Towards Security- and IIoT-Aware BPMN: A Systematic Literature Review

Markus Hornsteiner, Christoph Stoiber and Stefan Schönig
University of Regensburg, Regensburg, Germany

Keywords: Security, Industrial Internet of Things, BPMN.

Abstract: The Industrial Internet of Things (IIoT) paradigm constitutes the connection of uniquely identifiable things to the internet in an industrial context. Besides providing disruptive capabilities for companies, its connectivity and heterogeneous setup makes it vulnerable to external attacks. To properly implement security by design in the IIoT, the underlying business processes must be modelled both IIoT- and security-aware. Business Process Modeling and Notation (BPMN) is a suitable language for this purpose. In order to present the current state of research in this area, this study compares the requirements from practice and research on the basis of the EU security standard IEC62443 and reviews the current state of research in security- and IIoT-aware BPMN extensions. The findings contribute to the structured elaboration of this ambiguous research field while also elucidating the interplay of IIoT and security within BPMN. The derived research gaps constitute an agenda for further research and may guide further research endeavours in enhancing security within the IIoT.

1 INTRODUCTION

The Industrial Internet of Things (IIoT) offers a broad compendium of technologies from the Internet of Things (IoT) to automate and intelligently network production systems (Feki et al., 2013). This networking is achieved by connecting industrial operational technology (OT) with information technology (IT). The resulting convergence leads to more efficient systems and enables new solutions.

However, the convergence of IT and OT has a significant drawback: machines and plants become vulnerable to external attacks. In the context of digital production systems, it is essential to understand that cyber security is a joint and overarching task of both IT and OT areas. Therefore, security aspects for IIoT environments require special attention, while also new solutions for maintaining cyber security are necessary (Tange et al., 2020).

For this reason, there are regulatory efforts to establish the implementation of security measures like IEC62443 in the EU as a standard (Stanton et al., 2016). According to the IEC62443 standard, respective organizations should follow a ”security by design” paradigm (International Electrotechnical Commission, 2009). In this respect, to conduct meaningful and sustainable security management, it is crucial to know and define corporate assets that must be protected as well as operative processes and their information needs. Based thereon, risks can be identified, protective measures can be taken, and security incidents can be monitored. Against this background, the discipline of Business Process Management (BPM) offers numerous established methods, concepts, and technologies for the systematic modeling of operational IIoT processes that can also be exploited for improving IIoT security (Mayer, 2012; Petrasch and Hentschke, 2015; Graja et al., 2017; Dumas et al., 2018; Stoiber and Schönig, 2021). While there is already research on the integration of IoT and BPM technology in general (Janisch et al., 2020; Schönig et al., 2018; Schönig et al., 2020), we claim that BPM methods represent an unexploited source for improving cyber security in manufacturing companies (Schönig et al., 2022).

A formally defined process modeling notation, like the de-facto standard Business Process Modeling and Notation (BPMN) (OMG, 2011), is a fundamental means for implementing BPM-based security by design approach. However, since IIoT security is not yet supported, these notations must be designed or extended to represent security requirements and possible protective measures fully. While some notation extensions already exist for security aspects in the classical IT domain (Chergui and Benslimane, 2020; Maines et al., 2016; Zarour et al., 2019), many nec-

Hornsteiner, M., Stoiber, C. and Schönig, S.
Towards Security- and IIoT-Aware BPMN: A Systematic Literature Review.
DOI: 10.5220/0011317700003280
In *Proceedings of the 19th International Conference on Smart Business Technologies (ICSBT 2022)*, pages 45-56
ISBN: 978-989-758-587-6; ISSN: 2184-772X

essary language constructs for IIoT security are still missing. Both concepts must be represented accordingly to represent security and IIoT aspects in process models.

This paper is a starting point to fill the identified research gap. In a first step, we collect and consolidate security-aware IIoT modeling requirements from the latest industry standards like IEC62443 (International Electrotechnical Commission, 2009) as well as from related academic research endeavors (Tange et al., 2020). Second, we conduct two Structured Literature Reviews (SLR) where we explore the current state of the art and coverage of the identified requirements in respective BPMN extensions. The derived research gaps constitute an agenda for further research and may guide further endeavors in enhancing IIoT security utilizing BPM methods.

The remainder of this paper is organized as follows: in section 2 we discuss the theoretical background of our work and elaborate on related work. Afterward, in section 3 we discuss our research methodology and approaches. This is followed in section 4 with the merging of security requirements from science and industry and the description of our performed SLRs. From this, we explain in section 5 the findings of our research and potential future research. Which we conclude in section 6.

2 THEORETICAL BACKGROUND

2.1 Security within the IIoT

The IIoT constitutes a new era in industrial production since it marks the beginning of a fundamental paradigm shift (ENISA, 2018). By utilizing IoT technologies, it is possible to network machines, people, and whole factories. Thereby, new production processes such as personalized products on an industrial scale and new business models, like data-driven services, are possible (Stoiber and Schönig, 2022a; Stoiber and Schönig, 2022b). Whereas the IIoT brings new opportunities, networking also has its downsides. Through the networking of all industrial components, there are new ways for attackers to infiltrate, interrupt or maliciously modify processes in production (ENISA, 2018). One unique aspect of IIoT security, in contrast to IT security, is that it is mainly concerned with the security of OT and in that the availability (Tange et al., 2020). To ensure that, in industrial standards like the IEC62443, the security by design paradigm is required (International Electrotechnical Commission, 2009). That means that the security of processes and components must be ensured as early as in the design process. To consider security in industrial processes, there is a need for an inclusive modeling language that enables the modeling of security- and IIoT-aware processes.

