# SecEPM: A Security Engineering Process Model for Electronic Business Processes

Jörn Eichler
Fraunhofer Institute for Secure Information Technology (SIT)
Darmstadt, Germany
joern.eichler@sit.fraunhofer.de

***Abstract*—Business process management (BPM) and accompanying systems allow organizations to react faster both to environmental and market changes. Therefore, BPM is widely applied in industry. Although organizations depend on the secure enactment of electronic business processes, existing BPM languages and techniques provide only little support for security. Several approaches have been proposed to close the gap for security in the domain of BPM. Nevertheless, an approach to develop secure electronic business processes systematically is still missing. In this paper, we provide the design as well as key entities of our Security Engineering Process Model (SecEPM) for electronic business processes. SecEPM guides security, business process, and domain experts through the development of secure business processes from the identification of security goals to the selection and configuration of security controls. It integrates security in the development life cycle of electronic business processes in a flexible way, thus allowing for a secure, adaptable organization.**

***Index Terms*—Security Engineering, Business Process Management, Development Life Cycle**

## I. Introduction

Today's enterprises are confronted with increased competition and frequently changing environments. Therefore, enterprises need to efficiently organize their work in order to adapt quickly to actual requirements. The terms business process and business process management (BPM) have been coined for this challenge. Business processes are the way organizations work – a set of activities carried out to accomplish a business objective. Business process management subsumes design, administration, enactment, and analysis of business processes. Systems to support BPM are considered as important facilitators for the necessary alignment of people and organizational resources. [1, 2]

Hence, BPM and BPM systems (BPMSs) have seen a fruitful development in the last decades. Numerous languages and techniques for business process modeling have been introduced. BPMSs matured from simple information systems to capture process models to feature-rich management suites supporting simulation, execution, and controlling of business process instances. Current methodologies and tooling allow organizations to adapt business processes according to their needs with a minimum of technical skills in daily operation and are widely applied in industry. [3, 4]

Accepted for the 9th IEEE International Conference on e-Business Engineering (ICEBE 2012), September 9-11, 2012, Hangzhou, PR China.


Unauthorized observation, manipulation, and disruption of business processes threaten organizational assets. Nevertheless, BPM methodologies, languages, and tooling provide only little support to express the security needs of an organization or the security controls applied within business processes [5]. Most approaches to meet this need address the analysis of business process models with regard to security properties or augment business process models with security requirement or control specifications, e.g., [6, 7, 8]. However, an approach to develop secure electronic business processes systematically is still missing [9].

In this paper, we contribute the design as well as key entities of our Security Engineering Process Model (SecEPM) for electronic business processes. SecEPM guides security, business process, and domain experts to work collaboratively in order to allow for an adaptive organization integrating security as a first class citizen. It covers security engineering from the identification of security goals for a given business process model to the selection and configuration of applicable security controls.

The paper is structured as follows: The next section introduces briefly necessary terminology with regard to security and security engineering. A running example for the presentation of SecEPM is provided in section III. SecEPM is introduced in section IV covering a recap of key requirements, our design approach, key entities of the process model, and a more detailed description of the activities utilizing the running example. Section V discusses related work and distinguishes our proposal from existing approaches. A conclusion and an outlook on further research questions is given in section VI.

## II. Terminology

In the domain of information technology (IT), the term security and accompanying concepts are often blurred and defined in the context of security management instead of security engineering. This section introduces shortly relevant terms to provide a consistent terminology for security engineering as foundation for SecEPM. Our terminology is based on a current framework from academia [10] that we rendered more precisely on the basis of commonly referenced, international standards such as [11, 12].

We see *security* as a property of a system to take only those states that do not violate the security goals of the assets affected by the system. *Assets* in this sense are any

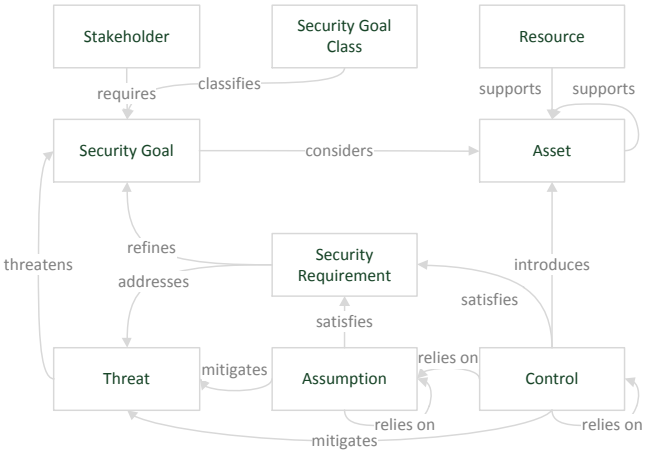


Figure 1. Security concepts and relations

entities that a stakeholder puts value upon with respect to security. Assets might support each other in a way that if one asset's security goals are violated, those of the supported asset are very likely to be violated as well (e.g., keys and confidential data encrypted using those keys). *Security goals* express stakeholder's concerns towards assets with regard to a security goal class. *Security goal classes* considered in this paper are confidentiality, integrity, availability, and non-repudiation. Therefore, a security goal is a high level security need by a stakeholder that considers an asset and is classified with regard to security goal classes.

