

## An Analysis and Evaluation of Security Aspects in the Business Process Model and Notation

Maria Leitner, Michelle Miller and Stefanie Rinderle-Ma

*University of Vienna*

*Faculty of Computer Science*

*Vienna, Austria*

*{maria.leitner,michelle.miller,stefanie.rinderle-ma}@univie.ac.at*

**Abstract**—Enhancing existing business process modeling languages with security concepts has attracted increased attention in research and several graphical notations and symbols have been proposed. How these extensions can be comprehended by users has not been evaluated yet. However, the comprehensibility of security concepts integrated within business process models is of utmost importance for many purposes such as communication, training, and later automation within a process-aware information system. If users do not understand the security concepts, this might lead to restricted acceptance or even misinterpretation and possible security problems in the sequel. In this paper, we evaluate existing security extensions of Business Process Model and Notation (BPMN) as BPMN constitutes the de facto standard in business modeling languages nowadays. The evaluation is conducted along two lines, i.e., a literature study and a survey. The findings of both evaluations identify shortcomings and open questions of existing approaches. This will yield the basis to convey security-related information within business process models in a comprehensible way and consequently, unleash the full effects of security modeling in business processes.

**Keywords**—BPMN; Business Processes; Modeling; Security;

### I. INTRODUCTION

Process-aware Information Systems (PAIS) support the automated execution of business processes [1]. In recent years, security has become a key factor in PAIS (e.g., [2]). So far, research and practice has centered on implementation aspects when it comes to security. Yet, recent developments (e.g., [3], [4]) show that not only secure process executions are of importance but also process modeling that enables to display security aspects in business processes. Typically, business process models are utilized for many purposes such as communication, training and later automation within PAIS. In particular, adding security concepts into business process models might provide a common language and understanding of business operations but also foster the collaboration between domain experts (e.g., security experts and process managers). In these scenarios, it is important to comprehend the process model which is influenced by personal factors (e.g., the amount of theoretical modeling knowledge) or model characteristics [5]. However, when it comes to understanding business process models enhanced with security concepts, additional domain knowledge (i.e., security knowledge) is necessary to fully comprehend the model. Recent publications try to provide a common language between domain experts (e.g., security experts)

and process modelers by proposing process modeling extensions, for example, in the Business Process Model and Notation (BPMN) such as in [3], [6]. As a primary concern, we noticed that most of these publications do not involve people at any stage during the development of the extensions. Hence, a systematic evaluation of process modeling extensions with people is still missing. As a consequence, if users do not understand the security concepts incorporated within the business process model, this might lead to restricted acceptance, misinterpretation, errors and possible security problems in the sequel.

In this paper, we analyze and evaluate security extensions in BPMN [7] as it constitutes the de facto standard for business process modeling languages. Specifically, we want to investigate (1) how security aspects in BPMN are modeled to identify whether the BPMN 2.0 standard and current research and practice supports security aspects. To do that, we will perform a literature review. Based on the results, we want to investigate (2) if people can comprehend security extensions in BPMN accurately using an online survey. Therefore, we examine the peoples understanding of security extensions in a business process and detached from a process. In addition, we want to identify (3) which symbols are suggested for access control and privacy.

The findings of this paper identify shortcomings and open questions of currently existing approaches. This will yield the basis to convey security-related information within business process models in a comprehensible way and is the start of a series of experiments on security modeling in business processes.

In this paper, we summarize current research and practice in process modeling notations in Section II. The research methodology of this paper is described in Section III and Section IV outlines the results. Furthermore, we interpret the findings with recommendations for future developments of process modeling extensions in Section V. A discussion on the validity threats and impact on future research is given in Section VI.

### II. BACKGROUND

Visual representations have a strong impact on the usability and effectiveness of software engineering notations [8]. The quality of conceptual models is essential to e.g., prevent errors and to improve the quality of delivered systems [9]. Several frameworks exist that provide guidelines

how to design and evaluate visual notations (e.g., [10], [8]). For example, the *Physics of Notations* in [8] consists of nine principles to design visual notations effectively.

