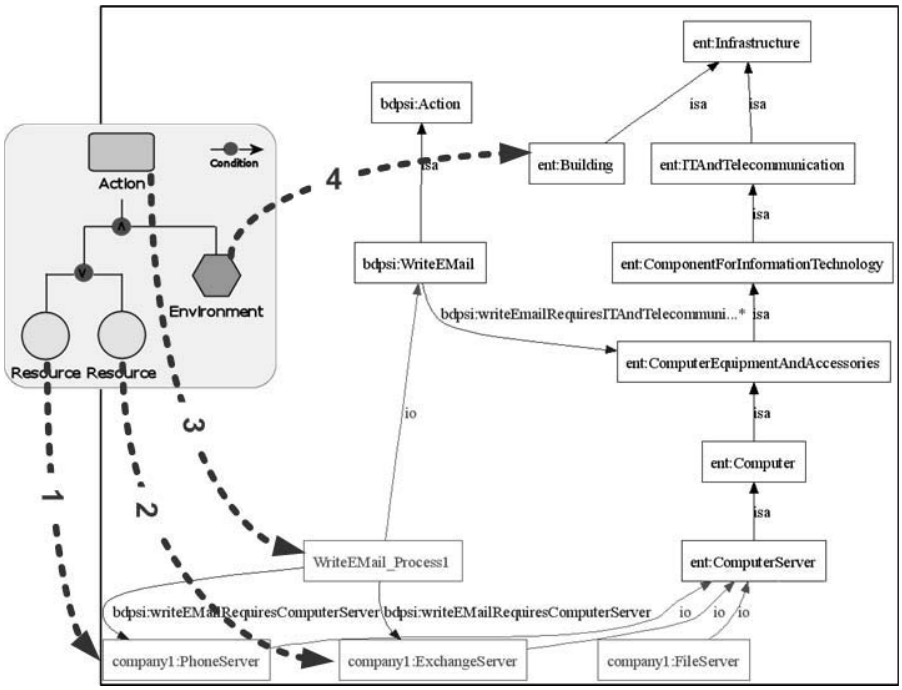

Fig. 4. CARE - Security Ontology Mapping

TABLE I
AND-linked RELATIONS OF ACTION ELEMENT *WriteEMail_Process1*

Relation Name	**Element**
bdpsi:writeEMailRequiresComputerServer	company1:PhoneServer **OR** company1:ExchangeServer
bdpsi:writeEMailRequiresITAndTelecommunicationDevice	company1:Pc3 **OR** company1:Pc4
bdpsi:writeEMailRequiresNetwork	abs:PhoneNetwork **OR** abs:Internet
bdpsi:writeEMailRequiresWriterRole	ent:Manager

provided for each threat. This is essential, if a company wants to prioritize its IT security strategy regarding the above mentioned dependability attributes. The occurrence of a threat often gives rise to or intensifies other threats, therefore these relationships are reflected in the ontology. Furthermore, each threat exploits one or more vulnerabilities which can be found in the *Vulnerability* sub-ontology. Understanding the relationships between threats and endangered assets, which are reflected by elements in the *Infrastructure* sub-ontology, is vital for a comprehensive security planning and thus these connections are integrated.

Vulnerabilities can be reduced by installing infrastructure resources (coming from sub-ontology *Infrastructure*), implementing organizational controls (coming from sub-ontology *Control*), and/or deploying specific software products (coming from sub-ontology *Software*), depending on the vulnerability's nature.

Organizational countermeasures are stored in the *Control* sub-ontology, which provides atomic controls derived from best-practice standards, guidelines, baselines, procedures and security frameworks such as ISO27001 [30], ISO17799 [11], CobiT [31], ITIL [32] and IT-Grundschutz Manual (literally, IT-Basis Protection Manual) [10]. For of a given threat the user, which models the detection, countermeasure, and recovery sub-processes in ROPE, is able to use controls which are mapped to the aforementioned standards to ensure that best practices are integrated.