2.2 Related Work

To the best of our knowledge, only two SLRs deal with BPMN extensions. The first one of Braun and Esswein (Braun and Esswein, 2014) examined and classified 30 existing BPMN extensions. Despite its extensiveness, it constitutes a general review and does not explicitly address the IIoT paradigm. Furthermore, it includes articles published before version 2.0 of BPMN and thus obsolete extensions. The second article in this area was done by (Zarour et al., 2020), which also deals with BPMN extensions in a general manner. They included literature from the year 2014 and ongoing, the year of publication by Braun and Esswein, and provide a comprehensive overview of the published BPMN extensions. However, they also provide a general overview without specializing in specific sub-topics. As we explicitly focus on security and IIoT, the two existing SLRs do not cover the required literature to unravel the phenomenon under consideration. Hence, we take a deeper look into the relevant BPMN extensions and provide a valuable reprocessing and structuring of the existing ones.

3 RESEARCH METHODOLOGY

To explore the current state of security- and IIoT-aware BPMN extensions, we conducted an extensive SLR. Methodically, we relied on Okoli (Okoli, 2015) who proposed an eight-step process to conduct literature reviews systematically. Following these steps, we thereby performed a forward and backward reference search as suggested by Levy and Ellis (Levy and J. Ellis, 2006). Thus, we present two SLRs in this paper, performed according to the criteria just discussed. The first one explored the current state of research in security extensions for BPMN. The second one focused on the current state of research in IIoT extensions for BPMN. The presentation of the search process and communication of the results has been performed using the PRISMA statement (cf. Figure 1) (Page et al., 2021).

To include or exclude literature, Okoli (Okoli, 2015) recommended to define specific screens in advance. These support a goal-oriented inclusion or exclusion of identified literature. Within the two conducted SLRs we have defined five screens:

Screen 1 - Duplicates. Articles that appeared more

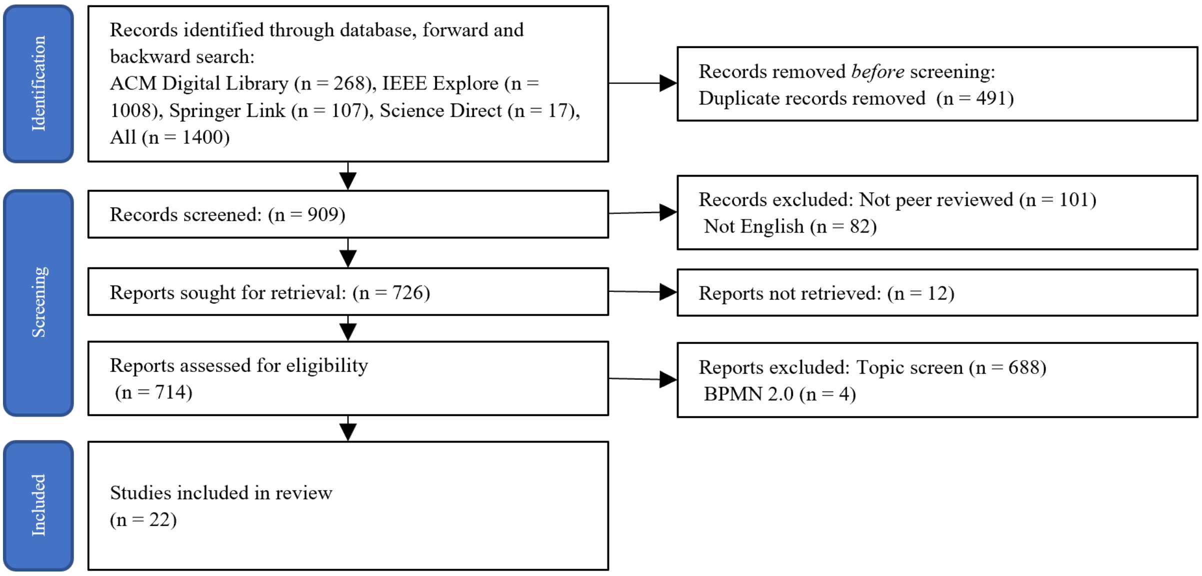
Identification
Records identified through database, forward and backward search:
ACM Digital Library (n = 268), IEEE Explore (n = 1008), Springer Link (n = 107), Science Direct (n = 17), All (n = 1400)
Records removed *before* screening:
Duplicate records removed (n = 491)
Screening
Records screened: (n = 909)
Records excluded: Not peer reviewed (n = 101)
Not English (n = 82)
Reports sought for retrieval: (n = 726)
Reports not retrieved: (n = 12)
Reports assessed for eligibility
(n = 714)
Reports excluded: Topic screen (n = 688)
BPMN 2.0 (n = 4)
Included
Studies included in review
(n = 22)

Figure 1: PRISMA flow diagram.

than once were marked as duplicates and only processed once. For this purpose, we used a self-developed Python script [1] for the automated evaluation of duplicates. This script automatically identified and marked duplicates.

Screen 2 - Journal or Conference Proceedings. Only articles that have been published either in a journal or in conference proceedings were eligible for further analysis. This ensured that only literature that has been recognized as relevant by other researchers was listed in the final set.

Screen 3 English & Access. Articles must have been written in English. Furthermore, they must have been accessible via established online sources. If this was not the case, we contacted the authors directly. If an article has not been accessible, it was marked as not accessible.

Screen 4: Topic Screen. Screen 4 specified that the literature fitted the subject area. This means that the article presented a BPMN extension to either a) security or b) IIoT. For example, the term *CPS* of our search string would have integrated work on *Clinical Pathways* (Braun et al., 2016). Though, as this research topic does not fit the phenomenon under consideration, screen 4 excluded it.

Screen 5: BPMN 2.0. The last screen indicated whether the literature introduced an extension for BPMN 2.0. Hence, articles that presented extensions for earlier versions of BPMN were excluded.