*Security requirements* are refinements of security goals and state the intent to counter threats. We consider *threats* as potential causes of violations of security goals. Threats might exploit weaknesses of a system that we call *vulnerabilities*. Security *controls* (also known as countermeasures or safeguards) are practices, procedures, or mechanisms that mitigate threats with regard to security requirements. Controls might introduce new assets like credentials which security goals and threats have to be considered as well. In order to work properly, controls might rely on other controls or assumptions. *Assumptions* constrain the environment of the system in order to mitigate threats and satisfy security requirements. Most likely, assumptions will be refined to organizational procedures. Figure 1 depicts security concepts central to this paper and their relationships.

Security engineering is commonly defined as *"building systems to remain dependable in the face of malice, error, or mischance"* [13]. Security engineering focuses security-related activities and provides systematic approaches for the integration and application of those activities. Analogous to software development life cycle terminology [14], we call a representation of all activities and work products necessary to augment traditional software development process models in order to build secure and trusted systems a security engineering process model.

## III. Running Example

In order to exemplify SecEPM, this section introduces a real world business process from the logistics domain – the Replan Process. The Replan Process is part of a business process chain to implement door-to-door delivery of shipments around the world operated by a large provider of integrated logistics services. To allow for proactive interventions in case of delays (or other deviations from the current planning), the logistics provider continuously monitors status data from freight forwarders. In case of any deviations by given thresholds, alternatives are calculated, approved, and transmitted.

The business process model of the Replan Process is depicted in figure 2 as Business Process Model and Notation (BPMN) diagram. It entails the interactions between the freight forwarder (Pool[1] P2) and the logistics provider (Pool P1) after pickup of shipments and before arrival at the shipments destination. Each Pool is divided in two Lanes: Lane L11 represents the dispatcher responsible for the routing of the shipments, Lane L12 the IT system from the logistics provider, Lane L21 the on-board unit (OBU) of the freight forwarder, and Lane L22 the driver responsible to transport the shipments to the next destination.

The Replan Process relies on external sensor data that is transmitted over the air, involves different administrative districts coupled by IT technology, communicates potential sensitive routing information, and includes human interaction. Manipulation of the enactment of the electronic business process like message blocking, tapping, or tempering as well as unauthorized access might lead to service level degradation, contractual fines, loss of goods, information disclosure, and other unwanted results. Therefore, security aspects of the electronic business process must be carefully analyzed and mitigation of identified threats must be considered and enforced.

## IV. Security Engineering Process Model (SecEPM)

This section presents SecEPM – our process model for security engineering of electronic business processes. The first subsection IV-A sums up key requirements for the process model. Main design aspects of SecEPM to satisfy those requirements are discussed in subsection IV-B. Subsection IV-C sketches key entities of SecEPM that will be used by the activities presented in subsection IV-D. The closing subsection IV-E presents the exemplary results of the application of SecEPM.

### A. Key Requirements

The support for a systematic procedure to develop secure electronic business processes is weak (cf. section V). This situation endangers one of the main objectives of BPM: supporting organizations to become adaptive. At the moment, they have to choose to focus on either the protection of their assets or on lightweight innovation and business process (re-) engineering cycles.

[1]All BPMN entities are be given capitalized.