On the infrastructure side of vulnerability mitigation, certain countermeasures demand other countermeasures to be effective, e.g. a fire extinguishing system depends on fire detectors. By adding links between these infrastructure elements this requirement can be modeled and helps the user modeling proper countermeasures within the countermeasure sub-processes in ROPE. Because detection and countermeasure actions can be implemented by several infrastructure elements the Security Ontology guides the user with possible detection (e.g., smoke detector, heat detector, ...) and countermeasure (e.g., pre-action pipe, hand fire extinguisher, ...) devices depending on the given threat (e.g., fire).

Figure 6 illustrates the mapping between the TIP diagram and the Security Ontology's threat, vulnerability and safeguard representation. Relation 2 in Figure 6 represents the mapping of the threat element *sec:PingOfDeath* to the corresponding threat elements in the TIP diagram. To support the TIP

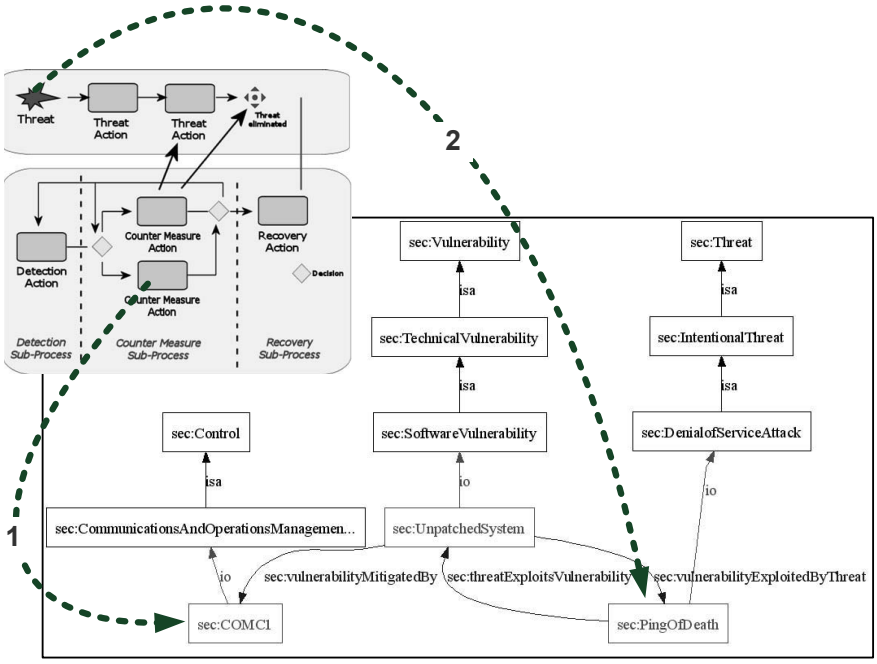

Fig. 6. TIP - Security Ontology Mapping

modeling user with further information about the threat, the Security Ontology provides information about the vulnerabilities associated with a given threat. The safeguard elements are mapped via Relation 1 (compare Figure 6) to a TIP detection, countermeasure or recovery action.

IV. Proof of Concept Prototype

We developed a proof of concept prototype to demonstrate how the introduced concepts could be realized by a toolset. The implementation of the prototypical application should test the feasibility of the approach and the added value gained through the combination of the Security Ontology with our approach of risk-aware process modeling and simulation (ROPE).

A. The Architecture

Our prototypical application consists of three core components as outlined in Figure 7:

- Security Ontology Web Service
- Business Process Modeling Tool ADONIS®
- Risk-Aware Business Process Simulation Engine

The communication between the services is performed via a XML-based exchange format. This ensures that the prototype is as flexible and extendable as possible.

