Business Process Management for IIoT Security

Dissertation zur Erlangung des Grades eines

Doktors der Wirtschaftswissenschaft

eingereicht an der

Fakultät für Wirtschaftswissenschaften

der Universität Regensburg

vorgelegt von:

Markus Hornsteiner

Berichterstatter

Prof. Dr. Stefan Schönig

Prof. Dr. Günther Pernul

Tag der Disputation: 01.Dezember 2025

“Don’t adventures ever have an end?
I suppose not.
Someone else always has to carry on the
story.”

J. R. R. Tolkien

Acknowledgement

My academic path has been anything but conventional. After being expelled from high school and later earning my secondary diploma through adult education, a doctorate seemed unlikely. And yet, here I am. To those who believed in me, and to those who didn't, you all played a part in this journey.

I am deeply grateful to Prof. Dr. Stefan Schönig, my primary supervisor, for his unwavering support and guidance, and to Prof. Dr. Günther Pernul, who sparked my passion for research and enriched the path with both academic and life lessons, including the perfect timing for Marillenknödel in the Wachau.

Special thanks go to Peter, who took the first step into university with me and has been a close friend ever since. A big thank-you also to Lena, with whom I shared an inspiring research journey and many profound conversations about science and life. Daniel S. pushed me to reach new heights, both in research and on my bike. I'm proud to have supported Linda and Daniel O. on their way to becoming doctoral students. Leo, who bridges science, software, and politics, has been a constant source of inspiration.

My deepest gratitude goes to my family, my siblings, Anki and Anton, who always believed in me, and my parents, Sepp and Evi, whose unwavering support has been invaluable. The Pernul research group, Marie-Therese, Sabrina, Manfred, Bene, Johannes, and Mathis, made every lunch and coffee break a pleasure. A special thank you to Petra, a steady lighthouse amid the fog of university administration.

Among my colleagues, Philip has been both a trusted collaborator and a true friend, a brother at heart, with whom I look forward to shaping the future of cybersecurity. Christoph set an inspiring example and encouraged me to aim higher. I will always remember our nights in budget ho(s)tels with beds far too small.

Finally, my deepest love and gratitude go to Mascha, my life partner, soulmate, and favorite travel companion. She has stood by me through every high and low, making this journey more meaningful than I could ever have imagined.

To all of you, thank you.

Abstract

Cybersecurity in the Industrial Internet of Things (IIoT) is complicated by heterogeneous assets, long lifecycles, and evolving regulations. This dissertation proposes a lifecycle-oriented, process-centric approach that leverages Business Process Management (BPM) to embed cybersecurity requirements directly into industrial workflows and to sustain continuous compliance. Aligned with the BPM phases DESIGN, CONFIGURATION, MONITORING, and DIAGNOSIS, the work contributes methods, notations, and tooling that connect design-time models to runtime compliance.

In DESIGN, the dissertation introduces structured guidelines for manual process discovery tailored to industrial settings and presents SIREN, a security-aware Business Process Management and Notation (BPMN) extension that models IIoT controls and compliance requirements (e.g., IEC 62443). In CONFIGURATION, it defines a standard-agnostic formal syntax for annotating BPMN models and a transformation pipeline that operationalizes modeled controls as machine-readable rules for enforcement and monitoring systems. In MONITORING, it proposes a layered framework for continuous, process-aware compliance verification that links model annotations to network-level evidence. In DIAGNOSIS, it demonstrates network-based process mining for IIoT by converting OPC UA network traffic into structured event logs to reveal undocumented participants, dependencies, and interactions.

The approach is evaluated through industrial case studies (including an automotive end-of-line process), digital-twin experiments, expert assessments, and a practitioner survey. Results show improved process transparency, traceable design-to-runtime enforcement, and automated compliance checks, with identified challenges around scalability and tool support. Overall, the dissertation establishes BPM as an integrating backbone for IIoT cybersecurity, advancing security-by-design, continuous verification, and diagnostically informed improvement across the industrial process lifecycle.

Contents

List of Tables

List of Figures

Abbreviations and Acronyms

BPM	Business Process Management
BPMN	Business Process Model and Notation
CRA	Cyber Resilience Act
CRISP-DM	Cross Industry Standard Process for Data Mining
DSR	Design Science Research
DTs	Digital Twins
ICS	Industrial Control Systems
IDS	Intrusion Detection Systems
IEC	International Electrotechnical Commission
IIoT	Industrial Internet of Things
INSIST	INduStrial IoT Security Operations CenTer
IS	Information Systems
ISO	International Organization for Standardization
IT	Information Technology
LLM	Large Language Models
NIS2	Network and Information Security Directive 2
OT	Operational Technology
SCIs	Security Compliance Indicators
SCMV	Security Compliance Monitoring and Verification
SIREN	Security IIoT pRocEss Notation
SLR	Systematic Literature Review
SOC	Security Operations Center

AI Disclaimer. This dissertation has benefited from the use of AI-based tools (e.g., Grammarly, ChatGPT, DeepL) for language editing and improvement. These tools were employed solely to refine clarity, coherence, and readability. All research ideas, analyses, and conclusions are entirely the work and responsibility of the author.

Part I

Dissertation Overview

1 Motivation

The Industrial Internet of Things (IIoT), often referred to as the Fourth Industrial Revolution, integrates industrial production with Information Technology (IT) and is frequently encapsulated by a single term: connectivity [10]. By extending IT capabilities into the Operational Technology (OT) domain, significant advantages are enabled, including improved efficiency, predictive maintenance, and the emergence of entirely new data-driven business models [8, 49].

As with many technological advancements, increased connectivity has a dual nature: it creates opportunities but also introduces vulnerabilities that malicious actors can exploit [17]. Consequently, industrial systems are increasingly exposed to cyberattacks and have become among the most frequently targeted assets, combining limited protection mechanisms with high-value incentives for cybercriminals [17, 28]. Another factor is their long operational lifespan, which often predates modern cybersecurity considerations [48].

The cybersecurity of industrial assets not only affects individual organizations but is also a matter of societal resilience, prompting increased regulatory attention [50]. In response, a broad set of cybersecurity frameworks and regulations, including the International Electrotechnical Commission (IEC) 62443 series of standards, the Network and Information Security Directive 2 (NIS2), International Organization for Standardization (ISO) 27001, and the Cyber Resilience Act (CRA), are increasingly mandated and adopted. Collectively, these initiatives embed security-by-design principles and require organizations to demonstrate continuous compliance with regulatory and standardization requirements [15, Annex 6.2], [29, Annex A 8.27], [44].

A key prerequisite for meeting such compliance requirements is maintaining a comprehensive, up-to-date asset inventory [29, Annex A Control 5.9], [15, Annex 12.4]). This remains a significant challenge, as industrial processes often evolve over decades, leaving organizations with limited visibility [4, 33]. Adapting DeMarco's [14] well-known assertion *You can't control what you can't measure*, the principle

> YOU CAN'T PROTECT WHAT YOU DON'T KNOW

highlights process transparency as a prerequisite for industrial cybersecurity.

In the business domain, similar challenges such as inefficient legacy processes and limited operational visibility were recognized in the 1990s [16]. Business Process Management (BPM) emerged as a structured response to this complexity, building on earlier work in business process reengineering and workflow management. Over time, BPM developed into a discipline for the continuous identification, design, improvement, and automation of business processes [16]. Although originally focused on operational efficiency, BPM has also proven effective at improving process transparency through systematic process modeling, which makes workflows and dependencies explicit [32].

This capability is highly relevant for securing IIoT systems, where understanding complex workflows is essential [40, 42]. By providing a repeatable methodology, BPM offers a systematic foundation for cybersecurity strategies in industrial environments, aligning cybersecurity controls with operational processes.

Despite its success in business domains, the potential of BPM to strengthen IIoT cybersecurity remains largely underexplored. This dissertation addresses this gap by adapting BPM methods and technologies for cybersecurity in industrial environments.

Following the BPM lifecycle of van der Aalst [1], which comprises the phases (Re)Design, Configuration/Implementation, Enactment/Monitoring, and Diagnosis/Requirements, this dissertation proposes a structured framework that integrates the BPM lifecycle with cybersecurity frameworks. For clarity, these phases are hereafter referred to as Design, Configuration, Monitoring, and Diagnosis. The resulting framework enhances process transparency, embeds security-by-design principles, and enables continuous compliance across IIoT workflows, while retaining alignment with established BPM terminology.

This dissertation is structured as follows. Chapter 2 introduces the BPM lifecycle and motivates opportunities to strengthen IIoT cybersecurity. Chapter 3 surveys prior research and synthesizes the resulting knowledge gaps. Chapter 4 formulates the overarching and phase-specific research questions derived from these gaps. Chapter 5 details the methodological foundation in Information Systems (IS) and the adoption of Design Science Research. Chapter 6 presents the core contributions, organized by lifecycle phase, and for each associated publication outlines the domain problem, contribution, methodology, and key findings. Finally, Chapter 7 synthesizes the results and outlines directions for future work. This dissertation is complemented by Part II, which encompasses the original scientific publications.

2 Research Context

The BPM lifecycle, as proposed by van der Aalst et al. [1], provides a structured methodology for the continuous management and improvement of processes. While originally intended for business optimization, its four phases also offer clear opportunities for addressing cybersecurity challenges in IIoT. Figure 1 illustrates the lifecycle and its iterative nature.

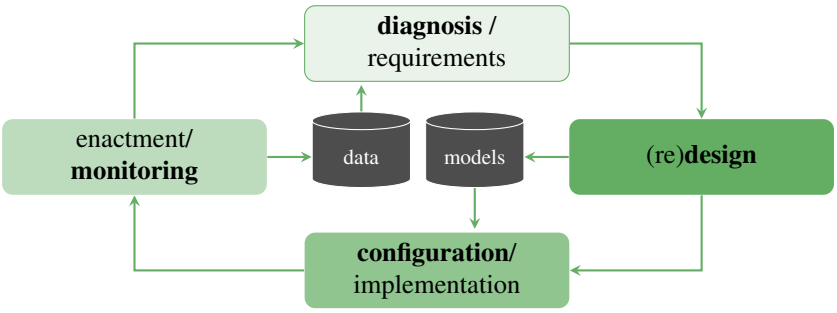


Figure 1: BPM lifecycle with full phase names; corresponding abbreviations are shown in **bold** within each name [1].

In its traditional scope, the DESIGN phase focuses on creating or redesigning process models to capture desired workflows and organizational objectives. CONFIGURATION translates these models into executable workflows within IS and supporting infrastructures. During MONITORING, the configured processes are executed and their performance is observed in real time. Finally, DIAGNOSIS evaluates process-execution data to identify deviations, inefficiencies, and requirements for further redesign. Beyond their role in efficiency and optimization, each phase of the BPM lifecycle provides distinct opportunities to enhance cybersecurity in IIoT.

In the DESIGN phase, the traditional focus lies on creating or redesigning process models. From a cybersecurity perspective, this phase establishes the foundation for protection by first achieving visibility into existing processes through process discovery. In IIoT settings, this visibility is critical for uncovering workflows, assets, and dependencies that are often undocumented. Building on this transparency, process models can be enriched with cybersecurity annotations that explicitly represent controls and compliance requirements, thereby embedding security-by-design from the outset.

The CONFIGURATION phase translates designed models into executable workflows within IS and infrastructures. In the cybersecurity context, this step enables the operationalization of modeled requirements by systematically embedding them into runtime environments. As a result, modeled controls, such as access restrictions, authentication mechanisms, or data protection rules, are not only documented but also enforced, ensuring that cybersecurity specifications actively shape process execution.

The MONITORING phase, traditionally concerned with observing process performance, can be extended toward cybersecurity assurance. By continuously comparing real execution data with reference models, it becomes possible to verify compliance with defined requirements and to detect deviations or anomalies as they occur. In this way, monitoring provides ongoing assurance that cybersecurity controls remain effective during process execution and that violations are identified in real time.

The DIAGNOSIS phase evaluates process-execution data to identify inefficiencies, bottlenecks, or requirements for redesign. From a cybersecurity perspective, this phase can be extended toward cybersecurity diagnostics by analyzing execution traces to reveal undocumented dependencies, unauthorized interactions, or hidden participants. In IIoT environments, such insights are particularly valuable as they shed light on complex system interactions and support the identification of potential vulnerabilities.

Taken together, these perspectives highlight how the BPM lifecycle provides a systematic, process-oriented foundation for cybersecurity management in IIoT. The subsequent chapter reviews prior research along these lifecycle phases to validate the practice-motivated opportunities and to delineate concrete knowledge gaps. Based on this synthesis, Chapter 4 formulates the research questions that guide the remainder of the dissertation.

3 Related Work

This chapter surveys literature relevant to BPM and security-aware Business Process Model and Notation (BPMN)[1] in IIoT environments, organized by the BPM lifecycle (cf. Figure 1). The review validates and refines the practice-motivated opportunities outlined in Chapter 2, highlights limitations of current approaches, and distills the knowledge gaps that motivate the research questions stated in Chapter 4.

Design Phase

Manual Process Discovery In traditional BPM, process discovery can be conducted using both manual and automated methods. The first focus of the Design phase in this dissertation is on manual process discovery, where human expertise and interpersonal techniques play a crucial role, especially in OT where processes are often undocumented or only partially understood.

Manual process discovery methods are discussed in foundational literature [16, 23]. Common approaches include document analysis, interviews, workshops, observations, on-site walkthroughs, focus groups, and questionnaires. These methods rely on expert knowledge and stakeholder input, making them well suited to capturing the nuances of complex industrial environments, provided they are adapted to IIoT-specific challenges.

> *However, guidelines for conducting manual process discovery in IIoT environments have not yet been proposed.*

Security-Aware Process Modeling Once processes are discovered, the next step in the Design phase is to create security-aware process models. Research on integrating IIoT with BPM has advanced, with categorizations by [13, 57] outlining IoT-driven BPMN extensions and key modeling requirements. EU-funded projects have promoted IIoT-specific BPMN extensions to include sensors, cloud devices, and tasks [37–39].

Research on cybersecurity in BPMN usually addresses the standard goals of IT cybersecurity (confidentiality, integrity, and availability) [3], including features such as encryption [45] or measures like delegation and binding of tasks [51]. SecureBPMN [9] integrates cybersecurity directly into BPMN and represents a comprehensive extension. However, most approaches focus on IT and overlook IIoT-specific concerns such as heterogeneous devices or the prioritization of availability over confidentiality.

> *An integrated modeling approach that jointly addresses both IIoT and cybersecurity requirements in BPMN has not yet been established.*

[1] https://www.omg.org/spec/BPMN/2.0/

CONFIGURATION Phase

Security-Aware Process Execution Although BPMN has been extended with IIoT-specific elements, cybersecurity considerations are often treated separately. Existing research on security-aware BPMN primarily focuses on modeling requirements (e.g., access restrictions and regulatory constraints) but lacks approaches for translating them into enforceable runtime controls.

For example, [20] emphasizes ensuring process executability in IIoT environments, while [37–39] discuss adding IIoT-specific features (e.g., sensor tasks) to BPMN. Yet these works do not detail how to implement and enforce cybersecurity constraints defined in process models. Similarly, [21] addresses executability in IIoT workflows but omits cybersecurity considerations.

> *To date, no approach systematically translates security-aware BPMN models into enforceable runtime rules for IIoT environments.*

MONITORING Phase

Continuous Compliance Monitoring In the MONITORING phase, processes run in production, and the primary goal is to monitor execution for both performance and compliance. Traditional BPM monitoring focuses on process performance (e.g., service level agreement adherence), whereas cybersecurity compliance in IIoT adds additional complexity: diverse devices, real-time constraints, and specialized network protocols.

Existing research on cybersecurity compliance monitoring draws on the broader field of compliance verification, but domain-specific adaptations for IIoT are still emerging. [52] outlines automated compliance tools and highlights challenges such as formalizing requirements and ensuring robust audit trails. [12] uses NLP to formalize standard requirements into audit scripts, while [19] employs semantic knowledge bases for compliance checks in ISO 27002. Formal methods are used by [34] to model Industrial Control Systems (ICS) behavior under IEC 62443-3-3, though scalability remains a challenge for broader IIoT use cases. Efforts such as [6, 7] propose architectures for continuous compliance verification in IIoT, but they do not fully integrate BPMN-based process modeling.

> *Although both process modeling and compliance monitoring are addressed, a unified approach that combines BPMN-based modeling with continuous compliance verification for IIoT cybersecurity has not yet been established.*

Diagnosis Phase

Network traffic based Process Mining for IIoT During (or after) Monitoring, organizations often enter the Diagnosis phase, relying on operational data to diagnose issues and define improvements. In IIoT contexts, this phase becomes particularly significant for uncovering hidden or evolving process structures that may not have been apparent during the initial Design phase.

While many studies examine automated process discovery and process mining in office environments [30, 47], they do not detail how event logs or network traffic can be leveraged to identify previously unknown participants, devices, or connections. Other approaches extract BPMN models from textual descriptions [22, 25], but these remain limited to office settings rather than IIoT. Network-based discovery research includes rule-based methods for converting network traffic into event logs [54], domain-specific adaptations for ERP or ICS [5, 18], and model-based (often unsupervised) learning techniques for generating event logs or process models from raw traffic [24, 35]. These latter approaches can reveal unknown devices, undisclosed process participants, or hidden infrastructure connections, vital for diagnosing cybersecurity risks and isolating unwanted communication channels. However, most studies rely on simulated data and do not account for the complexity of real-world IIoT environments.

Further work integrates real-time IoT events into BPM systems [46, 47], acknowledging that advanced mining techniques can uncover hidden process paths. Yet these studies do not describe how such discovery methods can be systematically applied to diagnose previously unknown participants or infrastructure changes within IIoT.

> *Automated process discovery has therefore not yet been systematically established as a method to identify hidden participants, dependencies, and infrastructure changes in IIoT environments.*

4 Research Questions

Building on the context in Chapter 2 and the knowledge gaps synthesized in Chapter 3, this dissertation investigates how BPM methods and technologies can be adapted to strengthen cybersecurity in IIoT environments. The research is guided by one overarching question that frames the overall contribution, complemented by a set of sub-questions that address the specific challenges arising in each phase of the lifecycle. These sub-questions reflect the need to consider cybersecurity systematically throughout the lifecycle of industrial processes. Together, they provide a structured pathway for examining how BPM can support transparency, enforcement, compliance, and continuous improvement in IIoT cybersecurity management. Accordingly, the overarching research question guiding this dissertation is:

> How can BPM methods and technologies be leveraged to systematically embed and enforce cybersecurity in the IIoT?

To align with the overarching question, Figure 2 maps the domain problems distilled from the literature in Chapter 3 to the respective BPM phases. This mapping forms the conceptual basis for the sub-research questions.

Domain Problems	Focus Areas
Lack of structured guidelines for manual process discovery and security-aware process modeling approaches for IIoT.	Design
Missing methods to operationalize modeled security controls.	Configuration
No framework combines BPMN security models with real-time compliance monitoring in IIoT.	Monitoring
Lack of process mining techniques based on industrial network traffic.	Diagnosis

Figure 2: Overview of the domain problems and the associated focus areas.

Focus Area Design

RQ1: Manual Process Discovery. *How can IIoT processes be systematically discovered to establish the transparency required for security-aware process management?*

Establishing effective cybersecurity in industrial environments requires transparency into workflows, assets, and interdependencies [40, 42]. Traditional BPM discovery methods combine manual approaches (e.g., interviews, document analysis) with automated techniques (e.g., log-based process mining) [16]. However, IIoT environments pose additional challenges, such as heterogeneous device landscapes and undocumented interdependencies [8, 56]. This research investigates how structured manual

process discovery can be adapted to IIoT environments to capture semi-automated workflows that lack reliable digital traces. Such process visibility is a prerequisite for subsequent cybersecurity analysis, ensuring that critical assets and dependencies are identified before process modeling begins.

RQ2: Security-Aware Process Modeling. *How can IIoT processes be modeled to formally incorporate security controls and compliance requirements?*
Once processes are discovered, they need to be formalized through process modeling in order to capture workflows in a structured and analyzable form. However, standard modeling languages such as BPMN lack native support for representing IIoT cybersecurity controls, which complicates the realization of security-by-design principles in industrial workflows [36]. This research therefore extends BPMN with IIoT security-aware extensions, enabling explicit representation of controls and compliance requirements in industrial environments.

Focus Area CONFIGURATION
RQ3: Security-Aware Process Execution. *How can security-aware IIoT process models be systematically operationalized into machine-readable rules to enable their enforcement and continuous verification?*
Defining cybersecurity controls in process models is insufficient unless these specifications can also be operationalized. Here, operationalization refers to the systematic transformation of security-aware BPMN models into machine-readable rule sets that can be interpreted by enforcement or monitoring systems. Traditional BPM execution engines lack such mechanisms, leaving a gap between modeled cybersecurity requirements and their practical application. This research explores how modeled controls can be translated into executable rules, enabling their continuous verification and enforcement in IIoT environments.

Focus Area Monitoring

RQ4: Cybersecurity Monitoring & Compliance Verification. *How can IIoT processes be continuously monitored to verify compliance with security standards and detect deviations in real time?*

Traditional BPM monitoring focuses on efficiency metrics and offers limited support for verifying cybersecurity compliance [16]. Verifying that executed processes conform to defined cybersecurity requirements requires runtime monitoring and automated compliance verification. This research investigates how process-aware monitoring mechanisms can be integrated into IIoT environments to continuously verify modeled cybersecurity controls and automatically detect compliance violations.

Focus Area Diagnosis

RQ5: Process Mining for Cybersecurity Analysis. *How can process mining techniques be adapted to industrial networks to uncover hidden participants and dependencies, thereby informing security-aware process redesign?*

Process mining enables the analysis of execution data to identify deviations, inefficiencies, and associated cybersecurity risks. In office settings, research has shown how network-traffic can be leveraged for process discovery [18]. In industrial environments, however, process mining approaches remain largely focused on event logs, and adaptations for raw network traffic are still lacking. This research examines how network-traffic-based process mining can be applied to IIoT network traffic to improve workflow transparency, with a focus on uncovering undocumented dependencies, participants, and unauthorized interactions. These insights strengthen transparency and provide a foundation for security-aware process redesign, enabling the continuous refinement of processes, participants, and controls in industrial settings.

5 Methodology

The research was conducted at the Chair of Process-Based Information Systems (University of Regensburg) and is situated in the field of IS (Wirtschaftsinformatik), i.e., the study of how information technologies are designed, implemented, and managed to address organizational and societal problems [2].

5.1 Information Systems Research

IS research addresses how individuals, organizations, and societies design, develop, implement, and manage IS [2]. It addresses both technical (e.g., software, infrastructure) and the social, behavioral, and managerial factors that influence technology adoption and impact. Drawing from computer science, management science, organizational studies, and the social sciences, IS research investigates the full lifecycle of IS, from conceptualization to eventual discontinuation, across diverse contexts.

Within the field, two complementary streams are commonly distinguished: behavioral IS research and Design Science Research (DSR) [27]. Behavioral IS research analyzes how people and organizations interact with IS, employing empirical methods (e.g., surveys, interviews, case studies, statistical modeling) to examine technology acceptance, user behavior, and organizational impact [2]. By contrast, DSR focuses on creating and evaluating innovative artifacts, such as models, frameworks, methods, or software tools, to address specific, well-defined problems [27]. This stream follows iterative cycles of development, evaluation, and refinement to ensure that resulting solutions are both practically applicable and academically relevant [2].

Although presented separately in the literature, the two streams frequently intersect in practice. For example, an IS study may develops a security-aware BPM framework following DSR, then empirically evaluate its effectiveness using behavioral methods (e.g. user studies or organizational assessment). This interdisciplinarity helps couple technological innovation with human, organizational, and societal considerations.

This dissertation adopts such a dual approach, combining DSR with behavioral IS perspectives. Core artifacts, aimed at integrating cybersecurity with BPM in IIoT environments, are iteratively designed and refined in accordance with DSR best practices. Their applicability and impact are assessed through qualitative and quantitative evaluations, including expert feedback, pilot studies, and performance assessments [43]. By merging artifact design with empirical validation, the dissertation contributes both academic insights and practical solutions for advancing security-aware BPM in IIoT.

5.2 Research Process

This dissertation adopts the six-step DSR methodology of Peffers et al. [43]. DSR is appropriate because the central aim is to create and evaluate artifacts, models, methods, notations, and system components, that address real IIoT cybersecurity problems. It provides (i) a rigor–relevance framework linking theory and practical utility [27], (ii) iterative build–evaluate cycles for systematic refinement [43], and (iii) guidance on fit-for-purpose evaluation (e.g., expert assessment, case studies, performance tests). Accordingly, each contribution in this cumulative dissertation was developed within the DSR process, with explicit problem–solution rationales and evaluations of utility, quality, and efficacy. This structured, iterative approach ensures both scientific rigor and practical applicability in IIoT cybersecurity.

Step 1 - Problem Identification IIoT environments are increasingly exposed to cybersecurity threats due to their highly interconnected and heterogeneous nature. Conventional cybersecurity typically addresses individual components rather than end-to-end industrial processes, resulting in gaps and inconsistencies. To address these, the present work investigates how BPM methods and technologies can provide a systematic, lifecycle-based approach to integrate cybersecurity across IIoT workflows.

Step 2 - Objective The overarching objective is to investigate how BPM methods and technologies can be leveraged to strengthen cybersecurity in the IIoT. In the Design phase, the focus is on developing methodologies to discover industrial processes, including those that are undocumented or only partially known, and on embedding cybersecurity requirements directly into formal process models (e.g., by extending BPMN). The Configuration phase addresses the operationalization of these models by providing mechanisms to transform security-aware process models into enforceable controls and monitorable policies at runtime, thereby supporting alignment with standards such as IEC 62443. In the Monitoring phase, continuous compliance verification is enabled, complemented by automated detection of policy violations and mechanisms that support adaptive responses to anomalies in IIoT process flows. Finally, the Diagnosis phase leverages process mining and automated discovery techniques to reveal unknown participants, hidden connections, or infrastructure changes, feeding these insights back into Design for iterative improvement. Taken together, this lifecycle perspective ensures that controls are not only conceptualized Design but also systematically deployed, monitored, and refined.

Step 3 - Design To achieve these objectives, the design of artifacts is guided by rigorous scientific methodologies. A Systematic Literature Review (SLR) establishes the theoretical foundation and identifies research gaps [41]. Building on these insights,

DSR serves as the primary methodological framework, enabling iterative cycles of artifact creation and evaluation [27]. For data-driven aspects, particularly those involving process mining, the Cross Industry Standard Process for Data Mining (CRISP-DM) methodology provides a structured approach to data preparation, modeling, and evaluation [55]. Finally, the development of design principles and the grounding of contributions in design theory ensure both conceptual soundness and practical viability in industrial environments [26, 31].

The resulting artifacts range from BPMN-based cybersecurity extensions to process-mining techniques for analyzing IIoT networks. Each artifact undergoes iterative refinement, informed by user feedback and collaboration with industrial partners, maintaining practical relevance alongside scientific rigor.

Step 4 – Demonstration The developed artifacts were demonstrated in two complementary settings. First, process discovery and security-aware modeling approaches were applied within partner companies, where industrial workflows were documented and validated through expert feedback, ensuring that the methods reflect authentic organizational practices and challenges.

Second, for monitoring and network-based process mining, recorded traffic from production systems was used to construct Digital Twins (DTs) of industrial networks. These digital environments provided a realistic yet controllable context for testing the transformation of BPMN cybersecurity controls into enforceable rules, integrating monitoring solutions for IEC 62443 compliance, and applying process mining to uncover hidden dependencies or undocumented devices.

By combining demonstrations in both live industrial environments and DTs environments, feasibility was established under conditions that balance realism with experimental control, laying the groundwork for subsequent large-scale validation.

Step 5 – Evaluation The evaluation methodology was tailored to each artifact, assessing both technical performance and conceptual relevance. Proof-of-concept evaluations demonstrated the feasibility of security-aware BPMN execution within IIoT workflows. Performance tests were conducted in DTs environments, where monitoring solutions and process-mining techniques were evaluated for efficiency and scalability, including stress tests with datasets containing up to 25,000 network packets. Complementing these technical assessments, qualitative evaluations with industry partners provided expert feedback on applicability, usability, and practical value.

By combining experimental validation in DTs with expert evaluations in industrial environments, the methodology ensured that the proposed artifacts were not only theoretically sound but also effective and usable in practice.

Step 6 - Communication The results are disseminated through peer-reviewed conferences and journal publications to contribute to academic discourse and industrial application. Additionally, software artifacts are made available in public repositories to facilitate further research and adoption. The communication strategy is designed so that the developed methodologies and controls can be leveraged by both the scientific community and industrial stakeholders.

5.3 Research Setting

This dissertation was carried out at the Chair of Process-Based Information Systems under the supervision of Prof. Dr. Stefan Schönig. The chair's emphasis on industrial processes, combined with collaboration in research projects with academic and industry partners, created an environment that enabled the development of this dissertation.

Research environment

INSIST Project Parts of this dissertation were conducted within the INduStrial IoT Security Operations CenTer (INSIST) project (2021–2024), funded by the Bavarian Ministry of Economic Affairs, Regional Development and Energy (StMWi). The project aimed to establish a Security Operations Center (SOC) for IIoT, focusing on the intersection of people, processes, and technologies. A key innovation was integrating DTs with the SOC, expanding IIoT capabilities to organizational-wide cybersecurity.

This dissertation leveraged INSIST's industrial collaborations to develop security-aware BPM approaches. Network traffic from two organizations was collected and analyzed using process mining, while parallel manual process discovery enabled a comparative evaluation. This led to the development of a framework for manual process discovery in industrial environments, contributing to the Design and Diagnosis phases.

SIREN Project Building on INSIST's findings, the Security IIoT pRocEss Notation (SIREN) project (2023–2026) expands the research focus to the entire lifecycle of industrial processes and facilities. Funded by StMWi, SIREN aims to enhance IIoT cybersecurity through the adaptation of BPM methods and technologies.

This project integrates DTs, process modeling, process mining, and network intrusion detection to improve cybersecurity. The objectives of SIREN align directly with this dissertation, as the research investigates how BPM-based cybersecurity controls can be executed and continuously monitored. The project's practical insights support contributions in the Design, Configuration, and Monitoring phases, ensuring that controls are not only modeled but also enforced and monitored in IIoT systems.

6 Results

Based on the methodologies presented in Chapter 5, this dissertation addresses four main focus areas, DESIGN, CONFIGURATION, MONITORING, DIAGNOSIS, which are aligned with the five research questions presented in Chapter 4. For each focus area, the following describes which research questions are answered by which approaches from the research papers that were created as part of the dissertation. For each paper, the problem, the contribution, the methodology and important findings are discussed.

6.1 Overview of Research Papers

Figure 3 summarizes the dissertation in a lifecycle-aligned schema: columns denote rationale (**Why**), approach (**How**), and artifacts (**Using**); rows correspond to DESIGN, CONFIGURATION, MONITORING, and DIAGNOSIS. The figure's role is orientation, and detailed explanations of each artifact appear in Sections 6.2 to 6.5.

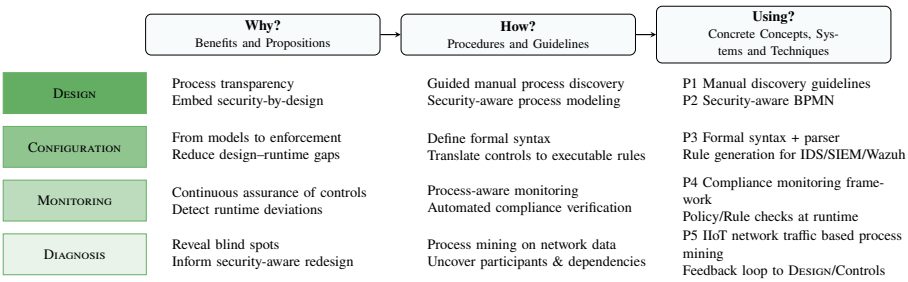


Figure 3: Lifecycle-aligned overview linking the rationale (**Why**), methodological approach (**How**), and concrete artifacts (**Using**) across DESIGN, CONFIGURATION, MONITORING, and DIAGNOSIS.

This cumulative dissertation has resulted in a total of six publications, which have either already been published (P2, P4, P5, P6) or are in revision (P1) or under review (P3). Each of the publications addresses a specific problem in the context on how to leverage BPM for the cybersecurity of the IIoT. Table 1 shows the individual publications, their authors and metrics of the respective outlet. Conferences are ranked according to JourQual 2024 (JQ) [1] or CORE 2023 [2], if available. Journal papers are classified by their Impact Factor (IF).

[1] https://www.vhbonline.org/fileadmin/vhb/Services/vhb-rating/WI/VHB_Rating_2024_Area_rating_WI.pdf

[2] https://portal.core.edu.au/conf-ranks/

Table 1: List of publications, status, and rankings.

No.	Publication	Status	Ranking
P1	Kölbel, L.; Hornsteiner, M.; Schönig, S. (2025). *Guideline for Manual Process Discovery in Industrial IoT*. In revision at *Information Systems and e-Business Management (ISeB)*.	rev.	IF 3.6
P2	Hornsteiner, M.; Schönig, S. (2023). SIREN: Designing Business Processes for Comprehensive Industrial IoT Security Management. In: *Design Science Research for a New Society: Society 5.0 — Proceedings of the 18th International Conference on Design Science Research in Information Systems and Technology (DESRIST 2023)*. LNCS, vol. 13873, pp. 379–393. Springer.	pub.	JQ B
P3	Kölbel, L.; Hornsteiner, M.; Schönig, S. (2025). Process-Oriented Industrial IoT Cybersecurity Management: A Modeling Framework with Formal Syntax. Submitted to *International Journal of Information Security (IJIS)*.	sub.	IF 3.2
P4	Oberhofer, D.; Hornsteiner, M.; Schönig, S. (2024). Process-Aware Security Standard Compliance Monitoring and Verification for the IIoT. In: *Proceedings of the 32nd European Conference on Information Systems (ECIS 2024)*, Paphos, Cyprus. AIS eLibrary, Paper 1698.	pub.	JQ A
P5	Hornsteiner, M.; Empl, P.; Bunghardt, T.; Schönig, S. (2024). Reading between the Lines: Process Mining on OPC UA Network Data. *Sensors*, 24(14), 4497.	pub.	IF 3.5
P6	Hornsteiner, M.; Kölbel, L.; Oberhofer, D.; Schönig, S. (2025). A Reflection on Process-Oriented Industrial IoT Cybersecurity Management. In: *Proceedings of the 11th International Conference on Information Systems Security and Privacy (ICISSP 2025)*, pp. 242–253.	pub.	CORE C

Status: pub. = Published, sub. = Submitted, rev. = In Revision.

6.2 Focus Area 1: Design

Focus Area 1 addresses the Design phase of the process lifecycle and addresses the discovery and modeling of security-aware processes in industrial environments. First, RQ 1 is answered by P1, which presents structured manual guidelines for discovering processes in the IIoT. Subsequently, P2 addresses RQ 2 by extending BPMN to embed cybersecurity controls and to model security-aware IIoT processes.