The queried databases of our SLR were i) ACM Digital Library, ii) IEEE Xplore, iii) Springer Link, and iv) Science Direct, as they are relevant databases in the corresponding research area. Furthermore, the performed forward, and backward searches also allowed the consideration of articles from other databases. To search for eligible literature, we developed two specific search strings: i) *[BPMN OR ”business process*”] AND [secur*] AND [extension OR annotation]* ii) *[BPMN OR ”business process*”] AND [IIoT OR ”Industrial Internet of Things” OR ”Cyber Physical Systems” OR CPS OR ”Industrie 4.0”] AND [extension OR annotation]*. The wild card operator * has been used to allow a broader query

In total, we found 1400 articles in the initial, backward, and forward searches. We excluded 491 duplicates and an additional 101 articles from this set as they were not published in journals or conference proceedings. Moreover, 82 articles were excluded because they were not written in English. Of the 726 remaining articles, 12 could not be accessed. As a result, 714 articles were assessed for eligibility. The full text of the articles were analyzed in detail regarding screens 4 and 5. After applying the screening rules, 22 articles remained and formed the final set.

[1] https://github.com/mahopy/slr_utils/blob/main/src/duplicate_finder.py

4 LITERATURE ANALYSIS

4.1 Elicit the Security Concepts

To set up appropriate security requirements, we have looked at the academic side on the one hand and the industry side on the other. On the academic side, we rely on the work of (Tange et al., 2020), which evaluated a total of 218 papers on the topic of IIoT security requirements. On the industry side, we rely on the requirements of the IEC62443 standard, which establishes technical security requirements for components of industrial automation systems (International Electrotechnical Commission, 2009).

4.1.1 Academic Security Requirements for BPMN

Authentication is defined as the process of establishing the identity of one party to another (Sandhu and Samarati, 1996). When a user logs on to a system, this can be done through knowledge, e.g., passwords, or possessions, e.g., fingerprints. However, authentication can also happen between systems and processes. In addition, authentication can always occur in both directions, i.e., both parties can identify each other. (Tange et al., 2020) subsume under this term research approaches to key distribution, mutual authentication, non-repudiation, anonymity and privacy, and attestation. They emphasize the special conditions in the IIoT context, such as particularly lightweight protocols and the number of different devices.

Access Control describes the permission that one party gives to another to view or modify resources and objects (Sandhu and Samarati, 1996). One precondition is usually authentication. For the IIoT, (Tange et al., 2020) highlights that also for access control, the most significant challenges lie in the lightweight nature of the protocols and methods and in availability. Especially in highly distributed environments like the IIoT, connections may fail, and access rules are unavailable.

Maintainability describes an entity's ability to be maintained. It expresses how easily, accurately, safely, and economically an entity can be maintained. (Blanchard et al., 1995) In the IIoT, maintainability is a mandatory requirement for systems, as they are exposed to ever new dangers due to their increasing networking (Tange et al., 2020). Again, the main challenges are the limited resources and the dynamic nature of the environment, wherefore traditional maintenance solutions reach their limits.

Resilience. Resilience in Business Information Systems describes the ability of systems to respond to unexpected impairments and continue to function (Müller et al., 2013). In this regard, unexpected means that these impairments could not have been planned for beforehand and thus represent an entirely new challenge for the system or the organization. According to (Tange et al., 2020), resilience is also a core component of security in the IIoT as, depending on the criticality of the system, failure can have severe consequences. Thus, systems should function as planned, even if they are partially compromised. To protect systems, depending on the type of system, redundant design, different systems, or hardening of systems can be possible solutions for resilience.

Security Monitoring is defined as a process in which data is recorded on the one hand and analyzed on the other to derive security-relevant events, e.g., (Bishop, 1989). Security monitoring is described by (Tange et al., 2020) who also identifies security monitoring as an essential aspect of the IIoT. Here, the focus is primarily on detection in order to be able to derive responses. This security requirement also stems from the fact that old, less secure systems are often connected to the network in the IIoT. These often have poor maintainability, so monitoring is essential here.

Data security and Data Sharing (Tange et al., 2020) summarize the aspects of data protection, data flow control, external parties, and data transport under data security and data transfer. This includes confidentiality of data as well as availability and integrity. In the industrial environment, availability and integrity are favored over confidentiality. Again, the biggest challenge in this area is the low resource availability, the heterogeneity of the devices, and the prevalent distribution. For example, classical cryptographic methods cannot be used for security as they are too computationally intensive.

Network Security is a broad field and can be seen as a subset of general computer security (Marin, 2005). It includes intrusion detection, traffic analysis, and network monitoring. Since these aspects are already present in the previous requirements, the network security of (Tange et al., 2020) refers to network infrastructure security. The biggest challenges in this area come from the high number of devices, their distribution, and the low computing power. At the same time, it must be ensured that the devices can also detect and control disconnections, e.g., while at the same time minimizing the management overhead. An important point that plays a more significant role in the IIoT is wireless communication security.

Models and Methodologies. In this subsection, (Tange et al., 2020) discuss various models and methodologies that are available in the existing literature. These include the security by design paradigm, which calls for security aspects to be considered as early as the system design stage. Furthermore, they deal with works that deal with risk and threat assessment, especially concerning the specific challenges of the IIoT.

4.1.2 IEC62443

The International Electrotechnical Commission (IEC) is a non-profit, non-governmental organization that issues internationally recognized standards in electrical engineering and electronics. It has developed the 62443 series of standards to reflect the specific requirements of IT security in industrial plants (International Electrotechnical Commission, 2009). Although the development of the standard is not yet complete, its acceptance in the industry is growing (Pierre Kobes, 2016). The standard consists of four areas. The first deals with general principles, the second with organizational measures and processes, the third with technical components, and the fourth with requirements for manufacturers of components used in automation solutions. One of the essential foundations of the standard is the *Defense-in-Depth* strategy. This is a strategy from the military context, which states that individual measures alone cannot be successful but that there must be several levels of protection. A potential attacker must always work his way through several layers of defense to disrupt one component. To achieve security in industrial facilities, the standard establishes seven basic requirements described in the following. The description of each concept is based on Kobes (Pierre Kobes, 2016):

Identification and authentication Control. All users, whether human, software, or device, must be identified and authenticated before gaining access to a system.