1) Security Ontology Web Service: Information from the Security Ontology is derived by querying the established knowledge base. Our Security Ontology framework implementation has five main characteristics, which are presented in the following itemization:

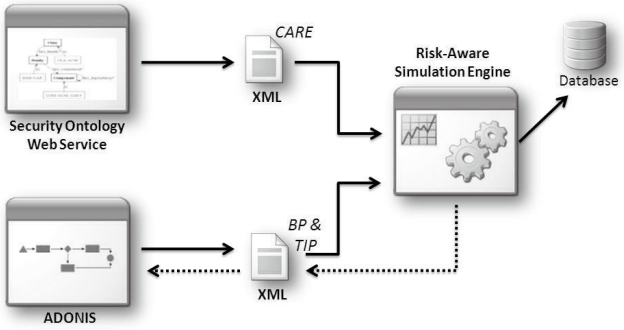

Fig. 7. Architecture of the prototype

- Flexibility: The framework is applicable for a broad semantic field of applications, requiring a minimum of customization.
- Maintainability: a clear separation of components (stored procedures, business logic, and interfaces) strongly supports this attribute.
- Web Ontology Language (OWL) Knowledge Base: the framework operates directly on OWL files
- Multiuser Environment: applications built on the semantic framework are not limited to one local installation, but have to follow a client-server model

The main component is the Security Ontology engine itself, which establishes the connection to the ontology and the stored procedure repository. Stored procedures are stored separately in XML files or in an XML database solution. This engine

provides a web service, which enables any application to request the results of a specific stored procedure (e.g., a query for specific infrastructure items in the Security Ontology) or a combination of *n* stored procedures (e.g., a query for a specific CARE element, depending on a specific infrastructure resource).

The gathered company data is subsequently exported via the XML interface in order to deliver the required input for the risk-aware simulation engine.

2) Business Process Modeling Tool: The business process modeling tool used to support the proof of concept prototype is ADONIS®[2]. The decision to use this tool had two particular reasons: firstly, it provides the possibility to extend the business process model through the ADOxx® meta[2] modeling tool[3]. Due to that fact, we were able to expand the original model in order to fit our risk-aware modeling and simulation requirements. Secondly, ADONIS® is a well known and widely accepted business process modeling and management tool. Especially the acceptance will be of high importance as we want to test our approach under real life conditions, which is planned within a case study within the next year. Currently, we model threat impact processes, action flows and business processes in this environment. The created process models are exported via the XML interface to provide the necessary information for the simulation engine.

3) Risk-Aware Process Simulation Engine: The risk-aware process simulation engine is the core of our prototype. It integrates the information retrieved from the process models (business processes, TIPs and action flows) as well as the Security Ontology (threat information and company data). This enables us to perform the risk-aware considerations of the business processes. The current implementation supports the risk-aware path analysis and follows the succeeding simulation steps:

- Simulation of all threat impact processes: Within this step we simulate the downtimes and delays of resources which are caused by occurred threats. Furthermore, we determine the costs caused by threats, counter and recovery measures.
- Simulation of the business processes: Our risk-aware approach extends the traditional business process simulation insofar that the determined downtimes and delays—caused by the threat impact simulation—are taken into account.

4) Visualization of the Results: Currently, we visualize the results of our simulation by importing them into the ADONIS® toolset via the XML interface. If downtimes or delays of activities are given, they are present within the business process activity's attributes and the graphical representation of the activity within the model changes (other color and added icon). As the risk-aware simulation data is persisted within a relational database, the basis for other visualizations and formatting of the information is given. Thus, we plan exhaustive reporting mechanisms as well as tree-based cause-effect diagrams regarding the impacts of threats on resources.

5) Proof of Concept Findings: First tests of our approach within our proof of concept prototype environment were promising. As also modeled in the Security Ontology, we used for our purposes the IT Baseline Protection Manual [10] of the German Federal Office for Information Security as fundamental guide for the process oriented representation of safeguard and recovery procedures within TIP models, for instance the *Safeguard S6.23 Procedures* in the event of computer virus infection. Typical customer business processes served as basis for further refinements and the linkage to Security Ontology based company information.

Regarding the quality of our proof of concept risk-aware simulation engine, we conducted two evaluations in order to substantiate our simulation results. (1) We compared the results of our business process simulation implementation with simulation outcomes of professional business process management software tools, such as ADONIS®. Concerning this evaluation, we can state that our results are within an acceptable range, small deviations are caused by different implementations regarding the generation of random variables used for decisions within the business process models. (2) As traditional business process simulations do not conduct risk-aware business process simulations, we consequently could not compare our risk-aware simulation results with reference software. Thus, as we perform a path-analysis algorithm, we took samples of resulting simulation paths and manually reviewed the outcomes. This evaluation also led to traceable and promising outputs. In order to conduct a more comprehensive evaluation of our risk-aware business process extensions, we will perform a deeper review of our proof of concept prototype and the resulting simulation outcomes within our planned case study, which will be performed in collaboration with a company of the Austrian social security sector.