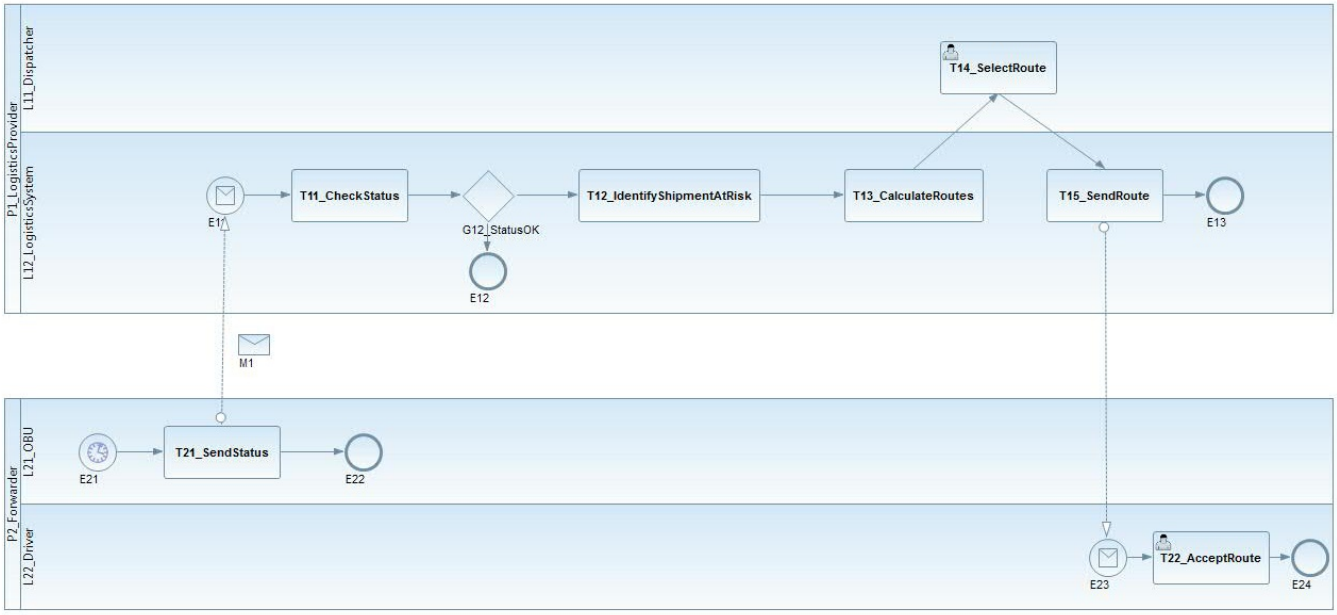


Figure 2. The Replan Process (BPMN diagram)

To bridge the current gap between (executable) business process models and secure electronic business processes the following key requirements apply to a security engineering process model in the domain of BPM (cf. [9]).

1) Restricted skill set necessary to design and configure security aspects of electronic business processes, i.e., security experts are not needed for every activity
2) Possibility to integrate the security engineering process model with different development approaches
3) Independence from run-time technology

These requirements stem from fundamental ideas of BPM: separation of technical and domain aspects as well as applicability notwithstanding environmental heterogeneity. Satisfaction of these requirements allow for business process design and configuration that integrates security considerations without endangering the adaptability gained by the application of BPM.

### B. Design Approach

The design of SecEPM rests on three strategies to satisfy the key requirements stated before:

- Specialization of existing general practices
- Separation of concerns
- Decoupling of activities

The specialization strategy takes an accepted security engineering process model as a sound starting point. It aims at restricting the skill set necessary to complete activities as well as focusing on imminent necessary activities and tasks (cf. requirement 1). Most prominently, the proposal from Breu et al. [15] for a formally based security engineering process model constitutes the basis of SecEPM. Furthermore, the (at least in German speaking countries) largely applied IT Baseline Protection Methodology (IT-BPM, [16]) provided supplemental activities and concepts for SecEPM.

The separation of concerns strategy is applied for several aspects. First, security-related tasks that require security experts have been separated from tasks that can be executed by other participants with sufficient guidance provided. These tasks have been concentrated in a preparatory activity as much as possible. Second, treatment of conceptual and implementation aspects have been separated as well. For example, the analysis of the security problem arising from the business process model and the design of proper controls is separated from individual capabilities of a given business process engine and its configuration. Third, security analysis situated in the problem domain is separated from security design situated in the solution domain. Fourth, activities (that provide a structure for the actual security engineering process) are separated from guidance artifacts (that explain on how to fulfill an activity). Hence, different methods can be applied within SecEPM. The application of the separation of concerns strategy addresses all requirements.

Decoupling of activities addresses the integrability requirement 2. It aims at a flexible configuration of activities and their deserialization. Although some activities use work products from other activities it should be possible to execute them in a way that allows for an iterative, incremental application and the integration in different development approaches.

### C. Key Entities

Key entities of SecEPM are grouped as roles, work products, or activities. Together they answer the question: “Who (role) is doing what (activity) with which result (work product) to secure an electronic business process?” A role is a set of responsibilities in a project that is filled by one or more

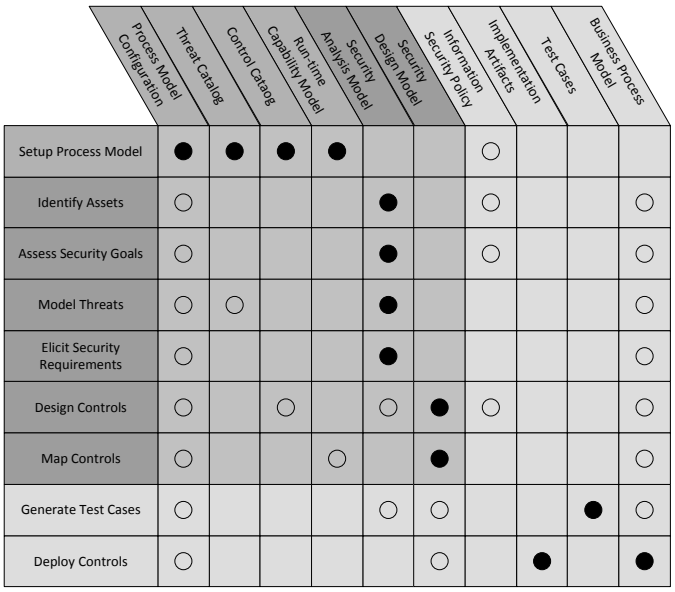


Figure 3. SecEPM activity vs. work product matrix

participants. An artifact produced by an activity is called work product. An activity is a set of tasks that is performed with a specific purpose. Additionally, SecEPM provides guidance artifacts encompassing templates, checklists, examples, reference material, and guidelines. Due to space restrictions these guidance artifacts will be covered only shortly together with the activities in the following subsection IV-D.