Use Control. Once users have been successfully identified and authenticated, their use must be limited to the actions intended for them. This means that they may only perform actions for which they have been granted authorization. In addition, depending on the implemented security level, the use of the authorization should be monitored.

System Integrity is the requirement that an industrial system behaves as intended at all times and that the data of the device cannot be changed unnoticed. In addition, depending on the security level, this also includes tracking and monitoring the component.

Data Confidentiality means that the data generated by systems is protected from unauthorized access and modification during transmission and storage.

Restricted Data Flow refers to a fundamental requirement of IEC62443 which states that network parts should be isolated from each other. In particular, critical networks should be logically or physically divided into zones so that no communication can occur between them or only according to predefined rules.

Timely Response to Events describes that operators should monitor their facilities to detect and respond to safety incidents with predetermined procedures and guidelines established based on a risk assessment. In other words, in the event of a detected security incident, the procedure should already be straightforward in order to be able to respond to it without delay.

Resource Availability describes that systems should be resistant to failure due to attack or malfunction. In particular, critical systems do not fail in their entirety even if sub-areas fail. Suitable measures should be in place to withstand and defend against targeted attacks by outsiders, such as denial of service attacks.

4.1.3 Merging the Requirements from Academic and Industry

Having previously elaborated on the various aspects of academics and industry, in the following, we make a first attempt to align them with each other and create a shared understanding. For this purpose, we use the basic requirements of Confidentiality, Integrity, and Availability and extend them by the points jointly required from academics and industry. Both sides describe in their requirement that users must be uniquely authenticated and authorized to access data and systems. To this end, they describe advanced models such as two-factor authentication, central user management, and the like. We subsume these requirements under the security basis requirement **Confidentiality**, which describes that resources must be protected from unauthorized viewing and access. Further, both sides describe that data and assets must be protected from changes being made to them by unauthorized people, processes, or devices. We subsume these requirements under the essential requirement

integrity, which defines precisely these requirements. Both sides describe that processes and components of systems must be protected against failure. For example, IEC62443 explicitly specifies that DDoS attacks must not lead to failure. In addition to this, the communication networks and data must also be designed to be fail-safe, according to the requirements. We subsume these requirements under the basic requirement **availability**. Another requirement, which can be derived from the requirements of academics and industry, is **maintainability**. This describes that components and software must offer the possibility of being updated. It has been shown that outdated systems for which updates are no longer available are particularly susceptible to attacks, especially if they are accessible from the Internet, as in IIoT. The academic side explicitly identifies **monitoring** as one of the security requirements, while IEC62443 only specifies fast response to events as a requirement. However, monitoring is necessary for a fast response, and the IEC standard specifies components such as 'testable events and their recording' in the sub-requirements. Thus, monitoring is also an explicit fundamental component of the IEC, so we identify it as a different security requirement. Both sides describe that in developing systems architecture and implementing security guidelines, one should rely on proven methodologies and procedures. In addition, procedures should be defined from the outset in the event of an incident to ensure the fastest possible action. Both sides cite security by design, for example, as an essential fundamental principle. In order to be able to map these criteria, we propose the requirement **Models and Methodologies**, which on the one hand, means the use of recognized principles and, on the other hand, the preparation of procedure plans for the mitigation of incidents.

4.2 Security Related BPMN Extensions

The following chapter presents the publications we found in the SLR with associated publications. For this purpose, all publications and associated publications are listed with an ID in table 1. The ID is used in table 2 to uniquely assign the papers that integrate a particular element. The *Associated Publications* column in table 1 contains papers that have done preliminary work on the papers listed in the *Publication* column. These are also found to be relevant in the SLR, but they contain only abbreviated content that is also contained in the papers in *Publication*. Finally, in the *Name of the Extension* column, we provide the name of the extension if the authors mention one.

In table 2 all security aspects are entered, which are handled by the papers considered relevant. This table has been shortened for clarity, and only elements addressed in more than one paper have been included. The complete table can be obtained from the authors upon request or from Github [2]. In table 2, the ID is entered in the first row, which refers to the ID in table 1. Subsequently, the various security aspects covered in the papers are listed in table 2. If an article contains a specific aspect, it is marked with a ✓in the table. If an article does not contain an aspect, it is marked with a ✗. The last row of the table shows the number of papers that contain a certain aspect. This shows that 11 of the 12 papers deal with the aspects *Confidentiality* and *Integrity*. 8 of the 12 papers deal with *Integrity* or *Authentication*. All other aspects are covered in 5 or fewer papers. In the following, we discuss the use cases of the individual works. In doing so, we reference them with the ID presented in table 1. The use case and corresponding specialization of 2, 4, and 8 are related to the healthcare sector. One deals with a use case from a generic internet store. The specialization of 1's work is that they model vulnerabilities and mitigation in addition to security requirements. Work 3,7,9 and 11 deals with use cases from business administration. Work 5 deals with outsourcing business processes to the cloud and the associated security requirements. Only work 6 refers to a use case from the manufacturing domain. Here they use the Software Quality Requirements Engineering (Mead and Stehney, 2005) and the Software Requirements Engineering Process (Mellado et al., 2007) to develop a security requirements engineering framework. Overall, however, it can be seen here that none of the works explicitly deals with the IIoT or integrates aspects of it. Furthermore, all the work only considers business processes, and none of the papers considers the processes from the IIoT device point of view.