Publication P1: Guideline for Manual Process Discovery in Industrial IoT

Domain Problem. Traditional BPM discovery techniques for office environments rely either on automated methods, such as process mining from event logs, or on structured manual approaches, such as interviews and document analysis [16]. While automated discovery is often unsuitable for IIoT due to incomplete or missing logs and the prevalence of semi-automated workflows, existing guidelines for manual discovery are likewise tailored to office processes and have not been systematically adapted to industrial environments. This research addresses that gap by providing structured guidance for conducting manual process discovery in IIoT environments, enabling organizations to document hybrid workflows as a prerequisite for cybersecurity analysis.

Contribution. P1 introduces a structured guideline for manual process discovery in IIoT, adapting established BPM discovery methods to hybrid industrial environments. It defines a framework that integrates document analysis, observations, interviews, and workshops, thereby addressing the challenges arising from the coexistence of manual and automated activities. The approach was validated in two industrial case studies from the automotive and warehouse management sectors, demonstrating its diverse industrial applicability.

Methodology. Following the DSR methodology by Hevner et al. [27], P1 was developed through a SLR and iterative refinement. The approach builds on BPM discovery principles from Dumas et al. [16] and Gronau [23], adapting them to IIoT environments. The guidelines were evaluated using case studies, expert discussions, and a survey with 28 participants, assessing their applicability and necessity.

Finding 1. *Combination of process discovery techniques enhances quality.*
P1 demonstrates that combining manual process discovery techniques, document analysis, observation, interviews, and workshops, results in more comprehensive and accurate process models. In complex IIoT environments, where documentations are often unavailable or incomplete, manual interventions, human decision-making, and undocumented process deviations play a crucial role in operations. Observations capture real-world process flows, interviews provide expert insights on undocumented steps, and workshops validate findings by aligning different perspectives. By integrating these techniques, the guidelines ensure that industrial processes are discovered in a structured, holistic manner, capturing all relevant aspects.

Finding 2. *Guidelines ensure adaptability to different industrial settings.*
The developed manual process discovery framework provides a structured methodology that is adaptable to different industrial settings, including low-data environments, mixed human-machine interactions, and legacy systems that lack automated logging

mechanisms. The guidelines enable flexible adaptation by allowing organizations to select the most effective combination of techniques based on process complexity, available documentation, and data accessibility. This makes process discovery accessible beyond fully automated digitalized environments, ensuring that security, efficiency, and compliance improvements are achievable even in traditional industrial setups.

Finding 3. *Survey confirms the demand for structured process discovery guidelines.* The survey conducted with industry professionals confirms that 96% of respondents recognize the need for a standardized, structured approach to process discovery in IIoT. Many organizations lack formalized methods, leading to inconsistent process documentation, inefficiencies in optimization efforts, and difficulties in compliance audits. The findings suggest that process discovery should be an integral part of IIoT digitalization strategies, ensuring that cybersecurity risks, operational inefficiencies, and compliance gaps are identified early. Furthermore, the study highlights that organizations using ad hoc or informal process discovery methods face higher operational inconsistencies and longer adaptation times for process improvements, emphasizing the value of structured guidelines in ensuring sustainable and efficient industrial process management.

Publication P2: SIREN: Designing Business Processes for Comprehensive Industrial IoT Security Management

Domain Problem. The IIoT brings unprecedented connectivity between machines, systems, and IT infrastructure. While this convergence enables efficiency gains and data-driven operations, it simultaneously exposes industrial environments to substantial cybersecurity risks. Standards such as IEC 62443 define requirements to mitigate these risks and are reinforced by regulatory frameworks, including the EU CRA and the German IT Security Act 2.0. Nevertheless, many organizations struggle to integrate such requirements into their operational processes, particularly with respect to continuous monitoring and compliance. Existing security-aware modeling approaches have not been tailored to IIoT environments and provide limited support for representing and monitoring cybersecurity controls at runtime. This gap highlights the need for a specialized BPMN-based modeling approach that explicitly supports IIoT cybersecurity requirements and compliance verification.

Contribution. P2 presents SIREN, a BPMN-based modeling approach designed to integrate IEC 62443 cybersecurity requirements into IIoT process models, as shown in Figure 4. Unlike existing BPMN cybersecurity extensions, SIREN is tailored specifically for IIoT environments, allowing cybersecurity controls to be represented, monitored, and enforced within industrial processes. By extending BPMN with cybersecurity controls, SIREN enables process designers to define cybersecurity requirements that are automatically translated into monitorable rules. These rules can then be integrated

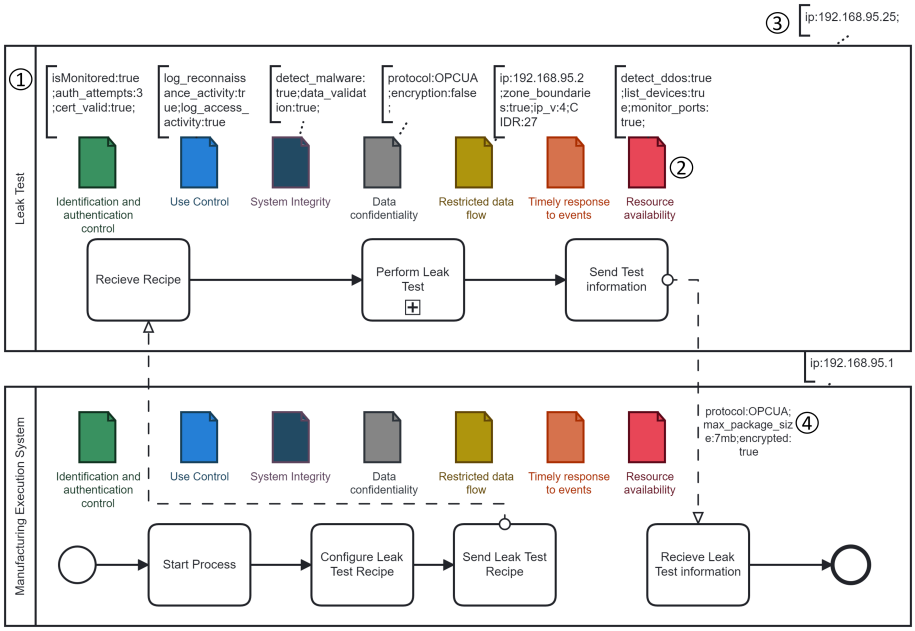


Figure 4: Abbreviated process of an automotive supplier modeled in SIREN.

into Intrusion Detection Systems (IDS), enabling real-time cybersecurity monitoring. The proposed approach is evaluated through an industrial use case in automotive manufacturing, demonstrating its practical applicability.

Methodology. P2 follows the DSR methodology, using an iterative development process to create and refine SIREN. The design process is guided by four key objectives: (1) Minimal complexity for usability, (2) Explicit focus on IIoT security, (3) Practical applicability for industrial use cases, and (4) Compliance with established modeling principles. The evaluation follows [53] framework for DSR evaluation, involving expert validation and an industrial case study to assess the effectiveness of SIREN.

Finding 1. *BPMN is suitable for security-aware process modeling in IIoT.*
P2 demonstrates that BPMN can effectively be extended to represent IIoT-specific cybersecurity controls, integrating concepts from IEC 62443 into industrial process models. However, standard BPMN lacks built-in mechanisms for modeling cybersecurity controls, necessitating a tailored extension that allows cybersecurity requirements, risk factors, and compliance rules to be explicitly embedded within process diagrams. The SIREN notation introduces security-aware modeling elements that ensure cybersecurity is not just an afterthought but an integral part of the entire process lifecycle.

Finding 2. *Security controls modeled in BPMN can be automatically translated.*
A key finding of the SIREN framework is the ability to convert modeled cybersecurity requirements into enforceable rules, enabling automated compliance monitoring and cybersecurity enforcement. By integrating BPMN-based cybersecurity controls with IDS and SOC, P2 showcases how BPMN can be leveraged for continuous verification of cybersecurity policies in industrial environments. This transformation ensures that modeled cybersecurity controls are actively monitored, rather than remaining static representations.

Finding 3. *Expert feedback confirms the viability of SIREN.*
The evaluation included feedback from industrial and cybersecurity experts, who confirmed that SIREN provides a structured and promising approach to security-aware process modeling in IIoT. However, they also highlighted several areas requiring further refinement, including enhanced tool support, broader integration with industrial systems, and improvements in usability for non-security experts. While the approach successfully bridges the gap between process modeling and cybersecurity monitoring, future research should focus on scalability, real-world deployments, and standardization to facilitate industry-wide adoption.

6.3 Focus Area 2: Configuration

Focus Area 2 addresses the Configuration phase of the process lifecycle, i.e., how BPMN models can be transformed from graphical representations into executable rules. This requires a well-defined syntax governing the arrangement and labeling of elements and controls, as well as clear textual descriptions. To address RQ3, P3 introduces a modeling framework with a formal syntax that specifies how BPMN elements and cybersecurity controls must be structured and annotated. The framework enables the resulting models to be processed by parsers and translated into enforceable rules for cybersecurity systems.

Publication P3: Process-Oriented Industrial IoT Security Management: A Modeling Framework with Formal Syntax

Domain Problem. The IIoT significantly expands the attack surface of industrial systems through the convergence of IT and OT. Although cybersecurity frameworks such as IEC 62443 define comprehensive requirements, they remain largely conceptual and provide limited support for operationalization, runtime enforcement, and continuous compliance verification in dynamic environments. This design-time–to–runtime gap has been exploited in incidents such as the TRITON attack and leaves organizations without a systematic method to embed and verify cybersecurity controls within operational workflows [11].

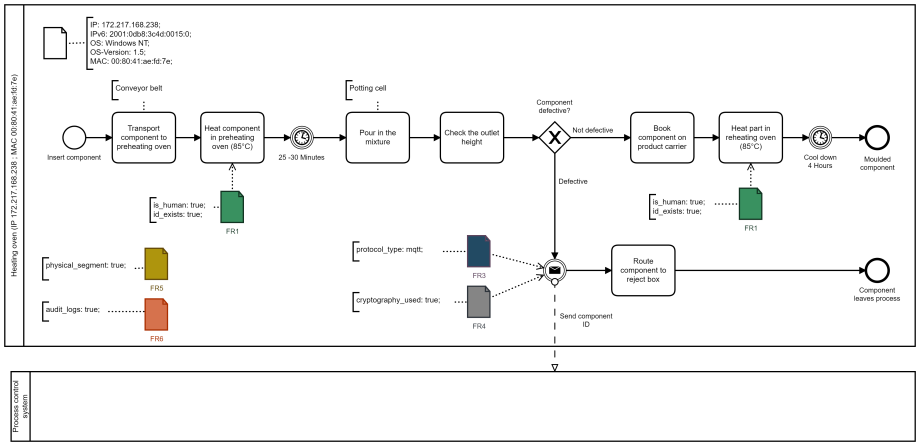


Figure 5: Example process for heating and filling components conforming to IEC 62443 controls.

Contribution. P3 builds on the foundations established in P2 by generalizing and formalizing its findings. Specifically, P3 introduces a formal syntax for extending BPMN that is security-standard agnostic, thereby broadening applicability. The syntax not only enables the translation of predefined cybersecurity controls but also supports integration of custom controls. Moreover, it allows automatic validation of modeled cybersecurity controls, including syntax checking and error reporting. Through these mechanisms, P3 makes the approach introduced in P2 independent of specific cybersecurity controls or modeling tools, enhancing robustness and generalizability.

Methodology. P3 was developed following the DSR methodology [27] in an iterative three-phase process. First, a formal, machine-readable syntax was defined to specify IEC 62443-based controls in a standardized manner. Second, modeling guidelines were created to embed these controls into BPMN workflows, associating them with process activities, system resources, and communication flows. Finally, a runtime enforcement pipeline was implemented, translating the modeled controls into executable rules and integrating them into industrial monitoring tools such as Suricata and Wazuh for continuous compliance verification. The approach aligns with the IEC 62443-2-1 lifecycle and was evaluated through a real-world manufacturing use case.

Finding 1. *A formal syntax enables machine-readable cybersecurity modeling.* A standardized syntax for extending BPMN ensures that requirements (e.g., IEC 62443 controls) are explicitly documented and consistently represented, reducing ambiguity and enabling automated interpretation by analysts and enforcement systems.

Finding 2. *Modeling guidelines structure the integration of controls into workflows.* Clear rules for linking controls to tasks, resources, and communication flows support systematic traceability from design to operation. This allows consistent embedding of requirements across the process lifecycle and facilitates extraction for enforcement.

Finding 3. *Runtime enforcement operationalizes design-time models.* By transforming modeled controls into executable rules for monitoring tools (e.g., Suricata or Wazuh), the framework provides continuous compliance verification and bridges the gap between modeled requirements and live enforcement in IIoT environments.

6.4 Focus Area 3: Monitoring

Focus Area 3 addresses the Monitoring phase of the process lifecycle, how security-aware processes in IIoT can be monitored against defined controls. In doing so, Monitoring answers RQ 4 by presenting a framework for monitoring process flows for compliance with cybersecurity standards (e.g. IEC 62443). This enables not only security-aware modeling but also continuous compliance assessment.

Publication P4: Process-Aware Security Standard Compliance Monitoring and Verification for the IIoT

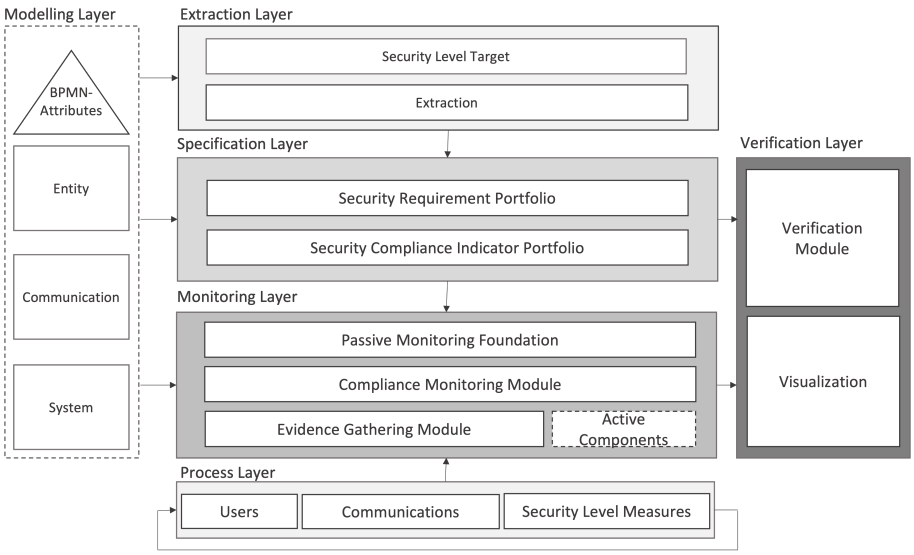


Figure 6: Layered, process-aware framework for cybersecurity standard compliance monitoring and verification, showing potential impact points of BPMN attributes.

Domain Problem. The IIoT integrates ICS with IT infrastructures, increasing connectivity and expanding the attack surface. ICS require continuous compliance monitoring with standards like IEC 62443 to ensure resilience. However, traditional compliance audits are manual, static, and inefficient. Current compliance monitoring solutions focus on general IT and lack IIoT-specific considerations, such as real-time monitoring, process-aware security, and the unique availability and integrity requirements of industrial systems. To address these challenges, a framework is needed that integrates automated compliance assessment with process-related cybersecurity controls for IIoT.

Contribution. P4 introduces Security Compliance Monitoring and Verification (SCMV), a modular framework for continuous cybersecurity standard compliance monitoring in IIoT. The framework automates verification of requirements from standards like IEC 62443, ensuring that implemented controls align with compliance expectations. A process-aware approach integrates BPMN annotations, linking controls directly to process models. This enhances transparency, enables real-time compliance tracking, and reduces reliance on manual compliance audits. The framework comprises extraction, specification, monitoring, and verification layers, supporting both passive and active techniques for detecting deviations. A prototype demonstrates automated verification, control validation, and real-time visualization using network monitoring tools and BPMN-based cybersecurity modeling.

Methodology. P4 follows the DSR methodology and is structured around three meta-requirements: (1) Defining the essential components of SCMV systems, (2) Integrating process-aware cybersecurity controls into compliance monitoring, and (3) Ensuring IIoT-specific adaptability, addressing availability and cybersecurity requirements. The framework builds upon passive network monitoring and BPMN-based cybersecurity modeling to enable real-time compliance assessment. A prototype SCMV system integrates IEC 62443 requirements, BPMN-based controls, and automated intrusion detection and compliance verification mechanisms.

Finding 1. *SCMV integrates process modeling with compliance monitoring in IIoT.* P4 formalizes compliance as a continuous, process-driven activity by linking BPMN models with monitoring tools. This ensures that cybersecurity requirements defined during modeling are systematically verified in real-time operations, improving traceability and accountability in the enforcement of industrial cybersecurity standards.

Finding 2. *Security Compliance Indicators (SCIs) make standards measurable.*
P4 introduces SCIs as a structured method for defining and extracting compliance-relevant indicators from both process models and network traffic. This makes compliance verification data-driven rather than manual, allowing organizations to directly assess adherence to cybersecurity requirements through observable evidence.

Finding 3. *SCMV supports non-intrusive compliance assessment.*
P4 employs passive network analysis to verify compliance without disrupting operations. Its modular design enables continuous monitoring of live IIoT traffic, detecting deviations from policies in real time while avoiding the overhead of intrusive or audit-based methods, making it particularly suitable for industrial settings where system availability is critical.

6.5 Focus Area 4: Diagnosis

Focus Area 4 addresses the Diagnosis phase of the BPM lifecycle and is concerned with the discovery of undetected processes, participants and interdependencies. P5 addresses the research question RQ 5 by presenting an approach for preparing OPC UA network traffic and converting it into structured logs, which can then be processed by established process mining techniques.

Publication P5: Reading Between the Lines: Process Mining on OPC UA Network Data

Domain Problem. While process mining is well established in organizational contexts relying on structured event logs, such logs are often unavailable in IIoT environments. Network traffic, e.g. OPC UA network traffic, offers a rich source of process-related information, yet deriving structured process models from raw traffic remains difficult due to missing event identifiers, industrial protocol complexity, and scalability constraints.

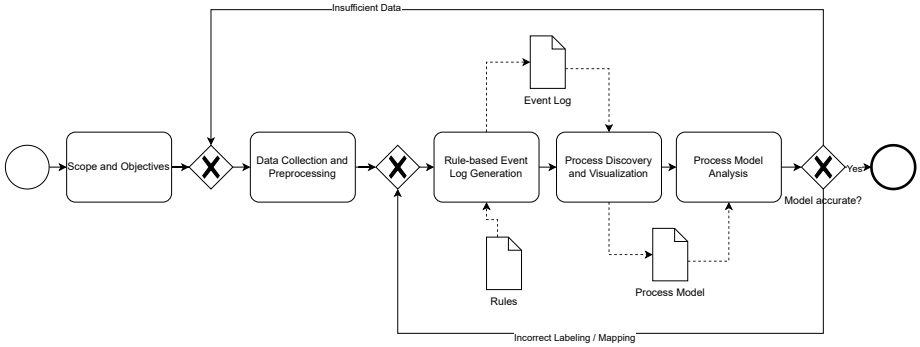


Figure 7: Generic process-mining approach for the IIoT.

Contribution. P5 introduces a novel approach to process mining in IIoT by transforming OPC UA network traffic into structured event logs (c.f. Figure 7). This enables automated process discovery without relying on pre-existing event logs, thereby addressing a major limitation in industrial environments. A proof-of-concept implementation was validated in an automotive end-of-line manufacturing process, demonstrating the feasibility of network-based process mining for both cybersecurity analysis and operational optimization.

Methodology. Building on a combination of DSR and the CRISP-DM framework [55], P5 employs a structured methodology for data collection, log extraction, and process mining. Passive network monitoring captures OPC UA network traffic, which is subsequently preprocessed through rule-based event extraction to build structured event logs. Process discovery techniques are then applied to derive visual models that reveal actual workflows and system interactions. The methodology was further assessed through scalability analysis and expert validation to ensure feasibility and applicability in industrial environments.

Finding 1. *OPC UA network traffic is a valuable source for process mining.*
P5 confirms that OPC UA network traffic contains rich process-related information, making it a promising alternative to traditional event logs for process mining in IIoT environments. However, raw network traffic lacks structured case identifiers, timestamps, and event relationships, requiring dedicated methods to construct event logs. By leveraging request–response pairs, session tracking, and heuristic case ID assignment, the study introduces a rule-based methodology to derive structured event logs from raw traffic. These methods are essential to transform unstructured communication data into actionable process insights, enabling process discovery, optimization, and compliance monitoring in industrial settings.

Finding 2. *Expert validation is necessary to interpret network-derived models.*
While process mining on OPC UA network traffic enables the discovery of hidden workflows and operational inefficiencies, the extracted process models often operate at a network level, requiring human interpretation to translate them into meaningful business process insights. Network-derived logs capture system interactions but lack explicit domain context, meaning that subject-matter experts must validate extracted process sequences to ensure their correctness and relevance. P5 emphasizes that without expert review, automated process mining on OPC UA network traffic may lead to misinterpretations, as certain variations in network traffic may stem from normal operations rather than actual inefficiencies or cybersecurity threats.

Finding 3. *Scalability is key, as processing time increases with larger datasets.* P5 highlights that processing OPC UA network traffic for process mining scales quadratically with dataset size, as shown in Figure 8, creating significant computational challenges when analyzing large-scale industrial networks. The methodology requires intensive preprocessing steps such as event correlation, case ID construction, and session alignment, which become increasingly time-consuming as data volume grows. This scalability limitation suggests that optimizations such as parallelized log processing, data filtering, and AI-driven event structuring are needed to enable real-time or near-real-time process mining applications in IIoT environments.

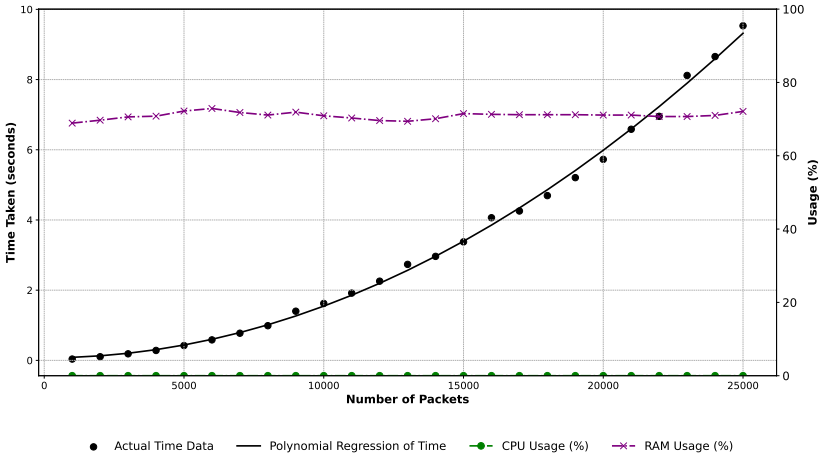


Figure 8: Performance analysis reporting analysis time, CPU utilization, and RAM usage.

6.6 Holistic Synthesis: Merging Research Contributions for Secure IIoT

A recurring question for cumulative dissertations is how the individual results relate and how they effect change in the addressed field. In P6, this question is answered by positioning the contributions within the BPM lifecycle and illustrating their combined use. The result is a process-centric view of IIoT cybersecurity that connects discovery, modeling, enforcement, monitoring, and diagnosis.

Figure 9 synthesizes how the six publications map to the BPM lifecycle and the five research questions, providing a single view that connects Design, Configuration, Monitoring and Diagnosis to the resulting artifacts (P1, P2, P3, P4, P5).

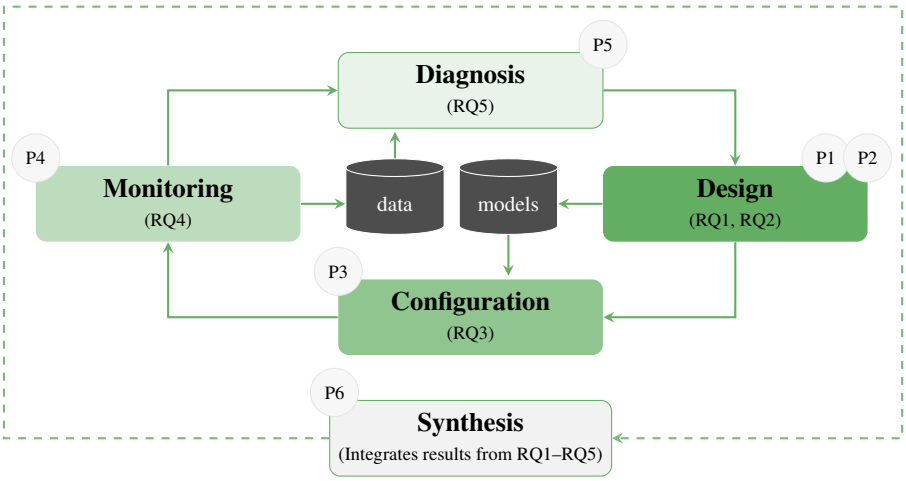


Figure 9: Publications mapped to lifecycle phases and research questions (RQ1–RQ5).

Publication P6: A Reflection on Process-oriented IIoT Security Management

Domain Problem. The IIoT poses substantial cybersecurity challenges due to the scale and interconnection of industrial systems. Traditional IT security often focuses on components rather than end-to-end workflows, leaving process-level risks insufficiently addressed. A process-oriented approach can embed cybersecurity requirements into industrial workflows across the lifecycle and align with standards such as IEC 62443.

Contribution. P6 synthesizes this dissertation's contributions, manual process discovery, network-based process mining, security-aware BPMN modeling, continuous compliance monitoring, and runtime enforcement, into a lifecycle-aligned management framework. It shows how BPM techniques operationalize security-by-design, enabling traceable requirements from design to execution and continuous verification.

Methodology. P6 follows a structured research approach, incorporating SLR, gap identification, and artifact-based analysis to evaluate existing BPM applications in IIoT cybersecurity management. The research questions focus on (1) the effectiveness of BPM-based IIoT security, (2) the methodologies for integrating BPM-based IIoT cybersecurity controls, and (3) the technical tools and techniques required to execute and monitor security-aware process models. A structured methodology is applied to each BPM lifecycle phase (discovery, modeling, execution, and monitoring), evaluating its impact on IIoT cybersecurity and identifying specific gaps that need to be addressed. The study is supported by real-world industrial case studies, including a heating and filling component manufacturing process, demonstrating the practical applicability of BPM-based cybersecurity techniques.

Finding 1. *BPM provides the integrating backbone for process-level cybersecurity.* Embedding controls in models and maintaining traceability to runtime enables end-to-end management, from vulnerability identification to continuous compliance, so security is designed in rather than added later.

Finding 2. *Secure BPMN plus formal syntax enables enforcement and verification.* Extensions such as SIREN and a standard-agnostic formal syntax allow controls (e.g., IEC 62443) to be modeled, validated, and transformed into executable/monitorable rules. Coupled with process-aware monitoring (e.g., SCMV), this supports continuous, evidence-based compliance.

Outlook. Future work should strengthen tool support and scalability (e.g., parallel log construction, selective filtering), extend real-world evaluations, and explore AI-assisted explanations and risk assessments for security-annotated models. A structured method to elicit process-specific cybersecurity requirements would further streamline lifecycle adoption in practice.

6.7 Complementary Publications

Additionally to the core contributions of this work, seven complementary papers were completed before and during the doctoral period. Two early papers (C1 and C2) are out of topic but are included as formative work that paved the way for the doctoral journey. The remaining five papers are thematically aligned with the dissertation and provide supplementary perspectives. An overview is provided in Table 2. Because all papers are already published, the status column shown in Table 1 is omitted here. The ranking notation and evaluation scheme (JQ/CORE/IF) follow the conventions used in Table 1.

Publication C1 marks the start of my scientific journey and was published as part of the *Security for Data-intensive Applications* course at the University of Regensburg. It represents my first contact with research and led to the decision to pursue a PhD. The paper discusses how measures from e-commerce, e.g., *Customers who bought x also bought y* can be used in the context of an IAM Entitlement Shop.

Publication C2 was created as part of the *Sensor Data* research group at the chair of Professor Kesdogan under the supervision of Dr. Christian Roth. The group focused on using gyroscope and accelerometer data from smartphones, which do not require authorization and consume little battery power, to detect vehicle movements and thereby perform GPS-free navigation or privacy attacks, for example.

Table 2: List of complementary publications.

No.	Publication	Ranking
C1	Hornsteiner, M., Groll, S., Puchta, A. (2021). Towards a user-centric IAM entitlement shop: Learnings from the e-commerce. In: *Proceedings of the 13th International Conference on Security of Information and Networks (SIN 2020)*. ACM, New York, pp. 1–4.	CORE C
C2	Roth, C., Dinh, N. T., Hornsteiner, M., Schröppel, V., Roßberger, M., Kesdoğan, D. (2022). ROADR: Towards road network assessment using everyone-as-a-sensor. *IET Conference Proceedings*.	-
C3	Schönig, S., Hornsteiner, M., Stoiber, C. (2022). Towards process-oriented IIoT security management: Perspectives and challenges. In: *Enterprise, Business-Process and Information Systems Modeling (BPMDS 2022, EMMSAD 2022)*. LNBIP, 450, Springer, Cham, pp. 18–26.	JQ C
C4	Hornsteiner, M., Stoiber, C., Schönig, S. (2022). Towards security- and IIoT-aware BPMN: A systematic literature review. In: *Proceedings of the 19th International Conference on Smart Business Technologies (ICSBT 2022)*. SciTePress/INSTICC, pp. 45–56.	-
C5	Ackermann, L., Käppel, M., Marcus, L., et al. (2024). Recent advances in data-driven business process management. Preprint at *arXiv*:2406.01786 [cs.DB].	-
C6	Oberhofer, D., Hornsteiner, M., Schönig, S. (2023). Market research on IIoT standard compliance monitoring providers and deriving attributes for IIoT compliance monitoring. Preprint at *arXiv*:2311.09991 [cs.CR].	-
C7	Hornsteiner, M., Kreussel, M., Steindl, C., Ebner, F., Empl, P., Schönig, S. (2024). Real-time text-to-Cypher query generation with large language models for graph databases. *Future Internet*, 16(12), 438.	IF 3.6

Publication C3 represents the starting point of this dissertation and raises the idea of using BPM to improve IIoT cybersecurity. It also discusses challenges and potential solutions. The papers presented in this dissertation were written based on these considerations and the questions raised in it are answered in detail in P6.

Publication C4 presents an SLR that deals with the intersection between BPMN extensions for IIoT and cybersecurity. The assumption was that dedicated extensions for IIoT cybersecurity already exist, but C4 was unable to find any contributions.

Therefore, the search strategy was changed accordingly: on the one hand, extensions of BPMN for IIoT and, on the other hand, for cybersecurity. By summarizing its findings, C4 lays the foundation for the subsequent contributions of this dissertation.

Publication C5 is a community paper, authored by researchers from eight research chairs across six universities, explores recent advancements in data-driven BPM. It highlights how AI, machine learning, and new data sources such as sensor logs, network traffic, and textual data are transforming process discovery, automation, and monitoring. C5 identifies five key research areas, including data quality, process discovery, hyperautomation, predictive monitoring, and automated process redesign, emphasizing the need for interdisciplinary collaboration. It advocates for advanced AI techniques to enhance BPM, ensuring more adaptive, automated, and data-driven business processes.

Publication C6 conducts a market study on IIoT compliance monitoring, focusing on providers implementing IEC 62443. It identifies challenges in standard compliance monitoring (e.g., lack of formal separation between cybersecurity architectures and compliance verification). Based on the findings, a catalog of attributes to assess compliance is derived, categorized in traffic-based, logical, and manual. The research serves as a foundation for developing automated compliance monitoring systems, offering insights into practice and standard alignment in IIoT cybersecurity management.

Publication C7 presents an Large Language Models (LLM)-based system for real-time natural-language–to-Cypher translation to improve interaction with graph databases (e.g., Neo4j). A chat interface converts user queries into Cypher and supports error correction with iterative refinement. C7 shows the chatbot reliably generates Cypher, selects the appropriate database, and increases accuracy through successive corrections, laying a foundation for extending LLM-driven query interfaces to additional database technologies.

7 Conclusion and Future Work

Cybersecurity in IIoT environments is a complex challenge that benefits from an integrated, process-aware approach. This dissertation has shown how BPM methods and technologies can enhance IIoT cybersecurity by embedding controls and compliance requirements directly into the process lifecycle. By aligning BPM methods and technologies with established industrial standards and regulatory frameworks (e.g., IEC 62443, NIS2, ISO 27001, and CRA), the work provides a structured foundation for achieving security-by-design across IIoT workflows.

The contributions were structured along the four phases of the BPM lifecycle [1]. In Design, methodologies for manual process discovery and security-aware process modeling were introduced to ensure transparency and embed requirements from the outset. In Configuration, a formal syntax was defined to transform security-aware BPMN specifications into enforceable rules for cybersecurity systems. In Monitoring, mechanisms for continuous compliance verification were established so that IIoT processes remain aligned with cybersecurity requirements during execution. Finally, in Diagnosis, process-mining techniques based on network traffic were explored to uncover undocumented participants, hidden dependencies, and unauthorized interactions, enabling continuous refinement of processes and controls.

Taken together, these results position BPM as a structured, lifecycle-oriented framework for managing cybersecurity in IIoT. The methods developed across Design, Configuration, Monitoring, and Diagnosis were evaluated in real industrial contexts, demonstrating applicability for increasing process transparency, operationalizing controls, verifying compliance, and refining processes through diagnostic insights. While this establishes a foundation for BPM-based cybersecurity management, several research directions remain.

Further automation across all lifecycle phases is a priority. AI-driven techniques (e.g., LLMs and automated reasoning) could assist Design by proposing security-aware models and Configuration by deriving enforceable rules. In Monitoring, AI can support detection of deviations and anomalies. Combining process-aware approaches with real-time threat intelligence would strengthen both Monitoring and Diagnosis, enabling continuous adaptation of controls to emerging threats.

Another avenue is extending process-aware management to a broader range of compliance frameworks. While this dissertation primarily aligned with IEC 62443, emerging and evolving regulations (e.g., NIS2, ISO 27001, CRA) motivate unified approaches that span multiple domains. Methodologies for cross-standard compliance management within IIoT processes would benefit organizations operating in heterogeneous, multi-jurisdictional settings.

Scalability remains critical. Although evaluated in real-world case studies, applicability to large-scale, multi-site IIoT environments with heterogeneous infrastructures requires further investigation. Future work should optimize security-aware models for scalability in DESIGN and CONFIGURATION, while distributed MONITORING and federated DIAGNOSIS support continuous compliance and refinement across geographically distributed ecosystems.

Finally, sustained interdisciplinary collaboration is essential. Discovering and modeling processes require integrating BPM and cybersecurity expertise, configuring and operationalizing controls demands coordination between system engineers and security architects, and effective monitoring and diagnosis rely on automation specialists and cybersecurity analysts. Strengthening collaboration among these will be key to producing adaptive, practically deployable frameworks suited to evolving industrial environments.