We keep the number of roles in SecEPM pragmatically small. We distinguish Process Model Experts, Business Process Experts, Domain Experts, Security Experts, Developers, and Testers. As SecEPM augments development process models, roles from SecEPM complement those from the development process model (cf. [17]). *Process Model Experts* are experts for internal development processes and their configuration. They decide on sequence and staffing of activities as well as resources provided for those activities. In smaller companies the role Process Model Expert is often bundled with duties of a project manager. In SecEPM Process Model Experts account for the work product Process Model Configuration. *Business Process Experts* are professionals translating business requirements in business process models and configure them for their enactment. Business Process Experts execute most of the activities in SecEPM, supported by Domain Experts, Developers, Testers, and Security Experts on request. *Domain Experts* provide knowledge from the application domain of a business process. In SecEPM they contribute to the work product Threat Catalog, support the identification of assets and the assessment of security goals. *Security Experts* are familiar with the analysis of security problems and their solution. In SecEPM they provide the Threat Catalog (supported by the Domain Expert), the Control Catalog, and detailed guidance for all activities. Furthermore, Security Experts validate the work products Security Analysis Model and Security Design Model. *Developers* contribute their technological know-how. In SecEPM they provide the work product Run-time Capability Model (supported by the Security Expert) and support the Business Process Expert in mapping controls to run-time capabilities and configuring the executable business process model. *Testers* ensure the quality of the electronic business process. In SecEPM they generate the work product Test Cases and execute them against the developed solution.

SecEPM distinguishes six main work products. The *Process Model Configuration* depicts the individual configuration of SecEPM either for a specific organization or a development project. The *Threat Catalog* contains threat classes that are considered relevant for a given Process Model Configuration. Threat classes represent classes of threats entailing entry or applicability conditions for individual threat classes, relations to other threat classes, and consequences of successful manifestations. The *Control Catalog* provides control classes detailing mitigation possibilities for one or more threat class, application consequences of a control class, and relations to other control classes. Interfaces to implementations of controls supported by components in the run-time environment (e.g., a business process engine) are provided by the *Run-time Capability Model*. It details configuration and implementation alternatives of control classes specified in the Control Catalog.

Core work products of SecEPM are the Security Analysis Model and the Security Design Model. They are created or updated by several SecEPM activities. The *Security Analysis Model* entails the security problem to be solved and captures assets affected by the business process, security goals for those assets, and threats to be mitigated. The *Security Design Model* depicts the solution to the security problem and describes the controls to be applied as well as their mapping onto the capabilities of the run-time environment. Both models, the Security Analysis Model and the Security Design Model, maintain references on relevant elements of the Business Process Model.

Several work products are necessary as input for activities of the SecEPM or result as output that is not considered by any SecEPM activity. The *Information Security Policy* defines high-level policies of the organization and is the foundation of the Threat and Control Catalog. Furthermore, it supports the identification of assets and the assessment of security goals providing asset classification schemata, rating criteria, and control guidelines. The (executable) *Business Process Model* is the most important input to nearly all activities of the SecEPM. *Test Cases* and *Implementation Artifacts* are possibly produced by SecEPM activities but are not considered in the scope of this paper.

Figure 3 depicts the relations between activities and work products: filled circles note a produce relation (i.e., an activity creates or updates a work product), empty circles note a consume relation (i.e., an activity uses a work product).

### D. Activities

As depicted in figure 3, SecEPM proposes nine activities, including one preparatory and two closing activities. We will

present them, developing exemplary controls for the Replan Process presented in section III.

*1) Setup Process Model:* The preparatory activity to setup the security engineering process aims at tailoring SecEPM for an organization, the application domain, or an development project. It is assigned mainly to the Process Model Expert together with the Security Expert. Supportive tasks are executed by the Domain Expert and the Developer. The Setup Process Model activity uses the Information Security Policy and provides the Process Model Configuration, the Threat and Control Catalogs, and the Run-time Capability Model.

In the first steps, the Security Expert defines a framework for the definition and assessment of security goals. Security goal classifications, a rating scale for security goals, damage scenarios to assess security goal ratings, and criteria to reproducibly rate security goals have to be provided as input for the Process Model Configuration. The next steps encompass the provision of the Threat and Control Catalog as well as the Run-time Capability Model.