4.3 IoT Related BPMN Extensions

For projects that extend BPMN with IIoT elements, we found a total of 10, as shown in table 3. Here, the names of the independent research projects are listed in the table's first column. The second column lists the associated publication. In the third column, related publications are listed. We define related publications as follows: Related works by the same author deal with the same topic and differ only slightly, for example, by individual added sections. For example, both (Graja et al., 2016) and (Graja et al., 2017) were present in our result set. Where (Graja et al., 2016) is the original paper, and (Graja et al., 2017) extends it with temporal properties. For IoT-A, both papers ap-

[2] https://github.com/mahopy/IIoTSecBPMN/blob/master/security_extensions.csv

Table 1: Included publications of SLR with associated publications.

ID	Publication	Associated Publications	Name of the Extension
1	(Altuhhova et al., 2013)		
2	(Chergui and Benslimane, 2020)	(Chergui and Benslimane, 2018)	
3	(Argyropoulos et al., 2017)		
4	(Sang and Zhou, 2015)		
5	(Zarour et al., 2019)		BPMON
6	(Zareen et al., 2020)		
7	(Turki et al., 2012)		
8	(Ramadan et al., 2018)	(Salnitri et al., 2017; Salnitri et al., 2016)	SecBPMN2
9	(Brucker, 2013)	(Brucker and Hang, 2012)	SecureBPMN
10	(Maines et al., 2016)		
11	(Mülle et al., 2011b)	(Mülle et al., 2011a)	
12	(Pullonen et al., 2019)		PE-BPMN

Table 2: Overview of the covered security aspects.

ID	Confidentiality	Integrity	Availability	Attack / harm detection and prevention	Accountability	Auditability	Non-Repudiation	Authorization	Authentication	Secure Channel	Encrypted Message	Access Control	Separation / Binding of Duty	Anonymity	Privacy	Delegation
1	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
2	✓	✓	✓	✓	✗	✓	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗
3	✓	✓	✓	✗	✗	✗	✗	✓	✓	✓	✗	✗	✗	✗	✗	✗
4	✓	✓	✓	✓	✗	✗	✓	✓	✓	✓	✓	✓	✗	✗	✗	✗
5	✓	✓	✓	✗	✗	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗
6	✓	✓	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
7	✓	✓	✗	✗	✗	✗	✓	✗	✓	✗	✗	✗	✓	✗	✓	✗
8	✓	✓	✓	✗	✓	✓	✓	✗	✓	✗	✗	✗	✓	✓	✓	✗
9	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✗	✗	✓
10	✗	✓	✓	✓	✓	✗	✗	✗	✗	✗	✗	✓	✗	✗	✓	✗
11	✓	✓	✗	✗	✗	✓	✗	✓	✓	✗	✗	✗	✓	✗	✗	✓
12	✓	✓	✗	✗	✗	✗	✗	✗	✓	✓	✓	✗	✗	✓	✓	✗
∑	11	11	8	3	3	3	5	4	8	3	2	3	4	2	4	2

pearing in our result set are in the Publication column since they belong to the same research project but present separate concepts. The article (Meyer et al., 2013) presents how IoT Devices can be integrated into BPMN models and (Meyer et al., 2015) presents how ”things” can be represented.

Table 4 shows the extensions presented by each article. This is an abbreviated representation of the table, listing only the elements proposed by more than one paper. For example, (Graja et al., 2017) presents an extension that includes temporal properties such as start and end times. However, since it is the only publication that considers these aspects, it is not shown in this overview. An unabridged table can be requested

Table 3: Included publications of SLR with associated publications.

Name of the extension	Publication	associated publications
BPMN4CPS	(Graja et al., 2017)	(Graja et al., 2016)
I4PML	(Petrasch and Hentschke, 2016)	(Petrasch and Hentschke, 2015)
IoT-A	(Meyer et al., 2013) (Meyer et al., 2015)	(Mayer, 2012)
BPMN4WSN	(Sungur et al., 2013)	
PyBPMN	(Bocciarelli et al., 2017)	(Bocciarelli and D'Ambrogio, 2011) (Bocciarelli et al., 2014)(Bocciarelli et al., 2016)
IOBP 4.0	(Ribeiro et al., 2021)	
uBPMN	(Yousfi et al., 2016)	
Cheng et al.	(Cheng et al., 2019)	
Chiu et al.	(Chiu and Wang, 2015)	

Table 4: Overview of the covered IoT aspects.

Extension	Actuator	Sensor	Cloud Services	Physical Entity	Mobility aspect	Real Data Store	Real Data Object	IoT Device
BPMN4CPS	✓	✓	✓	✓	✓	✗	✗	✗
I4PML	✓	✓	✓	✗	✓	✓	✓	✓
IoT-A	✓	✓	✗	✓	✓	✓	✓	✓
BPMN4WSN	✓	✓	✗	✗	✗	✗	✗	✓
PyBPMN	✓	✓	✗	✗	✗	✗	✗	✗
IOBP 4.0	✓	✓	✗	✗	✗	✗	✗	✗
uBPMN	✗	✓	✗	✗	✗	✗	✓	✗
Cheng et al.	✗	✓	✗	✗	✗	✗	✗	✗
Chiu et al.	✓	✓	✗	✗	✗	✗	✗	✗

from the authors or can be found at Github [3].

The table again shows the individual publications line by line. In the first column is the name, followed by if an extension deals with an IoT aspect. If the aspect is present in the paper, this is marked with an ✓at the respective position in the table. If the paper does not cover the aspect, this is marked with a ✗. Here, all but two, uBPMN and Cheng et al. incorporate the actuator. All works integrate the sensor as an IoT aspect. The Cloud Services aspect is included by only two publications, BPMN4CPS and I4PML. Physical Entities represent real-world objects, which deliver information to the digital world, is included by two papers, BPMN4CPS and IoT-A. BPMN4CPS, I4PML, and IoT-A represent the mobility aspect, while I4PML has taken the aspect from IoT-A. The Real Data Store for storing real-world data recorded by sensors is represented by I4PML and IoT-A, where I4PML references IoT-A. The Real Data Object as a representation of data from the real world, digitized by sensors, is modeled by I4PML, IoT-A, and uBPMN. I4PML also references IoT-A as the source here. The IoT Device as a representation of an IoT Device with capabilities such as Actuating or Sensing and as an interface of the real to the digital world is represented by I4PML, IoT-A, and BPMN4WSN. Here, too, I4PML refers to IoT-A.