V. Conclusion and Further Research

In this paper we presented our approach which combines the capabilities of the risk-aware business process management methodology ROPE [14] and the Security Ontology [19] [18]. The major benefits from the business process management perspective are as follows:

- Modeling support for process designers through the enhanced knowledge basis provided by the Security Ontology (web service). As the Security Ontology comprises not only threats and threatened infrastructure elements, but also relevant risk-attributes, it delivers essential value for the risk-aware process modeling and simulation.
- Provision of ontological restrictions (e.g., each server has to be assigned to a location) improves the quality of the risk-aware process models' design.

[2]ADONIS®: http://www.boc-eu.com/, last access: 6 June 2007
[3]ADOxx® meta[2]: http://www.boc-eu.com/, last access: 6 June 2007

- Furthermore, our risk-aware process simulation enables designers to improve the security and robustness of their modeled business processes. The outcomes of the risk-aware simulation provide essential information on potential single points of (business process) failure, weaknesses in the selection of security mechanisms, and detailed information on costs and benefits of implemented security measures.

Initially we developed a proof of concept implementation in order to test our improvement assumptions and gained corroborative results during the evaluation phase. Currently we are extending our prototype with the Security Ontology integration concept, as presented in this paper.

Furthermore, we intend to perform research activities to enable the support of standards through the usage of the Security Ontology and process templates (TIP, CARE action model, and BP model). We further plan to provide a more precise threat classification for human resources. We assume that a further threat classification extension will be necessary to improve our risk-aware simulation approach in order to consider the threat to human life, because all threats concerning the life or health of people have to be prioritized as critical. We are convinced that supplemental information coming from the Security Ontology can provide essential and valuable details for decision makers in the event of an emergency.

VI. Acknowledgments

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

References

[1] Bank Of Japan, "Business Continuity Planning at the Bank of Japan," September 2003.

[2] ——, "Business Continuity Planning at Financial Institutions," July 2003.

[3] D. A. Alberts, C.J., "OCTAVE Method Implementation Guideline Version 2.0 - Volume 1: Introduction," 2001.

[4] CERT, "OCTAVE," 2005. [Online]. Available: http://www.cert.org/octave

[5] L. F. BCI, NaCTSO, "Expecting the unexpected - Business continuity in an uncertain world," 2003.

[6] D. Karagiannis, S. Junginger, and R. Strobl, *Business Process Modelling*. Springer, Berlin, 1996, ch. Introduction to Business Process Management Systems Concepts, pp. 81–106.

[7] BOC, "The BPMS Paradigm," 1996-2004. [Online]. Available: http://www.boc-eu.com/bochp.jsp?file=WP_582571cc1ed802de.b05236.f598e2482c

[8] A. W. Scheer, G. Keller, and M. Nüttgens, "Semantische Prozeßmodellierung auf der Grundlage Ereignisgesteuerter Prozeßketten (EPK)," *Veröffentlichungen des Instituts für Wirtschaftsinformatik, Heft 89, Saarbrücken*, 1992. [Online]. Available: http://www.iwi.uni-sb.de/nuettgens/Veroef/Artikel/heft089/heft089.pdf

[9] Business Continuity Institute, "Good Practice Guidelines," http://www.thebci.org/gpgdownloadpage.htm, July 2007. [Online]. Available: http://www.thebci.org

[10] BSI, "IT-Grundschutz Manual (english version)," 2004. [Online]. Available: http://www.bsi.de/english/gshb/manual/download/index.html

[11] International Organization for Standardization and International Electrotechnical Commission, "ISO/IEC 17799:2005 Information technology - Security techniques - Code of practice for information security management," http://www.iso.org/, 2006.