For the Replan Process, the Security Expert utilizes selected elements of the IT-BPM methodology [16]. Respective definitions of "Integrity", "Confidentiality", "Availability", and "Non-repudiation" as security goal classifications are included as well as definitions of the rating scale (ordinal three-step scale from "Normal" as limited and calculable impact to "Very High" as impact threatening the survival of the organization). Accordingly and supported by the Domain Expert, damage scenarios and corresponding criteria to rate security goals are defined, e.g., the damage scenario "Financial Consequences" and the criteria "Limited fincancial losses" assigning the rating "Normal" to the condition "Financial losses are below 50,000 EUR". Guidelines from the IT-BPM methodology detailing the application of the definitions are included to ease the execution of following activities.

The definition of the Threat and Control Catalogs takes considerable effort. The quality of the results achieved by applying SecEPM depend largely on completeness and coherence of these catalogs. To ease the adoption of SecEPM, it is feasible to start with rather general and small catalogs and to complete them in the course of several projects. Alternatively (or complementary), existing catalogs can be taken as basis for the derivation of the catalogs.

In case of the Replan Process, the Security Expert starts with a rather general Threat Catalog adopting the STRIDE method [18] for the threat analysis of electronic business processes. Therefore, initially 12 threat classes are included by applying the adverse actions spoofing, tempering, repudiation, information disclosure, denial of service, and elevation of privilege to processes and data entities of business process models. Exemplary, one threat class is defined as "Tempering execution sequence" endangering security goals of the class integrity that can be assigned to Pool entities manipulating the Control Flow entities of those Pool entities. In the course of the application of SecEPM activities, this or other threat classes might be further refined separating different attack vectors, e.g., with the help of attack trees [19].

The Control Catalog in this example is adopted from a control catalog provided by a national authority [20]. One exemplary control class derived from the control "AU-12 Audit Generation" is defined as "Log process execution" that mitigates the threat class "Tempering execution sequence" by providing means to detect successful attacks. Control classes reference their origin and the source catalog might be used as guiding reference material.

As the Replan Process will be enacted utilizing a BPMS, the Run-time Capability Model is derived from security manuals provided by the software vendor. To ease reproducibility, the open source solution Activiti[2] will be taken as example. An exemplary capability is "Activiti logging" with the property "Log Level" that implements the control class "Log process execution". Certainly, in many cases an interplay of several technical features will be necessary to implement an effective control, e.g., to generate temper-proof audit trails.

*2) Identify Assets:* After setup of the process model, the Business Process Expert (supported by the Domain Expert) identifies assets impacted by the electronic business process and relates them to elements of the Business Process Model. The activity consumes the Process Model Configuration and the Business Process Model and creates or updates the Security Analysis Model detailing assets and their relations.

The activity entails four steps: At first, business assets are identified that are affected by the business process in question. These assets are normally not directly represented in the Business Process Model but drive design and enactment of the electronic business process. Then, assets directly represented (or modeled) in the Business Process Model are identified. Following the guidance provided by the Security Expert in the previous task, Messages and Process entities are candidate assets. Supporting resources represented in the Business Process Model are identified next. Those resources are captured at the maximum level of abstraction. The last step analyzes the dependencies between the assets and resources to allow for an impact propagation in following activities.

For the Replan Process, the main business asset is the successful proof of delivery (POD, i.e., the shipment is transported in time to the designated destination without damage). Example assets represented in the Business Process Model are M1 (status message) and P1 (process in the controlled administrative district of the logistics service provider). Exemplary resources are P2 (the process of the participating freight forwarder) or Message Flows as representation of the communication channel between freight forwarder and logistics service provider. Dependency relations are established for example between the POD and the Pool P1 (a successful POD is endangered by violations of security goals of the process modeled with P1).

*3) Assess Security Goals:* As a precondition for the elicitation of security requirements, the Business Process Expert supported by the Domain Expert analyzes and rates security goals for the identified assets. The assessment consumes the

[2]http://www.activiti.org/

Process Model Configuration, the Business Process Model and the Security Analysis Model, which is updated by the activity.

The first step of the assessment is the initial definition of security goals. Each asset will be assigned with one security goal for each security goal classification defined in the Process Model Configuration. After that, security goals will be rated with regard to their damage potential. Guidance from the security experts details, that in order to rate the security goals every security goal is checked with regard to each damage scenario (cf. [16]). Every criterion that fits to the security goal will be assigned to the security goal. To evaluate the individual rating for the security goals, for every asset the maximum rating from the criteria assigned to the corresponding security goal class is taken. The dependencies between the assets are incorporated into the rating by assigning the maximum rating from all assets an asset depends upon.

Three assets have been identified so far for the Replan Process. For each asset four security goals are defined, e.g., the security goal "Process integrity" for the asset related to Pool P1 and the security goal classification "Integrity". This security goal is assigned to the criterion "Limited financial losses" with the help of the Domain Expert. Therefore, the security goal is rated as "Normal".