5 FINDINGS AND RESEARCH OPPORTUNITIES

Having conducted two SLRs, we identified two major research gaps that should be tackled by future research. Currently, there is a gap in the research on inclusive consideration of security and IIoT in BPMN.

[3] https://github.com/mahopy/IIoTSecBPMN/blob/master/iiot_extensions.csv

This means that currently, there are only extensions that allow the modeling of either security or IIoT aspects. As a result, modeling of security and IIoT has no interconnections and is done individually by the corresponding experts in both areas. Joint modeling is not possible. While it has already been shown that the integration of different business units by a common modeling language can help to bridge the communication gap (Zor et al., 2011; Meyer et al., 2013; Cheng et al., 2019). For example, (Zor et al., 2011) states that by extending BPMN to represent tasks at the manufacturing operations level, the communication gap between management, where BPMN is already standard, and the shop floor can be closed. They see this as an advantage for companies since the two levels can then exchange information using a common language, while, e.g., business analysts have the opportunity to understand and optimize processes on the shop floor. In addition, the authors see an advantage in the fact that business analysts have a common language with engineers and can therefore communicate more effectively with them. This should lead to better performance for companies. We also see these benefits of a common modeling language for security and IIoT experts, as they can use it to optimize processes in the IIoT together in a secure manner. To the best of our knowledge, this approach is only present in (Ribeiro et al., 2021) since they have additionally integrated the security elements of private and shared data and regularities in their IoT extension.

We see another research gap beside the inclusive representation of security and IIoT in BPMN. Prior security-aware BPMN extensions are, in some cases, already based on existing security methods and prevalent best practices. However, the requirements from practice, especially from IEC62443, have not been included so far. For example, (Chergui and Benslimane, 2020) and (Maines et al., 2016) use the ontology of (Maines et al., 2015) to build their extension on it. However, the problem is that the ontology was created based on published BPMN extensions and, thus, only covers the already known aspects from academics. (Altuhhova et al., 2013) build their extensions based on the work of (Dubois et al., 2010; Mayer, 2009), which covers a wide range of security requirements. Yet, there is no explicit view of the required aspects on the industry side. (Brucker, 2013) base their work on the Reference Model of Information Assurance and Security (RMIAS), which covers eight essential security goals based on research on information security and information assurance. This is an extension of the CIA baseline requirements and covers a broad area but does not explicitly target the requirements of IIoT. Overall, however, the perspective from practice, particularly IEC62443, is missing, and thus aspects such as maintainability or monitoring are missing in the extensions as security requirements.

6 CONCLUSION AND IMPLICATIONS

This study provides an overview of the current state of research in the area of security- and IIoT-aware extensions for BPMN. By conducting two extensive SLRs, based on (Okoli, 2015), a comprehensive analysis of past research and existing research gaps could be performed. As part of the SLRs, we examined 1400 sources, of which 22 were then identified as relevant to our research. Twelve of them are for security-aware BPMN and 10 for IoT-aware BPMN. The core theoretical implications of our study are twofold as they structure and elaborate existing knowledge on security- and IIoT-aware BPMN and lay the foundation for further theorizing and research endeavors. In this regard, especially two findings should be highlighted. On the one hand, existing security-aware BPMN extensions do not yet consider the requirements of IEC62443, which is an important security standard in the industrial environment. On the other hand, no extension enables the joint modeling of security and IIoT with the help of BPMN. Consequently, two potential research areas in this area are comparing security requirements from academics and industry and developing an extension for BPMN that enables security and IIoT aware modeling. The results of this study may lay the foundation for further research on secure IIoT, while the identified research gaps should be starting points.

ACKNOWLEDGEMENTS

This work is funded by the “Bavarian Ministry of Economic Affairs, Regional Development and Energy” within the project *INduStrial IoT Security Operations CenTer (INSIST).*

REFERENCES

Altuhhova, O., Matulevičius, R., and Ahmed, N. (2013). An extension of business process model and notation for security risk management. *IJISMD*, 4(4):93–113.

Argyropoulos, N., Mouratidis, H., and Fish, A. (2017). Attribute-Based Security Verification of Business Process Models. In *Conf. Business Informatics (CBI)*, volume 01, pages 43–52.

Bishop, M. (1989). Model of security monitoring. In *ACSAC*, pages 46–52. IEEE Comput. Soc. Press.

Blanchard, B. S., Verma, D. C., and Peterson, E. L. (1995). *Maintainability: A Key to Effective Serviceability and Maintenance Management*. John Wiley & Sons.

Bocciarelli, P. and D'Ambrogio, A. (2011). A BPMN Extension for Modeling Non Functional Properties of Business Processes. In *Symposium on Theory of Modeling &amp; Simulation*, page 160–168.

Bocciarelli, P., D'Ambrogio, A., Giglio, A., and Paglia, E. (2014). Simulation-based performance and reliability analysis of business processes. In *Proc. Winter Simulation Conference*, pages 3012–3023. IEEE.

Bocciarelli, P., D'Ambrogio, A., Giglio, A., and Paglia, E. (2016). A BPMN extension to enable the explicit modeling of task resources. In *CEUR Workshop Proceedings*, volume 1728, pages 40–47.

Bocciarelli, P., D'Ambrogio, A., Giglio, A., and Paglia, E. (2017). A BPMN extension for modeling Cyber-Physical-Production-Systems in the context of Industry 4.0. In *Int. Conf. on Networking, Sensing and Control (ICNSC)*, pages 599–604.