This dissertation proposes and evaluates a lifecycle-oriented BPM framework for strengthening cybersecurity in IIoT environments. By structuring the contributions around the lifecycle phases, it demonstrates how process-management methods and technologies can embed cybersecurity into industrial workflows, operationalize controls, ensure continuous compliance, and support diagnostic refinement. Continued work on automation, scalability, and cross-domain applicability will further improve the long-term cybersecurity and resilience of IIoT systems.

References

[1] W. M. P. van der Aalst. *Process Mining - Data Science in Action, Second Edition*. Springer, 2016. ISBN: 978-3-662-49850-7. DOI: 10.1007/978-3-662-49851-4.

[2] M. Ali. *Information Systems Research - Foundations, Design and Theory*. Springer, 2023. ISBN: 978-3-031-25469-7. DOI: 10.1007/978-3-031-25470-3.

[3] O. Altuhhova, R. Matulevicius, and N. Ahmed. "An Extension of Business Process Model and Notation for Security Risk Management". In: *Int. J. of Information System Modeling and Design* 4.4 (2013), pp. 93–113. DOI: 10.4018/IJISMD.2013100105.

[4] R. Antrobus, B. Green, S. Frey, and A. Rashid. "The Forgotten I in IIoT: A Vulnerability Scanner for Industrial Internet of Things". In: (2019), pp. 1–8. DOI: 10.1049/cp.2019.0126.

[5] F. Apolinário, N. Escravana, É. Hervé, M. L. Pardal, and M. Correia. "FingerCI: Generating Specifications for Critical Infrastructures". In: *SAC '22: The 37th ACM/SIGAPP Symposium on Applied Computing, Virtual Event, April 25 - 29, 2022*. ACM, 2022, pp. 183–186. DOI: 10.1145/3477314.3507323.

[6] A. Bicaku, M. Tauber, and J. Delsing. "Security Standard Compliance and Continuous Verification for Industrial Internet of Things". In: *Int. J. Distributed Sensor Networks* 16.6 (2020). DOI: 10.1177/1550147720922731.

[7] A. Bicaku, M. Zsilak, P. Theiler, M. Tauber, and J. Delsing. "Security Standard Compliance Verification in System of Systems". In: *IEEE Systems J.* 16.2 (2022), pp. 2195–2205. DOI: 10.1109/JSYST.2021.3064196.

[8] H. Boyes, B. Hallaq, J. Cunningham, and T. Watson. "The Industrial Internet of Things (IIoT): An Analysis Framework". In: *Computers in Industry* 101 (2018), pp. 1–12. DOI: 10.1016/J.COMPIND.2018.04.015.

[9] A. D. Brucker, I. Hang, G. Lückemeyer, and R. Ruparel. "SecureBPMN: Modeling and Enforcing Access Control Requirements in Business Processes". In: *17th ACM Symposium on Access Control Models and Technologies, SACMAT '12, Newark, NJ, USA - June 20 - 22, 2012*. ACM, 2012, pp. 123–126. DOI: 10.1145/2295136.2295160.

[10] I. Butun, ed. *Industrial IoT*. 1st ed. Springer, 2020. DOI: 10.1007/978-3-030-42500-5.

[11] A. Carcano, R. Carbone, M. Figueroa, I. N. Fovino, F. Maggi, and S. Zanero. "TRITON: How It Disrupted Safety Systems and Changed the Threat Landscape of Industrial Control Systems Forever". In: *Black Hat USA*. 2018. URL: https:

//i.blackhat.com/us-18/Wed-August-8/us-18-Carcano-TRITON-How-It-Disrupted-Safety-Systems-And-Changed-The-Threat-Landscape-Of-Industrial-Control-Systems-Forever-wp.pdf.

[12] D. C. Cheng, J. B. Villamarin, G. Cu, and N. R. Lim-Cheng. "Towards End-to-End Continuous Monitoring of Compliance Status across Multiple Requirements". In: *Int. J. of Advanced Computer Science and Applications* 9.12 (2018).

[13] I. Compagnucci, F. Corradini, F. Fornari, A. Polini, B. Re, and F. Tiezzi. "A Systematic Literature Review on IoT-aware Business Process Modeling Views, Requirements and Notations". In: *Software and Systems Modeling* 22.3 (2023), pp. 969–1004. DOI: 10.1007/S10270-022-01049-2.

[14] T. DeMarco. *Controlling Software Projects: Management, Measurement, and Estimates*. USA: Prentice Hall PTR, 1986. ISBN: 0131717111.

[15] *Directive (EU) 2022/2555 of the European Parliament and of the Council (NIS2)*. Annex 6.2: Secure Development Life Cycle, Annex 12.4: Asset Inventory. 2022. URL: https://eur-lex.europa.eu/eli/dir/2022/2555/oj.

[16] M. Dumas, M. L. Rosa, J. Mendling, and H. A. Reijers. *Fundamentals of Business Process Management, Second Edition*. Springer, 2018. ISBN: 978-3-662-56508-7. DOI: 10.1007/978-3-662-56509-4.

[17] F. Ebbers, S. Hacks, and R. Thakurta. "The Business Impact of IIoT Vulnerabilities". In: *25th Pacific Asia Conf. on Information Systems, PACIS 2021, Virtual Event / Dubai, UAE, July 12-14, 2021*. 2021, p. 225. URL: https://aisel.aisnet.org/pacis2021/225.

[18] G. Engelberg, M. Hadad, and P. Soffer. "From Network Traffic Data to Business Activities: A Process Mining Driven Conceptualization". In: *Enterprise, Business-Process and Information Systems Modeling - 22nd Int. Conf., BPMDS 2021, and 26th Int. Conf., EMMSAD 2021, Held at CAiSE 2021, Melbourne, VIC, Australia, June 28-29, 2021, Proceedings*. Vol. 421. LNBIP. Springer, 2021, pp. 3–18. DOI: 10.1007/978-3-030-79186-5_1.

[19] S. Fenz and T. Neubauer. "Ontology-based Information Security Compliance Determination and Control Selection on the Example of ISO 27002". In: *Information and Computer Security* 26.5 (2018), pp. 551–567. DOI: 10.1108/ICS-02-2018-0020.

[20] F. Gallik, Y. Kirikkayis, and M. Reichert. "Modeling, Executing and Monitoring IoT-Aware Processes with BPM Technology". In: *Int. Conf. on Service Science, ICSS 2022, Zhuhai, China, May 13-15, 2022*. IEEE, 2022, pp. 96–103. DOI: 10.1109/ICSS55994.2022.00023.

[21] F. Gallik, Y. Kirikkayis, and M. Reichert. “Modeling, Executing and Monitoring IoT-Aware Processes with BPM Technology”. In: *2022 Int. Conf. on Service Science (ICSS)*. 2022, pp. 96–103. DOI: 10.1109/ICSS55994.2022.00023.

[22] A. Ghose, G. Koliadis, and A. Chueng. “Rapid Business Process Discovery (*R*- BPD)”. In: *Conceptual Modeling - ER 2007, 26th Int. Conf. on Conceptual Modeling, Auckland, New Zealand, November 5-9, 2007, Proceedings*. Vol. 4801. LNCS. Springer, 2007, pp. 391–406. DOI: 10.1007/978-3-540-75563-0_27.

[23] N. Gronau. *Geschäftsprozessmanagement in Wirtschaft und Verwaltung: Analyse, Modellierung und Konzeption*. 2nd ed. GITO mbH Verlag, 2017.

[24] M. Hadad, G. Engelberg, and P. Soffer. “From Network Traffic Data to a Business-Level Event Log”. In: *Enterprise, Business-Process and Information Systems Modeling - 24th Int. Conf., BPMDS 2023, and 28th Int. Conf., EMMSAD 2023, Zaragoza, Spain, June 12-13, 2023, Proceedings*. Vol. 479. LNBIP. Springer, 2023, pp. 60–75. DOI: 10.1007/978-3-031-34241-7_5.

[25] X. Han, L. Hu, L. Mei, Y. Dang, S. Agarwal, X. Zhou, and P. Hu. “A-BPS: Automatic Business Process Discovery Service using Ordered Neurons LSTM”. In: *2020 IEEE Int. Conf. on Web Services (ICWS)*. 2020, pp. 428–432. DOI: 10.1109/ICWS49710.2020.00063.

[26] P. Heinrich and G. Schwabe. “Communicating Nascent Design Theories on Innovative Information Systems through Multi-grounded Design Principles”. In: *Advancing the Impact of Design Science: Moving from Theory to Practice - 9th Int. Conf., DESRIST 2014, Miami, FL, USA, May 22-24, 2014. Proceedings*. Vol. 8463. LNCS. Springer, 2014, pp. 148–163. DOI: 10.1007/978-3-319-06701-8_10.

[27] A. R. Hevner, S. T. March, J. Park, and S. Ram. “Design Science in Information Systems Research”. In: *MIS Quarterly* 28.1 (2004), pp. 75–105. URL: http://misq.org/design-science-in-information-systems-research.html.

[28] IBM Corporation. *X-Force Thread Intelligence Index 2024*. Tech. rep. 2024.

[29] *ISO/IEC 27001:2022 Information Security, Cybersecurity and Privacy Protection — Information Security Management Systems*. Annex A 8.27: Secure System Architecture and Engineering Principles, Annex A 5.9: Inventory of Information and Other Associated Assets. International Organization for Standardization, 2022. URL: https://www.iso.org/standard/27001.

[30] C. Janiesch, A. Koschmider, M. Mecella, B. Weber, A. Burattin, C. Di Ciccio, G. Fortino, A. Gal, U. Kannengiesser, F. Leotta, F. Mannhardt, A. Marrella, J. Mendling, A. Oberweis, M. Reichert, S. Rinderle-Ma, E. Serral, W. Song, J.

Su, V. Torres, M. Weidlich, M. Weske, and L. Zhang. “The Internet of Things Meets Business Process Management: A Manifesto”. In: *IEEE Systems, Man, and Cybernetics Magazine* 6.4 (2020), pp. 34–44. DOI: 10.1109/MSMC.2020.3003135.

[31] D. Jones and S. Gregor. “The Anatomy of a Design Theory”. In: vol. 8. 5. 2007, p. 19. DOI: 10.17705/1JAIS.00129.

[32] L. Klotz, M. Horman, H. H. Bi, and J. Bechtel. “The Impact of Process Mapping on Transparency”. In: *Int. J. of Productivity and Performance Management* 57.8 (Oct. 2008), pp. 623–636. ISSN: 1741-0401. DOI: 10.1108/17410400810916053.

[33] S. S. V. K. Kolla, D. M. Lourenço, A. A. Kumar, and P. W. Plapper. “Retrofitting of Legacy Machines in the Context of Industrial Internet of Things (IIoT)”. In: Procedia Computer Science 200 (2021), pp. 62–70. DOI: 10.1016/J.PROCS.2022.01.205.

[34] T. Kulik, P. W. V. Tran-Jørgensen, and J. Boudjadar. “Compliance Verification of a Cyber Security Standard for Cloud-connected SCADA”. In: *2019 Global IoT Summit, GIoTS 2019, Aarhus, Denmark, June 17-21, 2019*. IEEE, 2019, pp. 1–6. DOI: 10.1109/GIOTS.2019.8766363.

[35] M. Lange, F. Kuhr, and R. Möller. “Using a Deep Understanding of Network Activities for Workflow Mining”. In: *KI 2016: Advances in Artificial Intelligence - 39th Annual German Conf. on AI, Klagenfurt, Austria, September 26-30, 2016, Proceedings*. Vol. 9904. LNCS. Springer, 2016, pp. 177–184. DOI: 10.1007/978-3-319-46073-4_17.

[36] R. Matulevicius. *Fundamentals of Secure System Modelling*. Springer, 2017. ISBN: 978-3-319-61716-9. DOI: 10.1007/978-3-319-61717-6.

[37] S. Meyer, A. Ruppen, and L. M. Hilty. “The Things of the Internet of Things in BPMN”. In: *Advanced Information Systems Engineering Workshops - CAiSE 2015 Int. Workshops*. Vol. 215. LNBIP. Springer, 2015, pp. 285–297. DOI: 10.1007/978-3-319-19243-7_27.

[38] S. Meyer, A. Ruppen, and C. Magerkurth. “Internet of Things-Aware Process Modeling: Integrating IoT Devices as Business Process Resources”. In: *Advanced Information Systems Engineering - 25th Int. Conf., CAiSE 2013, Valencia, Spain, June 17-21, 2013. Proceedings*. Vol. 7908. LNCS. Springer, 2013, pp. 84–98. DOI: 10.1007/978-3-642-38709-8_6.

[39] S. Meyer, K. Sperner, C. Magerkurth, S. Debortoli, and M. Thoma. “Internet of Things Architecture IoT-A Project Deliverable D2.2 – Concepts for Modelling IoT-Aware Processes”. In: *IoT-A Project* (2012).

[40] D. Myers, K. Radke, S. Suriadi, and E. Foo. “Process Discovery for Industrial Control System Cyber Attack Detection”. In: *ICT Systems Security and Privacy Protection - 32nd IFIP TC 11 Int. Conf., SEC 2017, Rome, Italy, May 29-31, 2017, Proceedings*. Vol. 502. IFIP Advances in Information and Communication Technology. Springer, 2017, pp. 61–75. DOI: 10.1007/978-3-319-58469-0_5.

[41] C. Okoli and K. Schabram. “A Guide to Conducting a Systematic Literature Review of Information Systems Research”. In: *SSRN Electronic J.* 10 (2010).

[42] C. Pascoe, S. Quinn, and K. Scarfone. *The NIST Cybersecurity Framework (CSF) 2.0*. 2024. DOI: https://doi.org/10.6028/NIST.CSWP.29. URL: https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=957258.

[43] K. Peffers, T. Tuunanen, M. A. Rothenberger, and S. Chatterjee. “A Design Science Research Methodology for Information Systems Research”. In: *J. of Management Information Systems* 24.3 (2008), pp. 45–77. DOI: 10.2753/MIS0742-1222240302.

[44] *Regulation (EU) 2024/2847 of the European Parliament and of the Council - Cyber Resilience Act (CRA)*. 2024. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R2847.

[45] K. S. Sang and B. Zhou. “BPMN Security Extensions for Healthcare Process”. In: *15th IEEE Int. Conf. on Computer and Information Technology, CIT 2015; 14th IEEE Int. Conf. on Ubiquitous Computing and Communications, IUCC 2015; 13th IEEE Int. Conf. on Dependable, Autonomic and Secure Computing, DASC 2015; 13th IEEE Int. Conf. on Pervasive Intelligence and Computing, PICom 2015, Liverpool, United Kingdom, October 26-28, 2015*. IEEE, 2015, pp. 2340–2345. DOI: 10.1109/CIT/IUCC/DASC/PICOM.2015.346.

[46] S. Schönig, R. Jasinski, and A. Ermer. “Data Interaction for IoT-Aware Wearable Process Management”. In: *Service-Oriented Computing - ICSOC 2020 Workshops - AIOps, CFTIC, STRAPS, AI-PA, AI-IOTS, and Satellite Events, Dubai, United Arab Emirates, December 14-17, 2020, Proceedings*. Vol. 12632. LNCS. Springer, 2020, pp. 67–71. DOI: 10.1007/978-3-030-76352-7_10.

[47] R. Seiger, L. Malburg, B. Weber, and R. Bergmann. “Integrating Process Management and Event Processing in Smart Factories: A Systems Architecture and Use Cases”. In: *J. of Manufacturing Systems* 63 (2022), pp. 575–592. ISSN: 0278-6125. DOI: https://doi.org/10.1016/j.jmsy.2022.05.012.

[48] M. Serror, S. Hack, M. Henze, M. Schuba, and K. Wehrle. “Challenges and Opportunities in Securing the Industrial Internet of Things”. In: *IEEE Transactions on Industrial Informatics* 17.5 (2021), pp. 2985–2996. DOI: 10.1109/TII.2020.3023507.

[49] E. Sisinni, A. Saifullah, S. Han, U. Jennehag, and M. Gidlund. “Industrial Internet of Things: Challenges, Opportunities, and Directions”. In: *IEEE Transactions on Industrial Informatics* 14.11 (2018), pp. 4724–4734. DOI: 10.1109/TII.2018.2852491.

[50] M. Taddeo. “Is Cybersecurity a Public Good?” In: *Minds and Machines* 29.3 (2019), pp. 349–354. DOI: 10.1007/S11023-019-09507-5.

[51] S. H. Turki, F. Bellaaj, A. Charfi, and R. Bouaziz. “Modeling Security Requirements in Service Based Business Processes”. In: *Enterprise, Business-Process and Information Systems Modeling - 13th Int. Conf., BPMDS 2012, 17th Int. Conf., EMMSAD 2012, and 5th EuroSymposium, held at CAiSE 2012, Gdańsk, Poland, June 25-26, 2012. Proceedings*. Vol. 113. LNBIP. Springer, 2012, pp. 76–90. DOI: 10.1007/978-3-642-31072-0_6.

[52] K. W. Ullah, A. S. Ahmed, and J. Ylitalo. “Towards Building an Automated Security Compliance Tool for the Cloud”. In: *12th IEEE Int. Conf. on Trust, Security and Privacy in Computing and Communications, TrustCom 2013 / 11th IEEE Int. Symposium on Parallel and Distributed Processing with Applications, ISPA-13 / 12th IEEE Int. Conf. on Ubiquitous Computing and Communications, IUCC-2013, Melbourne, Australia, July 16-18, 2013*. IEEE Computer Society, 2013, pp. 1587–1593. DOI: 10.1109/TRUSTCOM.2013.195.

[53] J. R. Venable, J. Pries-Heje, and R. L. Baskerville. “FEDS: a Framework for Evaluation in Design Science Research”. In: *Eur. J. of Information Systems* 25.1 (2016), pp. 77–89. DOI: 10.1057/EJIS.2014.36.

[54] C. Wakup and J. Desel. “Analyzing a TCP/IP-Protocol with Process Mining Techniques”. In: *Business Process Management Workshops - BPM 2014 Int. Workshops, Eindhoven, The Netherlands, September 7-8, 2014, Revised Papers*. Vol. 202. LNBIP. Springer, 2014, pp. 353–364. DOI: 10.1007/978-3-319-15895-2_30.

[55] R. Wirth and J. Hipp. “CRISP-DM: Towards a Standard Model for Data Mining”. In: *Proc. of the 4th Int. Conf. on the Practical Applications of Knowledge Discovery and Data Mining*. Vol. 1. Manchester. 2000, pp. 29–39.

[56] M. Wollschlaeger, T. Sauter, and J. Jasperneite. “The Future of Industrial Communication: Automation Networks in the Era of the Internet of Things and Industry 4.0”. In: *IEEE Industrial Electronics Magazine* 11.1 (2017), pp. 17–27. DOI: 10.1109/MIE.2017.2649104.

[57] K. Zarour, D. Benmerzoug, N. Guermouche, and K. Drira. “A Systematic Literature Review on BPMN Extensions”. In: *Business Process Management J.* 26.6 (2020), pp. 1473–1503. DOI: 10.1108/BPMJ-01-2019-0040.

Part II

Research Papers

P1: Guideline for Manual Process Discovery in Industrial IoT

Status	Published	
Date of Submission	01 Aug 2024	
Decision: Revision	17 Feb 2025	
Resubmission Date	29 Apr 2025	
Journal	Sensors	
Authors Contribution	Linda Kölbel	60%
	Markus Hornsteiner	30%
	Stefan Schönig	10%
Full Citation	Kölbel, L., Hornsteiner, M., Schönig, S. (2025). Guideline for Manual Process Discovery in Industrial IoT. In revision at *Information Systems and e-Business Management*.	

Journal Description: Information Systems and e-Business Management (ISeB) is a publication concentrating on the management, design, and deployment of information systems and all e-business related topics.

- Publishes novel research findings that fundamentally advance the field of information systems management and e-business.
- Highlights innovative research across all aspects of information systems management.
- Features analytical, behavioral, and technological perspectives in research.
- Serves as a dynamic forum for both academics and industry practitioners.

Guidelines for Manual Process Discovery for Semi-Automated Processes

Linda Kölbel[1*], Markus Hornsteiner[1] and Stefan Schönig[1]

[1]University of Regensburg, Universitätsstraße 31, Regensburg, 93053, Germany.

*Corresponding author(s). E-mail(s): linda.koelbel@ur.de;
Contributing authors: markus.hornsteiner@ur.de; stefan.schoenig@ur.de;

Abstract

Semi-automated operational environments, where human operators and automated systems coexist, pose significant challenges for traditional process discovery approaches, which typically target either fully manual or fully automated workflows. This paper presents a comprehensive guideline for manual process discovery specifically tailored to semi-automated contexts. Building on established techniques (document analysis, direct observation, structured interviews, and collaborative workshops), we adapt and extend each method to capture both human-driven activities and machine-generated events. The resulting artifact comprises four modular guideline packages, offering step-by-step procedures, guiding questions, and optional tooling to uncover control flow, data flow, resource assignments, and system interactions. A use case in an Industrial Internet of Things (IIoT) setting illustrates how these guidelines can be applied to complex, data-intensive scenarios, though the approach remains domain-agnostic and can be transferred to other semi-automated environments. The development followed the Design Science Research (DSR) cycle, incorporating iterative refinement and validation via expert workshops, surveys, and real-world pilot studies. Our evaluation confirms that the proposed guidelines enhance the completeness, accuracy, and efficiency of manual process discovery in hybrid human–machine landscapes.

Keywords: Business Process Management; Process Discovery; Industrial Internet of Things; Guideline Development, Semi-Automated Processes

1 Introduction

Business Process Management (BPM) constitutes a well-established framework for the identification, analysis, optimization, and monitoring of business processes (Dumas et al 2021). The initial phase in any BPM initiative is process discovery, which entails the systematic detection and documentation of relevant processes.

Traditional process discovery techniques are typically tailored either to fully manual processes, often supported by interviews and workshops, or to fully automated processes, where the availability of log data permits the application of process mining methods (Ackermann et al 2024; Dumas et al 2021). Nevertheless, numerous real-world workflows, particularly in operational environments, exhibit a semi-automated character: they encompass both machine-driven activities and manual tasks that frequently remain undocumented. Under such circumstances, traditional discovery approaches tend to exhibit shortcomings (Langer and Söffker 2011).

Despite the critical importance of process discovery within BPM, practical and detailed guidance for its execution in complex or semi-automated contexts remains scarce. Our survey findings confirm a pronounced demand for structured, actionable guidelines, yet existing literature typically offers only high-level descriptions of discovery phases. Consequently, practitioners are frequently left without concrete instructions on how to proceed, especially when both technical systems and human activities must be discovery and aligned.

To address this deficiency, a suite of four complementary process discovery guidelines has been developed, each grounded in a distinct discovery method (e.g., interviews, observation, collaborative workshops). These guidelines are modular, adaptable, and intended to support both novice and experienced users in conducting methodologically rigorous process discovery activities. They include explicit procedural steps, guiding questions, and optional tools to facilitate the capture of control flow, data flow, and system interactions within complex settings.

The Industrial Internet of Things (IIoT) serves as the chosen use case for both demonstration and evaluation of the proposed guidelines. The IIoT interconnects people and machines to foster more rapid and cohesive industrial processes (Boyes et al 2018), yet it presents major challenges for process discovery: legacy equipment and smart devices coexist (Raptis et al 2019), manual interventions remain undocumented (Wang et al 2018), and real-time responsiveness is often required (Szelągowski et al 2022). For instance, an automated production line may generate detailed system logs from robotic stations, whereas human quality inspections are neither digitized nor formally recorded. Such conditions render the IIoT an instructive and demanding context for assessing manual process discovery in complex environments.

The development of the guidelines adhered to the Design Science Research (DSR) methodology (Hevner et al 2004) and involved iterative refinement through multiple evaluation rounds with both academic and industry stakeholders. This multi-perspective validation strategy ensures that the guidelines are both practically applicable and methodologically sound.

The structure of this paper is as follows: In Section 2, the research method and its application are presented. In Section 3, the fundamental background of the contexts of this paper is discussed. In Section 4, the related work is reviewed, its discovery

recounted, and its influence on this paper assessed. In Section 5, the developed guidelines and their application are introduced. In Section 6, a combined example of the different methods is presented. In Section 7, the guidelines are applied to specific use cases. In Section 8, the guidelines and their effectiveness are evaluated. Finally, in Section 9, the limitations are summarized and potential directions for future research are outlined.

2 Research Method

In this study, the DSR framework of Hevner et al (2004) is employed to develop a suitable artifact addressing a specific problem in the domain of information systems. The framework comprises seven steps, which are outlined below, and their instantiation in the context of the present research is subsequently described. The sequence and mode of guideline implementation are not rigidly prescribed, thereby preserving the creative latitude of the researchers.

Design as an Artifact states that the research process must lead to an artifact, such as a model or a method. The artifact of this work is a novel method for manual discovery of processes, including semi-automated processes, that is described in detail and applicable in practice.

Problem Relevance requires that the problem is not only relevant academically, but also in industry. Since guidelines for discovering semi-automated processes do not yet exist, but the importance of automation and digitalization in industry is constantly increasing, discovering such processes using traditional methods is becoming increasingly complex. The developed artifact should extend and adapt established BPM methods to systematically discover semi-auomated processes.

Design Evaluation requires that the artifact to be developed is comprehensively evaluated. This evaluation for various criteria is discussed in Section 8. The evaluation is divided into three rounds and consists of an application of the artifacts in form of use cases, a survey and expert groups.

Research Contribution requires that the artifact to be developed provides a novel contribution to the state of the art. In order to determine the state of the art, a systematic literature search is carried out, which is discussed in Section 4. No published scientific papers addressing manual process discovery guidelines for semi-automated processes could be found. Therefore, the artifact developed in this paper represents a novel research contribution.

Research Rigor requires that the artifact is developed using accepted and therefore reproducible scientific methods. For this purpose, this paper utilizes the already described DSR methodology according to Hevner et al (2004) for the development of the artifact. In addition, a literature review followed the guideline of Okoli and Schabram (2010) is carried out in Section 4, on the results of which the artifact developed in this paper is based.

Design as a Search Process emphasizes that the development of the artifact is characterized by multiple iterative cycles rather than a singular occurrence. This was also the case in the development of the artifact presented in this paper.

Based on the literature, several iterations of the artifact were created and continuously improved to the current status using, for example, procedures from various research disciplines and expert feedback.

Communication of Research requires that the artifact be made accessible to an informed and interested public. Usually in the form of a publication in a specialist medium. Accordingly, the publication of the artifact of this paper in a journal.

3 Background

3.1 Business Process Management and Process Discovery

BPM encompasses various tasks and measures to make processes more efficient and effective (Hansen et al 2019). BPM should serve as a decision-making aid for process improvement and support the management of companies (Weske 2012). In particular, the aim is to shorten throughput times, increase efficiency, save costs and minimize error rates, which then contributes to increasing competitiveness (Dumas et al 2021; Bernardo et al 2017). BPM is also seen as a strategy for gaining a competitive advantage, whereby numerous definitions exist (zur Muehlen and Ho 2005). This paper is based on the definition by Dumas et al (2021):
A body of methods, techniques, and tools to identify, discover, analyze, redesign, execute, and monitor business processes in order to optimize their performance.

The emphasis of this study is placed on the process discovery phase, explicitly addressing the underlying concepts, methods, and techniques. A comprehensive understanding of the process is required to facilitate its subsequent analysis, discussion, and optimization (Jakobs and Spanke 2011). Accordingly, information about the process is discovered using a variety of methods to capture and document the actual state of affairs. Traditional discovery techniques include document analysis, observation, interviews, and workshops (Dumas et al 2021; Hansen et al 2019; Gronau 2017). The collected data, whether written, visual, or verbal, is then formalized in a process model (Dumas et al 2021; Hansen et al 2019). The objective of process discovery is to amass all necessary information for modeling the relevant processes, encompassing organizational structures, workflows, procedural instructions, assigned responsibilities, utilized documents, and technical infrastructure (e.g., warehouse layouts, conveyors, production machinery) (Dumas et al 2021; Becker et al 2012), as well as data and system-related aspects (Dumas et al 2021; Becker et al 2012).

For clarity and traceability, modeling is typically carried out in well-established modeling languages such as Event-driven Process Chains (EPC), Unified Modeling Language (UML), flowcharts, or Business Process Modeling Notation (BPMN) (Dumas et al 2021). Modeling helps in process analysis, optimization, and also serves as a knowledge base for training (Jakobs and Spanke 2011). The result of this phase is an as-is process model that represents the current process status (Dumas et al 2021).

The challenges of process identification and discovery lie in the organization of processes based on division of labor, the use of consistent terminology, and the complexity of the processes, alongside terminology inconsistencies and process complexity (Hansen et al 2019). Often, several iterations are required to fully discover and model a

process, as misunderstandings, generalizations, errors, or ambiguities can occur during the data discovery phase (Hansen et al 2019; Jakobs and Spanke 2011).

3.2 Industrial IoT

The IIoT is defined as a specialized subset of the Internet of Things (IoT) that is specifically tailored to industrial use cases. Both paradigms are comprised of networked devices exchanging data; however, the IIoT is engineered for large-scale, machine-centric environments, such as manufacturing and logistics, where stringent requirements for reliability, security, and real-time performance must be satisfied (Gilchrist 2016; Sisinni et al 2018). In contrast, the broader IoT landscape encompasses consumer, commercial, and industrial verticals, each characterized by distinct user groups and technical constraints. Consumer-oriented IoT applications, such as smart homes and wearable devices, are primarily designed to enhance user convenience (Gilchrist 2016). The IIoT, by comparison, emphasizes the improvement of operational efficiency, automation, and responsiveness through machine-to-machine communication, supporting novel use cases such as predictive maintenance and robotics (Sisinni et al 2018). IIoT-processes are a type of semi-automated process.

In the context of BPM, the integration with the IIoT is of particular significance. IIoT systems continuously generate large volumes of real-time data, which can be directly incorporated into process models to enable dynamic process execution, real-time monitoring, automated decision-making, and data-driven process discovery. This transforms traditional BPM approaches by enhancing their adaptability and responsiveness to changing environmental and operational conditions. Conversely, IIoT-relevant components within industrial processes must remain manageable and governable through BPM methodologies to ensure reliability, traceability, and compliance. Therefore, there is a growing need for BPM frameworks specifically tailored to the requirements of IIoT environments, capable of discovering and orchestrating complex, data-intensive, and event-driven processes.

3.3 Perspectives

For a complete and accurate discovery and modeling of processes, different perspectives must be considered (Jablonski and Götz 2007; Tiftik et al 2022; van der Aalst 2016). They offer points of view on different aspects that contribute to a comprehensive understanding. These perspectives are interlinked and cannot be viewed in isolation due to interdependencies. Accordingly, several perspectives should be included in the process model. Five relevant perspectives are identified, each of which contributes to a holistic view of the process (Jablonski and Götz 2007).

Data Perspective includes input and output objects of a process, such as documents, files or artifacts and time for provision. The perspective shows how a task is performed and establishes a link between the process and (external) data models (Jablonski and Götz 2007; Dumas et al 2021). It also allows the effects of data on the process to be analyzed (Tiftik et al 2022).

As part of the process, and also for IIoT processes, it is important to record

the connections of machines, measurement sensors, data processing systems and their generated data and forwarding paths to present them in the process model. The network traffic data is therefore a part of the data perspective (Hornsteiner et al 2024).

Functional Perspective defines a process step or subprocess and asks what needs to be done. It serves as the basic unit for the execution of a process and specifies which activity or task is executed, whereby the execution can be carried out either by a person or an automated user (Jablonski and Bussler 1996; Awadid 2017).

Operational Perspective encompasses the tools, applications or services that are used within a process step (Schönig et al 2012; Awadid 2017; Jablonski and Götz 2007). It defines how a process step is executed (Jablonski and Bussler 1996).

Resource Perspective enables the examination of process execution with regard to the organizational structure. It considers where activities are performed and who is responsible for the execution (Awadid 2017). It assigns responsibilities for tasks that are assigned to both human actors and systems (Jablonski and Bussler 1996).

Control Flow Perspective focuses on the sequence of process steps without considering time (Jablonski and Götz 2007; Dumas et al 2021). It specifies the sequence in which activities, functional units and events appear, thus illustrating the workflow and showing the causal dependencies between all modeling elements (Jablonski and Götz 2007; Awadid 2017). The control flow specifications must be adhered to during process execution. These can be modeled using control flow constructs such as sequence, parallel branching, conditional branching and merging (Jablonski and Bussler 1996).

4 Related Work

To provide the scientific basis for the design of the artifact presented in this paper, a systematic literature review (SLR) was conducted following Okoli and Schabram (2010). A SLR helps to ensure that potentially relevant information is reviewed as comprehensively as possible and that a selection of the required facts and details can be made. The SLR presented in this paper is based on eight main steps, where first the literature search was planned, then the relevant literature was searched and selected, and finally it was extracted and analyzed.

The *Web of Science* metadatabase and the *ACM Digital Library* were used for the literature search. In the *Web of Science*, the literature searched was restricted to the databases *Springer Nature*, *Elsevier*, *Emerald* and *IEEE Xplore* as these are of particular relevance to the community. Articles, proceeding papers and book chapters were included in the selection of papers in order to cover as wide a range of information as possible. In addition, several screening criteria were defined:

1. **Duplicates:** Duplicates are eliminated.
2. **Publish date after 2007:** Only literature published from 2007 onward was considered. Following the formalization of the de facto process-modeling standard BPMN in 2006, BPM as a holistic discipline consolidated existing methodologies and established consistent terminology. Likewise, references to the IoT and

its industrial counterpart began to proliferate in the mid-2000s. Consequently, publications predating 2007 were excluded from this study.
3. **English as language:** Only papers written in english are included.
4. **Access to paper:** Only papers we had access to were included.
5. **Relevance for research:** Papers that are not thematically relevant to our research question are excluded.

In order to find related work, the following research questions were defined:

Q1. Are there BPM methodologies and tools specific to process discovery in the IIoT?
Q2. How to efficiently discover processes in the IIoT?

To answer the research questions, a search string was defined and continuously developed within an iterative process. As the defined search string yielded few relevant results, the research questions were adapted in order to obtain more relevant information in the literature search. Therefore, research questions Q3 and Q4 were formulated to address related issues.

Q3. What connections between BPM and the IIoT have already been explored including process discovery?
Q4. Are there already established approaches for general process discovery in processes that maybe transferable to the IIoT context?

To answer Q3, the databases were searched using the iteratively developed search string below and six duplicates were eliminated. In a second step, six papers that could not be accessed were excluded. At last the content of the literature found was analyzed including IIoT context and relevance to the present paper. We identified 12 of the 24 retrievable papers as relevant. These selected papers are discussed in more detail below.