In PAIS, recent publications show increased interest in the visual representation of process modeling languages (e.g., [11]). For example in [11], an evaluation of cognitive effectiveness of BPMN using the principles of *Physics of Notations* is performed. Further studies investigate certain characteristics such as the usage of labels and icons (e.g., [12]).

While research centers mostly on the technical implementation of security controls, recent publications also provide process modeling extensions to add security aspects in process models (e.g., in BPMN diagrams in [3]). Typically, process models are created by process modelers or process managers in an organization. These managers have an expertise in process modeling, but are often not experts in security. A security expert provides know-how and collaborates with the process modeling expert to enable security in a process. Hence, modeling security aspects in a process model provides a common language and basis between domain experts. Security extensions exist in various process modeling languages such as UML and BPMN (cmp. [13]) but e.g., no common patterns exist (cf. [14]). In this paper, we center only on BPMN extensions for security, as BPMN constitutes a de facto standard for business process modeling languages [7].

### III. METHODOLOGY

In this section, we will outline the research questions and methods used in this paper. Our research was guided by the following questions (RQ):

- (1) How are security aspects modeled in BPMN?
  - (1.1) How does the BPMN 2.0 standard support security?
  - (1.2) Do BPMN extensions that support security aspects exist?
- (2) Can BPMN security extensions be comprehended accurately?
  - (2.1) Can BPMN security extensions be identified and correctly interpreted in business processes?
  - (2.2) Can BPMN security extensions be identified and correctly interpreted as isolated symbols?
  - (2.3) Which extensions are often interpreted accurately and which are not?
- (3) Which symbols are suggested for displaying access control and privacy?

With research question (RQ1), we investigate current state of the art in security modeling in BPMN conducting a literature review. First, we identify if and how the BPMN 2.0 standard supports security (RQ1.1) in business process models. Secondly, we examine current research and practice of security extensions or security modeling techniques in BPMN (RQ1.2). We carry out a survey to investigate if participants (e.g., process modelers, process participants) can comprehend BPMN security extensions (RQ2). Therefore, we embed BPMN extensions in an example business process (RQ2.1) and also examine the

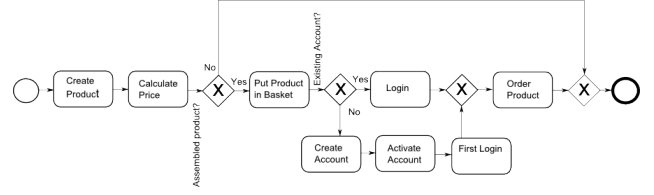


Figure 1. Example 1: Order Business Process

symbols detached from the process i.e., as isolated symbols (RQ2.2). Furthermore, we assess what extensions are often or infrequently identified and interpreted by participants (RQ2.3). In the last research question (RQ3), we investigate what symbols for access control and privacy are suggested by participants.

#### A. Literature Review

In a first step, a literature review (e.g., [15]) was conducted of contributions referring to security modeling in BPMN (RQ1).

For this literature review, we used the meta search engine Google Scholar (retrieval date 08/25/2012) which also includes libraries of the major publishers e.g., IEEE, ACM or Springer. Unfortunately, keywords such as “*Security BPMN*” (4.070 results) or “*Security BPMN extension*” (994) returned too many (and too fuzzy) results. However, the keyword “*Security “BPMN extension”*” returned only 108 publications. Similar results were returned using these keywords in libraries of major publishers.

The goal of the literature search was to identify publications that investigate security modeling in BPMN; this also includes the proposal of BPMN security extensions. Based on these 108 publications, we analyzed title, abstract and keywords to determine if the paper can be selected. However, most of the times, we had to read the full paper to assess if the publication contained security-related modeling in BPMN. We selected a publication if security extensions of BPMN were proposed or additional security icons were used in BPMN. In total, 7 publications were selected, namely [6], [3], [4], [16], [17], [18] and [19].