*4) Model Threats:* In order to explicate the security challenges for the Replan Process, the Business Process Expert instantiates threats that endanger the security goals identified so far. The activity uses the Process Model Configuration, the Threat Catalog, and the Security Analysis Model, which in turn is enriched with actual threats for the electronic business process.

To identify relevant threats, candidate threats are selected from the Threat Catalog that address entities from the Business Process Model referenced by the assets documented so far. Candidate threats are checked with regard to the classification of security goals they are directed to. Matching threats are assigned to the security goal and included in the Security Analysis Model. As a last step, entities of the Business Process Model that are potentially affected by the threat are documented as annotation to the threat.

In the case of the Replan Process, the threat class "Tamper execution sequence" matches the asset related to Pool P1. As the threat class endangers the integrity of the Pool P1, it is instantiated as "Tamper P1 execution sequence" and assigned to the security goal "Process integrity". The threat affects potentially all Sequence Flows entities entailed in the Pool P1.

*5) Elicit Security Requirements:* Now security requirements can be elicited by the Business Process Expert. The security requirement elicitation uses the Process Model Configuration, the Business Process Model, and the Security Analysis Model that is updated by the activity.

To identify security requirements, all entities of the Business Process Model that are potentially affected by a threat are identified. Security goals for those entities are refined to security requirements. Security requirements state what entities have to be protected with regard to which security goal

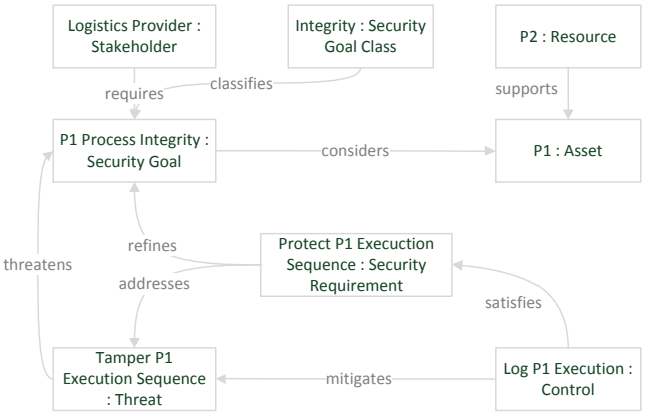


Figure 4. Exemplary entities of the Security Analysis and Security Design Model and their relations

classification considering which threats. After the specification of all security requirements, overlapping requirements might be merged.

For the Replan Process, the security requirement "Protect execution sequence" is refined from the security goal "Process integrity". It requires protection for all Sequence Flow entities contained in the Pool P1 against the threat "Temper execution sequence".

*6) Design Controls:* With the elicitation of security requirements the Security Analysis Model is completed. To address the security requirements appropriately, the Business Process Expert supported by the Security Expert proceeds from the problem domain to the solution domain. This activity addresses the selection of an appropriate control set to cover the security requirements. It uses the Process Model Configuration, the Business Process Model, the Control Catalog, and the Security Analysis Model. The Security Design Model is created or updated by the activity.

First, applicable controls from the Control Catalog are identified. Controls are applicable, if they address one or more threats and match the entities of the Business Process Model that are referenced by a security requirement as well as their rating. Then, appropriate controls are selected and detailed with regard to their effect on the entities of the Business Process Model. Controls will often depend on other controls in order to work properly. Those controls have to be included as well or equivalent assumptions have to be stated. If controls introduce new assets, those assets have to be integrated as well and the corresponding activities have to be repeated. Finally, it has to be checked that all security requirements are covered by the controls.

The control class "Log process execution" addresses the threat "Temper P1 execution sequence" and applies to Sequence Flow entities. It is therefore instantiated as "Log P1 execution" and detailed that it applies to all Sequence Flow entities from the Pool P1. It covers the security requirement "Protect execution sequence".

*7) Map Controls:* The mapping of controls onto the actual run-time environment provides necessary information to in-

stantiate corresponding implementation artifacts. The Business Process Expert supported by the Developer selects and assigns matching run-time capabilities for the controls specified in the Security Design Model from the Run-time Capability Model and updates the Security Design Model accordingly. The Process Model Configuration and the Business Process Model is utilized as necessary.

First, actual components from the run-time environment and corresponding Run-time Capability Models have to be selected. Applicable capabilities are identified, selected and assigned to the respective controls. Properties of the selected capabilities are configured as appropriate.

The business process engine Activiti has been selected for the enactment of the Replan Process. The capability "Activiti logging" matches the control "Log process execution". The capability is selected and it's property "Log Level" is set to the value "Fine".

*8) Generate Test Cases and Deploy Controls:* The activities Generate Test Cases and Deploy Controls allow for the generation of test as well as implementation artifacts that are used for testing or deployment of the electronic business process. They are assigned to the Tester and Developer respectively – supported by the Business Process Expert. As they depend largely on the run-time environment their application will not discussed in this paper.