TI=(("BPM" OR "business process management" OR "process management") AND ("IIoT" OR "Industrial IoT" OR "Industrial Internet of Things" OR "IoT" OR "Internet of Things" OR "Industry 4.0")) OR (TI=("BPM" OR "business process management" OR "process management") AND AB=("IIoT" OR "Industrial IoT" OR "Industrial Internet of Things" OR "IoT" OR "Internet of Things" OR "Industry 4.0"))

To answer Q4, a second search string was used to find existing process analysis methods. One duplicates and five papers we had no access were removed. After analyzing the remaining six papers the four papers not related to manual process discovery methods were removed.

TI=("Process discovery methods") OR TI=("Business process discovery")

In Figure 1, the search process and the steps taken for both research questions are shown using a PRISMA diagram. (Page et al 2021). In Table 1 the related works and their contents found for the two research questions described above are presented.

Our analysis (see Table 1) reveals the absence of specialized manual methods for IIoT process discovery in existing literature, with current efforts predominantly focusing on process mining approaches. While some studies incorporate IIoT processes, they do not detail the methodologies employed for their identification. The key findings from the related literature are elaborated upon below.

Authors	IIoT and BPM included	IIoT process used	Discovery described	Manual method used	Manual method described
Houy et al (2010)	✓	✓	✓	✗	✗
Grefen et al (2018)	✓	✗	✗	✗	✗
Schönig et al (2020b)	✓	✓	✗	✗	✗
Schönig et al (2020a)	✓	✓	✗	✗	✗
Giudice (2016)	✓	✗	✗	✗	✗
Bazan and Estevez (2022)	✓	✓	✗	✗	✗
Seiger et al (2022)	✓	✓	✗	✗	✗
Schönig et al (2020)	✓	✓	✗	✗	✗
Janiesch et al (2020)	✓	✗	✗	✗	✗
Mass et al (2016)	✓	✓	✗	✗	✗
Schönig et al (2018)	✓	✗	✗	✗	✗
D'Hondt et al (2019)	✓	✓	✗	✗	✗
Ghose et al (2007)	✗	✗	✗	✗	✓
Han et al (2020)	✗	✗	✓	✓	✓

Table 1 Review of thematically relevant literature with regard to the mentioned criteria.

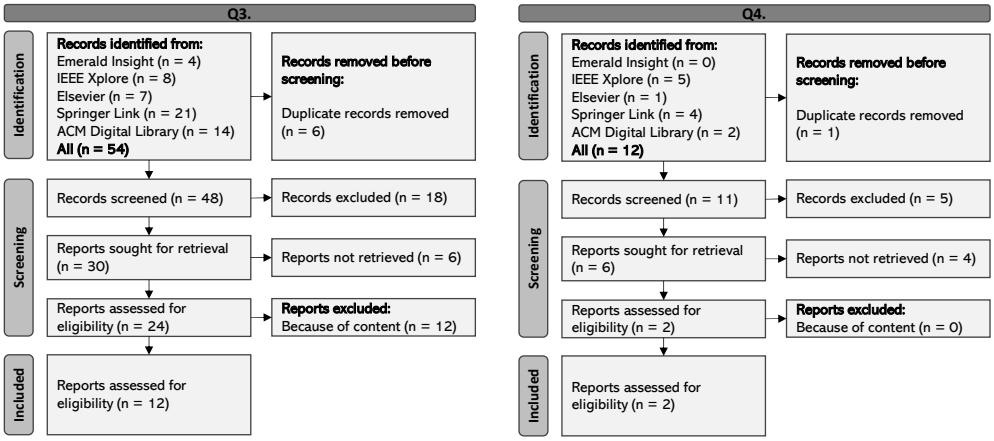


Fig. 1 PRISMA-diagram for Q3 and Q4. (Page et al 2021)

The literature review by Giudice (2016) describes the potential impact of IoT on BPM, both inside and outside the enterprise. In particular, these impacts relate to the support of BPM in process optimization and implementation. Although a connection between IoT and BPM is described here, it is the reverse of this paper, as the influence of IoT on BPM is examined. The use of IoT is understood in an industrial context, but not explicitly mentioned. In addition, the literature review does not mention process discovery.
Bazan and Estevez (2022) presents a similar approach to Giudice (2016). They examine the impact of IoT on BPM and emphasize that successful BPM in an organization makes it easier to deal with the challenges of Industry 4.0. Although process discovery is implicitly addressed in this context, it is not explicitly mentioned.
Schönig et al (2020b) presents an approach for interacting with IIoT data during process execution. This approach enables portable real-time user interfaces to inform process participants about current tasks and thus support efficient task execution. Schönig et al (2020b) describe an adaptation of process execution for industrial processes using IIoT data, but do not address how the processes used (which are obviously industrial processes) were discovered.
Seiger et al (2022) investigate the integration of BPM and IIoT to provide benefits to both research areas. This includes the development of an IIoT system architecture that is integrated with BPM systems in smart factories. The goal is to enable sensor events to interact with existing BPM systems. To achieve this, IIoT and BPM technologies are integrated along the BPM lifecycle. The focus is on process modeling, automation and process mining. Although process discovery is not a central topic, it is mentioned that process mining techniques can be used to discover processes based on logs and obtain statistics. However, there is no detailed explanation of discovery.
Janiesch et al (2020), similar to Giudice (2016), discusses the relationship between IoT and BPM. The goal is to highlight the challenges of connecting the previously separate domains of IoT and BPM. Process discovery is also addressed, which is performed using log files and the process data itself. Apart from process mining, no other discovery techniques are described.
Ghose et al (2007) presents a self-developed method for deriving process models from textual descriptions, which supports the answer to Q4. This approach is based on the assumption that documents serve as a source of information for traditional modeling. Although it is an evolution of document analysis that can accelerate process discovery, this approach does not provide a detailed description of a specific process discovery method. The goal is not to model a process from scratch, but to automatically obtain an initial model that can then be edited by the modeler.
Similar to Ghose et al (2007), Han et al (2020) presents an automated business process service that aims to streamline the process discovery phase of BPM projects. Unlike existing approaches that rely heavily on human knowledge to derive hierarchical structural relationships between activities from textual process documentation, the approach uses a neural network. It is designed to automatically find the latent hierarchical structure in the documents. Through process-level language modeling, it can accurately identify process elements and generate BPMN scripts, significantly reducing the time and effort required for process discovery.

As the literature review revealed that previous literature does not contain manual methods for process discovery in the IIoT context, additional literature was consulted. In particular, Dumas et al (2021) and Gronau (2017), as these are considered standard literature in process discovery and describe traditional methods.

Dumas et al (2021) provide insights into possible *established approaches to general process discovery*. The methods of document analysis, observation, interviews, and workshops are explained. A description and an example are given for each method. Brief guidelines for conducting interview and workshop-based discovery methods are provided. However, the document analysis and observation methods are covered in less detail. However, the methods presented relate to traditional BPM tasks in an office environment, for example, and not to industrial processes.

Gronau (2017) explain methods such as interviews, questionnaires, focus groups (understood as workshops), observations, the inventory method (which includes document analysis) and automatic procedures. The differences between the individual approaches are explained and vary in detail with regard to the implementation of the individual methods. The focus is primarily on the interpersonal component, without any industrial reference.

The search for related work shows that no manual approaches for process discovery in the IIoT context have yet been described. Janiesch et al (2020) and Seiger et al (2022) only mention the possibility of process discovery based on log files and data generated during process execution. Moreover, no general guidelines for process discovery were found that are independent of the IIoT context. This identified research gap is closed in this paper by developing structured methods for manual process discovery in an industrial context based on Dumas et al (2021).

5 Guidelines for Manual Process Discovery

This Section provides an application proposal for the traditional discovery methods *document analysis*, *observation*, *interview* and *workshop*. Every subsection is divided into two parts: *(i)* the traditional background and fundamentals of the process discovery method and *(ii)* the description of the guideline of the method.

The descriptions presented are guidelines that can be applied, but whose suggested procedures do not have to be strictly adhered to. In order to successfully discover a process, the sequence of the discovery can be changed. At the end of the discovery it is important to ensure that all perspectives from Section 3.3 have been discovered.
Figure 2 shows the requirements that must be fulfilled after a process has been identified. Different discovery methods can also be combined with each other, whereby only individual discovery aspects of the methods can be addressed. An example proposal for combining the methods can be found in Section 7. The individual components of the respective discovery methods are presented here in a possible sequence that can be used by inexperienced process discoverer (PD), for example.
The guidelines are explicitly aimed at people with little or no knowledge of traditional process discovery methods. People who already have prior knowledge can modify the guidelines or pick up on individual aspects if necessary.

We recommend drawing up a corresponding process map and identifying relevant processes within this map before discovering processes. The process to be discovered should be considered in the context of the previous and subsequent processes. In addition, the objective and purpose of the process discovery should be defined prior to discovery in order to adjust the focus and level of detail accordingly. The discovery can be carried out top-down, depending on the desired level of detail.

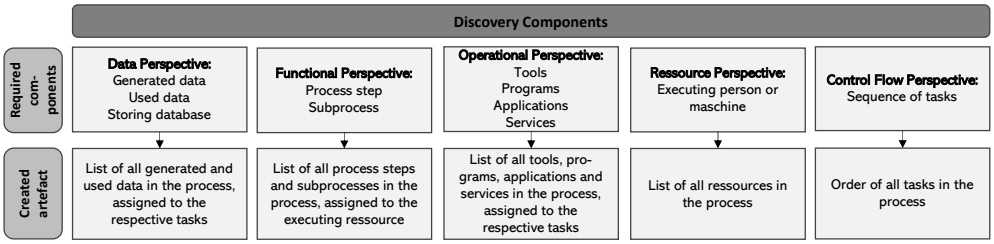


Fig. 2 These process components must have been discovered at the end of the process discovery.

5.1 Document Analysis

5.1.1 Traditional Document Analysis

Existing process descriptions such as internal policies, organizational charts, manuals, models or instructions can be used for process discovery (Dumas et al 2021). Similarly, information from business distribution plans, regulations, budget, economic, personnel, and staffing plans, directives, job descriptions, requirement documents, design documents, order statements or meeting protocols can be obtained by the PD (Federal Ministry of the Interior and Community 2012). The collected documents, containing information about the current state of the process, are reviewed and process-relevant information is extracted (Federal Ministry of the Interior and Community 2012). Based on this information, a model of the process can be created. During document analysis, the following information can be extracted for process discovery (Federal Ministry of the Interior and Community 2012): Task structures, areas, and carriers; organizational structures and process workflow; specifications and conditions within the process; decision points; time required; linked and used documents in IT systems.

There is no information on the approach or techniques for extracting information from the documents and converting it into a process model. Documents are usually not process-oriented and therefore not uniformly granular. This leads to different levels of detail in the various documents, making direct derivation of processes from the documents usually not possible (Dumas et al 2021). Furthermore, the documents used may be outdated or incorrect and do not guarantee the correctness of the information contained therein as they refer to past states (Dumas et al 2021; Hansen et al 2019). However, documents are free from personal evaluations and thus provide an objective basis for familiarizing oneself with a process. They serve as a starting point for process

discovery (Dumas et al 2021; Hansen et al 2019; Federal Ministry of the Interior and Community 2012).

5.1.2 Guideline for Document Analysis

Preparation

The preparation of the document analysis starts with the collection of all process-relevant documents. These include for example business distribution plans, business regulations, budget, economic, personnel, and staffing plans, instructions, job descriptions, requirement and design documents, order declarations, machine manuals and operating instructions, specification documents for involved individuals, site plans of the production facility and other documents related to the process or involved entities.

Sort the documents according to their level of detail and check short and structured documents first, followed by more extensive documents. Finally, focus on machine-specific documents due to their specificity. This top-down approach provides a clear overview before delving into details systematically.

Discover Resources

In this step, the documents are reviewed from the *resource perspective*. All documents are examined to determine which executing instances, i.e. people and machines (short: resources), are involved in the process execution. Each document is worked through individually, and notes are taken as soon as a machine or a role of a person performing a specific activity is mentioned. Person roles are often terms describing activities, i.e. "truck driver". Machines are usually identified by their own names i.e. "welding machine". If explicit names for machines or person roles are not provided in the documents, the PD should assign appropriate designations. It is crucial that these designations are used consistently to avoid confusion, duplicates, or other errors.

Discover Tasks

As soon as all resources have been identified and noted, we recommend recording the associated tasks, the *functional perspective*, and assigning them directly to the discovered resources. All documents should be reviewed and every activity and task (short: task) mentioned should be noted. It should also be noted which resource performs the task that this can be assigned directly during modeling later. A task is one step of work in the process.

It is important to capture all tasks that can be performed by a resource. This applies regardless of whether the tasks appear to be related, occur only in special cases, or have other peculiarities. If a task can be performed by different resources, the task is noted for each participating resource, along with an indication which other resources can also perform this task. This will be taken into account later in the modeling by creating an exclusive decision node, which ensures that the task is only executed once. It is also possible to discover the tasks independently of the previous resource acquisition. Nevertheless, it should be ensured that the tasks can be assigned to the correct resource later.

Discover Tools

The *operational perspective* is captured by discovering the he tools, programs, applications, services, and software components (short: tools) used to perform a task. For each task, it is determined how it is implemented in practice. All available documents must be reviewed and searched for the mentioned tools and the task where they are used. A direct assignment of the tools to the task is recommended directly when the tool is discovered. For example, if the ERP system is used, this is noted for the corresponding task. It is also possible to detect the tools independently of the previous task detection. Nevertheless, it should be ensured that the tools can be assigned to the correct task later.

Discover Data

The data which is produced or used in each task covers the *data perspective*. The documents should be read through chronologically and any data element mentioned should be noted. For each data element noted, the task in which it is produced and used should be noted. If a data element is produced in a task, details such as the type of sensor used, data capture intervals, data format, and destination are useful to record. If a data element is used in a task, the purpose, format and source of the data are possibly interesting. In both cases, the storage location of the data, typically a database, is also indicated. In order to manage the discovered information clearly, it is recommended to use tables that record the aforementioned properties as columns and the data elements as rows.

Discover Sequence

The sequence of individual tasks is extracted from the documents to represent the *control flow perspective*. All documents are read through, examining which task the process starts with and which subsequent tasks follow. It is advisable to identify the starting point of the process and then sequentially determine the next step. If there are decision points or intermediate events within the process, these should also be recorded. This may include information such as the duration of certain process steps, the conditions under which certain tasks are executed and identifying which tasks sensors produce data.

Validation

Whether the process has been accurately captured cannot be immediately verified. There is the possibility of conducting the entire document analysis again and recreating the model independently of the initial capture. An alternative method for validating the model is to choose another discovery method like observation, interviews or workshops and execute it. Subsequently, the two process models can be compared. If discrepancies are found between the two models, this indicates that at least one of the captures was flawed or incomplete. In such a case, it is necessary to review the documents again to identify and rectify any errors and incompleteness.
In order to collect the individual perspectives, the documents can be run through in several iterations for one perspective at a time or all perspectives can be run through

within one iteration. For the sake of clarity, we recommend proceeding in several iterations and identifying the resources first. Then discover the tasks and assign them to the corresponding resources. Discover the data and tools at the same time and assign them directly to the tasks. Finally, the tasks can then be put in the correct order using the documents.

Advantages and Disadvantages

The advantages of document analysis include that it does not interfere with ongoing production processes, allowing operations to continue without outages or disruptions. Additionally, it incurs no extra personnel resource costs and provides detailed documentation that enables a comprehensive understanding of the processes. These documents remain available at all times, serving as a continuous point of reference.
However, document analysis also presents some disadvantages. It demands a significant time investment from the PD, with analysis time increasing as more documents are included. There is also the risk of misunderstandings arising from complex technical machine descriptions, often requiring the involvement of additional experts for clarification. Furthermore, the accuracy of process models can suffer from outdated or incomplete information. Particularly in IIoT environments, documentation may be lacking or not detailed enough in crucial areas such as data flows and machine communication.
In conclusion, conducting document analysis is sensible when there is a solid base of up-to-date and detailed documentation and when processes cannot be disrupted. It is especially useful in stable, well-documented environments where process understanding is needed without interfering with ongoing operations. However, in highly dynamic or poorly documented IIoT settings, alternative methods or supplementary interviews and observations may be necessary to avoid incomplete or inaccurate results.

5.2 Observation

5.2.1 Traditional Observation

During observation, the PD observes the execution of the process and can directly capture the current process activities (Dumas et al 2021; Gronau 2017). In business processes, the PD can take an active role (e.g. the perspective of the customer) or a passive role (e.g. the perspective of the employee) to conduct overt or covert observations (Dumas et al 2021; Gronau 2017). The PD documents their observations and subsequently translates them into a process model. Similar to document analysis, the literature does not provide specific techniques or instructions for conducting observations. Since observation is passive, no workflows or processes are interrupted. There are no additional costs due to work interruptions or production stops during process discovery (Gronau 2017; Hansen et al 2019; Dumas et al 2021). Furthermore, observation enables the PD to gain a better understanding of process boundaries and reduces reliance on information from documents or process participants (Dumas et al 2021). Observation allows for an objective view of the process from the perspective of the PD and is not subject to the subjective influences of process participants. However, it should be noted that employees may change their behavior if they know they

are being observed, and may work in a more structured or faster manner than usual (Dumas et al 2021; Hansen et al 2019). Additionally, observation requires that the PD has access to the process, which may require access to remote facilities or locations (Dumas et al 2021). It may be temporally or spatially impossible to continuously observe a process. In such cases, the PD may need to observe the process multiple times to ensure that all possible process paths have been observed at least once.

5.2.2 Guideline for Observations

It is recommended to model the process during observation. This allows the process to be captured based on the sequence of execution, enabling the components to be recorded directly in the correct order. Thus, the guiding perspective for observation is the *control flow perspective*.
The PD tracks the manufacturing of a particular component from the beginning to the end of the process. For example, if a piece of wire is clamped into a machine at the beginning, the PD follows this piece of wire until the end of the process, where a complete final product is produced. The PD starts at the beginning of the process and records the trigger of the process. Then, they track the first process step. If there are multiple ways the process can start, one possible starting event is chosen, while all other possible starting events are noted. After the observation is completed, the process is observed from another starting event until the first common task reached after all starting paths. Familiarity with the specific domain where a process takes place can be advantageous for a PD, as it facilitates the identification, differentiation, and detailed specification of individual tasks. However, such domain-specific expertise is not an essential prerequisite. As demonstrated in the use case presented in Section 7.2, effective process observation and modeling can also be conducted by a PD without prior specialist knowledge.

Discover Tasks

For each process step, the PD observe what happens in the process step to cover the *functional perspective*. A process step in the observation is an executed activity and is thus differentiated from the next or previous step. It should be possible to record the observed activities as compactly as possible. The level of detail of a task depends on the previously defined granularity of the process.

Discover Resources and Tools

At the same time as observing the task, the PD can make a direct note of who performs this process step (which resource) and whether it is apparent which tools are used for execution. This covers the *resource* and *operational perspectives*. The resources and tools can also be discovered independently of each other and of the tasks. However, it is important that they are allocated correctly. We therefore recommend assigning a task directly to the executing resource and noting the tools used. The executing resource can be directly modeled as a lane. If it already exists, the step is skipped. The observed task is modeled as a task and assigned to the corresponding resource. Then, any tools used are linked to the task. Once all components are captured, the PD moves on to the next process step and repeats the process.

Discover Sensors for the Data Perspective

The discovery of data perspective is not possible in the observation. Nevertheless, sensors that are sighted during the process can be included in the model. This allows the model to show where data is generated in the process.

Handling Branches

Once the PD recognizes that the process branches, it is advisable to follow one path at a time and not try to capture multiple paths simultaneously, because the size and complexity of the process can lead to confusion. The model could become faulty or incomplete if the PD forgets parts of the process or neglects a path. To maintain clarity, the following approach is recommended when encountering a process branch:

1. The PD notes in a separate document the task where the process branched and the number of possible additional paths at this point.
2. The PD choose one of these paths and continue through the process.
3. Once the PD reach the end of the selected path, they return to the marked point and choose the next path.
4. The process is fully traversed again, and this process is repeated until all noted branches are addressed.

If there are further branches of the process in a path, the task and the number of paths are noted. The processing of the noted branching points is done chronologically according to the notation, with initially noted branches being processed first. This ensures that all branches are addressed, and the process is modeled along the control flow.

Handling Overlooking of Paths

The overlooking of paths in forward observation occurs when paths are rarely executed. If a path is not activated during observation, it cannot be observed and therefore cannot be captured in the model. However, backward observation does not guarantee the capture of rarely executed paths. To reduce the likelihood of overlooking paths, the following measures can be taken:

- *Multiple iterations:* Observation can be conducted multiple times, both forward and backward. Each additional iteration increases the chance of capturing rarely executed paths.
- *Increased observation duration:* To ensure that even rare paths are captured, the observation duration at each process branch can be extended. This allows for the discovery of unusual or less frequent process flows.

Validation

The accuracy of the observation process discovery can be validated. To do this, the observation is repeated from the end of the process. This ensures that paths or tasks that may have been overlooked in the forward observation are discovered in the backward observation. The observation begins usually at the finished product. Each previous task is considered and compared with the process model. Special attention is paid to process path mergers. This occurs when a task has multiple possible preceding tasks, resulting in multiple process paths leading to this task. The observed task

is noted together with the number of triggering options, as with forward observation. Subsequently, one of these possibilities is selected, and the observation is conducted backward until the beginning of the process is reached. If additional path mergers occur during this backward observation, they are also re-noted. All mergers should be processed chronologically until all have been traversed. The goal of backward observation is to uncover paths that were overlooked during forward observation. For example, if only three possible paths were identified at a process branch, when there are actually four possible paths, the backward observation might uncover four converged paths. Once all these paths have been traversed backward, a path that is not included in the current model can be identified and added.

Using Observation for IIoT Processes

Although it is not possible to discover the *data perspective*, observation is suitable for recording IIoT processes. This is because prior observation helps the PD to understand the process and provides initial insights into the process, which the PD can use to develop questions and initial models based on their prior knowledge using other discovery methods, e.g. in an interview. This is shown in Section 7.

Advantages and Disadvantages

The advantages of conducting observations for process discovery include gaining an objective view of the process and obtaining a clear overview of all visible process components. Observation can be carried out within a defined physical space, such as a production facility, without interfering with ongoing operations. It does not require additional resources or costs, and the process flow often becomes quickly apparent to the PD.

However, this approach also has disadvantages. Certain process operations, especially those occurring inside machines, are not visible. Critical aspects like data usage, network traffic, and machine communication remain hidden. Additionally, physical constraints, such as machine placement, can limit the PD's ability to observe all steps. Rarely executed process paths may be missed, leading to incomplete models. Furthermore, measuring waiting times can slow down the process discovery and add to the overall time consumption.

In conclusion, conducting an observation-based process discovery is sensible when the goal is to quickly gain an initial, unbiased understanding of visible process flows without interrupting the process itself. It is particularly effective when the majority of critical activities are externally visible. However, for complex processes with significant hidden operations or data-driven components, observation should be supplemented by document analysis or expert interviews to achieve a complete and accurate process model.

5.3 Interview

5.3.1 Traditional Interview

In the interview-based method, a subject matter expert (process owner) involved in the process is personally interviewed (Dumas et al 2021; Gronau 2017). If multiple process owners are involved in the process, multiple different interviews must be conducted.

Dumas et al (2021) propose two strategies for conducting interviews: *(i)* backward and *(ii)* forward process discovery. In *(i)* the interview starts at the end of the process and works backwards through the process, asking "What happens before?" and continues until the trigger of the process is reached. *(ii)* operates in reverse, discovering data on the process from the beginning to the end state of the process. Furthermore, Dumas et al (2021) recommend choosing between a structured or open interview approach. Structured interviews involve predefined questions and hypotheses that need to be confirmed or corrected. This ensures that specific questions of the PD are answered. However, important information may be overlooked in a structured interview as it may not be included in the predefined questions. Additionally, exceptional cases may remain unaddressed. Open interviews allow the process owner to present important aspects of the process from their perspective, potentially revealing information that would have remained hidden in a structured interview. On the other hand, the process process owner may omit important information, thus keeping it hidden from the PD (Dumas et al 2021).
To conduct process interviews, the Bundesverwaltungsamt (2013) has created a *"Guideline for the Collection of Business Processes"*. To prepare the interview, existing documents should be reviewed and a structure of the process should be prepared based on their information. Subsequently, this information must be verified during the interview.

They provide tips for interpersonal aspects that facilitate conducting interviews. No further guidance on structured interview conduct is provided. Gronau (2017) point out general principles for conducting interviews:

- Interview questions must be formulated and asked precisely.
- The PD must be aware of their role as an interviewer. Their interpersonal skills influence the success of the interview and the relationship with their interviewees.
- The information obtained must be carefully documented.
- The interview questions must be tailored to the expertise of the process owner.

The process model is created from the interview notes or parallel during the interview (Dumas et al 2021).

Overall, conducting interviews requires significant time and resource investment. When multiple process owners are involved in a process, contradictions may arise that the PD must clarify. This requires verifying the correct process flow, leading to increased time investment (Dumas et al 2021). Qualified subject matter process owners familiar with the process details are required. During interviews, subject matter process owners may not be able to perform their regular duties, potentially impacting operations (Krallmann et al 2002).

5.3.2 Guideline for Interviews

One or more interviews can be conducted for the interview-based discovery. This depends on the complexity and size of the process and the personal preferences of the PD and the process owner. We recommend conducting a separate validation interview after the discovery, which takes place on a separate date, to check the correctness of the model once it has been fully modeled.

Interviews with Multiple Process Owners

If processes are large and complex (especially IIoT-processes) they can be divided into different sections. Each section typically has different process owners. To conduct a process discovery through interviews, the PD should invite all process owners to separate interviews. These interviews can follow or use parts of the guideline described below with each invited participant separately. Once all sections of the process are discovered, the PD must assemble them in the correct sequence. If there are interactions or cross-connections between the interviews or if process owners contradict each other, it is advisable to talk to the process owners involved together to clarify the affected process component.

Preparation through Questionnaire

At the outset, the PD should provide the process owner with a preliminary questionnaire regarding the process. The questionnaire should include questions covering all process perspectives. It is important to use terms in the questionnaire that are familiar to individuals without a background in process modeling. Possible questions for the questionnaire could include:

- What is the main goal or output of the process? What is produced, and what is the outcome of the process?
- Are there specific triggers or conditions starting the process?
- Which individuals, machines and IT systems are involved in the process? (*Resource perspective*)
- What is the flow of the process? Please describe chronologically what happens in the process. (*Functional and control flow perspective*)
- Are supporting software or other tools used to perform tasks? If yes, please name the tasks where such support is provided and describe the type of software, tools, or other aids involved. (*Operational perspective*)
- Are there specific procedures or measures that are executed in case of an error occurrence?
- What happens to unusable or defective parts identified during the process? Are there mechanisms for monitoring and segregating such parts? Please explain these.
- Which sensors are present within the process? Where in the process are these sensors used (at which tasks)? What data do these sensors each capture and produce? Please describe this briefly. (*Data perspective*)
- Where are the captured data sent? Where does data processing take place? (*Data perspective*)

- Which machines within the process are interconnected? How do these machines communicate with each other? What information or data do the machines exchange?
- Is there a data network within the process? If yes, please describe and sketch it briefly. (*Data perspective*)

Based on the answers, the PD can create an initial process model, considering the various perspectives. The questionnaire allows minimizing the duration of the subsequent interview and gives the PD the opportunity to familiarize themselves with the process before the interview. The PD can already prepare more detailed questions for the first interview, considering the following topics:

- Have any uncertainties or contradictions arisen due to the answers from the first questionnaire?
- Is the process model complete or are there paths that do not have a defined end?
- Does the sequence of tasks in the process make sense?

Starting the Interview

We recommend dividing the interview into several parts to allow the PD and the process owner to take breaks. However, it is also possible to conduct only one interview where only parts of the proposed methods are used.
The PD invites the process owner to the interview. Two forms of interview can be conducted: a closed interview with prepared questions that already explicitly address specific content. This is particularly recommended if a questionnaire has been sent out in advance. During the interview, the PD asks the process owner the prepared questions and notes down the answers. Otherwise, in an open interview, the process owner can be explicitly asked to talk about the process on their own initiative using open questions. This gives the process owner the opportunity to address additional comments and ensures that the PD receives information that may not have been explicitly asked for. Examples of conducting interviews using open and closed interviews can be found in Dumas et al (2021). Further literature on conducting interviews is provided by Taherdoost (2022), Turner III (2010), Gubrium et al (2012) and DiCicco-Bloom and Crabtree (2006).

Check Understanding

To check if the PD has understood the answers and process descriptions of the process owner correctly, we recommend carrying out the following step: The PD goes through their notes with the process owner and asks them about each process step, confirming whether the representation and understanding of the process flow are correct to avoid potential errors in modeling. If there are any errors or incompleteness, the process owner correct them. Alternatively, the PD can integrate the information received during the interview into the existing process model and expand it or, if no model is available yet, model it. If a model already exists, the PD goes through the process model with the process owner and explains the modeled steps. Here again, the process owner should point out any errors or incompleteness and make corrections. It is important to note that the PD should never assume that the process owner is familiar with the modeling language. Therefore, the PD should explain each modeled

process step by describing what happens at that point according to the model. If a correction or addition is necessary, the process owner should communicate this verbally. The PD can either note this information and integrate it into the model later or make the changes directly in the model.
After going through the notes or model once, the PD should ask the process owner if there are any additional information or process components that have not been captured yet (e.g. a process branching that triggers another, previously unrecorded path). If such information is available, it should be integrated into the notes or the model. If desired, a pause can be taken between the interviews at this point.
Depending on the duration of the first interview and the extent of the model changes, it may be useful to end the interview at this point and conduct a second part in a separate session. This allows the PD to integrate new insights from their notes into the model without causing unnecessary waiting time for the process owner. Updating the model can take several hours depending on the extent of the notes and the complexity of the process. Additionally, the concentration of the participants decreases after a certain duration.

Detail Contents

In a second interview or as a second step, the process can be detailed and process exceptions identified. It can be assumed that the first model does not have a high level of detail yet and that none of the rarely executed paths have been captured. These details should be worked out in the second interview. This includes identifying subtasks, defining decision rules at relevant branches, integrating sensors at suitable locations in the model for data discovery, documenting the data forwarding and usage at the respective goals, and verifying that all possible process paths are mapped in the model, regardless of their rarity of execution. To discover this information in a structured manner, the PD can question the process owner based on the revised model from the first interview. It is recommended to go through the following questions for each task to capture all necessary information:

- Does the task divide into further subtasks? If yes, into which ones?
- Are data discovered at this point in the process? If yes, which ones, why are they discovered, where are they sent (to which other process task), and where are they stored (at which storage location)?
- Are there additional paths that can follow this task that have not been mapped so far?

The PD may further divide tasks and create multiple tasks or model subprocesses if necessary. Data are attached or referenced as data objects to the respective tasks, and connections are documented. Once all tasks have been traversed, all branches are traversed chronologically, and for each path, it is determined what conditions must be met for the path to be executed, the interview ends. The PD can add the information into the model now. In order to pursue the top-down approach, the interview can also be conducted several times in order to discover the process more and more granularly until the desired level of detail of the process is achieved.

Area Expert

If the process owner (contrary to the assumption) does not have sufficient detailed knowledge of the process to answer the questions and describe the process at a certain point, an area expert must be involved. This person is also familiar with the process but has specific expertise in a particular area. The area expert is called in for a discussion and supports the process owner where they lack detailed knowledge of the process. The area expert is explicitly involved only for this specific section of the process.

Validation

We recommend using a validation interview where the PD and the process owner again go through the extended process model to check for correctness and completeness. The process should traversed chronologically and at each task it is checked whether the task is correct, the associated data is correct, the executing resource is correctly assigned, and the task order is correct. It should be verified whether the tasks before and after are actually executed at this point in the process flow. When the process reaches a branching point, its paths and the conditions required for them are checked. Subsequently, the cooperation between the individual machines and roles is examined, with each connection being verified to ensure it actually exists and connects the correct resources. If the process owner has no corrections and confirms that the model is complete and correct, the process discovery is completed. If errors are found by the process owner, they should be corrected after the interview. The interview can be repeated until the process owner confirms the model as correct and complete. However, the model can also be terminated after the corrections of the validation interview or terminated after a certain number of validation steps. The PD decides when the model and the process discovery are complete.

Advantages and Disadvantages

The advantages of conducting interviews for process discovery include obtaining up-to-date and detailed information directly from the process owner. Interviews allow for immediate clarification of content-related questions and misunderstandings, ensuring that even hidden aspects - not visible through observation or documentation - can be addressed. Additionally, interviews make it possible to inquire about all process paths, data flows, and network interactions, offering extensive opportunities also to gather IIoT-related insights. This method significantly increases the likelihood of developing a complete and accurate process model.
However, interviews also have notable disadvantages. They can be both time- and cost-intensive, disrupting normal process flows as the process owner is occupied and unable to perform their usual tasks. The accuracy of the discovered information heavily depends on the assumption that the process owner is thoroughly familiar with the process or can consult area experts. There is also the risk of receiving incomplete or incorrect information, especially if the process owner unintentionally presents an idealized version of the process rather than its current state, resulting in inaccuracies in the model.
In conclusion, conducting interviews is particularly sensible when in-depth knowledge,

hidden process details, and IIoT-specific information are required, especially in complex systems where neither observation nor documentation alone can capture the full picture. Interviews are most effective when combined with other methods and when process owners are well-informed and able to provide an honest and realistic depiction of the current process.

5.4 Workshop

5.4.1 Traditional Workshop

The workshop-based method is similar to the interview method, but involves several process experts simultaneously (Dumas et al 2021; Jadhav 2011). When selecting participants, it should be considered that small, hierarchically homogeneous groups work more efficiently than large groups or groups with hierarchical heterogeneity. It is not recommended to include executives and their employees in the same workshop (Richerzhagen 2015; Dumas et al 2021). Technical staff that is involved in the process indirectly, for example, through the management of supporting systems (e.g. ERP systems) should also be involved. However, the maximum number of twelve experts in a workshop should not be exceeded (Dumas et al 2021). Jadhav (2011) recommends conducting review workshops, where subject matter experts must approve the modeled process afterwards to ensure that the process is consistent and correct. Dumas et al (2021) suggest that a moderator moderate the workshop and should coordinate the contributions of the participants and equally involve the process experts in the workshop. Involving a moderator allows the process discoverer to design a model during the workshop.
In addition, a process analyst can be included as a third person to note relevant statements made by the participants, which may need to be followed up on later that no interruptions of the discussion for questions is needed. This approach is particularly suitable for complex processes involving many experts (Dumas et al 2021). If there are different opinions within the group regarding the content or presentation of the process, it is the moderator's task to steer the group discussion that ultimately the correct process can be identified (Bundesverwaltungsamt 2013).

Since a detailed model cannot be created in one session due to complexity, multiple sessions are required (Dumas et al 2021). The first session is used to establish the context, communicate the workshop's goals, and identify the participants' expectations (Jadhav 2011; Dumas et al 2021). In addition, the scope of the organisation to be considered must be defined, whereby the use of process maps, if available, is appropriate (Richerzhagen 2015).