#### B. Survey

As a type of survey, a questionnaire contains typically a series of questions to gather information from participants (e.g., [20]). The online questionnaire consisted of 48 open and closed questions. A pre-analysis of the questionnaire was performed in two rounds. In each round an expert in process modeling and empirical research evaluated the questionnaire and provided feedback for enhancements. This survey was targeting researchers, students and practitioners with knowledge in the area of security and/or process modeling. Answering all questions took about 20 minutes.

The online questionnaire consisted of three parts: *demographic data*, *sample process* and *BPMN security*. The first part, demographic data, consisted of 12 questions to evaluate the sample such as profession, knowledge of business processes and security and knowledge of process modeling techniques. In the second part, we used an

online order process, as shown in Figure 1, as running example. We asked the participants to answer if certain statements (e.g., user has to login before ordering the product) were true to assess if participants understood the sample process, if the example was comprehensible (answers: yes, no, I am not sure) and to explain their decision. Based on Example 1 (cf. Fig. 1), we created two more examples in which we integrated e.g., padlock symbols (cf. Example 2 in Fig. 2) to assess if the participants can identify and interpret BPMN extensions in a business process. We asked the participants to take a look at Example 1 and Example 2, to evaluate if there were differences in Example 2 and to describe them. For each integrated symbol, we asked the participants to select the meaning of the symbol. In the third part, we used BPMN security extensions detached from business processes and asked the participants questions on the understandability and interpretation of the meaning of these symbols. Specifically, the participants had to associate a purpose, to answer if the symbol was comprehensible and to describe the meaning of each symbol. For example, participants should associate a purpose for each of the 11 symbols (multiple choice questions (MCS) with exactly 11 options). Additionally, the participants had to describe the meaning of the symbols with their own words. At last, the participants were asked to describe symbols for access control and privacy.

#### IV. RESULTS

##### A. Literature Review

The first research questions aim to identify current research and practice in security modeling in BPMN.

1) *RQ1.1: How does the BPMN standard support security?*: BPMN supports the modeling of resource assignments with swimlanes i.e., pools and lanes (cf. <http://www.omg.org/bpmn/Samples/Elements/Swimlanes.htm>). A pool is a visual representation of a participant in a collaboration and can contain lanes [7]; a lane is a sub-partition of a process and utilized to organize activities within a pool. Often, lanes are used to describe internal roles. Additionally, text annotations can be used to provide additional information in a BPMN diagram. The Auditing element allows for a definition of attributes but its concrete specification is not included in BPMN. Further security extensions are inevitable to enable the modeling of e.g., separation of duty constraints which have been addressed by research and we will outline in the next sections.

2) *RQ1.2: Do BPMN extensions that support security aspects exist?*: Table I displays BPMN security extensions found in the literature review. We list title, reference and position in a BPMN diagram (e.g., attachment to an activity or a group of activities) for each symbol. In the following, we will summarize the BPMN security extensions found in the literature review.

**Padlock Symbols:** Padlock symbols are used in combination with text in [3] (symbols A-G) and with scale value in symbol R [17].

**Separation and Binding of Duty:** Separation of duty (SoD) is a principle to distribute tasks and privileges among multiple users to prevent error and fraud (cf. [21]). Although in literature, SoD constraints are very often used as example, the visual representation in a process modeling language is rather uncommon. For example in PAIS implementations (cmp. [22]), these constraints can be configured in popup windows associated to tasks. Three modeling approaches exist: the first in [6] (symbols J, K in Table I) and a year later a second in [16] (L, M) and another set (N, O) in [4]. A notation  $(n, m)$  is used in [6] to display SoD/BoD constraints:  $n$  defines the minimal number of different users that have to execute an activity and  $m$  is the sum of activity instances a user is allowed to execute. In [18], hybrid symbols (text and graphics) are used to represent SoD which resemble activities in shape but differ in color and graphics.