Braun, R. and Esswein, W. (2014). Classification of domain-specific BPMN extensions. In Frank, U., Loucopoulos, P., Pastor, O., and Petrounias, I., editors, *The Practice of Enterprise Modeling - 7th IFIP WG 8.1 Working Conference, PoEM 2014, Manchester, UK, November 12-13, 2014. Proceedings*, volume 197 of *Lecture Notes in Business Information Processing*, pages 42–57. Springer.

Braun, R., Schlieter, H., Burwitz, M., and Esswein, W. (2016). BPMN4CP Revised – Extending BPMN for Multi-perspective Modeling of Clinical Pathways. In *HICSS*, pages 3249–3258.

Brucker, A. D. (2013). Integrating Security Aspects into Business Process Models. *it – Information Technology*, 55(6):239–246.

Brucker, A. D. and Hang, I. (2012). Secure and Compliant Implementation of Business Process-Driven Systems. In Rosa, M. L. and Soffer, P., editors, *Business Process Management Workshops - {BPM} 2012 International Workshops, Tallinn, Estonia, September 3, 2012. Revised Papers*, volume 132 of *Lecture Notes in Business Information Processing*, pages 662–674. Springer.

Cheng, Y., Zhao, S., Cheng, B., Chen, X., and Chen, J. (2019). Modeling and Deploying IoT-Aware Business Process Applications in Sensor Networks. *Sensors*, 19(1).

Chergui, M. E. A. and Benslimane, S. M. (2018). A Valid BPMN Extension for Supporting Security Requirements Based on Cyber Security Ontology. In *Model and Data Engineering*, pages 219–232, Cham. Springer.

Chergui, M. E. A. and Benslimane, S. M. (2020). Towards a BPMN Security Extension for the Visualization of Cyber Security Requirements. *IJTD*, 11(2):1–17.

Chiu, H.-H. and Wang, M.-S. (2015). Extending Event Elements of Business Process Model for Internet of Things. In *ICCIT; UBICC; DASC; PICom*, pages 783–788. IEEE.

Dubois, É., Heymans, P., Mayer, N., and Matulevičius, R. (2010). *A Systematic Approach to Define the Domain of Information System Security Risk Management*, pages 289–306. Springer.

Dumas, M., La Rosa, M., Mendling, J., and Reijers, H. (2018). *Fundamentals of business process management*. Springer.

ENISA (2018). *Good Practices for Security of Internet of Things in the context of Smart Manufacturing*. European Union Agency for Cybersecurity.

Feki, M. A., Kawsar, F., Boussard, M., and Trappeniers, L. (2013). The Internet of Things: The Next Technological Revolution. *Computer*, 46(2).

Graja, I., Kallel, S., Guermouche, N., and Kacem, A. H. (2016). BPMN4CPS: A BPMN extension for modeling cyber-physical systems. In *Proceedings - 25th IEEE Int. Conf. Enabling Technologies: Infrastructure for Collaborative Enterprises, WETICE 2016*, pages 152–157. IEEE.

Graja, I., Kallel, S., Guermouche, N., and Kacem, A. H. (2017). Modeling and verification of temporal properties in cyber-physical systems. In *CCNC*, pages 325–330. IEEE.

International Electrotechnical Commission (2009). IEC 62443.

Janisch, C., Koschmider, A., et al. (2020). The internet-of-things meets business process management. a manifesto. *IEEE Systems, Man, and Cybernetics Magazine*, 6(4):345–44.

Levy, Y. and J. Ellis, T. (2006). A Systems Approach to Conduct an Effective Literature Review in Support of Information Systems Research. *InformingSciJ*, 9.

Maines, C. L., Llewellyn-Jones, D., Tang, S., and Zhou, B. (2015). A cyber security ontology for BPMN-security extensions. In *ICCIT*, pages 1756–1763.

Maines, C. L., Zhou, B., Tang, S., and Shi, Q. (2016). Adding a Third Dimension to BPMN as a Means of Representing Cyber Security Requirements. In *DeSE*, pages 105–110.

Marin, G. A. (2005). Network security basics.

Mayer, N. (2009). *Model-based Management of Information System Security Risk*. PhD thesis, Université de Namur, Belgium.

Mayer, S. (2012). Internet of Things Architecture IoT-A Project Deliverable D2.2 – Concepts for Modelling IoT-Aware Processes. *IoT-A Project*.

Mead, N. R. and Stehney, T. (2005). Security quality requirements engineering (SQUARE) methodology. *ACM SIGSOFT Software Engineering Notes*, 30(4).

Mellado, D., Fernández-Medina, E., and Piattini, M. (2007). A common criteria based security requirements engineering process for the development of secure information systems. *Computer Standards and Interfaces*, 29(2).

Meyer, S., Ruppen, A., and Hilty, L. (2015). The things of the internet of things in BPMN. In *Lecture Notes in*

Business Information Processing, volume 215, pages 285–297. Springer.

Meyer, S., Ruppen, A., and Magerkurth, C. (2013). Internet of things-aware process modeling: Integrating IoT devices as business process resources. In *Lecture Notes in Computer Science*, volume 7908 LNCS, pages 84–98. Springer.

Mülle, J., Stackelberg, S. v., and Böhm, K. (2011a). A Security Language for BPMN Process Models. Technical Report 9, KIT.

Mülle, J., von Stackelberg, S., and Böhm, K. (2011b). Modelling and transforming security constraints in privacy-aware business processes. In *SOCA*, pages 1–4.

Müller, G., Koslowski, T. G., and Accorsi, R. (2013). Resilience - A new research field in business information systems? In *Lecture Notes in Business Information Processing*, volume 160, pages 3–14. Springer.

Okoli, C. (2015). A Guide to Conducting a Standalone Systematic Literature Review. *Communications of the Association for Information Systems*, 37(1):43.