5.4.2 Guideline for Workshops

A process discovery through workshops should involves the preparation and at least one or more workshops. The workshop-based discovery can be carried out in one or in several workshops. The PD can incorporate the information into the process model between the workshops. Otherwise, the model can be created in parallel to the workshop or afterwards. For the workshop, we also recommend analyzing the

individual perspectives and pursuing a top-down approach. For tips on moderation and interaction within a workshop, see the literature by Lauttamäki (2014), Linds and Gee (2023), Pavelin et al (2014), Jolles (2017) and Storvang et al (2018).

Preparation

To conduct a process discovery through a workshop, the PD has the opportunity to decide whether to moderate the workshop and gather information simultaneously or delegate one of these tasks to another person. Additionally, as suggested by Dumas et al (2021), an analyst may be involved. The planning of the workshop begins with the selection of relevant participants. The PD needs to determine which participants have a detailed understanding of the process. It is important to ensure that at least one participant from each process area attends the workshop to ensure that the entire process is adequately represented by different participants. Participants can include employees who perform direct tasks in the process, as well as those who are indirectly involved in the process, i.e. machine operators or developers of the programs executed in the machines. The PD schedules the dates for the workshop and invites the selected participants, taking care to find dates when all invited participants are available. For the execution of the workshops, it is advisable to follow the suggested approach of Camunda BPM by Richerzhagen (2015).

Starting the Workshop

At the beginning, the PD should introduce the process being elicited and briefly explain the planned approach for the discovery. Then, all participants should introduce themselves and explain their involvement in the process by describing their roles and providing rough descriptions of their tasks.

Set up a Process Profile

We recommend starting the workshop by creating a process profile to get a overview of the process. To do this, the participants are asked to list the roles involved in the process (*resource perspective*) and jointly describe a rough process flow (*control flow perspective*). When describing the rough process flow, the participant responsible for each area should explain what happens in that section of the process. The moderator should ensure that all participants contribute equally to the discussion and asks targeted questions. The PD records the information gathered and may directly capture it as a model, while the analyst takes note of additional information that may require further investigation through follow-up questions.
Once all necessary information has been gathered, the analyst can raise any follow-up questions. These questions should be answered by the participants, allowing the PD to directly capture the information. Then, the PD presents their findings and shares their understanding of the process flow, the roles involved and process outcomes with the participants. Participants are encouraged to make any necessary corrections and provide additional comments. This discussion is also guided by the moderator. This part of the workshop is the ideal place to take a break that the PD then can document the results in the form of a process model.

Working in Groups

Depending on the group size, the process discovery can be done collectively with the moderator in the entire group or, for a large number of participants, in separate groups working independently. Working in small groups is advisable if the moderator deems the overall group to be too large. When working in small groups, the process should be divided into several sections, with each small group assigned a specific section of the process. Each small group should include participants who hold roles in that section of the process. If a role appears in multiple sections of the process, the participant is assigned to the section they consider to be the most complex or the group work is not carried out at the same time to allow the participant to be present in both groups. Once the work in the small groups is completed, they present their results. This is done in the order of the process flow. After all small groups have presented their results, further additions and corrections are discussed in the entire group. Participants, who were required in several stages of the process, were asked to contribute to this discussion. The PD notes the comments for each section. If the workshop is conducted with all participants simultaneously, the work is similar to that in small groups.

Discovering Tasks, Tools and Data

We recommend to focus on the *functional*, *operational* and *data perspectives* after discovering the process profile. The PD should present the current process model if this is already existing. Subsequently, the refinement of the process and the identification of operational support are carried out.

The hole group or each small group discusses, based on the current process model or information, the refinements needed in each task and whether all tasks for each role in that section are mentioned (*functional perspective*). The additions and refinements should be documented in writing.

For each task, the software and other support tools used should be noted chronologically (*operational perspective*).

A list can be created that enumerates all data generated or used during the process to focus the *data perspective*. It is then recorded for each data record which task generated it, what type of information it contains and where it is used in the process. If the data originates from another process or is sent to another process, this must also be documented. Together with the participants, the PD then assigns the respective data to the producing and consuming tasks, thus establishing the connections between the machines. Finally, the storage location for all data objects (usually the respective database) is determined and noted. The process steps could be detailed and refined, and the support tools used are added. Subsequently, the PD should integrate the new information into the process model. The PD can directly represent this in the modeling tool and make the process model visible to all participants, for example, by using a canvas projection. The order and level of detail in which the various perspectives are recorded can be customised.

The moderator has to ensure that each discussion is continued until the participants agree on the correctness of the discussion component. It is important to ensure that participants are not persuaded to make a statement or agree due to hierarchy, as this

could jeopardize the correctness of the process. Higher-ranking employees should not have decisive authority.

Complete Workflow

To complete the model all decision nodes in the model should be reviewed. This can be done during the creation of the process profile, separately at the end of the workshop or in a separate workshop. When this discovery should take place can be made dependent on the size and complexity of the process and the number of decision nodes. At each decision node, discussions are held regarding the conditions triggering the paths, and the triggering data values are noted. Once all decision nodes have been examined, the analyst asks questions about the recorded information. Once these questions are answered, the workshop is concluded, and the PD can finalize the process model.

Validation

In the final workshop, the PD presents the completed model and explains the entire process flow to the participants. If all participants agree with the presented process model, the workshop, and thus the process discovery, is considered complete. If there are any improvements, corrections, or additions, these are noted and added into the model. The final workshop can be repeated until all participants agree with the process model or, as with the interview, can be terminated after a certain number of runs or other cancellation criteria.

Advantages and Disadvantages

Workshops offer several advantages for process discovery. They enable the involvement of multiple individuals at once, allowing for the immediate resolution of contradictions and examination of the process from various expert perspectives. This collaborative environment ensures a more complete understanding of semi-automated related information, data flows, and machine connectivity. As a result, workshops significantly increase the likelihood of developing an accurate and comprehensive process model compared to relying on the input of a single process owner.
However, workshops also come with some disadvantages. They are resource-intensive, requiring participants to step away from their regular duties, leading to higher personnel costs. Scheduling becomes more complex and time-consuming as the number of participants grows, and process disruptions may occur during the workshop. Additionally, there's always the risk that certain technical aspects remain unclear if no participant has complete knowledge of those areas.
In conclusion, conducting a workshop is particularly sensible for complex processes that span multiple areas and require input from various specialists. They are most effective when comprehensive knowledge from different domains is essential, and when the effort and cost of organizing the workshop are justified by the need for accuracy and completeness in modeling the process.

6 Combination Opportunity Example

As mentioned in Section 5, it is possible to combine the components of the guidelines with each other as required. This makes it possible to avoid the disadvantages of the individual methods or to give them less weight. In this Section, we present a possible combination and explain the reasons and objectives of such a combination. By combining the methods, we focus to create a comprehensive, accurate and verifiable model that could also contain all IIoT-relevant information. We want to ensure that the time and cost investment are kept to a minimum without compromising the completeness, accuracy, and verifiability of the process model.
This combined method example starts with observing the process. This is followed by a brief document analysis and an interview. Subsequently, another interview and a workshop are conducted for validation purposes, as shown in Figure 3.
The observation is intended to provide the PD with an initial insight into the process

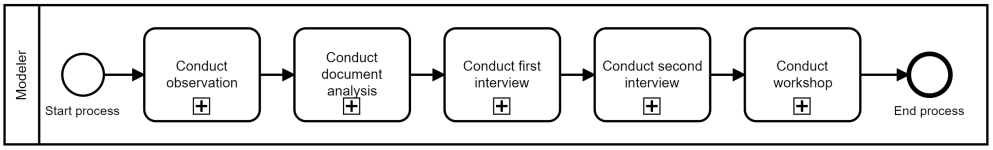


Fig. 3 Combination of the individual methods into one process discovery.

and allows for the design of a rough model containing the involved resources and their visibly executed activities. Through observation, aspects of the *resource*, *control flow*, and *functional perspectives* are partially covered. To conduct the observation, the PD follows the instructions outlined in Section 5.2.2 and pass through the process, noting the sequence of performed tasks and the corresponding executing resources. Process branches are handled as explained. The result of the observation is an initial process model where the resources are modeled as lanes and their executed tasks are modeled as tasks in the correct sequence.
Next, the PD proceeds to document analysis and reviews the existing documents for the following information in the given sequence:

1. Additional tasks and paths that were not captured during observation. (Completion of the *control flow* and *functional perspective*.)
2. Software used and supporting tools related to each task. (Discovering the *operational perspective*.)
3. Produced and used data related to each task. (Discovering the *data perspective*.)
4. Connections between the involved machines. (Discovering the *connectivity*.)

To obtain this information, the PD iterates through the documents multiple times. In the first iteration, the focus is on the *control flow* and *functional perspective*. In the second iteration, the *operational* and *data perspectives* are captured. In the third iteration, information about *machine connectivity* is gathered. Subsequently, the PD also notes any uncertainties and questions arising from the existing model. For the document analysis, the PD should refer to Section 5.1.2. If the PD finds contradictory

information in the documents compared to what was discovered during the observation, this information from the documents should be ignored as its accuracy is not guaranteed, unlike the observation. Upon completion of the document analysis, the PD already possesses a comprehensive and detailed process model. The correctness of the model has been partially ensured through observation. So far, only costs and time commitments for the PD have been incurred.
In the third step, the process owner is invited to an initial interview session. As mentioned in Section 5.3.2, it may be necessary to interview multiple process owners. The following formulations refer to a single process owner, but can also be optionally conducted with multiple process owners for different process areas. A detailed questionnaire is not sent in advance to avoid further increasing the time commitments of the process owner. Instead, the process owner is simply informed about the process that will be discovered and provided with the questions that the PD has noted for preparation. In the interview, the PD proceeds according to the instructions in Section 5.3.2. The PD asks the previously noted questions and records the answers from the process owner. The process owner then has the opportunity to contribute additional relevant aspects. Afterwards, the PD presents the current process model. The modeled process is then worked through chronologically, and the following questions are clarified for each task:

- Does the task break down into further sub-tasks? If yes, in which ones?
- Are data discovered at this point in the process? If yes, what data is discovered, where is it sent (to which other process task), and where is it stored (at which storage location)?
- Are data used at this point in the process? If yes, what are these data used for, where were they previously discovered (at which process task), and where are they stored (at which storage location)?
- Are the tools used correctly assigned? Are tools missing from the task?
- Are there any additional paths that can occur after this task that have not been depicted so far?

If questions cannot be answered or only partially answered, area experts can also be consulted here. Once the process has been walked through, the first interview ends. The PD processes all the information obtained during the interview and incorporates it into the model.
In the fourth process step, the process is validated through another interview with the process owner. In the second interview, the entire process is presented to the process owner again. If the process owner has no comments, the interview and the first validation unit are completed. However, if the process owner still has suggestions for improvements and corrections, the PD incorporates these into the model during the meeting. This avoids the need for further interview sessions with the process owner. The interview ends once the process owner perceives the model as complete and correct. Completeness and correctness also refer to the capturing of data and machine connectivity.
The second validation unit comprises a workshop with the relevant process participants. As outlined in Section 5.4.2, several relevant process participants are identified and invited to the workshop. In this workshop, the process model previously created

with the process owner's assistance is reviewed. The workshop follows the structure of the last workshop presented in Section 5.4.2. This is to ensure that all parties involved agree on the completeness and correctness of the model, including data collection and connectivity. Upon completion of this workshop, there should be a process model that is highly likely to be correct and complete. Figure 4 shows the combined process discovery guideline in BPMN.

7 Use Cases: Discover IIoT-Processes by Combining the Guidelines

This Section presents the case studies conducted. The guidelines we proposed were applied in two independent case studies. Both case studies are described in detail below and are part of the evaluation in Section 8.

7.1 Use Case: Automotive Industry

In the first use case, we analyzed a manufacturing IIoT process from the automotive industry by ourselves combining parts of our guideline. The application took place as part of the evaluation in order to possibly initiate a further phase in the DSR cycle. The name of the company remains anonymous for competitive reasons. The process model created can only be published in black. The production involves the manufacture of a component for automobiles and is therefore a production process where several machines and human actors are involved. The component produced is made up of 27 individual components, which are assembled in six higher-level, sequential process steps (bending, welding, assembly, moulding, testing, packaging).
The process discovery was started with a document analysis. This was followed by several interviews and subsequent observation combined with a workshop for validation purposes.

Document Analysis - Preparation
: The process discovery began with document analyzes, as these were only available to a limited extent. The PD used the document analysis guideline to gain an initial insight into the process and defined questions for the interview based on the documents. The questions followed a top-down approach and were initially kept generic without going into process details in depth. The questions could therefore be taken from the suggestions for the questionnaire prior to conducting interviews.

Interview - discover resources, tasks and work flow
: In a first, closed interview, the process owner enquired about the resources involved, their tasks and the process flow. The PD explained his understanding of the process and noted the corrections made by the process owner. After the interview, the PD then modeled an initial model based on the information provided. The PD noted open questions and ambiguities that arose during the modeling.

Interview - discover data and tools
: The PD discussed the questions in a second interview with the process owner using the previous model. Once the questions had been clarified, the tools and data used in the process were discovered. It turned out that the connectivity and

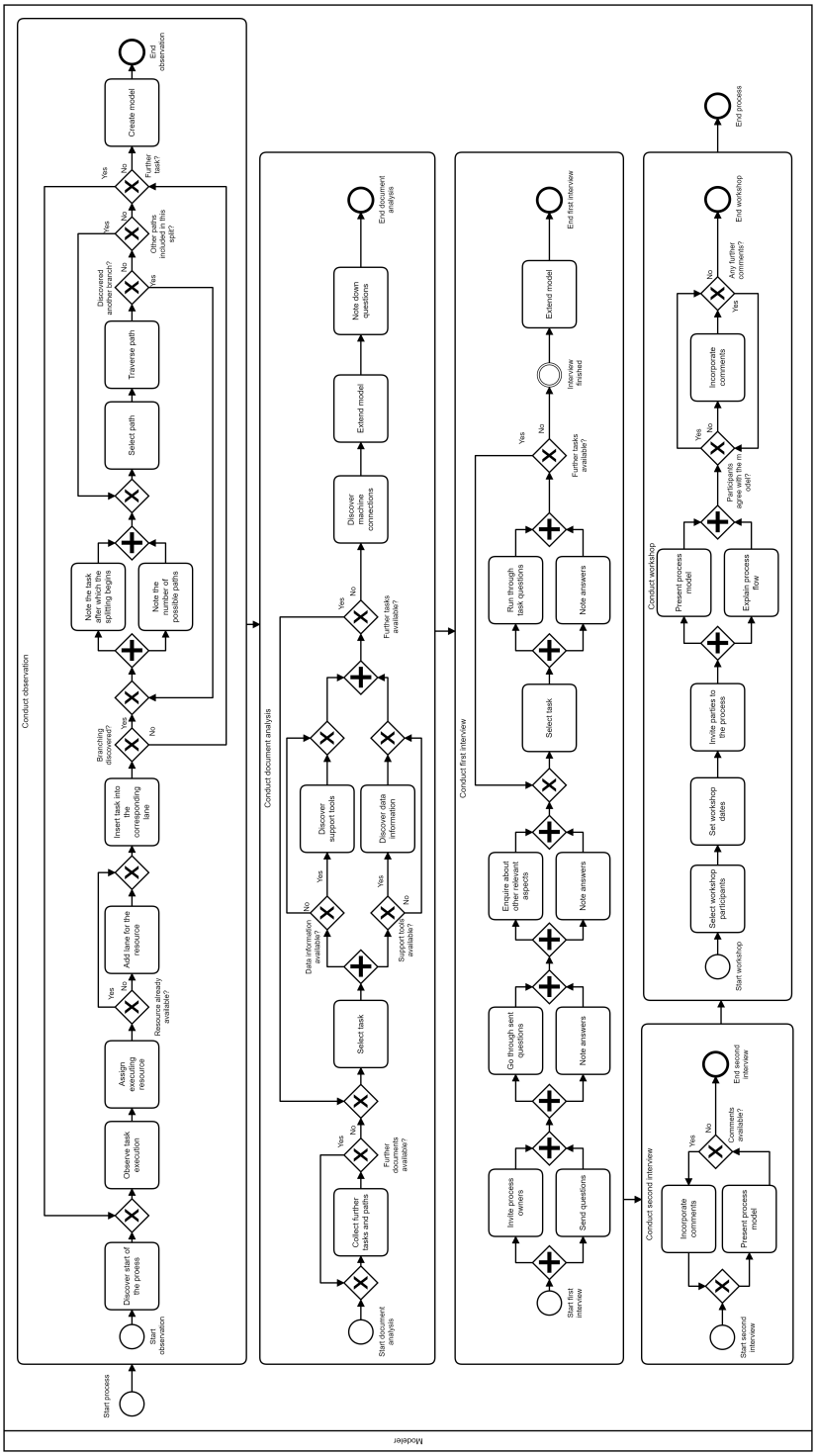


Fig. 4 Combined process discovery guideline, presented in BPMN.

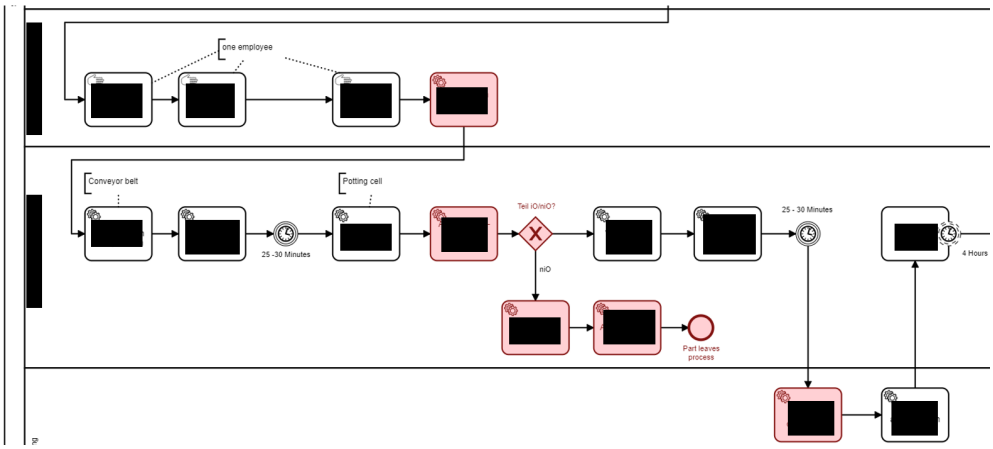


Fig. 5 Red tasks were detected during validation.

data connection could not be explained by any of the process participants, who were consulted as area experts. The process owner was then asked in an open interview whether there were any other process components that had not been addressed yet. The information from the second interview was then integrated into the model by the PD.

Interview - Validation

The third and final interview was used for process validation. The PD discussed the model with the process owner task by task and was assured that the sequence, tasks, tools, data and resources were correct and complete. The process owner's comments and corrections were incorporated directly into the model during the interview.

Observation and Workshop - Validation

For validation, the PD then observed the process on site. This was combined with a workshop in which the PD had employees explain to him exactly what took place in the individual process steps observed. He compared this with the model in parallel. Observation of the process on site showed that the results of the interviews already corresponded almost completely to the actual process flow. The chronological order was completely consistent. All process steps in the interview could be seen in the observation. There were no errors in content (e.g. incorrectly described tasks). The process steps that could not be recorded using the interview amount to a small number of five tasks in relation to the overall size of the model. Only three of these tasks were relevant to the process.

The resulting model can be seen redacted in Figure A1 in the Appendix. The inserted tasks after validation are also shown in Figure 5. The model created does not contain any gaps or incomplete paths. Based on the validation, it can be assumed that the model is correct and complete. The granularity of the process could be deepened. Figure A2 in the appendix shows the process model of the autostore process after the observation.

Task	Number of triggers	Associated resource	Associated tools	Previous task	Subsequent task	Modelling status
01 - Start Commissioning	1	R04	Order list		02	x
02 - Accept order	1	R04	Label	01	03	x
03 - Robot starts	1	R01, R02		02	04a/04b	x

Table 2 Table to handle process observation informations.

7.2 Use Case: Warehouse Management

In a second use case, the *autostore warehouse management* process was discovered at SOMIC, a company specializing in the manufacturing of packaging machines. The process includes warehouse management using mobile robots that take required components from the stored boxes according to a production needs and transport them to the output portal. The robots travel on an aluminium construction that serves as rails to remove the individual bins from their container stacks as required.
The guidelines were handed out to three novices with no prior knowledge of process discovery. They discovered the process together using the following procedure:

Preparation

The preparation began with contacting the company and making an appointment for the observation and an interview. In addition, process documents for the document analysis and employees for the workshop were requested. The questionnaire for the interview was already sent along. As no process documents were available and due to a lack of time, the document analysis and workshop were not carried out.

Observation

The observation was carried out independently of other discovery methods. For this purpose, each process step was observed individually in the forward observation and recorded in tabular form, as can be seen in Table Table 2. As a result, all perspectives were discovered during the observation of a task. The modeling was carried out simultaneously. Subsequently, a backward observation was carried out in which the observed tasks were compared with the model.

Interview

To conduct the interview, a questionnaire was sent to the process owner in advance, but this could not be completed due to a lack of time. The questionnaire was therefore discussed in the first interview, in which the resources, tasks, control flow, data and tools were inquired about. At the same time, an initial model was created. In the second interview, details were provided and queries clarified. The model created, which was discovered independently of the previous observation, can be seen in the appendix in Figure A3. Finally, the model was sent to the process owner by email for validation.

Combination

Finally, the findings from the observation and the interview were combined. The result was that new tasks and a resource could be added to the observation. Overall, this resulted in a more detailed model, which can be seen in Figure A4 in the appendix.

The model created does not contain any gaps or incomplete paths. Due to the subsequent merging, it can be assumed that the model is correct and almost complete. The granularity of the process could be deepened. The IIoT perspective was clarified via the integrated database, which is linked to the respective tasks. The aim is to organize a workshop to possibly complete the model.

8 Evaluation

To evaluate the design artifact, our developed guidelines, we conducted a comprehensive, multi-stage evaluation process based on the evaluation dimensions proposed by Prat et al (2015), focusing on different criteria as depicted by Table 3.

8.1 Initial Perception Study

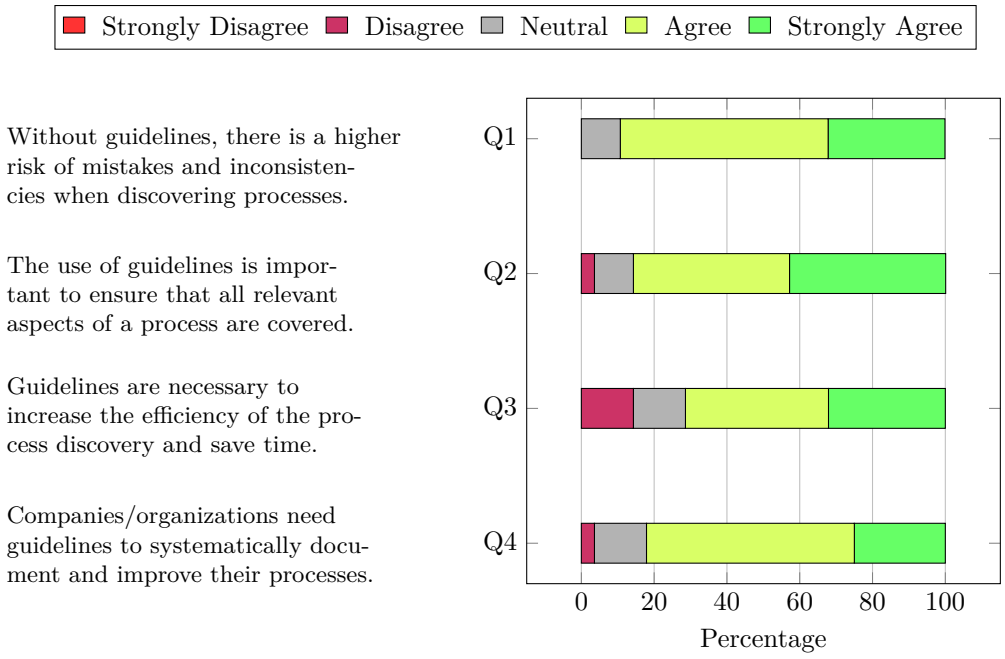


Fig. 6 Questions and percentages of the necessity.

As a first step, we assessed the general perception and acceptance of manual process discovery guidelines through a survey involving 28 participants from both academia and industry. The questionnaire was developed based on the evaluation dimensions proposed by Prat et al (2015) and designed following established usability assessment approaches (Laugwitz et al 2008). Participants covered a wide range of experience levels, with more than 70% having previously conducted process discovery activities.

Evaluation Phase	Method	Focus Areas	Learnings	Improvements Made
Perception Study (Pre-study)	Survey with 28 participants (academia + industry)	Necessity, usefulness, expected outcomes, support potential (H1–H3)	High acceptance across experience levels; clear perceived benefits of guidelines; demand for standardization	Confirmation of relevance and user interest; used as foundation for artifact design
Round 1: Expert Feedback	Expert interviews and follow-up survey	Completeness, clarity, usefulness, necessity, modularity	Generalizability beyond IIoT, need for examples, preference for flexible toolkit structure	Example questions added; structure reframed to allow modular use
First Use Case	Application in IIoT project at automotive supplier	Practical applicability of methods; real-world relevance	Observation helpful for control flow; interview better for tools; method mix needed; practical method guidance missing	Added method-specific suggestions; emphasized mixed-method flexibility
Focus Group 1 (Theoretical)	Discussion with researchers with process discovery background	Interpretation, target groups, guideline applicability	Guidelines must work for novices and experts; include support materials (e.g., checklists); discuss integration of automated techniques	Added support tools; opened future extension path (e.g., process mining); clarified audience focus
Focus Group 2 (Practical)	Industry experts with hands-on experience	Practical structure, completeness, real-world usability	Need for compact structure; standard procedure lacking in SMEs; role of psychological factors in interviews/workshops	Added guidance on scope, process context, psychological aspects; promoted top-down approach
Round 2: Expert Field Test	Modeling of IIoT line by experienced analyst	Guideline structure, real-world usability, process logic	traditional process perspective structure not practical	Reorganized structure into intuitive process phases (e.g., Workshop Start, Group Work, etc.)
Second Use Case	Application in new IIoT context	Practical challenges in multi-method discovery, black box effects	Observation timing crucial; live modeling > survey validation; black-box processes challenge completeness	Added recommendations for kickoff, stakeholder involvement, method sequencing and validation techniques
Round 3: Novice vs. Expert	Novices and expert model same industrial process; validated by company experts	Usability across skill levels, result comparability, output quality	Novices achieved similar structure and completeness; expert added detail; wording differed due to vocabulary	Validated applicability for different user levels; confirmed expert knowledge adds value, not dependency

Table 3 Overview of evaluation activities, learnings, and improvements aligned with Prat et al (2015).

The results clearly highlighted the perceived relevance and value of such guidelines: Over 85% of participants agreed or strongly agreed that guidelines are necessary to ensure completeness, avoid errors, and increase efficiency in process discovery. In addition, 96% of participants indicated that they would use such guidelines if available, independently of their background or prior experience, thereby confirming hypothesis

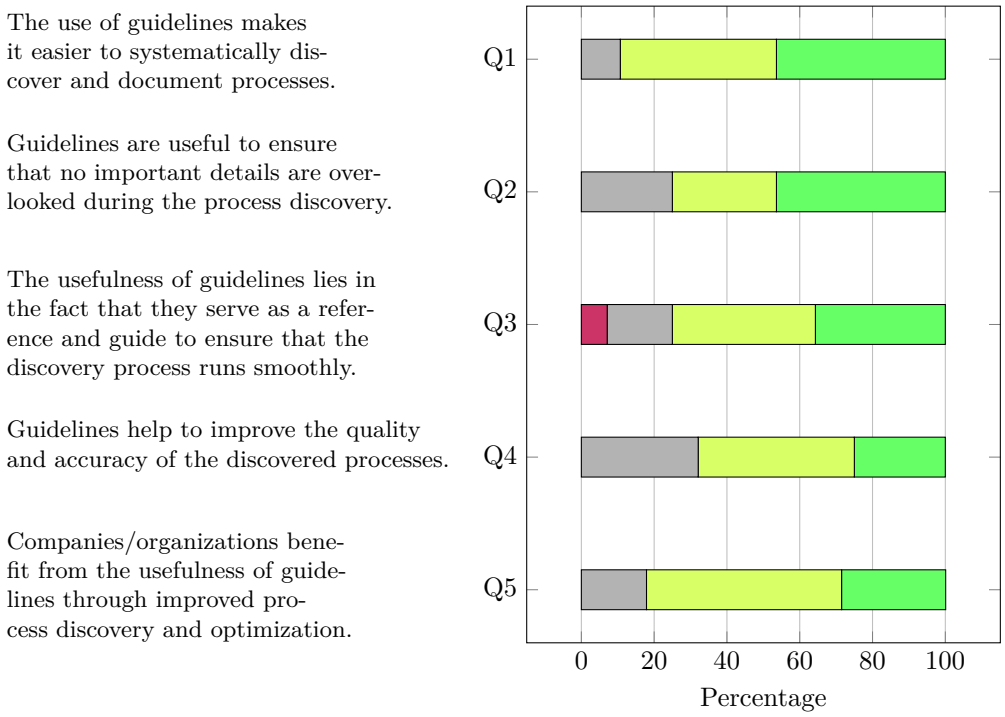


Fig. 7 Questions and percentages of the usefulness.

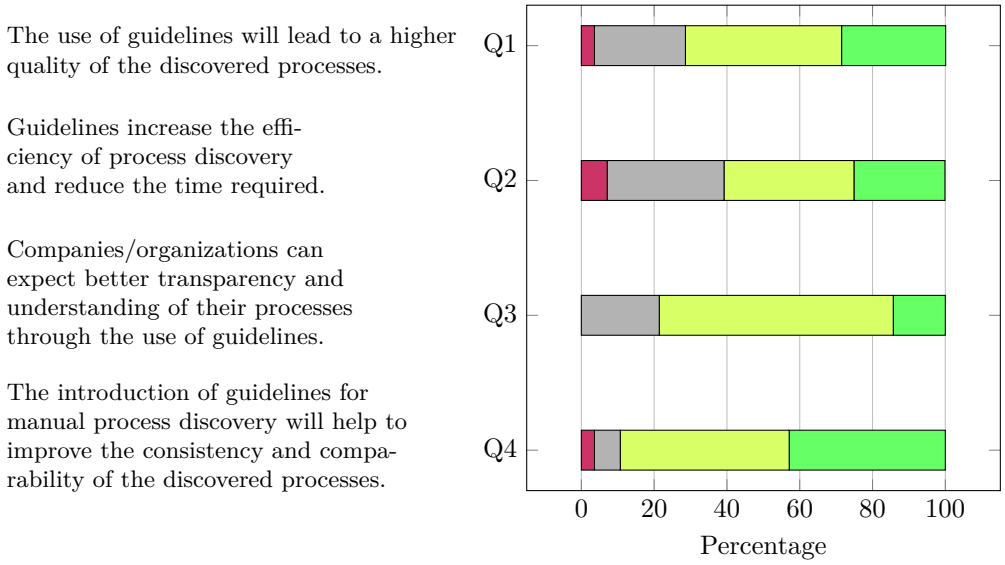


Fig. 8 Questions and percentages of the expected result.

The provision of guidelines helps employees to learn process discovery more quickly and carry it out more quickly and carry it out more effectively.

The introduction of guidelines can help to ensure a uniform approach to process discovery in the organization.

The leadership team should actively support the use of guidelines for manual process discovery and promote their implementation.

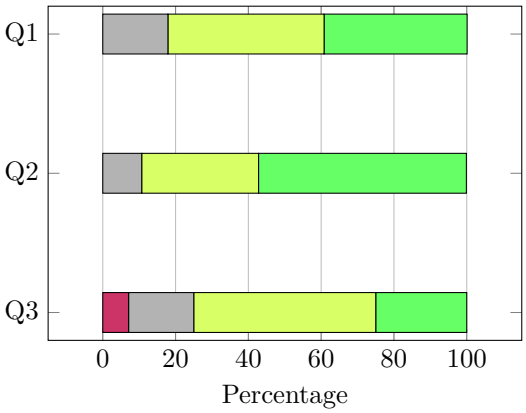


Fig. 9 Questions and percentages of the supporting potential.

H1. The consistently high agreement with statements related to error prevention, discovery completeness, and efficiency also confirmed hypotheses **H2** and **H3**.

Taken together, these results demonstrated a strong demand for structured support during process discovery and provided a robust foundation for the development of our guideline artifact. More importantly, they justified the need for further iterative evaluation rounds to refine the design and validate its practical applicability and effectiveness. A detailed breakdown of the results can be found in Figures 6 to 9.

8.2 Round 1 – Expert Feedback

In the first artifact evaluation round, we conducted expert interviews and a follow-up survey. The focus was on completeness, clarity, necessity, and usability. Experts emphasized the potential generalizability of the approach beyond IIoT, an encouraging signal, though we maintained our focus on this domain for now. The need for example questions and flexible, modular use was raised. Based on this, we integrated illustrative prompts and reframed the guideline as a toolkit rather than a rigid step-by-step manual.

8.3 First Use Case Study

Subsequently, the guideline was applied in a real-world IIoT scenario at an automotive supplier (Section 7.1). While the guideline supported the modeling task, open questions remained regarding the choice of discovery methods. This highlighted the need for a more precise description of method use. Additionally, observation, previously underemphasized, proved useful, especially for identifying where IIoT data (e.g., scan points) is captured. A key insight was that combining observation with interviews improved completeness: control flow was better captured through observation, while tool usage was best clarified via interviews. These findings led to the integration of method-specific recommendations into the guideline.

8.4 Focus Group Feedback (Theoretical and Practical Perspectives)

The adapted guidelines were discussed in two consecutive focus groups:

- **Focus Group 1 (Theoretical Perspective)**: Involved researchers and academics with background in process discovery. Emphasis was placed on flexible applicability across levels of expertise. Support tools (e.g., checklists, questions, literature) were requested. The person-centered discovery approach was discussed critically and suggestions were made to include automated methods (e.g., process mining) in future versions.
- **Focus Group 2 (Practical Perspective)**: Comprised industry professionals with hands-on experience in process discovery. Experts confirmed the relevance of structured discovery guidelines, especially for SMEs. Key feedback included the need for a compact and clear structure, a top-down modeling approach, early clarification of scope and objectives, and reference to psychological aspects in interviews and observations. These insights resulted in several structural and content-based improvements.

8.5 Round 2 – Field Test with Expert

An experienced process analyst used the revised guideline to document an IIoT production process. This round revealed that the previously used structure, based on traditional process perspectives such as control flow, data, organization, and resources (following Jablonski and Götz (2007)), was not practical in real world settings.

As a result, the entire structure of the guidelines was reworked. Instead of organizing content strictly by process perspectives, the revised version follows a more intuitive, phase-based structure reflecting the practical flow of a process discovery project. For example, for Section 5.4.2, these new sections include *Starting the Workshop*, *Setting up a Process Profile* and *Working in Groups*. Corresponding changes to follow a real-world process discovery procedure have been applied consistently to all guideline types. This holistic restructuring improved usability and made the guidelines more accessible in real-world scenarios across all methods.