**Role Hierarchy:** So far, only “flat” role hierarchies can be displayed in BPMN using pools and lanes (cf. Section IV-A1). With nested lanes as proposed in [6], a role-based task authorization inheritance and role hierarchy can be modeled (e.g., Fig. 3 in [6]). However, nested lanes provide only one additional hierarchy layer and more complex role hierarchies cannot be displayed.

Furthermore, *Organizational Trust* (symbol S) defines the trust relationship between two or more participants and *Security Group* (T) defines security intentions for a group of activities, data objects or pools.

##### B. Survey

With an online questionnaire, we investigated research questions (2), (2.1), (2.2) and (3). In total, 44 participants answered the online questionnaire. The participants consisted of a mix of scientists (57%), practitioners (11%), students (16%) and others (16%). The participants work in the area of computer science such as information systems, BPM, visualization and software engineering. Most participants stated that they have a high or basic expertise in business processes. Most participants have no or basic knowledge of security. 10 participants stated they are experts in security. Furthermore, most participants are very familiar with process modeling languages such as BPMN and UML.

1) *RQ2.1: Can BPMN security extensions be identified in business processes?*: In general, the sample process was well understood by most participants. In Example 1, we integrated padlock symbols (cf. Section IV-A) and 37 participants recognized and identified the new additional elements. However, to define the meaning of the padlock symbol *Privacy* returned a mixed result between privacy (17), binding of duty (10) and access control (8). Most participants were not sure if their answer was correct. On the other hand, the padlock symbol *Access Control* was identified by most participants and most participants were certain that the answer was correct.

In Example 2, we integrated a BoD symbol for a group of activities from [6] and a manual task. Most participants found all new elements in the process model. Many participants identified the manual (i.e., human) task (27) and

#	Symbol(s)	Title (Meaning)	Ref.	Position					
				Pool	Lane	Group	Activity	Message Flow	Data Object
A		Access Control	[3]	☒	☒	☒	☒	☐	☐
B		Privacy	[3]	☒	☒	☒	☐	☐	☐
C		Non-repudiation	[3]	☐	☐	☐	☐	☒	☐
D		Attack Harm Detection	[3]	☒	☒	☒	☒	☒	☒
E		Integrity	[3]	☐	☐	☐	☐	☒	☒
F	none	Security Role	[3]	☒	☒	☒	☐	☐	☐
G	none	Security Permission	[3]	☐	☐	☐	☒	☒	☒
H		Manual Task	[6]	☐	☐	☐	☒	☐	☐
I		Automatic Task	[6]	☐	☐	☐	☒	☐	☐
J		Separation of Duty (2007)	[6]	☐	☒	☒	☒	☐	☐
K		Binding of Duty (2007)	[6]	☐	☒	☒	☒	☐	☐
L		Separation of Duty (2008)	[16]	☐	☐	☒	☒	☐	☐
M		Binding of Duty (2008)	[16]	☐	☐	☒	☒	☐	☐
N		Separation of Duty (2008)	[4]	☐	☐	☒	☒	☐	☐
O		Binding of Duty (2008)	[4]	☐	☐	☒	☒	☐	☐
P		Manual Task (2008)	[4]	☐	☐	☐	☒	☐	☐
Q		Automatic Task (2008)	[4]	☐	☐	☐	☒	☐	☐
R		Overall Asset Value Scale	[17]	☐	☐	☐	☒	☐	☒
S		Organizational Trust	[17]	☒	☐	☐	☐	☐	☐
T		Security Group	[17]	☒	☐	☒	☐	☐	☒

Table I  
OVERVIEW OF SECURITY-RELATED BPMN EXTENSIONS

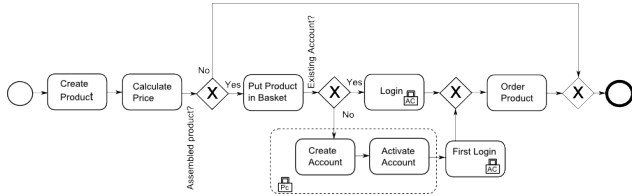


Figure 2. Example 2 includes Padlocks for Access Control and Privacy

as authentication of a user (13). Hence, the participants also associated the manual task symbol with a human (or user) authentication. The SoD symbol was mostly misunderstood and often described as BoD (23) followed by SoD (8). One reason could be that the participants were not familiar with the concepts of BoD/SoD. Another reason could be that the numbers (2, 1) might have been confusing or can easily be misinterpreted by participants.