OMG (2011). Business Process Model and Notation (BPMN), Version 2.0.

Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Shamseer, L., Tetzlaff, J. M., Akl, E. A., Brennan, S. E., Chou, R., Glanville, J., Grimshaw, J. M., Hróbjartsson, A., Lalu, M. M., Li, T., Loder, E. W., Mayo-Wilson, E., McDonald, S., McGuinness, L. A., Stewart, L. A., Thomas, J., Tricco, A. C., Welch, V. A., Whiting, P., and Moher, D. (2021). The prisma 2020 statement: an updated guideline for reporting systematic reviews. *BMJ*, 372.

Petrasch, R. and Hentschke, R. (2015). Towards an Internet-of-Things-aware Process Modeling Method An Example for a House Suveillance System Process Model. In *MITiCON)*, pages 168–172.

Petrasch, R. and Hentschke, R. (2016). Process modeling for industry 4.0 applications: Towards an industry 4.0 process modeling language and method. In *JCSSE*, pages 1–5. IEEE.

Pierre Kobes (2016). *Leitfaden Industrial Security IEC62443 einfach erklärt*. VDE Verlag, Berlin.

Pullonen, P., Tom, J., Matulevičius, R., and Toots, A. (2019). Privacy-enhanced BPMN: enabling data privacy analysis in business processes models. *Software and Systems Modeling*, 18(6):3235–3264.

Ramadan, Q., Strüber, D., Salnitri, M., Riediger, V., and Jürjens, J. (2018). Detecting Conflicts Between Data-Minimization and Security Requirements in Business Process Models. In Pierantonio, A. and Trujillo, S., editors, *Modelling Foundations and Applications*, pages 179–198, Cham. Springer International Publishing.

Ribeiro, V., Barata, J., and Rupino Da Cunha, P. (2021). A BPMN Extension to Model Inter-Organizational Processes in Industry 4.0. In *ISD*.

Salnitri, M., Dalpiaz, F., and Giorgini, P. (2017). Designing secure business processes with SecBPMN. *Software & Systems Modeling*, 16(3):737–757.

Salnitri, M., Paja, E., and Giorgini, P. (2016). Maintaining Secure Business Processes in Light of Socio-Technical Systems' Evolution. In *REW*, pages 155–164. IEEE.

Sandhu, R. and Samarati, P. (1996). Authentication, access control, and audit. *ACM Computing Surveys (CSUR)*, 28(1):241–243.

Sang, K. S. and Zhou, B. (2015). BPMN Security Extensions for Healthcare Process. In *ICCIT; UBICC; DASC; PICom*, pages 2340–2345.

Schönig, S., Ackermann, L., Jablonski, S., and Ermer, A. (2020). Iot meets BPM: a bidirectional communication architecture for iot-aware process execution. *Softw. Syst. Model.*, 19(6):1443–1459.

Schönig, S., Aires, A. P., Ermer, A., and Jablonski, S. (2018). Workflow support in wearable production information systems. In *Information Systems in the Big Data Era*, volume 317, pages 235–243.

Schönig, S., Hornsteiner, M., and Stoiber, C. (2022). Towards process-oriented iiot security management: Perspectives and challenges. In *Enterprise, Business-Process and Information Systems Modeling*.

Stanton, B., Theofanos, M. F., Prettyman, S. S., and Furman, S. (2016). Security Fatigue. *IT Professional*, 18(5):26–32.

Stoiber, C. and Schönig, S. (2021). Process-aware decision support model for integrating internet of things applications using AHP. In *Proceedings of the 23rd International Conference on Enterprise Information Systems, ICEIS*, pages 869–876.

Stoiber, C. and Schönig, S. (2022a). Digital transformation and improvement of business processes with internet of things: A maturity model for assessing readiness. In *55th Hawaii International Conference on System Sciences, HICSS*.

Stoiber, C. and Schönig, S. (2022b). Patterns for iot-based business process improvements: Developing a metamodel. In *Proceedings of the 24th International Conference on Enterprise Information Systems, ICEIS*, pages 655–666.

Sungur, C. T., Spiess, P., Oertel, N., and Kopp, O. (2013). Extending BPMN for Wireless Sensor Networks. In *2013 IEEE 15th Conf. Business Informatics*, pages 109–116.

Tange, K., De Donno, M., Fafoutis, X., and Dragoni, N. (2020). A Systematic Survey of Industrial Internet of Things Security: Requirements and Fog Computing Opportunities. *IEEE Commun. Surv. Tutor.*, 22(4):2489–2520.

Turki, S. H., Bellaaj, F., Charfi, A., and Bouaziz, R. (2012). Modeling Security Requirements in Service Based Business Processes. In *Enterprise, Business-Process and Information Systems Modeling*, pages 76–90, Berlin, Heidelberg. Springer Berlin Heidelberg.

Yousfi, A., Bauer, C., Saidi, R., and Dey, A. K. (2016). uBPMN: A BPMN extension for modeling ubiquitous business processes. *Inf. Softw. Technol.*, 74:55–68.

Zareen, S., Akram, A., and Ahmad Khan, S. (2020). Security Requirements Engineering Framework with

BPMN 2.0.2 Extension Model for Development of Information Systems. *Applied Sciences*, 10(14).

Zarour, K., Benmerzoug, D., Guermouche, N., and Drira, K. (2019). A BPMN Extension for Business Process Outsourcing to the Cloud. In *New Knowledge in Information Systems and Technologies*, pages 833–843.

Zarour, K., Benmerzoug, D., Guermouche, N., and Drira, K. (2020). A systematic literature review on BPMN extensions. *Bus. Process. Manag. J.*, 26(6):1473–1503.

Zor, S., Schumm, D., and Leymann, F. (2011). A Proposal of BPMN Extensions for the Manufacturing Domain. *ICMS 2011*, pages 1–6.