8.6 Second Use Case

A second industrial application (Section 7.2) confirmed and extended previous learnings. It became evident that:

- A pre-defined observation schedule improves observation quality.
- Validation of the completeness of IIoT models is difficult without cross-method triangulation.
- Some process parts (e.g., operated by external providers) remain black boxes, necessitating questions about participant expertise early on.
- Live modeling during validation yields richer feedback than surveys.
- Method combinations improve quality but increase effort, highlighting the importance of a thoughtfully defined method sequence.

These insights were integrated into the guideline, particularly in the form of new sections addressing method selection, sequencing, and stakeholder coordination.

8.7 Round 3 – Novice and Expert Comparison

In the final evaluation round, novice and expert users modeled the same industrial process using the updated guideline. The results showed that novices could produce models comparable in completeness and structure to those of the expert. Differences were primarily found in wording and level of detail, reflecting varying process vocabulary and experience levels. Importantly, all models were validated by process owners and found to be accurate and useful. This confirmed the guideline's usability across experience levels and highlighted that domain knowledge enhances result granularity.

8.8 Conclusion of Evaluation

The evaluation process was iterative, rigorous, and incorporated both theoretical and practical feedback. Each stage contributed to improving the artifact, as detailed in Table 3, resulting in guidelines that are flexible, useful, and also applicable in real-world IIoT settings, and that lay the foundation for future generalization beyond this domain.

9 Conclusion

This study set out to determine how organizations can capture business processes systematically and reproducibly when they rely on established manual process discovery techniques such as interviews, workshops, or document analysis. Although these techniques are commonplace in both research and practice, the academic literature provides no operational guidelines that specify how they should be executed step by step.

Summary of key findings.

A survey of 28 participants from academia and industry shows that over 80% believe that clear guidelines lead to higher-quality process models, and all respondents agree that guidelines improve overall manual process discovery outcomes. Controlled experiments with novice and expert modelers corroborate this perception: when both groups applied our guideline, they produced highly similar models whose differences were limited to naming conventions and minor structural details. We also observed that several companies already use informal, in-house guidelines, whereas an equivalent artifact has been missing in the scholarly domain.

Theoretical contribution.

By publishing a domain-independent, step-by-step guideline for manual process discovery, we close the gap between scattered practitioner know-how and the lack of a consolidated methodological reference in research. The guideline bridges theory and practice by *(i)* codifying tacit practitioner knowledge, *(ii)* aligning it with established modeling principles, and *(iii)* validating it in two real-world use cases from IIoT. While IIoT provided a demanding validation context, the guideline itself is not limited to this domain.

Practical implications.

For organizations, the guideline offers a ready-to-use playbook that can be embedded in quality-management or digital-transformation initiatives. Standardizing interviews, workshops, and document analysis enables teams to reduce discovery effort, obtain more complete process views, and establish a shared vocabulary across departments, all prerequisites for automation, compliance auditing, and continuous improvement.

Limitations and future research.

Despite these strengths, we cannot guarantee exhaustive coverage of every component, especially in highly automated and poorly documented environments. Future work should therefore *(i)* combine the guideline with process-mining techniques to discover machine-generated event traces automatically, and *(ii)* employ NLP and computer-vision tools to accelerate document and observation analysis (Hornsteiner et al 2024; Fichtner et al 2020; Ackermann et al 2021; Neuberger et al 2023). Evaluating the guideline in additional domains (e.g., healthcare or logistics) and across different process maturities also remains an open avenue.

Take-away.

By formalizing and empirically validating a practical guideline for manual process discovery, this study delivers a missing methodological link between academic research and industrial practice, enabling both communities to capture complex processes faster, more consistently, and with demonstrably higher quality.

Appendix A Extended Data

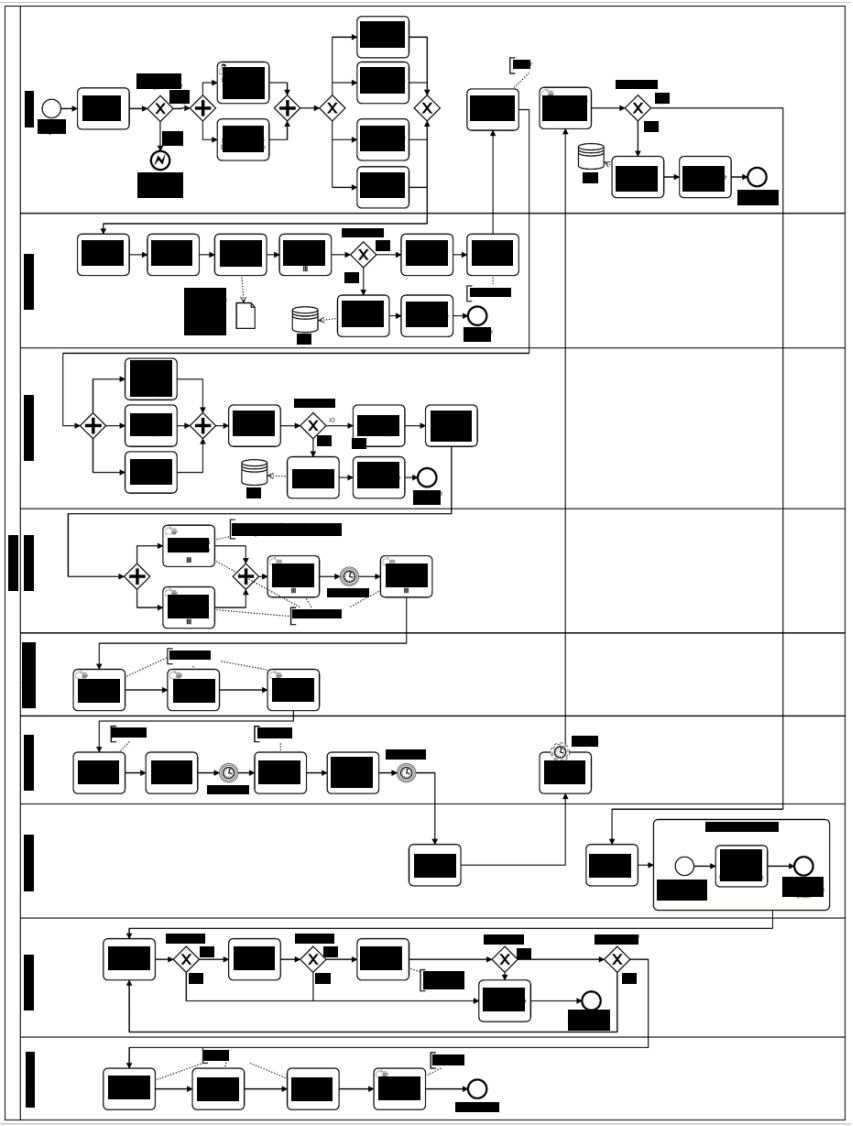


Fig. A1 Blackened industrial process for the manufacture of engine components.

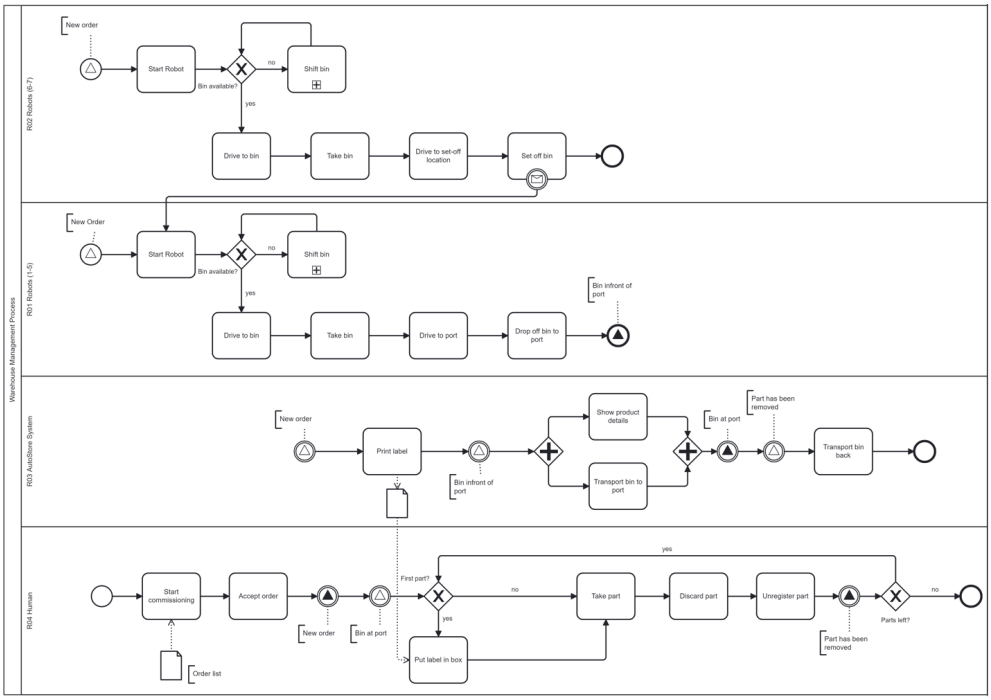


Fig. A2 Model of the autostore process at Somic after observation.

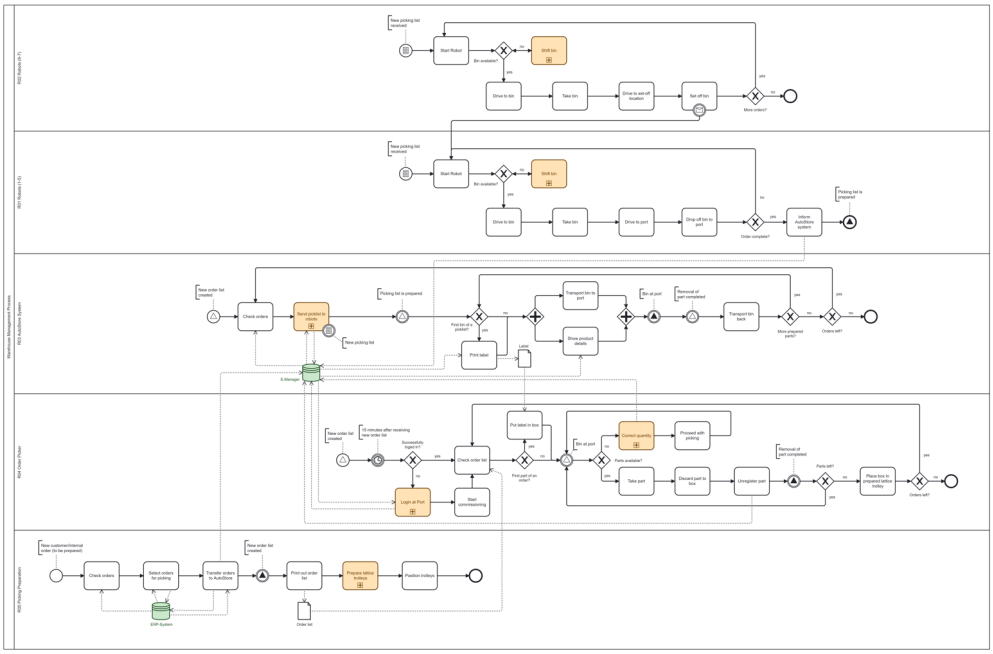


Fig. A3 Model of the autostore process at Somic after interview.

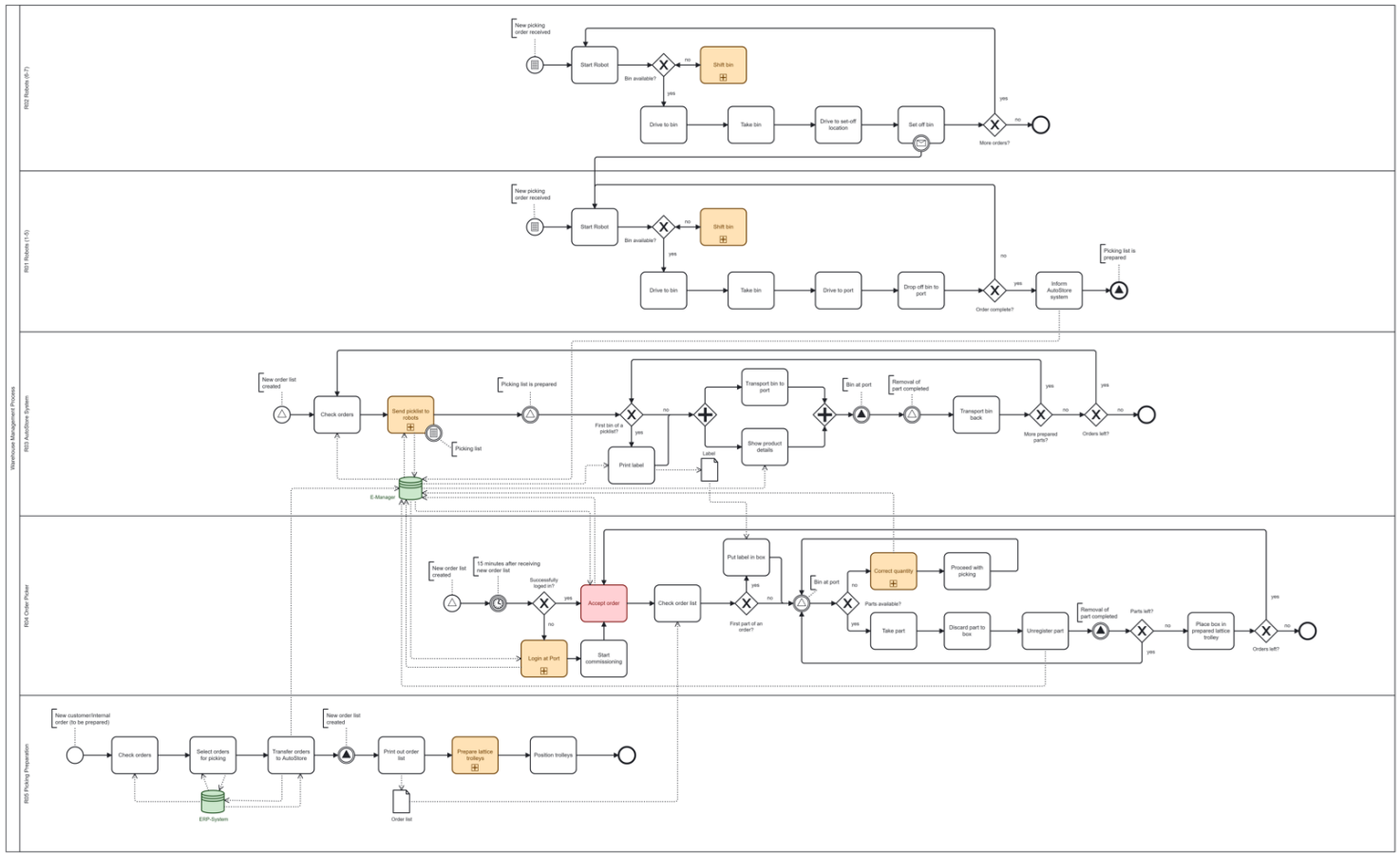


Fig. A4 Model of the autostore process at Somic after combining observation and interview.

References

van der Aalst WMP (2016) Process Mining - Data Science in Action, Second Edition. Springer, https://doi.org/10.1007/978-3-662-49851-4

Ackermann L, Neuberger J, Jablonski S (2021) Data-driven annotation of textual process descriptions based on formal meaning representations. In: Advanced Information Systems Engineering - 33rd International Conference, CAiSE 2021, Melbourne, VIC, Australia, June 28 - July 2, 2021, Proceedings, Lecture Notes in Computer Science, vol 12751. Springer, pp 75–90, https://doi.org/10.1007/978-3-030-79382-1_5

Ackermann L, Käppel M, Marcus L, et al (2024) Recent advances in data-driven business process management. URL https://arxiv.org/abs/2406.01786, 2406.01786

Awadid A (2017) Supporting the consistency in multi-perspective business process modeling: A mapping approach. In: 11th International Conference on Research Challenges in Information Science, RCIS 2017, Brighton, United Kingdom, May 10-12, 2017. IEEE, pp 414–419, https://doi.org/10.1109/RCIS.2017.7956568

Bazan P, Estevez E (2022) Industry 4.0 and business process management: state of the art and new challenges. Bus Process Manag J 28(1):62–80. https://doi.org/10.1108/BPMJ-04-2020-0163

Becker J, Kugeler M, Rosemann M (2012) Prozessmanagement: Ein Leitfaden zur Prozessorientierten Organisationsgestaltung, 7th edn. Springer Verlag, Berlin, Heidelberg, https://doi.org/10.1007/978-3-642-33844-1

Bernardo R, Galina SVR, de Pádua SID (2017) The BPM lifecycle: How to incorporate a view external to the organization through dynamic capability. Bus Process Manag J 23(1):155–175. https://doi.org/10.1108/BPMJ-12-2015-0175

Boyes H, Hallaq B, Cunningham J, et al (2018) The industrial internet of things (iiot): An analysis framework. Comput Ind 101:1–12. https://doi.org/10.1016/J.COMPIND.2018.04.015

Bundesverwaltungsamt (2013) Leitfaden für die erhebung von geschäftsprozessen im bundesministerium des innern und seinen nachgeordneten behörden. URL https://www.bva.bund.de/SharedDocs/Downloads/DE/Behoerden/Beratung/Prozessmanagement/Leitfaeden/Erhebung_Prozesse.pdf?___blob=publicationFile&v=2, Accessed 16 Feb 2024

D'Hondt T, Wilbik A, Grefen P, et al (2019) Using BPM technology to deploy and manage distributed analytics in collaborative iot-driven business scenarios. In: Proceedings of the 9th International Conference on the Internet of Things, IoT 2019, Bilbao, Spain, October 22-25, 2019. ACM, pp 19:1–19:8, https://doi.org/10.1145/3365871.3365890

DiCicco-Bloom B, Crabtree BF (2006) The qualitative research interview. Medical education 40(4):314–321. https://doi.org/10.1111/j.1365-2929.2006.02418.x

Dumas M, La Rosa M, Mendling J, et al (2021) Grundlagen des Geschäftsprozessmanagements, 1st edn. Springer Verlag, Berlin, Heidelberg, https://doi.org/10.1007/978-3-662-58736-2

Federal Ministry of the Interior and Community (2012) 6.1.1 dokumentenanalyse. URL https://www.orghandbuch.de/OHB/DE/Organisationshandbuch/6_MethodenTechniken/61_Erhebungstechniken/611_Dokumentenanalyse/dokumentenanalyse_inhalt, Accessed 16 Feb 2024

Fichtner M, Schönig S, Jablonski S (2020) Using image mining techniques from a business process perspective. In: Enterprise Information Systems - 22nd International Conference, ICEIS 2020, Virtual Event, May 5-7, 2020, Revised Selected Papers, Lecture Notes in Business Information Processing, vol 417. Springer, pp 62–83, https://doi.org/10.1007/978-3-030-75418-1_4

Ghose A, Koliadis G, Chueng A (2007) Rapid business process discovery (R- BPD). In: Conceptual Modeling - ER 2007, 26th International Conference on Conceptual Modeling, Auckland, New Zealand, November 5-9, 2007, Proceedings, Lecture Notes in Computer Science, vol 4801. Springer, pp 391–406, https://doi.org/10.1007/978-3-540-75563-0_27

Gilchrist A (2016) Industry 4.0. Springer

Giudice MD (2016) Discovering the internet of things (iot) within the business process management: A literature review on technological revitalization. Bus Process Manag J 22(2):263–270. https://doi.org/10.1108/BPMJ-12-2015-0173

Grefen P, Ludwig H, Tata S, et al (2018) Complex collaborative physical process management: A position on the trinity of bpm, iot and DA. In: Collaborative Networks of Cognitive Systems - 19th IFIP WG 5.5 Working Conference on Virtual Enterprises, PRO-VE 2018, Cardiff, UK, September 17-19, 2018, Proceedings, IFIP Advances in Information and Communication Technology, vol 534. Springer, pp 244–253, https://doi.org/10.1007/978-3-319-99127-6_21

Gronau N (2017) Geschäftsprozessmanagement in Wirtschaft und Verwaltung: Analyse, Modellierung und Konzeption, 2nd edn. GITO mbH Verlag, Berlin

Gubrium JF, Holstein JA, Marvasti AB, et al (2012) The SAGE Handbook of Interview Research: The Complexity of the Craft, 2nd edn. Sage Publications, Thousand Oaks, CA, https://doi.org/10.4135/9781452218403

Han X, Hu L, Mei L, et al (2020) A-BPS: automatic business process discovery service using ordered neurons LSTM. In: 2020 IEEE International Conference on Web Services, ICWS 2020, Beijing, China, October 19-23, 2020. IEEE, pp 428–432, https:

//doi.org/10.1109/ICWS49710.2020.00063

Hansen H, Mendling J, Neumann G (2019) Wirtschaftsinformatik, 12th edn. De Gruyter Oldenbourg, Berlin, https://doi.org/10.1515/9783110608731

Hevner AR, March ST, Park J, et al (2004) Design science in information systems research. MIS Q 28(1):75–105. https://doi.org/10.2307/25148625

Hornsteiner M, Empl P, Bunghardt T, et al (2024) Reading between the lines: Process mining on opc ua network data. Sensors 24(14). https://doi.org/10.3390/s24144497, URL https://www.mdpi.com/1424-8220/24/14/4497

Houy C, Fettke P, Loos P, et al (2010) Bpm-in-the-large - towards a higher level of abstraction in business process management. In: E-Government, E-Services and Global Processes - Joint IFIP TC 8 and TC 6 International Conferences, EGES 2010 and GISP 2010, Held as Part of WCC 2010, Brisbane, Australia, September 20-23, 2010. Proceedings, IFIP Advances in Information and Communication Technology, vol 334. Springer, pp 233–244, https://doi.org/10.1007/978-3-642-15346-4_19

Jablonski S, Bussler C (1996) Workflow Management: Modeling Concepts, Architecture and Implementation, 1st edn. Cengage Learning Verlag, Holborn

Jablonski S, Götz M (2007) Perspective oriented business process visualization. In: Business Process Management Workshops, BPM 2007 International Workshops, BPI, BPD, CBP, ProHealth, RefMod, semantics4ws, Brisbane, Australia, September 24, 2007, Revised Selected Papers, Lecture Notes in Computer Science, vol 4928. Springer, pp 144–155, https://doi.org/10.1007/978-3-540-78238-4_16

Jadhav S (2011) Business process discovery. Tech. rep., BP Trends (February) Citeseer

Jakobs EM, Spanke J (2011) Sprache als erfolgsfaktor industrieller prozessmodellierung. In: Evolution der Informationsgesellschaft: Markenkommunikation Im Spannungsfeld der Neuen Medien. VS Verlag für Sozialwissenschaften, Wiesbaden, pp 181–195, https://doi.org/10.1007/978-3-531-92860-9_12

Janiesch C, Koschmider A, Mecella M, et al (2020) The internet of things meets business process management: A manifesto. IEEE Systems, Man, and Cybernetics Magazine 6(4):34–44. https://doi.org/10.1109/MSMC.2020.3003135

Jolles RL (2017) How to Run Seminars and Workshops: Presentation Skills for Consultants, Trainers, Teachers, and Salespeople, 4th edn. John Wiley & Sons, Hoboken, NJ

Krallmann H, Frank H, Gronau N (2002) Systemanalyse Im Unternehmen: Vorgehensmodelle, Modellierungsverfahren und Gestaltungsoptionen, 4th edn. Oldenbourg Verlag, München

Langer M, Söffker D (2011) Human guidance and supervision of a manufacturing system for semi-automated production. In: 2011 IEEE Jordan Conference on Applied Electrical Engineering and Computing Technologies (AEECT), pp 1–6, https://doi.org/10.1109/AEECT.2011.6132501

Laugwitz B, Held T, Schrepp M (2008) Construction and evaluation of a user experience questionnaire. In: HCI and Usability for Education and Work, 4th Symposium of the Workgroup Human-Computer Interaction and Usability Engineering of the Austrian Computer Society, USAB 2008, Graz, Austria, November 20-21, 2008. Proceedings, Lecture Notes in Computer Science, vol 5298. Springer, pp 63–76, https://doi.org/10.1007/978-3-540-89350-9_6

Lauttamäki V (2014) Practical guide for facilitating a futures workshop. Finland futures research centre pp 2–11

Linds W, Gee T (2023) What Is Workshop? Springer Nature Singapore, Singapore, https://doi.org/10.1007/978-981-99-2291-8_3

Mass J, Chang C, Srirama SN (2016) Wiseware: A device-to-device-based business process management system for industrial internet of things. In: 2016 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Chengdu, China, December 15-18, 2016. IEEE, pp 269–275, https://doi.org/10.1109/ITHINGS-GREENCOM-CPSCOM-SMARTDATA.2016.69

zur Muehlen M, Ho DT (2005) Risk management in the BPM lifecycle. In: Business Process Management Workshops, BPM 2005 International Workshops, BPI, BPD, ENEI, BPRM, WSCOBPM, BPS, Nancy, France, September 5, 2005, Revised Selected Papers, pp 454–466, https://doi.org/10.1007/11678564_42

Neuberger J, Ackermann L, Jablonski S (2023) Beyond rule-based named entity recognition and relation extraction for process model generation from natural language text. In: Cooperative Information Systems - 29th International Conference, CoopIS 2023, Groningen, The Netherlands, October 30 - November 3, 2023, Proceedings, Lecture Notes in Computer Science, vol 14353. Springer, pp 179–197, https://doi.org/10.1007/978-3-031-46846-9_10

Okoli C, Schabram K (2010) A guide to conducting a systematic literature review of information systems research. SSRN Electronic Journal 10. https://doi.org/10.2139/ssrn.1954824

Page MJ, McKenzie JE, Bossuyt PM, et al (2021) The PRISMA 2020 statement: an updated guideline for reporting systematic reviews. BMJ p n71. https://doi.org/10.1136/bmj.n71

Pavelin K, Pundir S, Cham JA (2014) Ten simple rules for running interactive workshops. PLoS Comput Biol 10(2). https://doi.org/10.1371/JOURNAL.PCBI.1003485

Prat N, Comyn-Wattiau I, Akoka J (2015) A taxonomy of evaluation methods for information systems artifacts. J Manag Inf Syst 32(3):229–267. https://doi.org/10.1080/07421222.2015.1099390

Raptis TP, Passarella A, Conti M (2019) Data management in industry 4.0: State of the art and open challenges. IEEE Access 7:97052–97093

Richerzhagen B (2015) Königsdisziplin Prozess-Workshops. Camunda Inc.

Schönig S, Ackermann L, Jablonski S (2018) Internet of things meets BPM: A conceptual integration framework. In: Proceedings of 8th International Conference on Simulation and Modeling Methodologies, Technologies and Applications, SIMULTECH 2018, Porto, Portugal, July 29-31, 2018. SciTePress, pp 307–314, https://doi.org/10.5220/0006824803070314

Schönig S, Ackermann L, Jablonski S, et al (2020a) Iot meets BPM: a bidirectional communication architecture for iot-aware process execution. Softw Syst Model 19(6):1443–1459. https://doi.org/10.1007/S10270-020-00785-7

Schönig S, Jasinski R, Ermer A (2020b) Data interaction for iot-aware wearable process management. In: Service-Oriented Computing - ICSOC 2020 Workshops - AIOps, CFTIC, STRAPS, AI-PA, AI-IOTS, and Satellite Events, Dubai, United Arab Emirates, December 14-17, 2020, Proceedings, Lecture Notes in Computer Science, vol 12632. Springer, pp 67–71, https://doi.org/10.1007/978-3-030-76352-7_10

Schönig S, Günther C, Jablonski S (2012) Process discovery and guidance applications of manually generated logs. In: Proceedings of the 7th International Conference on Internet Monitoring and Protection (ICIMP 2012). IARIA, Stuttgart, Germany, pp 61–67

Schönig S, Ackermann L, Jablonski S, et al (2020) Iot meets bpm: a bidirectional communication architecture for iot-aware process execution. Software and Systems Modeling 19(6):1443–1459

Seiger R, Malburg L, Weber B, et al (2022) Integrating process management and event processing in smart factories: A systems architecture and use cases. Journal of Manufacturing Systems 63:575–592. https://doi.org/10.1016/j.jmsy.2022.05.012

Sisinni E, Saifullah A, Han S, et al (2018) Industrial internet of things: Challenges, opportunities, and directions. IEEE Trans Ind Informatics 14(11):4724–4734. https://doi.org/10.1109/TII.2018.2852491

Storvang P, Mortensen B, Clarke AH (2018) Using workshops in business research: A framework to diagnose, plan, facilitate and analyze workshops. Collaborative Research Design pp 155–174. https://doi.org/10.1007/978-981-10-5008-4_7

Szelągowski M, Lupeikiene A, Berniak-Woźny J (2022) Drivers and evolution paths of bpms: State-of-the-art and future research directions. Informatica 33(2):399–420

Taherdoost H (2022) How to conduct an effective interview; a guide to interview design in research study. International Journal of Academic Research in Management 11(1):39–51

Tiftik MN, Erdogan TG, Tarhan AK (2022) A framework for multi-perspective process mining into a bpmn process model. Mathematical Biosciences and Engineering 19(11):11800–11820. https://doi.org/10.3934/mbe.2022550

Turner III DW (2010) Qualitative interview design: A practical guide for novice investigators. The qualitative report 15(3):754. https://doi.org/10.46743/2160-3715/2010.1178

Wang J, Zhang W, Shi Y, et al (2018) Industrial big data analytics: Challenges, methodologies, and applications. CoRR https://doi.org/10.48550/arXiv.1807.01016

Weske M (2012) Business Process Management - Concepts, Languages, Architectures, 2nd Edition. Springer, https://doi.org/10.1007/978-3-642-28616-2

P2: SIREN: Designing Business Processes for Comprehensive Industrial IoT Security Management

Status	Published
Date of Submission	24 January 2023
Date of Acceptance	27 March 2023
Date of Publication	19 May 2023
Conference	International Conference on Design Science Research in Information Systems and Technology
Location	Pretoria, Süd Afrika
Period	31.05.2023 - 02.06.2023
Authors Contribution	Markus Hornsteiner 90% Stefan Schönig 10%
Full Citation	Hornsteiner, M., Schönig, S. (2023). SIREN: Designing Business Processes for Comprehensive Industrial IoT Cybersecurity Management. *Proceedings of the 18th International Conference on Design Science Research in Information Systems and Technology (DESRIST)*. LNCS, vol. 13873, pp. 379–393. Springer.
DOI	10.1007/978-3-031-32808-4_24

Conference Description: The LNCS series, including its subseries LNAI and LNBI, has established itself as a medium for the publication of new developments in computer science and information technology research, teaching, and education. LNCS enjoys close cooperation with the computer science R&D community, the series counts many renowned academics among its volume editors and paper authors, and collaborates with prestigious societies. Its mission is to serve this international community by providing an invaluable service, mainly focused on the publication of conference and workshop proceedings and postproceedings. LNCS commenced publication in 1973.

SIREN: Designing Business Processes for Comprehensive Industrial IoT Security Management *

Markus Hornsteiner[1 [0000−0002−8024−1220]] and Stefan Schönig[1 [0000−0002−7666−4482]]

University of Regensburg, Germany
firstname.lastname@ur.de
https://go.ur.de/iot

Abstract. The Industrial Internet of Things (IIoT) paradigm means that "things" in an industrial context are equipped with connectivity. The convergence of formerly isolated Operational Technology with IT provides disruptive opportunities for organizations but is also vulnerable to cyberattacks. To mitigate these risks, the IEC62443 standard was developed, which will be mandatory for critical infrastructure organizations due to the EU Cybersecurity Act. This standard demands various requirements for the technology and organizational aspects of organizations. To implement the standard's technical requirements and demonstrate compliance, applications can be used. This paper utilizes Design Science Research (DSR) to design, develop, and demonstrate *Security Iiot pRocEss Notation (SIREN)*, an approach based on Business Process Model and Notation (BPMN) to model and monitor processes and compliance. Previous research have yet to cover the IIoT explicitly and lack the monitoring of the modeled attributes. Therefore, a novel specialized approach is presented, enhancing the model with monitorable attributes based on the standard. Thus, this paper presents a BPMN-based approach to model and monitor security-aware processes in IIoT.

Keywords: Industrial Internet of Things Security · Process Aware Monitoring · Security Aware Processes · Security Aware Modeling

1 Introduction

The Industrial Internet of Things (IIoT) offers a broad compendium of technologies from the Internet of Things (IoT) to automate and network production systems [7]. 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.

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

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 [29].

For this reason, there are regulatory efforts to establish the implementation of security measures like IEC62443 in the EU as a standard [13]. According to this standard, respective organizations should follow a "security by design" paradigm [12]. In this respect, to conduct meaningful and sustainable security management, it is crucial to know and define corporate assets, their 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 systematic modeling of operational IIoT processes that can also be exploited for improving IIoT security [1,30,33]. How SIREN differs from these is thoroughly discussed in Section 3.2. Also an in-depth analysis has already been published [11]. While there is already research on the integration of IoT and BPM technology in general [14,24,25,27,28], we claim that BPM methods represent an unexploited source for improving cyber security in manufacturing companies [26].

A formally defined process modeling notation, like the de-facto standard Business Process Modeling and Notation (BPMN) [20], is a fundamental means for implementing a BPM-based security by design approach. However, since the IIoT security requirements from the IEC62443 standard are not yet supported, a method must be created to represent security requirements and possible protective measures accordingly. While some notations already exist for security aspects in the IT domain [3,15,34], a specialized approach for the IIoT with its unique requirements is still missing.

In this paper, strictly following DSR, we develop *Security Iiot pRocEss Notation (SIREN)*, a BPMN-based modeling approach for specifying IIoT processes enhanced with security requirements compliant with the IEC62443 standard. Our notation is based on clearly defined functional requirements and security levels extracted from the IEC standard. SIREN uses standard BPMN elements to map security aspects without requiring language extensions and therefore remains completely executable and monitorable. Additionally, as depicted in Figure 1, we present tool support that enables automated mapping of SIREN-based process models to computer-interpretable security rules that can be monitored within an intrusion detection system. Therefore we deem SIREN comprehensive, because it supports the entire process lifecycle, from identification to monitoring [26]. The evaluation of our approach is twofold: first we applied the notation within a real-life industrial use case, and, based thereupon, we extensively evaluated the artifact with experts from various fields, based on a 4-episode evaluation schema.