2) *RQ2.2: Can BPMN security extensions be identified as isolated symbols?*: Table II displays the results for all isolated symbols and should be examined column by column. Underlined numbers indicate the correct answer. In general, most symbols were correctly identified by the participants, especially if they use well known letters or symbols (e.g., symbol A, C and E). Detaching the icons from a flow object (e.g., an activity) also signified that a substantial part of the context of the symbol was removed

(e.g., an activity for Q and P in Table II). As the activity was not part of the symbol anymore, we renamed the symbols. Q related to the automation of activities with a given systems' security. As human task, P is used in a security context where user rights are required to perform an activity.

We investigated both privacy symbols (U and P) for comparison reasons. While the authors in [3] state that "x" can be removed in case of no specific privacy is stated, they display only padlocks "Px" and "Pc" in [3]. Therefore, we examined also "Px". In this case, we chose to use common terms such as (high) privacy to determine if the participants could relate to that. Even though we assumed that high privacy was related to "Px" because it enforces anonymity and confidentiality (opposing to "Pc" which only enforces confidentiality) and the most participants chose the meaning correctly, we are unsure if we can interpret this also as such. We think that the participants related the abbreviation "Pc" to privaCy and they could relate "Px" to either high privacy or privacy.

3) *RQ2.3: Which extensions are often identified accurately and which are not?*: As can be seen from Table II, symbols P, A, C and E were accurately identified by most participants. However, some other symbols Q, D, K and J were only correctly interpreted by some participants.











Answer/Symbol										
	Q	P	A	U	C	D	E	B	K	J
Access Control	0	2	<u>40</u>	3	1	1	1	1	1	2
Attack Harm Detection	26	0	0	0	0	<u>14</u>	0	0	0	0
Binding of Duty	2	2	0	0	0	1	0	0	<u>9</u>	11
High Privacy	1	0	0	6	0	0	2	<u>14</u>	0	0
Integrity	0	0	0	0	0	2	<u>31</u>	0	0	0
Non-Repudiation	0	2	0	0	<u>31</u>	0	0	0	0	1
Privacy	0	0	0	<u>24</u>	2	1	0	11	0	0
Separation of Duty	0	1	0	2	0	0	0	0	17	<u>12</u>
System Security	<u>7</u>	0	1	1	1	2	0	1	2	2
User Rights	0	<u>27</u>	0	0	0	1	1	1	2	2
I do not know	6	4	2	6	6	18	8	12	9	12

Table II  
RESULTS FOR RELATING ISOLATED SYMBOLS TO MEANING

4) *RQ3: Which symbols are suggested for displaying access control and privacy?*: The participants suggested several symbols for access control: lock (7 times stated), key (6) and padlock (4). Often the participants suggested to combine these symbols with text such as “AC” (7) and “Access control” (3). In case of privacy, the most frequent answers were lock (11) and padlock (4) symbols. Two participants mentioned a human shape surrounded by a circle or cover. Participants suggested to add text such as “P” (4), “Privacy” (2), “PC” (2) and “Px” (2). Both results for access control and privacy support overall the BPMN extension symbols presented in earlier sections.

## V. INTERPRETATION AND RECOMMENDATIONS

In general, we perceived that security extensions in BPMN were accepted as important domain feature (and not rejected). We discovered several advantages and disadvantages of the extensions: Overall the participants of our study identified and interpreted the most security extensions in a business process correctly. However, separation and binding of duty principles were not easily perceived. This is surprising because most literature on security in PAIS uses SoD and BoD examples in case studies (e.g., [16], [18], [22]). Furthermore current extensions only provide a basic set of symbols. Further security aspects could be covered with symbols such as encryption and risks. However, a thorough investigation would be needed of what organizations and modelers really need and which security concepts should be selected.