### *E. Exemplary Results*

We demonstrated the application of SecEPM using the Replan Process as an example. Figure 4 depicts some selected entities of the Security Analysis Model and the Security Design Model as well as their relations: The logistics provider as primary stakeholder in the Replan Process relies on the integrity of the execution of the process specified with the Pool P1 in the Business Process Model. As the execution sequence of the process might get tempered by an adversary, the security goal is refined to the security requirement to protect the execution sequence of the process. Logging of the execution sequence is selected as control in order to monitor the process execution and detect possible violations of the execution sequence.

These results represent only a very limited extract of the Replan Process' Security Analysis and Design Model. The intention is to demonstrate the functioning of SecEPM as well as the relations between activities, work products, participants, and guidance artifacts.

## V. Related Work

The need for security in the domain of BPM has been articulated by several authors [5, 21]. The majority of current proposals in the active research on security in the domain of BPM address either the analysis of security properties (e.g., [8, 22]) or the augmentation of business process models with security requirement or control specifications (e.g., [6, 7, 23]).

Support for the development of secure business processes remains weak. An early approach by Röhrig et al. focuses the problem domain and does not support the design of enforceable controls [24]. This applies also to a more recent approach by Neubauer et al. focusing on the economical efficient selection of controls [25]. Other approaches address only specific activities like security requirements elicitation [26, 27]. The more elaborated approach by Hafner et al. addresses security engineering for service-oriented architectures including secure electronic business processes [28]. Nevertheless, it is focused on the security of web services in a specific MDA tool chain.

Manifold general approaches for security engineering have been proposed. Especially model-driven approaches are an active research topic [29]. In industry, general frameworks like Microsoft SDL or OWASP CLASP are becoming common practice [30]. The provision and systematic integration of security knowledge and best practices in security engineering has been proposed by several authors, often using the notion of security patterns (e.g., [31, 32, 33]). Nonetheless, general security development life cycles, security engineering process models, and patterns are to broad to be applied effectively in the domain of BPM. However, SecEPM is not a monolithic approach. Individual, commonly accepted methods like attack trees [19] or STRIDE [18] can be easily integrated into SecEPM as it has been demonstrated in subsection IV-D.

## VI. Conclusion

BPM and BPMS allow organizations to become adaptive: to react faster to environmental and market changes. This benefit is endangered by the lack of an appropriate approach to develop secure electronic business processes systematically. This paper presents with SecEPM a security engineering process model for electronic business processes that guides security, business process, and domain experts from the identification of security goals to the selection and configuration of security controls. It provides all means for the integration of security as first class citizen in the development of secure electronic business processes allowing for a secure, adaptable organization.

One focus of this paper is on the design approach for SecEPM applying three strategies: specialization of general process models to incorporate best practices but allow for a restricted skill set necessary to complete the activities, separation of concerns to provide good integrability and independence from organizational and technical environment, as well as decoupling of activities to enhance the flexibility of SecEPM. The second focus is on key entities of SecEPM. We describe main constituents of our process model – roles, work products, and activities – as well as their relations. An exemplary application of SecEPM utilizing a real world business process demonstrates the functioning of SecEPM.

Applying SecEPM, the Business Process Expert is being burdened with considerable responsibility. Currently, we are working on a domain specific modeling language and corresponding tooling to facilitate the creation and analysis of the work products of SecEPM. To streamline SecEPM with established development approaches, the provision of plug-ins is intended that integrate SecEPM into these approaches.

## References


[1] T. Davenport, "The coming commoditization of processes," *Harvard Business Review*, vol. 83, no. 6, pp. 100–108, 2005.

[2] P. Tallon, "Inside the adaptive enterprise: an information technology capabilities perspective on business process agility," *Information Technology and Management*, vol. 9, no. 1, pp. 21–36, 2008.

[3] R. Ko, S. Lee, and E. Lee, "Business process management (BPM) standards: a survey," *Business Process Management Journal*, vol. 15, no. 5, pp. 744–791, 2009.

[4] J. Recker, M. Rosemann, M. Indulska, and P. Green, "Business process modeling: a comparative analysis," *Journal of the Association for Information Systems*, vol. 10, no. 4, pp. 333–363, 2009.

[5] T. Neubauer, M. Klemen, and S. Biffl, "Secure business process management: A roadmap," in *Availability, Reliability and Security (ARES 2006)*, IEEE, 2006.

[6] C. Wolter, M. Menzel, A. Schaad, P. Miseldine, and C. Meinel, "Model-driven business process security requirement specification," *Journal of Systems Architecture*, vol. 55, no. 4, pp. 211–223, 2009.

[7] A. Rodríguez, E. Fernández-Medina, J. Trujillo, and M. Piattini, "Secure business process model specification through a UML 2.0 activity diagram profile," *Decision Support Systems*, vol. 51, no. 3, pp. 446–465, 2011.