[12] British Standards Institute, "Bs 25999," http://www.bsonline.bsi-global.com/server/index.jsp, 2006.

[13] International Organization for Standardization and International Electrotechnical Commission, "ISO/IEC 13335-2:1997 Techniques for information and communications technology security risk management," http://www.iso.org/, 1997.

[14] S. Jakoubi, S. Tjoa, and G. Quirchmayr, "ROPE: A Methodology for Enabling the Risk-Aware Modelling and Simulation of Business Processes," in *ECIS, 15th European Conference on Information Systems*, 2007.

[15] S. Jakoubi, "A Methodology for the Visualisation of Risks in Business Processes as an Enabler for a Holistic Documentation and Risk Evaluation by means of Simulation for Software Projects (in German)," Master's thesis, University of Vienna, 2006.

[16] S. Tjoa, "A Methodology for the Enhancement of Business Process Modelling by means of Process-oriented Modelling, Evaluation, and Simulation of IT-Infrastructure (in German)," Master's thesis, University of Vienna, 2006.

[17] G. Stoneburner, A. Goguen, and A. Feringa, "Risk Management Guide for Information Technology Systems," NIST(National Institute of Standards and Technology), Tech. Rep., July 2002, special Publication 800-30. [Online]. Available: http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

[18] A. Ekelhart, S. Fenz, M. Klemen, and E. Weippl, "Security Ontologies: Improving Quantitative Risk Analysis," in *Proceedings of the 40th Hawaii International Conference on System Sciences (HICSS 2007)*, Jan 2007.

[19] ——, "Security Ontology: Simulating Threats to Corporate Assets," in *Information Systems Security*, ser. Lecture Notes in Computer Science, A. Bagchi and V. Atluri, Eds., vol. 4332. Springer, Dec 2006, pp. 249–259.

[20] PricewaterhouseCoopers, "Information Security Breaches Survey," http://www.pwc.com/uk/eng/ins-sol/publ/pwc_dti-fullsurveyresults06.pdf, 2006.

[21] AusCERT, "Australian Computer Crime and Security Survey," http://www.auscert.org.au/render.html?it=2001&template=1, 2006.

[22] Silicon.de, "IT-Sicherheit Studie," http://www.silicon.de/downloads/ siliconDEStudie_IT_Sicherheit2005.pdf, 2005, English title: IT security study.

[23] Basel Committee on Banking Supervision (BCBS), "Basel 2 - International Convergence of Capital Measurement and Capital Standards - A Revised Framework," 2001.

[24] SOX, "One hundred seventh congress of the united states of america, sarbanes oxley act - to protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to the securities laws, and for other purposes." 2002.

[25] NIST, "An Introduction to Computer Security - The NIST Handbook," NIST(National Institute of Standards and Technology), Tech. Rep., October 1995, special Publication 800-12. [Online]. Available: http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf

[26] United Nations, "United Nations Standard Products and Services Code," http://www.unspsc.org/, 2006.

[27] M. Grüninger and M. S. Fox, "Methodology for the Design and Evaluation of Ontologies," in *Proceedings of the Workshop on Basic Ontological Issues in Knowledge Sharing, IJCAI-95*, Apr. 1995. [Online]. Available: http://www.eil.utoronto.ca/enterprise-modelling/papers/gruninger-ijcai95.pdf

[28] T. R. Peltier, *Information Security Risk Analysis*. Boca Raton, Florida: Auerbach Publications, 2001.

[29] A. Avizienis, J.-C. Laprie, B. Randell, and C. E. Landwehr, "Basic Concepts and Taxonomy of Dependable and Secure Computing," *IEEE Trans. Dependable Sec. Comput.*, vol. 1, no. 1, pp. 11–33, 2004.

[30] International Organization for Standardization and International Electrotechnical Commission, "ISO/IEC 27001:2005, information technology - security techniques - information security management systems-requirements," http://www.iso.org/, 2005.

[31] ISACA, "COBIT," http://www.isaca.org/, 2006.

[32] The Office of Government Commerce, "ITIL," http://www.itil.co.uk/, 2006.