In the following, we discuss and present several recommendations for designers and developers of future BPMN (security) extensions.

- A. **Use of Scientific Principles:** The use of scientific principles to design and evaluate process modeling languages is strongly recommended. For example, evaluating the quality of models (e.g., [9]) or evaluating visual notations (e.g., [8]). This rich set of principles provides designers and developers with methods to analyze and evaluate their languages. We were surprised that this was not common knowledge and practice.
- B. **Integration of End Users is Indispensable:** As this study was the first approach to evaluate BPMN

security extensions with participants, further studies are important to evaluate when e.g., designing and developing new process modeling languages (cmp. [8]) or extending it with additional symbols. An evaluation with end users who will later work with these models is required and should be performed beforehand.

- C. **Transfer of New Domain Knowledge:** For the participants, their level of security knowledge was the most challenging factor. We received multiple feedback in the questionnaire that our participants were uncertain about several security concepts. This can be also seen in the results in Table II. Based on the feedback, we propose that for an evaluation of new extensions concepts should be explained to novices beforehand or shortly explained (e.g., in a legend).

## VI. DISCUSSION

In the survey, the participants were asked to write down the meaning of each symbol. With this, we were trying to identify what meaning participants associate with each symbol. However, because of the closed multiple choice answers before, one can assume that they used the same answers in the open questions. We are surprised that this was often not the case. With these open questions, participants could provide an insight to what they think of a symbol and described often what they did not understand. Therefore, this section was very important to our research.

Due to the low quality of some visualizations in the publications and the nonavailability of all modeling concepts in tools we decided to redraw the symbols. Although we tried to paint the symbols as similar as we could, one can see that there are minor differences between the published and the redrawn symbols. However, we think that the meaning of each symbol was still transported and the evaluation is valid.

Several opportunities for future research emerge from our study. For example, one could test how these BPMN security extensions are handled and utilized during the act of process modeling (e.g., on paper or on computer). Another experimental setup (e.g., [23]) could be the evaluation of hand-sketched drawings of people.

## VII. CONCLUSION

This paper analyzed and evaluated the modeling of security aspects in BPMN. Therefore, we first analyzed current state of the art to find out how security can be modeled in BPMN. While the BPMN standard supports security only indirectly via resource assignments (i.e., swimlanes), further extensions exist that provide additional symbols such as for access control and integrity. Additionally, we performed a survey to evaluate the comprehensibility of BPMN security extensions. We found that the participants could identify and interpret many symbols in the business process context. However, it was difficult for them to interpret symbols where domain knowledge is required.

## ACKNOWLEDGMENT

The authors would like to thank the experts of the pre-analysis and the participants of the survey for their support and contributions.