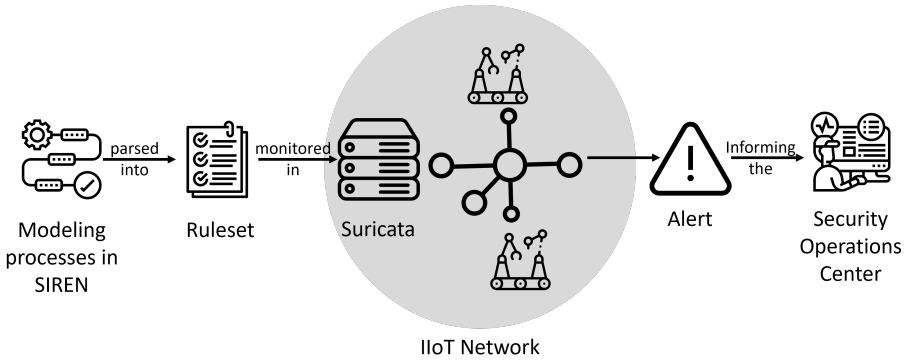


Fig. 1. Overview of IIoT security management with SIREN

The remainder of this paper is structured as follows: in Section 2, the research method that guided this paper is discussed. Followed by Section 3 in which the underlying concepts and technologies for the suggested approach is discussed, related work is explained, and the design objectives that guided the development are presented. This is followed in Section 4 with the design and development of the approach. After that in Section 6, we extensively evaluate the approach with various experts.

2 Research Method

This paper is based on the DSR Methodology that aims at creating valuable artifacts within the information systems discipline. [10] To enable systematic and rigorous research, the established procedure model of [21] has been applied, which provided methodological guidance. It consists of six iterative phases, including (i) the identification and motivation of the underlying problem, (ii) the definition of the objectives of the solution, (iii) the actual design and development, (iv) the demonstration, (v) an evaluation, and (vi) the communication to an appropriate audience. While the identification and motivation have already been outlined in Section 1, a set of fundamental design objectives are discussed in Section 3 that have been derived from the formulated research questions. These design objectives form the basis for subsequent design and development decisions performed iteratively. As a proper evaluation is crucial within any DSR endeavor, a comprehensive evaluation strategy has been created, based on Venable et al. [31]. This strategy included formative and summative evaluation episodes performed before and during (ex-ante) and after (ex-post) the design and development phase. Objective evaluation criteria (cf. Prat et al. [22]) were defined to measure conformance with the design objectives. The design of the artifact follows Moody [19].

3 Theoretical Background

3.1 Industrial Internet of Things meets Cybersecurity

The IIoT constitutes a new era in industrial production since it marks the beginning of a fundamental paradigm shift [6]. 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. Whereas IIoT brings new opportunities, it also has its downsides. Through connecting industrial components, there are new ways for attackers to infiltrate, interrupt or maliciously modify processes [5,6]. 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 [29]. To ensure that, in industrial standards like the IEC62443, the security by design paradigm is required [12]. That means the security of processes and components must be ensured as early as in the design stage. To consider security in industrial processes, there is a need for an inclusive modeling approach of security- and IIoT-aware processes [26].

3.2 Related Work

During the development of SIREN, we have made several design and development steps. Initially, we conducted an extensive systematic literature review (SLR) for knowledge curation. The detailed paper is already published [11]. In the following, this paper only discusses the implications that the SLR raised.

IIoT Extensions for BPMN In science, the importance of IIoT is already recognized, and by that, a lack of a modeling language to represent IIoT aware processes [16]. For that an EU-funded research project developed a comprehensive BPMN extension that covers sensors, IIoT-specific tasks, and cloud devices. [16,17,18]. However, it doesn't address security or executability. [9] closes this gap by explicitly considering the execution of modeled processes, but doesn't cover security.

Security Extensions for BPMN BPMN has been extended to represent security in processes, including classic goals like confidentiality, integrity, and availability [1], encrypted messages [23], and delegation/binding of duty [30]. However, only one paper explicitly deals with an industrial use case [33], but from a business perspective. No explicit integration of IIoT security into BPMN has occurred and there are no concepts for executing secure processes. This paper aims to address these gaps by presenting a BPMN extension that considers the IIoT and enables execution of modeled processes.

Previous work has not explicitly addressed security in IIoT environments, and transforming process models into monitorable rules is, to the best of our knowledge, a novelty. Therefore, our contribution includes using BPMN for IIoT security and transforming process models into monitorable rules.

3.3 Design Objectives

Based on the research question **how can BPMN be used to model processes in IIoT cybersecurity aware and to monitor compliance with the rules**, the following design objectives (DO) emerge. These serve as guidance during development and are used to measure development completion, as described in Section 6. The four main objectives are defined and described in the following.

- **DO 1: As little as possible, as much as necessary.** When developing notations, such as SIREN, it is necessary to keep the complexity as low as possible to maximize comprehensibility [19]. Therefore, the first requirement for the artifact is that it contains only essential information.
- **DO 2: Specialized for the IIoT.** As shown in Section 3.2, there are already security extensions for BPMN. However, these are either generic or specialized for specific use cases. So far, none explicitly addresses the IIoT, which is why we see a gap in the research here. Therefore, the second requirement for the artifact is that it explicitly addresses IIoT security.
- **DO 3: Relevant, useful and applicable in practice.** A fundamental goal of DSR projects is to create an artifact that is relevant and applicable in the real world [2]. Herefore, the third goal of the artifact is that it is advantageous for the real world, i.e., the IIoT environment.
- **DO 4: Compliance with rules for comprehensibility.** To ensure that the artifact is understandable and thus accessible to people with disabilities, it should comply with standard rules for understandability and readability.

4 Notation Design and Development

4.1 Building the Theoretical Foundations

As shown in Section 3, research already enhances BPMN with security attributes, but these lack the specific challenges of the IIoT [11]. In order to establish security requirements for the IIoT, specific requirements must be taken into account. IEC62443 is a comprehensive standard that defines how the security of industrial communication networks can be increased [12]. The standard is divided into three perspectives, manufacturers, integrators, and operators. On the manufacturer side, research already supports compliance with the standard [8]. SIREN focuses on the operator's perspective. SIREN contributes to three corners of security in organizations. i) documentation of processes and security attributes to gain and keep an overview. ii) communication of information so processes can be discussed, optimized, or adapted graphically with various stakeholders, and compliance with regulations can also be proven externally. iii) monitor modeled processes to detect, e.g., intrusions or malicious activities in the network.

Fundamental Requirements (FR). The seven FRs of IEC62443 refer to the security of industrial automation and control systems (IACS) and their components. A list of system, component, network devices, embedded devices, host

devices, software application requirements, and requirement enhancements specifies the FR. This paper will limit the focus to the Fundamental and System Requirements described in more detail in Section 4.2. In the following, the FR are listed with their respective definitions.

- **FR1 - Identification and authentication control.** Identify and authenticate all users (humans, processes, devices), and grant access to the IACS.
- **FR2 - Use Control.** Enforce the assigned privileges of an authenticated user (human, process, or device) to perform the requested action on the system or assets and monitor the use of these privileges.
- **FR3 - System Integrity.** Ensure the integrity of information on communication channels and in data repositories to prevent unauthorized actions.
- **FR4 - Data confidentiality.** Ensure the confidentiality of information on communication channels and in data repositories to prevent dissemination.
- **FR5 - Restricted data flow.** Segment the system via zones and conduits to limit the unnecessary flow of data
- **FR6 - Timely response to events.** Respond to security violations by notifying the proper authority, reporting needed forensic evidence of the violation, and taking timely corrective action when incidents are discovered.
- **FR7 - Resource Availability.** Ensure the availability of the system or assets against the denial of essential services.

Security Levels (SL). The FR and their specifications are categorized into four security levels. Each represents a specific attacker with the respective motivation, capabilities, and resources. SIREN supports these by allowing the security level to be annotated to entities. An alert can be triggered in the event of deviations from the defined security level and attached monitoring annotations. However, this exact functionality is outside this work's scope.

4.2 Technical Aspects of SIREN

Tool Supported Development. The extension is implemented in Camunda Modeler[1]. This is an extensible open-source modeling tool for BPMN 2.0. It offers two perspectives on the BPMN model. One is a graphical display of the modeled process, and the other is a text editor to display the underlying Extensible Markup Language (XML). Python is used for parsing the rules modeled in BPMN. Parsing means they are translated into monitorable rules. Therefore the XML from Camunda is read and processed by the Python scripts. The exact workflow is described in Section 5. Suricata[2] is used to implement network monitoring. Suricata is an open-source network analysis and threat detection tool whose behavior can be configured with self-defined rules. The open-source platform Wazuh[3] is used in this paper for the Security Operations Center (SoC). An SoC is a centralized unit that combines security-related data from multiple sources to provide a comprehensive view of the current cybersecurity status [32].

[1] https://camunda.com/de/download/modeler/
[2] https://suricata.io/
[3] https://wazuh.com/

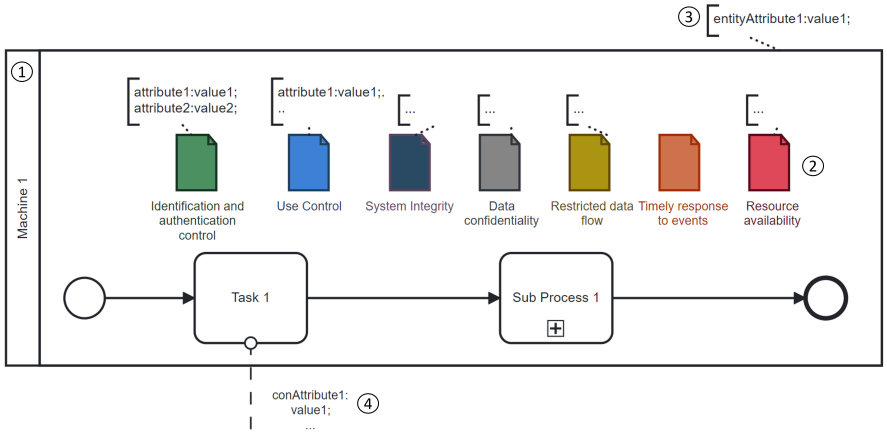


Fig. 2. Example IEC62443-aware process model based on SIREN.

Elements of the Notation. The process shown in Figure 2 contains numbered circles. These reference to the descriptions of SIREN elements given below, each with an explanation of their use. These indicators are also given in the industrial use cases Figure 3.

1. **Pools.** The participants of a SIREN process are network entities. These entities are each represented by a pool. Security requirements and entity attributes can extend each entity.
2. **Security Requirements with Attributes.** Data objects are used to extend the entities with the requirements described in Section 4.1. Each entity is assigned all requirements with a unique color and name. The requirements are represented in the standards order, and attributes can be added via TextAnnotations which indicate characteristics to fulfill each requirement.
3. **Participant Attribute.** To extend an entity with basic information, TextAnnotations are used, which are attached to it. This information can be, e.g., IP addresses, targeted security levels, or similar.
4. **Network Connection.** The network communication between the entities is represented by MessageFlows. These MessageFlows correspond to a communication connection between two entities and can be enriched with information via TextAnnotations.

Physics of the Notation. Following Moody [19], three different levels of visual distinction are used. First, arrangement, which means that each element has a fixed place in the set of the seven requirements, following the structure of the FR (cf. Section 4.1). Secondly, each element is provided with a label that names the FR. The third level of distinction is color. The colors are based on the WCAG

Table 1. Shortened table of mappings.

Fundamental Requirement	System Requirement	Attributes
FR 1	SR 1.11 Unsuccessful login attempts	isMonitored:[true,false]; auth_attempts:int;
	SR 1.8 Public key infrastructure (PKI) certificates	cert_valid: [true;false]
FR 2	SR 2.8 Auditable events	log_reconnaissance_activity:[true;false]; log_access_activity:[true;false];
FR 3	...	...

2.0 guidelines [4] to support people with impaired vision. All colors have at least a Contrast Ratio of 3, so AA conformance is the minimum. However, color is only one of the three levels of distinctiveness, so if, e.g., the model is printed in black and white, the position and the text remain distinguishing features.

5 Implementation and Rule Monitoring

5.1 From Process Modeling to Rule Monitoring

The workflow shown in Figure 1 is the path of a SIREN user from modeling to monitoring a process. At first, the process is modeled with its participants, dependencies, relationships, and attributes. Various sources can be used for this, e.g., existing documents, process mining, or interview methods [4]. The modeler then enriches the process with the security attributes. These are in a catalog with information about which attributes are needed for a specific security level. After creation, the SIREN parser reads the underlying XML. This parser extracts the required information from the model. The data structure is object-oriented and accordingly creates classes for the entities, which should increase traceability and adaptability. The SIREN rule builder then derives rules based on this information. These can currently be divided into communication and entity rules. Example rules are shown in Listing 1. These rules are then fed into Suricata. This monitors the network based on the rules and examines the data packets for deviations. If it detects some, it informs the SoC.

5.2 Mapping of Security Requirements to Model Attributes

Section 3-3 of IEC62443 is the fundamental of SIREN, which focuses on security requirements for industrial control systems. In the following each requirement is named, followed by a brief description and an example of how SIREN can support it.

[4] https://www.w3.org/TR/2008/REC-WCAG20-20081211/0

- **FR1 - Identification and Authentication Control.** To meet this requirement, e.g., the control systems must be able to identify and authenticate all users (cf. IEC62443-3-3 SR1.1). To detect unauthorized access attempts, rules can monitor login attempts. SIREN contains a rule that tracks login attempts and triggers an alert after a certain threshold is reached.
- **FR2 - Use Control.** The control system shall provide the ability to generate audit records relevant to security. For activities such as access restrictions, operating system events, backup or restore events, and potentially malicious activities on the network (cf. IEC62443-3-3 SR2.8). Continuous network monitoring supports this capability, e.g., unusual activities can be recorded and detected. In addition, records of security-relevant events, such as unusual access activities, are continuously created.
- **FR3 - System Integrity.** To ensure system integrity, control systems shall provide the ability to detect, prevent and minimize the impact of malicious code (cf. IEC62443-3-3 SR 3.2). For this purpose, SIREN can integrate publicly available libraries, which detect malicious operations in the network and can trigger an alert in the SoC if so. This means that these can be detected and prevented at an early stage.
- **FR4 - Data Confidentiality.** Confidentiality should be ensured for data exchanged or stored between control systems (see IEC62443 - SR 4.1, SR 4.3). To ensure this, SIREN can monitor the network traffic of entities and check if secure protocols and encryption are used. If a deviation from the specification is detected as an alert can be raised.
- **FR5 - Restricted Data Flow.** The control system should provide the possibility to separate networks according to task and security level and monitor this separation (cf. IEC62443 SR 5.1, 5.2). SIREN can support this in that it offers a visualization option in the first step and can monitor the separation of the networks in the second step. If an exchange of packets from entities of different, independent networks is detected, the SoC is alerted.
- **FR6 - Timely Response to Events.** The control system should provide the ability to continuously monitor activity on the network to allow for rapid intervention if needed (cf. IEC62443-3-3 SR 6.2). By continuously monitoring the network, depending on the configuration, with intrusion detection and detection of suspicious traffic, requests, and packets, SIREN can support this requirement on a network basis.
- **FR7 - Resource Availability.** To fulfill this requirement, the control systems should not stop working in case of a DDOS attack, and unused ports, functions, and protocols should be disabled (cf. IEC62443 3-3 SR7.1, SR7.7). In addition, a permanent inventory of the network components should be made (cf. IEC62443 3-3 SR7.8). In order to fulfill this requirement, SIREN offers the possibility of quickly detecting DDoS attacks, including affected systems, through its continuous monitoring. In addition, alerts can be triggered in the SoC when unknown protocols, ports, or services are used. In addition, SIREN informs the SoC about unknown participants.

```
------------------
Network rules
pass OPCUA 192.168.95.1 22 > 192.168.95.25 24
pass OPCUA 192.168.95.25 any > 192.168.95.1 any
------------------
Entity rules
alert tcp any any -> 192.168.95.25 any (msg:"More than 3 login
↪  attempts!"; content:"admin"; flowint: usernamecount, +, 1;
↪  flowint:usernamecount, >, 3;)
```

Listing 1: Automated generated rules.

To add attributes to each FR in the monitored model, a mapping table was created. The table contains attributes that can be inserted into the model. Currently, the table has limited examples which will be expanded in future development stages. A shortened version of the table is shown in Table 1. For example, the two attributes, *isMonitored* and *auth_ attempts*, can monitor failed login attempts. The former sets a Boolean value to indicate if login attempts should be monitored, while the latter sets a threshold for how many consecutive failed attempts should trigger an alert in the SoC.

5.3 Automatically Generating Monitorable Rules

The BPMN model with added attributes is parsed and transformed into monitorable rules using Python programs called xml_parser and rule_generator. The xml_parser extracts relevant information from the BPMN XML and the rule_generator generates monitorable rules based on this information, using the open-source intrusion detection system Suricata. Examples of generated rules from Figure 3 are given in Listing 1. SIREN is developed modularized to allow the integration of different monitoring systems and is thus not limited to Suricata. In this paper, Suricata serves as a proof of concept.

5.4 Monitoring Security within IIoT Networks

The last step is monitoring the rules generated in the previous step. For this purpose, they are fed into Suricata. Based on this, Suricata then monitors the network and provides the central SoC, based on Wazuh, with information. If, e.g., deviations from the defined process are detected, Suricata reports this to the SoC. Decisions or countermeasures can then be taken in the SoC to ensure or restore the network's security.

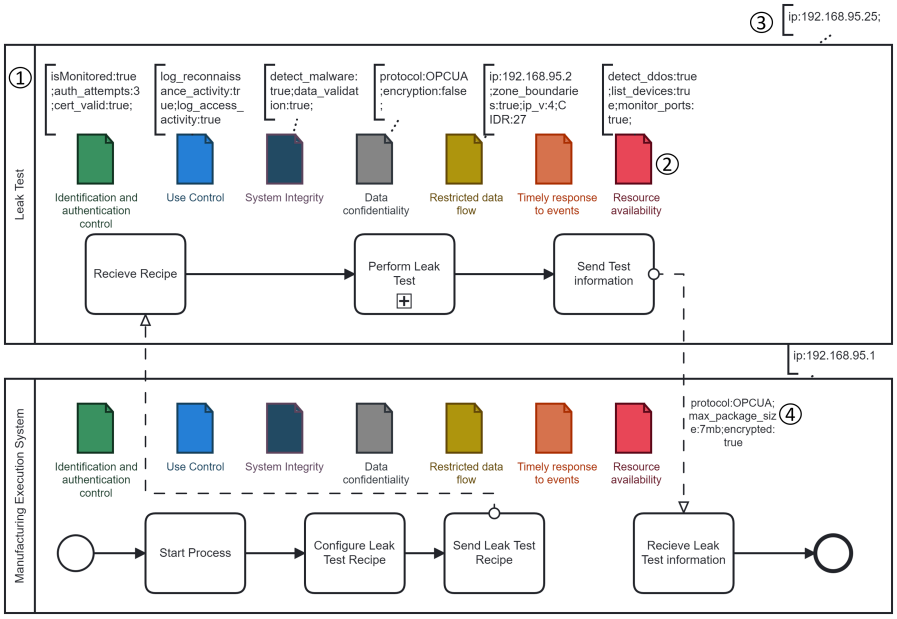


Fig. 3. An abbreviated process of an automotive supplier modeled in SIREN.

6 Evaluation

6.1 Demonstration in Industrial Use Case

For the evaluation, a finishing process of an automotive supplier was modeled in SIREN. An abbreviated representation of this process is shown in Figure 3. The overall process checks components for specific criteria. Various systems and equipment are involved in this process. In the abbreviated version included in this paper, a manufacturing execution system prepares a so-called recipe, and sends it to the Leak Test machine. A recipe is an instruction with precise information about the test. After processing the recipe, the machine send the result to the central system. Communication takes place via the OPC-UA protocol.

6.2 Execution of the Evaluation

The evaluation was divided into five episodes, as shown in Table 3. The first four have already been carried out, and the fifth is planned after the completion of the overall project. Four evaluation criteria were selected based on the DO. *(i) Conciseness:* The notation contains only essential components, *(ii) Efficacy:* The artifact meets the design objectives established in Section 3.3, *(iii) Operational feasibility:* Experts believe that SIREN is usable and helpful for them in their

Table 2. Participants of the Evaluation.

Participant Id	Job Title	Work / Company
1.	Cyber Security Associate	Big 4 Consulting (1)
2.	Assistant Manager Cyber Security	Big 4 Consulting (2)
3.	Security & Senior Security Engineer	International Automotive Supplier
4.	Information Security Consultant	Leading Business and IT Consulting
5.	Consultang Cybersecurity (Industrial Sector)	Leading Business and IT Consulting
6.	Cybersecurity Expert	Automation Technology

everyday work, and *(iv) Effectiveness:* SIREN proves the achievement of the design objectives in reality.

The evaluation was carried out as follows. First, an example use case was modeled (cf. Figure 3), and the authors discussed the compliance with the evaluation criteria of conciseness and efficacy (EV 1). Once the authors decided these criteria were met, semi-structured interviews were conducted with eight experts on compliance with the criteria. Expert interviews are a well-established method for gathering insights from knowledgeable individuals in a specific field [22]. The Interviews revealed that version 1 of the artifact was too complex and overloaded, raising doubts about its feasibility. As a result, the decision was made to regress from the evaluation phase to the design phase and intensify efforts to meet the four design objectives and evaluation criteria. After Version 2 reached, in the authors opinion, the status of meeting the evaluation criteria (EV 3), the experts listed in Table 2 were invited for unstructured interviews. These were carried out according to the following scheme:

Step 1. Request contextual information such as familiarity with IEC62443, cybersecurity domain knowledge, and process modeling experience.
Step 2. (If needed) Brief introduction of the IEC62443 standard.
Step 3. Presentation of the components of SIREN and the workflow.
Step 4. Open question/discussion with the guiding questions:
- Do you think all important elements are included/is anything missing?
- Do you think SIREN is easy to apply?
- Do you think you could work with SIREN?
- Do you think it would be helpful for the company to use SIREN?
- What do you think might be challenging in using it?
- What should be added in the future?

All survey participants found the tool concise and usable, with a solid practical relevance due to its focus on IEC62443 (participants 1, 3, 4, 5, and 6). Future challenges include embedding the artifact in a structured cycle, clarifying its limited organizational cybersecurity coverage, mapping additional requirements, and testing it in a real-world deployment. Following expert confirmation of the evaluation criteria in EV 4, the monitoring attributes will be extended, and a large-scale practical test is planned in EV 5 with a partner company.

Table 3. Performed and planned evaluation episodes.

Evaluation episode	**Why?** Function	**How?** Evironment	Timing	Method	**What** Criteria
EV 1	Formative	Artificial	Ex-ante	Static analysis	Conciseness, Efficacy
EV 2	Formative	Artificial & naturalistic	Ex-ante	Semi-structured interviews	Conciseness, Efficacy, Operational feasibility
EV 3*	Formative	Artificial	Ex-ante	Static analysis	Conciseness, Efficacy
EV 4	Formative	Artificial & naturalistic	Ex-ante	Semi-structured interviews	Conciseness, Efficacy, Operational feasibility
EV 5	Summative	Naturalistic	Ex-post	Real-world use	Effectiveness

**Restart of the development after EV2.*

7 Conclusion

While IIoT security is becoming increasingly important, and the process perspective is an essential part of security by design, research lacks modeling possibilities. In particular, one cannot use modeling as a basis for effective monitoring. To fill this research gap, this paper presents SIREN, a BPMN based modelling notation which enhances industrial processes with attributes of IEC62443 and transforms them to monitorable rules. This novel approach has been shown to be effective in practice in accompanying surveys. In order to further develop SIREN and increase its usability, future work will focus on the following aspects:

- **IEC62443 conformance** SIREN needs to expand its capabilities beyond IEC62443 3-3 to include, for example, section 4-2. Additionally, the rule generator must be further developed to support security levels, such as detecting deviations from the desired security level to the actual security level. The rules presented in Section 5 are just an example to explain the basic approach of SIREN and therefore, they need to be extended.
- **Scalability** SIREN represents one monitoring device for one industrial plant. SIREN should provide the possibility of equipping entire factories. Therefore an scalabe architecture for SIREN must be developed, so that is is capable of larger tasks.
- **Real world usage** SIREN must be used in practice to further evaluate its usability. According to EV 5 (cf. Section 6 a large spanned evaluation of SIREN in an real world scenario must be done, to gather insights on its capabilitis in the IIoT environment.

As representing assets, processes, and security infrastructure is crucial for organizations seeking IEC62443 certification, we hope to offer added value by providing SIREN's comprehensive attribute representation.

References

1. Altuhhova, O., Matulevičius, R., Ahmed, N.: An extension of business process model and notation for security risk management. IJISMD **4**(4) (2013)
2. vom Brocke, J., Hevner, A., Maedche, A.: Introduction to Design Science Research, pp. 1–13. Springer International Publishing, Cham (2020)
3. Chergui, M.E.A., Benslimane, S.M.: Towards a BPMN Security Extension for the Visualization of Cyber Security Requirements. IJTD **11**(2) (2020)
4. Dumas, M., Rosa, M.L., Mendling, J., Reijers, H.A.: Fundamentals of Business Process Management, Second Edition. Springer (2018)
5. Empl, P., Pernul, G.: A flexible security analytics service for the industrial iot. In: Proceedings of the 2021 ACM Workshop on Secure and Trustworthy Cyber-Physical Systems. SAT-CPS '21, ACM (2021)
6. ENISA: Good Practices for Security of Internet of Things in the context of Smart Manufacturing. European Union Agency for Cybersecurity (2018)
7. Feki, M.A., Kawsar, F., Boussard, M., Trappeniers, L.: The Internet of Things: The Next Technological Revolution. Computer **46**(2) (2013)
8. Fockel, M., Merschjohann, S., Fazal-Baqaie, M., Förder, T., Hausmann, S., Waldeck, B.: Designing and integrating IEC 62443 compliant threat analysis. In: Systems, Software and Services Process Improvement - 26th European Conference, EuroSPI 2019, Edinburgh, UK, September 18-20, 2019, Proceedings. vol. 1060. Springer (2019)
9. Gallik, F., Kirikkayis, Y., Reichert, M.: Modeling, executing and monitoring iot-aware processes with BPM technology. In: International Conference on Service Science, ICSS 2022, Zhuhai, China, May 13-15, 2022. IEEE (2022)
10. Hevner, A.R., March, S.T., Park, J., Ram, S.: Design science in information systems research. MIS Quarterly: Management Information Systems **28**(1) (2004)
11. Hornsteiner., M., Stoiber., C., Schönig., S.: Towards security- and iiot-aware bpmn: A systematic literature review. In: Proceedings of the 19th International Conference on Smart Business Technologies - ICSBT. SciTePress (2022)
12. IEC: Cybersecurity for Operational Technology in Automation and Control Systems. Standard, International Electrotechnical Commission, Geneva, CH (July 2009)
13. International Society of Automation: United Nations commission to integrate ISA/IEC 62443 into Cybersecurity Regulatory Framework. InTech Magazine (2019)
14. Janisch, C., Koschmider, A., et al.: The internet-of-things meets business process management. a manifesto. IEEE Systems, Man, and Cybernetics Magazine **6**(4) (2020)
15. Maines, C.L., Zhou, B., Tang, S., Shi, Q.: Adding a Third Dimension to BPMN as a Means of Representing Cyber Security Requirements. In: DeSE (2016)
16. Mayer, S.: Internet of Things Architecture IoT-A Project Deliverable D2.2 – Concepts for Modelling IoT-Aware Processes. IoT-A Project (2012)
17. Meyer, S., Ruppen, A., Hilty, L.: The things of the internet of things in BPMN. In: Lecture Notes in Business Information Processing, vol. 215. Springer (2015)
18. Meyer, S., Ruppen, A., Magerkurth, C.: Internet of things-aware process modeling: Integrating IoT devices as business process resources. In: Lecture Notes in Computer Science, vol. 7908 LNCS. Springer (2013)
19. Moody, D.: The "Physics" of Notations: Toward a Scientific Basis for Constructing Visual Notations in Software Engineering. IEEE TSE **35**(6) (2009)

20. OMG: Business Process Model and Notation (BPMN), Version 2.0 (2011)
21. Peffers, K., Tuunanen, T., Rothenberger, M.A., Chatterjee, S.: A design science research methodology for information systems research. JMIS **24**(3) (2007)
22. Prat, N., Comyn-Wattiau, I., Akoka, J.: A Taxonomy of Evaluation Methods for Information Systems Artifacts. JMIS **32**(3) (2015)
23. Sang, K.S., Zhou, B.: BPMN Security Extensions for Healthcare Process. In: ICCIT; UBICC; DASC; PICom (2015)
24. Schönig, S., Ackermann, L., Jablonski, S., Ermer, A.: Iot meets BPM: a bidirectional communication architecture for iot-aware process execution. Softw. Syst. Model. **19**(6) (2020)
25. Schönig, S., Aires, A.P., Ermer, A., Jablonski, S.: Workflow support in wearable production information systems. In: Inf. Sys. in the Big Data Era. vol. 317, pp. 235–243 (2018)
26. Schönig, S., Hornsteiner, M., Stoiber, C.: Towards process-oriented iiot security management: Perspectives and challenges. In: Enterprise, Business-Process and Information Systems Modeling. vol. 450. Springer (2022)
27. Stoiber, C., Schönig, S.: 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. pp. 1–10 (2022)
28. Stoiber, C., Schönig, S.: Improving business processes with the internet of things - A taxonomy of iiot applications. In: 30th European Conference on Information Systems - New Horizons in Digitally United Societies, ECIS (2022)
29. Tange, K., De Donno, M., Fafoutis, X., Dragoni, N.: A Systematic Survey of Industrial Internet of Things Security: Requirements and Fog Computing Opportunities. IEEE Commun. Surv. Tutor. **22**(4) (2020)
30. Turki, S.H., Bellaaj, F., Charfi, A., Bouaziz, R.: Modeling Security Requirements in Service Based Business Processes. In: Enterprise, Business-Process and Information Systems Modeling. Springer Berlin Heidelberg, Berlin, Heidelberg (2012)
31. Venable, J., Pries-Heje, J., Baskerville, R.: FEDS: a Framework for Evaluation in Design Science Research. European Journal of Information Systems **25**(1) (2016)
32. Vielberth, M., Glas, M., Dietz, M., Karagiannis, S., Magkos, E., Pernul, G.: A digital twin-based cyber range for SOC analysts. In: Data and Applications Security and Privacy XXXV - 35th Annual IFIP WG 11.3 Conference, DBSec 2021, Calgary, Canada, July 19-20, 2021, Proceedings. vol. 12840. Springer (2021)
33. Zareen, S., Akram, A., Ahmad Khan, S.: Security Requirements Engineering Framework with BPMN 2.0.2 Extension Model for Development of Information Systems. Applied Sciences **10**(14) (2020)
34. Zarour, K., Benmerzoug, D., Guermouche, N., Drira, K.: A BPMN Extension for Business Process Outsourcing to the Cloud. In: New Knowledge in Information Systems and Technologies (2019)

P3: Process-Oriented Industrial IoT Security Management: A Modeling Framework with Formal Syntax

---

Status	Submitted
Date of Submission	19 Aug 2025
Journal	International Journal of Information Security
Special Issue	Cybersecurity Risk Assessment and Mitigation Strategies for Digital Infrastructures
Authors Contribution	Linda Kölbel 45% Markus Hornsteiner 45% Stefan Schönig 10%
Full Citation	Kölbel, L., Hornsteiner, M., Schönig, S. (2025). Process-Oriented Industrial IoT Cybersecurity Management: A Modeling Framework with Formal Syntax. Submitted to *International Journal of Information Security*.
Artifact	`https://github.com/mahopy/siren.exe`

Journal Description: The International Journal of Information Security is a comprehensive resource for critical advancements in the field of information security.

- Presents important technical work in information security, whether theoretical, applicable, or related to implementation
- Covers system security, network security, content protection, applications
- Contents include privacy, access control, authentication, identification, applied cryptography, and formal methods in information security

Process-Oriented Industrial IoT Security Management: A Modeling Framework with Formal Syntax

Linda Kölbel[a,1], **Markus Hornsteiner**[b,1], **Stefan Schönig**[c,1]

[1]University of Regensburg, Regensburg, Germany

Received: date / Accepted: date

Abstract The Industrial Internet of Things (IIoT) poses complex cybersecurity challenges due to the integration of operational technology (OT) and information technology (IT) systems. While standards such as IEC 62443 cover organizational processes, lifecycle management, and detailed security requirements, they provide little guidance on how these requirements can be operationalized and enforced at runtime in dynamic environments. This paper presents a lifecycle-aligned framework for security policies that formalizes IEC 62443-based security controls and integrates them into structured security policy models. These models are specified using a formal syntax and built on the Business Process Model and Notation (BPMN) to provide a standardized representation of operational workflows. A dedicated policy engine verifies the compliance of live system behavior by converting the defined controls into machine-executable policies that are enforced and continuously monitored at runtime by a policy enforcement module integrated into tools such as Suricata and Wazuh. By embedding this mechanism in the security lifecycle according to IEC 62443-2-1, the approach ensures continuous compliance verification and facilitates real-time detection of policy violations in IIoT environments. A real-world manufacturing use case demonstrates the practical applicability and effectiveness of the approach in operational environments.

Keywords Business Process Management · Industrial Internet of Things · IEC 62443 · Security Requirements

[a]e-mail: linda.koelbel@ur.de
[b]e-mail: markus.hornsteiner@ur.de
[c]e-mail: stefan.schoenig@ur.de

1 Introduction

The increasing connectivity in industrial processes, driven by human–machine interaction and machine–to–machine communication, has ushered in the Industrial Internet of Things (IIoT), the industrial extension of the conventional Internet of Things [1,2]. The convergence of Information Technology (IT) and Operational Technology (OT) within the IIoT has significantly increased the attack surface of industrial systems, and the associated interconnectivity poses new security challenges for organizations [3]. As autonomous interactions and data-driven workflows proliferate (e.g., predictive maintenance, remote operation, digital twins), enforceable, lifecycle-aware security policies become critical [4,5]. Consequently, continuous security monitoring in IIoT environments is essential, motivating new approaches to safeguard IIoT assets [6]. In response, regulators have introduced requirements to mandate and support the implementation of security measures.

Standards such as IEC 62443, the NIS2 Directive, and the EU Cyber Resilience Act define structured catalogs of security controls and security levels to guide the protection of industrial assets. However, these frameworks often remain at a conceptual level and lack executable mechanisms for operational compliance and runtime compliance checking [7]. This gap between design-time and runtime limits the effectiveness of security controls in dynamic IIoT environments: controls are typically defined at design time but are rarely validated or monitored during operation, and organizations often lack structured methods to embed security policies into operational behavior [8]. This disconnect has been exploited in real incidents. For example, the 2017 TRITON attack on industrial Safety Instru-

mented Systems directly altered process control logic governing automated shutdowns [9]. By embedding malicious changes into the operational workflow, the attackers bypassed safety mechanisms without triggering alarms, a clear case where continuous runtime enforcement of lifecycle-defined controls could have prevented or detected the compromise [10]. This gap motivates a structured, machine-executable approach that transforms lifecycle-defined security controls into machine-executable policies and supports their continuous validation at runtime.