[8] A. Armando, E. Giunchiglia, M. Maratea, and S. E. Ponta, "An action-based approach to the formal specification and automatic analysis of business processes under authorization constraints," *Journal of Computer and System Sciences*, vol. 78, no. 1, pp. 119–141, 2012.

[9] J. Eichler, "Towards a security engineering process model for electronic business processes," in *European Dependable Computing Conference (EDCC 2012), Fast Abstracts & Student Forum*, CoRR, 2012.

[10] B. Fabian, S. Gürses, M. Heisel, T. Santen, and H. Schmidt, "A comparison of security requirements engineering methods," *Requirements Engineering*, vol. 15, no. 1, pp. 7–40, 2010.

[11] ISO/IEC, "ISO/IEC 13335-1: Information technology – security techniques – management of information and communications technology security," 2004.

[12] ISO/IEC, "ISO/IEC 15408-1: Information technology – security techniques – evaluation criteria for IT security – part 1: Introduction and general model," 2009.

[13] R. J. Anderson, *Security Engineering: A Guide to Building Dependable Distributed Systems*. Wiley, 2 ed., 2008.

[14] IEEE, "IEEE 1074: Standard for developing software life cycle processes," 1997.

[15] R. Breu, K. Burger, M. Hafner, J. Jürjens, G. Popp, G. Wimmel, and V. Lotz, "Key issues of a formally based process model for security engineering," in *Software & Systems Engineering and their Applications (ICSSEA 2003)*, 2003.

[16] Bundesamt für Sicherheit in der Informationstechnik, "BSI-Standard 100-2: IT-Grundschutz methodology," 2008.

[17] B. Chadha, "A model driven methodology for business process engineering," in *Computers in Engineering (ICEC 1995)*, pp. 1165–1182, ASME, 1995.

[18] F. Swiderski and W. Snyder, *Threat modeling*. Microsoft, 2004.

[19] B. Schneier, "Modeling security threats," *Dr. Dobb's Journal*, December 1999.

[20] R. Ross, G. Stoneburner, E. Porter, G. Rogers, M. Swanson, R. Graubart, B. Hodge, A. Johnson, S. Katzke, G. Turner, K. Dempsey, and C. Enloe, "Recommended security controls for federal information systems and organizations," SP 800-53, NIST, 2010.

[21] S. Kokolakis, A. Demopoulos, and E. Kiountouzis, "The use of business process modelling in information systems security analysis and design," *Information Management and Computer Security*, vol. 8, no. 2/3, pp. 107–115, 2000.

[22] K. Weldemariam and A. Villafiorita, "Procedural security analysis: A methodological approach," *Journal of Systems and Software*, vol. 84, no. 7, pp. 1114–1129, 2011.

[23] Y. Badr, F. Biennier, and S. Tata, "The integration of corporate security strategies in collaborative business processes," *IEEE Transactions on Services Computing*, vol. 4, no. 3, pp. 243–254, 2011.

[24] S. Röhrig and K. Knorr, "Security analysis of electronic business processes," *Electronic Commerce Research*, vol. 4, no. 1, pp. 59–81, 2004.

[25] T. Neubauer and M. Pehn, "Workshop-based risk assessment for the definition of secure business processes," in *Information, Process, and Knowledge Management (eKNOW 2010)*, pp. 74–79, IEEE, 2010.

[26] P. Herrmann and G. Herrmann, "Security requirement analysis of business processes," *Electronic Commerce Research*, vol. 6, no. 3, pp. 305–335, 2006.

[27] A. Rodríguez, I. G.-R. de Guzmán, E. Fernández-Medina, and M. Piattini, "Semi-formal transformation of secure business processes into analysis class and use case models: An MDA approach," *Information and Software Technology*, vol. 52, no. 9, pp. 945 – 971, 2010.

[28] M. Hafner and R. Breu, *Security engineering for service-oriented architectures*. Springer, 2009.

[29] J. Jensen and M. Jaatun, "Not ready for prime time: A survey on security in model driven development," *International Journal of Secure Software Engineering*, vol. 2, no. 4, pp. 49–61, 2011.

[30] D. Geer, "Are companies actually using secure development life cycles?," *Computer*, vol. 43, no. 6, pp. 12–16, 2010.

[31] M. Schumacher, E. Fernandez-Buglioni, D. Hybertson, F. Buschmann, and P. Sommerlad, *Security Patterns: Integrating Security and Systems Engineering*. Wiley, 2006.

[32] D. Hatebur, M. Heisel, and H. Schmidt, "A security engineering process based on patterns," in *Database and*

*Expert Systems Applications (DEXA 2007)*, pp. 734–738, IEEE, 2007.

[33] R. Evans, A. Tsohou, T. Tryfonas, and T. Morgan, "Engineering secure systems with ISO 26702 and 27001," in *System of Systems Engineering (SoSE)*, IEEE, 2010.