## REFERENCES

- [1] M. Weske, *Business Process Management: Concepts, Languages, Architectures*. Springer, 2007.
- [2] V. Atluri and J. Warner, "Security for workflow systems," *Handbook of Database Security: Applications and Trends*, p. 213, 2007.
- [3] A. Rodriguez, E. Fernandez-Medina, and M. Piattini, "A BPMN extension for the modeling of security requirements in business processes," *IEICE TRANSACTIONS on Information and Systems*, vol. E90-D, no. 4, pp. 745–752, Apr. 2007.
- [4] C. Wolter, M. Menzel, and C. Meinel, "Modelling security goals in business processes," in *Modellierung*, ser. volume 127 of LNI. Berlin, Germany, 2008. GI, 2008, p. 197–212.
- [5] J. Mendling, H. A. Reijers, and J. Cardoso, "What makes process models understandable?" in *Business Process Management*, ser. LNCS. Springer, 2007, no. 4714, pp. 48–63.
- [6] C. Wolter and A. Schaad, "Modeling of task-based authorization constraints in BPMN," in *Business Process Management*, ser. LNCS. Springer, 2007, vol. 4714, p. 64–79.
- [7] OMG, "Business process model and notation (BPMN) version 2.0," OMG, OMG Document formal/2011-01-03, Jan. 2011. [Online]. Available: <http://www.omg.org/spec/BPMN/2.0/>
- [8] D. Moody, "The physics of notations: Toward a scientific basis for constructing visual notations in software engineering," *IEEE Transactions on Software Engineering*, vol. 35, no. 6, pp. 756–779, Dec. 2009.
- [9] D. L. Moody, "Theoretical and practical issues in evaluating the quality of conceptual models: current state and future directions," *Data & Knowledge Engineering*, vol. 55, no. 3, pp. 243–276, Dec. 2005.
- [10] A. F. Blackwell *et al.*, "Cognitive dimensions of notations: Design tools for cognitive technology," in *Cognitive Technology: Instruments of Mind*, ser. LNCS. Springer, Jan. 2001, no. 2117, pp. 325–341.
- [11] N. Genon, P. Heymans, and D. Amyot, "Analysing the cognitive effectiveness of the BPMN 2.0 visual notation," in *Software Language Engineering*, ser. LNCS. Springer, Jan. 2011, no. 6563, pp. 377–396.
- [12] J. Mendling, J. Recker, and H. A. Reijers, "On the usage of labels and icons in business process modeling," *International Journal of Information System Modeling and Design*, vol. 1, no. 2, pp. 40–58, 2010.
- [13] M. Riesner and G. Pernul, "Supporting compliance through enhancing internal control systems by conceptual business process security modeling," in *ACIS 2010 Proceedings*, Jan. 2010.
- [14] M. Leitner, "Security policies in adaptive process-aware information systems: Existing approaches and challenges," in *2011 Sixth Int. Conference on Availability, Reliability and Security (ARES)*. IEEE, 2011, pp. 686–691.
- [15] H. M. Cooper, "Organizing knowledge syntheses: A taxonomy of literature reviews," *Knowledge in Society*, vol. 1, no. 1, pp. 104–126, Mar. 1988.
- [16] C. Wolter, A. Schaad, and C. Meinel, "Task-based entailment constraints for basic workflow patterns," in *Proc. of the 13th ACM symposium on Access control models and technologies*, ser. SACMAT '08. ACM, 2008, p. 51–60.
- [17] M. Menzel, I. Thomas, and C. Meinel, "Security requirements specification in service-oriented business process management," in *Availability, Reliability and Security, 2009. ARES '09. Int. Conference on*. IEEE, 2009, p. 41–48.
- [18] A. D. Brucker, I. Hang, G. Lückemeyer, and R. Ruparel, "SecureBPMN: modeling and enforcing access control requirements in business processes," in *SACMAT'12*, ser. Proc. of the 17th ACM symposium on Access Control Models and Technologies. ACM, 2012, p. 123–125.
- [19] O. Altuhhova, R. Matulevicius, and N. Ahmed, "Towards definition of secure business processes," in *Advanced Information Systems Engineering Workshops*, ser. LNBIP, vol. 112. Springer, 2012, p. 1–15.
- [20] J. Lumsden and W. Morgan, "Online-questionnaire design: establishing guidelines and evaluating existing support," in *16th Annual Int. Conference of the Information Resources Management Association (IRMA'2005)*, vol. 47436. National Research Council of Canada, 2005.
- [21] R. A. Botha and J. H. P. Eloff, "Separation of duties for access control enforcement in workflow environments," *IBM Systems Journal*, vol. 40, no. 3, pp. 666–682, 2001.
- [22] M. Leitner, J. Mangler, and S. Rinderle-Ma, "SPRINT- responsibilities: Design and development of security policies in process-aware information systems," *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA)*, vol. 2, no. 4, pp. 4–26, 2011.
- [23] N. Genon, P. Caire, H. Toussaint, P. Heymans, and D. Moody, "Towards a more semantically transparent i\* visual syntax," in *Requirements Engineering: Foundation for Software Quality*, ser. LNCS. Springer, 2012, no. 7195, pp. 140–146.