This leads to our central research question: *How can lifecycle-aligned, machine-executable security controls be developed from IEC 62443 and integrated with process models to support enforcement and monitoring in IIoT environments?*

To address this, we introduce a security policy management framework that enables the specification, runtime enforcement, and continuous monitoring of machine-readable security controls [11]. For the purposes of illustration, this document uses the IEC 62443 standard as a security guideline, whose control measures must be fulfilled. This is only an example and can be replaced with controls such as NIS2 or ISO 27001. The framework defines a formal control syntax and maps controls to operational actions, assets, and communication links. We structure these models using Business Process Model and Notation (BPMN)[1], providing a standardized method to represent workflows and integrate security semantics. We chose BPMN because it is widely adopted in industrial organizations and supported by mature toolchains. More broadly, Business Process Management (BPM) offers established methods for managing organizational processes [12]; prior research has shown that BPM concepts can be extended to formally represent industrial assets and their associated security controls, making them a suitable foundation for specifying, validating, and monitoring security-aware workflows in IIoT environments.

A dedicated policy engine interprets the machine-executable policies and ensures their continuous enforcement in real time through a policy enforcement module integrated with industrial monitoring tools. The framework aligns with the IEC 62443-2-1 security lifecycle, from control definition and design-time modeling to runtime enforcement and anomaly detection.

This work makes four contributions:

- **Define** a formal syntax for representing IEC 62443-based security controls as machine-executable policies, independent of any specific process modeling tool.
- **Provide** modeling guidelines for integrating these policies into BPMN process models.
- **Implement** a runtime enforcement architecture with a policy engine and integration into industrial monitoring stacks to support real-time detection of policy violations.
- **Evaluate** the approach in a real-world industrial scenario, demonstrating practical effectiveness for securing IIoT workflows.

The remainder of this paper is structured as follows: Section 2 provides an overview of the IEC 62443 itself and the 62443-2-1 Security Lifecycle and situates our work within the relevant phases. Furthermore, we introduce SIREN, the modeling language employed in this study. Section 3 reviews related work and delineates how our approach differs from existing contributions. Section 4 details the research methodology, including the underlying design components and the objectives pursued. In Section 5, we present the syntax and accompanying guidelines of the proposed framework. Section 6 reports on the evaluation, comprising both a prototype demonstration and a real-world use case. Finally, Section 7 summarizes our findings and discusses avenues for future research.

2 Background

2.1 Security Control Modeling in IEC 62443

This work is based on the IEC 62443 standard for illustrating the modeling of industrial security controls. To provide context for the subsequent sections, we briefly introduce the scope and structure of the IEC 62443 series. *IEC 62443 was developed to secure Industrial Automation and Control Systems (IACS) across their entire lifecycle* [13]. It defines a comprehensive framework for industrial cybersecurity, including structured control catalogs and Security Level (SL) classifications (SL 0–4).

Part 3-3 of IEC 62443 specifies seven *Foundational Requirements* (FRs) that guide the design of system-level protections:

FR1 – Identification and Authentication Control All users (humans, processes, devices) must be uniquely identified and authenticated before gaining system access.

FR2 – Use Control Limit the actions of authenticated entities (humans, processes, devices) to their assigned privileges and monitor privilege use.

FR3 – System Integrity Protect the integrity of information in communication channels and data repos-

[1] https://www.bpmn.org/

itories to prevent unauthorized modification or execution.

FR4 – Data Confidentiality Safeguard information in transit and at rest to prevent unauthorized disclosure.

FR5 – Restricted Data Flow Segment the system into zones and conduits to limit unnecessary or insecure data transfer.

FR6 – Timely Response to Events Detect and respond to security violations by notifying responsible parties, preserving forensic evidence, and applying corrective actions.

FR7 – Resource Availability Protect against denial-of-service conditions to maintain availability of essential system functions.

Each FR is supported by detailed *Security Requirements* (SRs), which form the basis for control selection and compliance validation. Our framework leverages this structure by formalizing selected SRs as machine-readable policy definitions. Controls are chosen according to SL targets and linked to specific system assets, workflows, or communication flows, ensuring traceability from design to runtime enforcement.

2.2 IEC 62443-2-1 Lifecycle for Industrial Systems Security

The secure design and operation of industrial systems requires a structured, lifecycle-oriented approach to cybersecurity. The IEC 62443-2-1 standard [14] defines a *Security Program Lifecycle* that provides a foundation for managing risks, implementing appropriate controls, and maintaining compliance throughout the operational life of an IACS. This lifecycle consists of eight interconnected phases, spanning from initial policy definition and risk assessment to system operation and eventual decommissioning.

To achieve continuous security and regulatory compliance in IIoT environments, security mechanisms must be embedded across all lifecycle phases. In practice, however, many organizations struggle to bridge the gap between design-time control specifications and their runtime enforcement and monitoring. Our framework addresses this challenge by aligning formal, machine-readable security control models with the IEC 62443-2-1 phases. This ensures that security controls are consistently defined, modeled, validated, and enforced throughout the system's lifecycle, enabling lifecycle-aligned security management for IIoT systems.

Table 1 provides an overview of the IEC 62443-2-1 lifecycle phases and illustrates how the proposed framework supports each step. It also shows that while the framework fully covers all phases up to runtime enforcement, decommissioning remains out of scope and is noted as a potential area for future extension.

2.3 SIREN – Security Modeling

The SIREN (Security Iiot pRocEss Notation) project addresses security in industrial processes by integrating controls from the IEC 62443-3 series and converting them into monitorable policies [11]. It promotes security-by-design in IIoT environments by embedding security controls directly during the process modeling stage. The method consists of three core steps:

1. **Process Modeling:** Model the process, including participants, dependencies, and security controls from a predefined catalogue, to achieve target SLs.
2. **XML Parsing and Rule Derivation:** Parse the model's XML representation using an object-oriented approach to derive communication and entity rules.
3. **Monitoring:** Feed the derived rules into the Suricata network monitoring system; forward detected deviations to the Security Operations Center via the Wazuh platform.

While SIREN offers a useful framework for integrating security into IIoT process models, it has several limitations:

- No formal syntax for defining control attributes, leading to inconsistent representations.
- Lack of standardized modeling policies, limiting flexibility across use cases.
- Absence of automated verification to ensure adherence to syntax and policies.

The SCMV approach [15] extends SIREN by adding compliance checks to verify whether modeled processes meet IIoT standards such as IEC 62443. SCMV also introduces a structured method for process representation and compliance checking. However, like SIREN, SCMV does not define a formal control syntax and does not verify whether models adhere to such a syntax. Its focus remains on compliance evaluation rather than model validation.

The framework presented in this paper addresses the limitations of both SIREN and SCMV by introducing a comprehensive, lifecycle-aligned methodology for specifying, validating, and enforcing security-aware IIoT processes. Key advancements are discussed in Section 4.2.

To support formal, lifecycle-oriented control specification, our approach uses BPMN as a structural representation for security-relevant workflows and control

Table 1 Integration of the Proposed Framework into the IEC 62443-2-1 Security Program Lifecycle

Lifecycle Phase	IEC 62443-2-1 Description	Implementation in Proposed Framework	Support
1. Security Policy & Organization	Establish cybersecurity governance, assign responsibilities, and define organizational structure.	Define a control catalog and modeling methodology to support consistent policy specification and enforcement.	◖
2. Risk Assessment & Threat Modeling	Identify critical assets, vulnerabilities, and threats, and determine required SLs.	Select controls based on risk-informed mappings to assets, workflows, and communication flows in the policy model.	◖
3. Security Requirements Definition	Specify technical and procedural controls to mitigate identified risks.	Use a formal syntax to define machine-readable controls (e.g., `encryption: true`) and link them to operational components.	●
4. System Design & Integration	Incorporate controls into system architecture and communication design.	Embed controls in BPMN-based workflow models to integrate them into operational behavior and data flows.	●
5. Implementation	Deploy defined controls into the system environment.	Parse policy definitions and convert them into executable enforcement rules for runtime application.	●
6. Validation & Testing	Verify correct implementation and effectiveness of controls.	Run syntax checks and consistency validation to confirm correct policy configuration.	●
7. Operation & Maintenance	Operate, monitor, and update the system and its security configuration.	Enforce rules at runtime using a policy enforcement module integrated with Suricata/Wazuh for continuous compliance monitoring.	●
8. Decommissioning	Retire systems and securely remove assets.	Not currently supported; potential future extension for policy-based decommissioning verification.	○

Legend: ● = fully supported, ◖ = partially supported, ○ = not supported.

assignments. While BPMN originates from BPM, it is employed here as a technical enabler rather than a conceptual focus. Its graphical notation and XML-based structure support consistent policy definition, parsing, and translation into machine-executable policies.

3 Related Work

3.1 Threat Modeling in IIoT Systems

Threat modeling is a core activity in the IEC 62443-2-1 lifecycle, supporting the identification of assets, vulnerabilities, and potential attack paths. Several established methodologies have been adapted to the industrial and IIoT context.

The **STRIDE** model, originally developed by Microsoft for IT systems [16], has been applied to ICS networks by mapping spoofing, tampering, repudiation, information disclosure, denial of service, and elevation of privilege to industrial scenarios [17]. While STRIDE offers a systematic taxonomy of threats, it does not prescribe how identified risks are linked to enforceable runtime controls, making integration into operational workflows difficult.

Attack Trees offer a familiar diagrammatic technique to model attack paths, notably used in SCADA/ICS contexts [18]. However, traditional Attack Trees rely on static, manually crafted structures that can become outdated as system configurations evolve. More advanced versions such as Sequential-AND Attack Trees enhance expressiveness and temporal modeling; e.g., Maynard et al. [19] use these to model real-world ICS attacks within the ICS Kill Chain framework. Despite these enhancements, threat modeling via attack trees remains resource-intensive and does not seamlessly translate into automated, enforceable runtime controls, reinforcing the need for process-integrated policy modeling that our approach enables.

The **MITRE ATT&CK for ICS** framework [20] provides a comprehensive knowledge base of adversary tactics and techniques specific to industrial systems. It is widely used for mapping observed behaviors during incident analysis. However, its focus is descriptive rather than prescriptive: ATT&CK does not define how identified threats should be translated into preventive controls or embedded into design-time models.

More recently, **STPA-Sec** [21] has been applied to industrial processes to identify unsafe control actions from a systems-theoretic perspective. STPA-Sec excels at modeling safety–security interactions but lacks direct support for generating machine-executable security policies or integrating them into operational monitoring.

In summary, existing threat modeling methods for IIoT and ICS provide structured ways to identify and classify threats, but they generally stop short of bridging the gap between identified risks and automated runtime enforcement. Our framework addresses this gap by linking risk-informed control selection directly to BPMN-based process models and by compiling these controls into executable policies for continuous compliance monitoring in dynamic IIoT environments.

3.2 Security Lifecycles & Standards

Security lifecycle models and established frameworks such as IEC 62443-2-1 and the NIST Cybersecurity Framework (CSF) provide clear guidance on managing cybersecurity across the entire system lifecycle.

IEC 62443-2-1 defines the *Automation Solution Security Lifecycle*, consisting of eight phases from organizational setup and risk assessment to final system decommissioning [14]. It serves asset owners as a process-oriented governance model for implementing cybersecurity programs in industrial control systems. Related standards extend this lifecycle to product manufacturers: IEC 62443-4-1 and IEC 62443-4-2 specify secure development practices, testing procedures, and patch management for components and systems [22].

The NIST CSF offers a widely adopted, risk-based governance model structured around five core functions: Identify, Protect, Detect, Respond, and Recover [23]. The NIST CSF is internationally recognized and applicable to organizations of all sizes, providing a flexible approach to managing cybersecurity risks.

Despite differences in scope and terminology, both IEC 62443 and the NIST CSF emphasize the continuous application and reassessment of security measures throughout the system's lifecycle. This principle underpins our approach, which formalizes security controls and integrates them into process models in a lifecycle-oriented manner, ensuring that both design-time intent and runtime enforcement remain aligned.

3.3 Formal Policy & Control Specification

A key challenge in cybersecurity engineering is the formal specification of security controls in a format that is both human-readable and machine-executable. Existing policy languages such as XACML (eXtensible Access Control Markup Language) and Rego (used by Open Policy Agent, OPA) provide structured formats for defining access control policies in distributed systems [24,25]. These approaches enable centralized policy management and automated enforcement through dedicated engines. However, they are typically decoupled from process-oriented system models and lack explicit integration with operational workflows in industrial environments.

In the context of industrial automation, recent research has explored formal approaches to specifying security controls based on established cybersecurity standards. Hosseini et al. [26,27] propose an OWL-based ontology to capture the semantics of IEC 62443 controls, enabling machine-readable modeling and automated reasoning via SQWRL. While their work supports security-by-design during system engineering, it does not extend to embedding controls in executable workflows or runtime models.

Amorim et al. [28] define formal protocol specifications to express expected behavior in ICS environments, offering high precision and strong verification capabilities. Similarly, Lanotte et al. [29] present a logic-based policy framework for specifying security properties in industrial systems. Although these approaches advance control formalization, they remain abstracted from dynamic process integration and do not inherently support lifecycle-aligned enforcement.

In contrast, our work introduces a structured policy syntax embedded directly into BPMN-based workflows. This allows IEC 62443-3-3 controls to be specified, validated, and linked to process activities, data flows, and runtime entities. By combining formal syntax with process integration, our approach bridges the gap between static policy formalisms and executable, continuously enforceable models.

3.4 Runtime Enforcement & Compliance Monitoring

Ensuring that defined security controls are consistently enforced during system operation is essential for resilient industrial automation. While formal policy modeling provides the foundation, practical enforcement requires integration with the system's communication, execution, and monitoring layers.

Amorim et al. [28] demonstrate how formally verified protocol specifications can be compiled into runtime monitors for detecting deviations from expected behavior in ICS networks. This enables dynamic attestation of message sequences and protocol compliance, but remains focused on communication-level behavior rather than broader lifecycle-aligned compliance.

Lanotte et al. [29] propose a runtime enforcement architecture for IIoT based on temporal logic, where user-defined security policies are automatically translated into enforcement monitors. Their approach targets low-level event verification in distributed systems,

yet does not explicitly integrate industrial cybersecurity standards such as IEC 62443 or provide structured modeling guidance.

Ontology-based models from Hosseini et al. [26,27] focus primarily on the specification phase. While their semantic representation could be leveraged for runtime analysis, enforcement mechanisms are not within their scope.

Our framework addresses these gaps by linking formalized IEC 62443 controls directly to executable process elements. A transformation pipeline converts modeled policies into machine-executable rule sets, which are then enforced at runtime via network- and host-level monitoring tools such as Suricata and Wazuh. This enables both inline enforcement and continuous compliance monitoring, ensuring that operational behavior remains aligned with the defined control objectives and the IEC 62443-2-1 and 62443-3-3 lifecycle phases.

3.5 Process Model-driven Security for IIoT

Several approaches have sought to embed security concepts directly into process modeling languages, particularly BPMN. For example, SecureBPMN [30] integrates access control concepts into BPMN through dedicated security annotations. Similarly, the SIREN framework [11] extends BPMN to support modeling of IEC 62443-related controls in IIoT scenarios. Other studies propose ontology-based representations or domain-specific languages to capture security semantics within process models [31,32].

In the IIoT domain, further BPMN extensions have introduced IoT-specific elements such as sensors, cloud services, and edge devices [33,34], increasing the expressiveness and potential executability of process models in operational contexts. While these approaches enhance design-time modeling, they generally stop short of providing mechanisms to automatically derive enforceable security policies or validate them during runtime. This lack of runtime integration limits their applicability in dynamic, heterogeneous industrial environments, where continuous enforcement and monitoring are critical for maintaining compliance with standards such as IEC 62443.

4 Methodology and Framework Design

4.1 Artifact Composition based on Design Science Research

This work adopts a structured engineering methodology based on the Design Science Research (DSR) framework proposed by Hevner et al. [35]. DSR is widely applied in information systems research to develop and rigorously evaluate artifacts that address complex socio-technical problems. In this study, DSR guides the development of a technical solution that enables the specification and enforcement of lifecycle-aligned security controls in IIoT environments. The resulting framework addresses a critical challenge in operational cybersecurity: the absence of machine-readable and verifiable mechanisms for aligning industrial processes with established security standards, such as IEC 62443, by runtime.

The DSR methodology is operationalized through seven guidelines, which provide a flexible yet structured approach for artifact development. These guidelines are applied below. However, the order and type of realization are not strictly defined to avoid restricting the creativity of the researchers.

- **Design as an Artifact.** The research results in a tangible artifact: a modeling framework with a formal syntax tailored for process-oriented IIoT security management.
- **Problem Relevance.** The addressed problem is relevant for both research and practice as discussed in Section 1. Industrial environments face increasing cybersecurity risks, and compliance with standards such as IEC 62443-3 is a key mitigation strategy. However, no automated mechanisms currently exist to verify whether industrial processes satisfy these controls.
- **Design Evaluation.** The artifact is evaluated through a case study in Section 6, in which its applicability is demonstrated via prototype implementation, alignment with design objectives, and an assessment of usability and practical relevance.
- **Research Contribution.** The framework provides a novel contribution to the state of the art by combining a formalized syntax with runtime enforcement capabilities, thereby advancing knowledge on process-oriented IIoT security management.
- **Research Rigor.** Artifact development is conducted using established scientific methods to ensure transparency and reproducibility. The design process follows an iterative and solution-oriented approach, encompassing three key phases: (1) formal specification of security controls, (2) integration of controls into structured operational models, and (3) enforcement at runtime through monitoring and validation. Each phase is documented comprehensively and is informed by both academic best practices and industrial requirements.
- **Design as a Search Process.** The artifact emerges from an iterative search process that builds upon prior research (Hornsteiner et al. [11]) and ex-

tends previously developed concepts to meet new requirements in IIoT cybersecurity.
– **Communication of Research.** The artifact and its implementation are publicly accessible, facilitating dissemination among both academic and industrial communities and serving as a reference for security policy enforcement in process-driven IIoT environments.

4.2 Framework Components and Objectives

The proposed framework comprises three integrated components:

– **Formal Control Syntax:** A structured, machine-readable syntax for expressing security controls based on IEC 62443. It uniformly defines how the controls are named, enabling them to be integrated into security monitoring at a later stage (e.g. `encryption: true`).
– **Control Assignment Rules:** A set of modeling guidelines for mapping security controls to operational actions, system assets, and communication links within modeled workflows.
– **Runtime Enforcement Pipeline:** A technical implementation for validating control syntax, translating controls into executable rules, and enforcing them at runtime using established monitoring tools.

To evaluate the completeness and functional adequacy of the framework, four design objectives were defined, building upon the work of Haverinen et al. [36], which deals with aspects of IEC 62443-4-1.

1. **Consistent Syntax:** The framework must provide a structured standardized, unambiguous syntax for defining security controls to enable cross-domain consistency and standard compliance.
2. **Control Integration Rules:** The framework must define explicit modeling guidelines that allow controls to be accurately and systematically associated to relevant operational entities.
3. **Error Detection and Validation:** The framework must include a mechanism to validate control definitions and assignments to detect syntactic or semantic inconsistencies.
4. **Runtime Usability:** The framework must enable the extraction and execution of defined controls as machine-readable policies, supporting enforcement through existing monitoring infrastructures.

Each design objective aligns with one or more framework components: Objectives 1 and 2 correspond to the formal syntax and modeling rules, whereas Objectives 3 and 4 address technical validation and runtime enforcement.

Despite its benefits, the framework has some limitations. Its current scope is limited to IEC 62443; future work will extend support to additional security standards (e.g., NIS2) to increase applicability. Moreover, industrial processes are often dynamic, whereas the present approach requires manual model updates. Automating model adaptation in response to evolving security threats remains an important direction for future research.

5 Syntax and Modeling Guidelines for BPMN-Based Security

5.1 Standardized Syntax for Security Controls

Building on the methodology and objectives defined in the previous section, this section introduces the formal policy specification syntax and modeling guidelines used to define and apply machine-readable security controls within BPMN-based workflows.

Each security control is aligned with the SRs of IEC 62443-3-3 and categorized according to their respective FRs. To ensure consistent specification, validation, and runtime enforcement, we define a structured syntax for expressing controls in process models.

This work is conceptually informed by the ontology-based modeling approach proposed by Hosseini et al. [26,27], who developed formal ontologies to represent IEC 62443 controls in engineering and automation system contexts. While their focus lies on semantic modeling and reasoning using OWL and SQWRL, our contribution extends this foundation by embedding control logic directly into executable workflow models. This enables automated compliance checking and integration of policy semantics into operational runtime behavior.

To that end, security controls are represented as key-value pairs, using a `:` (*Colon*) as a separator between the control key and its value (e.g., `encryption: true`).

```
controlName: controlValue;
```

Lines must always conclude with ";" (*Semicolon*).

```
protocolType: Kerberos;
```

In this case, `protocolType` represents the control, and `Kerberos` is the associated data value of the "list" data type. When a control contains multiple data values, they are enclosed in square brackets and separated by "," (*CommaSpace*).

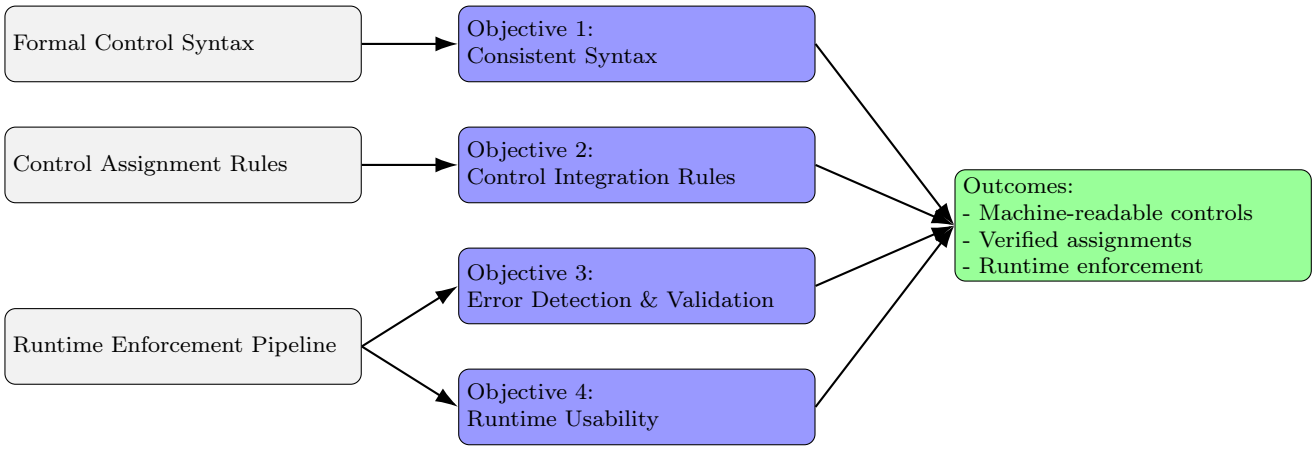


Fig. 1 Mapping of framework components to design objectives and outcomes.

```
protocolType: [Kerberos, EAP];
```

Multiple tuples or controls should be separated by ";" (*SemicolonNewLine*).

```
protocolType: [Kerberos, EAP];
isHuman: true;
```

Variable names are consistently written in `camelCase`, and the specified syntax must be adhered to in order to ensure proper parsing of the controls. Only the defined values are permitted for data values. The associated data type and possible values have been specified for each control. 2 presents selected example controls, along with their data type, value range, and the SRs they measure, which are used in the examples provided in this paper.

5.2 Security-Oriented Modeling of Participants (Pools and Lanes)

To support security-relevant modeling and enable the enforcement of control policies on a per-entity basis, each process participant (e.g., machine or system component) is explicitly modeled as a distinct resource within the BPMN diagram. These participants are represented as separate pools, following a one-to-one mapping between operational entities and process participants.

If a machine comprises multiple functional or network-visible components (e.g., individual robotic arms with separate control logic or network interfaces), these are modeled using multiple lanes within the pool. This structure provides a clear basis for assigning security controls at both the machine and subcomponent level.

Each participant is annotated with a Basic Identity (BI) object, a structured data object that captures key security-relevant controls such as IP address, protocol stack (IPv4/IPv6), operating system, version, and MAC address. This information defines the technical identity and communication interface of the entity, which is essential for associating process activities with runtime enforcement mechanisms (e.g., firewalls, IDS, policy agents).

In models where a participant is divided into multiple lanes, the BI object is placed in the uppermost lane by default. If each component has distinct network identifiers or security configurations, a separate BI is attached to each lane. The BI object is labeled *BI* and is positioned in the upper left-hand corner of the respective lane or pool. Figure 2 illustrates two examples: (left) a machine with a shared IP address across all components, and (right) a machine where each lane communicates via its own IP address.

5.3 Control Grouping and Enforcement Scope

In addition to the formal syntax, the SIREN framework defines grouping rules that classify security controls based on their enforcement context. This classification enables users to extend the framework with custom controls, while ensuring their correct representation and interpretation within the model.

Each FR from IEC 62443 is represented in the process model as a data object, labeled with its corresponding number (FR-1 to FR-7). Associated SRs that must be fulfilled at a specific point in the process are annotated as text labels attached to the relevant process element. A single process object may be linked to multiple FRs, and each FR may reference several SRs, depending on the security context.

Control Name	Data Type	Data Value	Measurable SRs
auditLog	boolean	true / false	6.1, 6.2
certificateUsed	boolean	true / false	1.8, 1.9
componentInventory	boolean	true / false	7.8
configurationExistence	boolean	true / false	7.6
cryptographyUsed	boolean	true / false	4.1
encryption	boolean	true / false	1.7, 1.10
identificationScheme	list	IP, MAC, uCode	1.1; 1.2; 1.6; 1.13
identifier	list		5.1, 5.2, 5.3, 5.4
isHuman	boolean	true / false	1.2, 1.3, 1.4, 2.1, 2.2, 2.3, 2.4, 2.12
monitoringConfiguration	list		6.2
passwordLength	integer	1 – 40	1.7
protocolType	list	Kerberos, EAP, IPSec, Access-list, IP/MAC-Filtering, MQTT	1.2, 1.3, 1.6, 1.8, 1.9, 1.10, 1.11, 2.1, 2.2, 2.3, 2.4, 3.1, 3.4, 3.8, 5.1, 5.3, 5.4
tlsUsed	boolean	true / false	1.2, 1.6, 3.1, 3.4, 3.8, 4.1

Table 2 Table of controls, data type, values and assigned SRs.

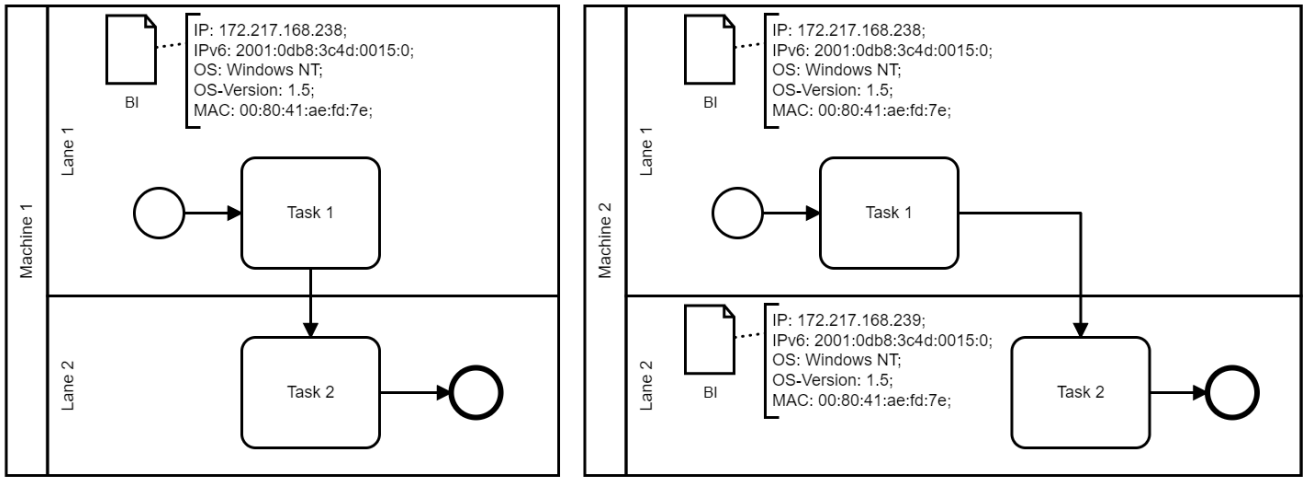


Fig. 2 Illustration of a machine with a single IP address for communication (left), and a machine with multiple lanes, each utilizing distinct IP addresses (right).

The assignment of controls is context-dependent, meaning a single control may apply to multiple scopes depending on its intended effect (e.g., a cryptographic requirement may influence both machine configuration and communication flows). Table 2 provides illustrative examples of controls in each group.

To support context-aware enforcement, the controls defined in the SRs are categorized into three enforcement scopes:

Communication Controls. These refer to security measures applied to the communication between distributed process participants (e.g., encryption, authentication, secure channels). This group comprises security controls that govern the *protection of communication flows* between two or more process participants within a networked industrial system. These controls typically enforce e.g. secure channels, message integrity, authentication, or encryption.

Communication between participants is modeled using `throwing` and `catching message events` in BPMN. Security-related FRs are attached to the `throwing message event` as data objects (documents), and the associated SR are represented as annotations linked to the corresponding FR.

To preserve semantic clarity and directionality, the control flow arrow must always originate from the data object and point towards the throwing message event. Each throwing message event is linked to exactly one catching message event or pool, reflecting a one-to-one communication channel, this is shown in Figure 3. Multiple FRs may be assigned to a single communication instance, and each FR may encompass several individual control statements. Controls that can be assigned to the group are, for example:

`tlsUsed` The control determines whether a TLS connection is used. This must be used for communica-

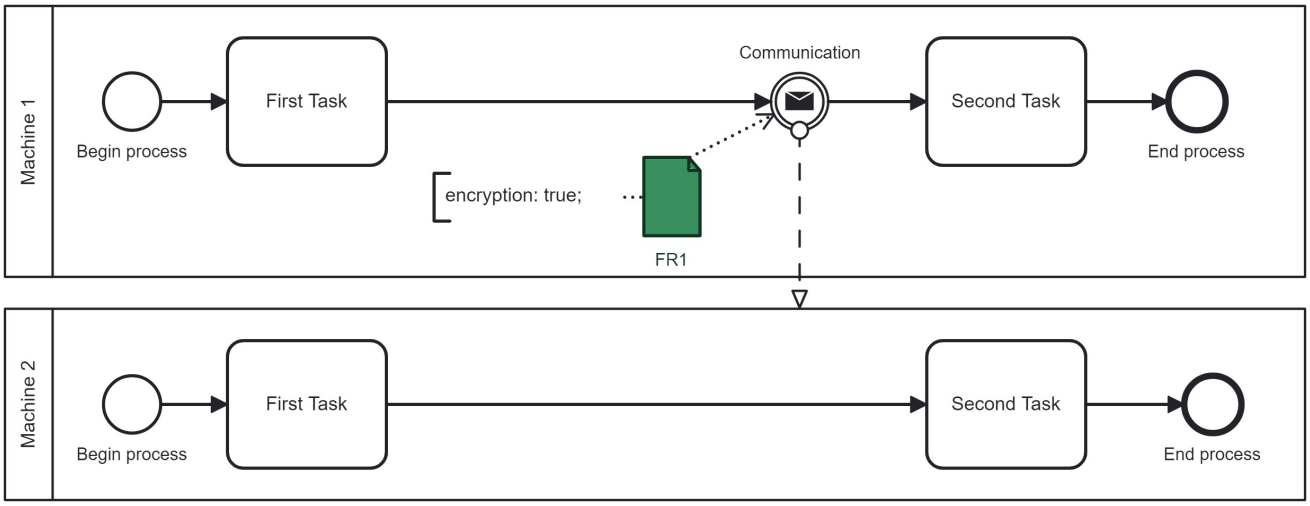


Fig. 3 Illustration of how an control from FR1 is attached to a communication path.

tion between resources and is assigned to the communication.

`encryption` The control describes whether communication between the resources must be encrypted and is then assigned to the communication.

Task Controls. These govern the security of individual process steps, such as the use of trusted software, authorization checks before execution, or integrity validation of inputs. Controls that are used or checked when executing a specific task or that must be observed when executing an explicit task are attached to the task itself. As before, the FR is attached to the task with the direction of the arrow pointing towards the task. The connected SRs are located on the FR (see the blue FR2 in Figure 4). It is possible to assign several FRs to one task and to assign several controls to one FR. Controls that can be assigned to tasks are, e.g., `isHuman`, or `passwordLength`. However, it is not possible to provide an conclusive list of possible controls, as these differ depending on the environment and the desired SL. Controls that could affect the execution of a task could include for example the following:

`isHuman`
The control describes whether a task must be explicitly executed by a person or confirmed before execution.

`passwordLength`
The control specifies how many characters a password must contain in order to check whether the password length is sufficient when logging in to perform a task.

Resource Controls. These target the configuration and security state of machines and components involved in the workflow (e.g., patch level, hardening status, interface lockdowns). Controls that are assigned to an individual resource, for example a machine, must be modeled in the lane of the resource, in the bottom left-hand corner. The FRs are modeled as documents with attached SRs. The FRs are not linked to other model elements. An example can be seen in Figure 5 by the red FR7. It is possible to assign several FRs to one lane and to assign several controls to one FR. Controls that can be assigned to the group are, for example:

`auditLog`
The control states that a machine generates audit logs of its activities.

`protocolType`
The control specifies which protocol type must be used for communication between re- sources. For example, the control could also be used for a resource if it always uses a specific protocol type.

5.4 Automated Error Detection based on Regular Expressions

A significant aspect of the developed artifact is the verification of syntax and modeling policies, which ensures proper alignment between these policies and various controls. Successful automation of process execution requires strict adherence to a predefined structure. Security controls should be represented within BPMN annotations, with each control type following its specified syntax; verification should occur for every pool and lane within the process model. Consequently, error detection is one of the defined requirements and must be integrated into architectures that implement this artifact. BPMN diagrams can be exported as XML

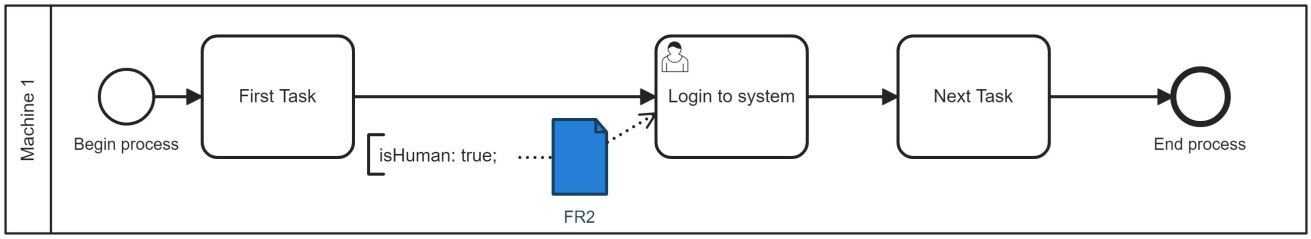


Fig. 4 Illustration how an control from FR2 is attached to a specific task.

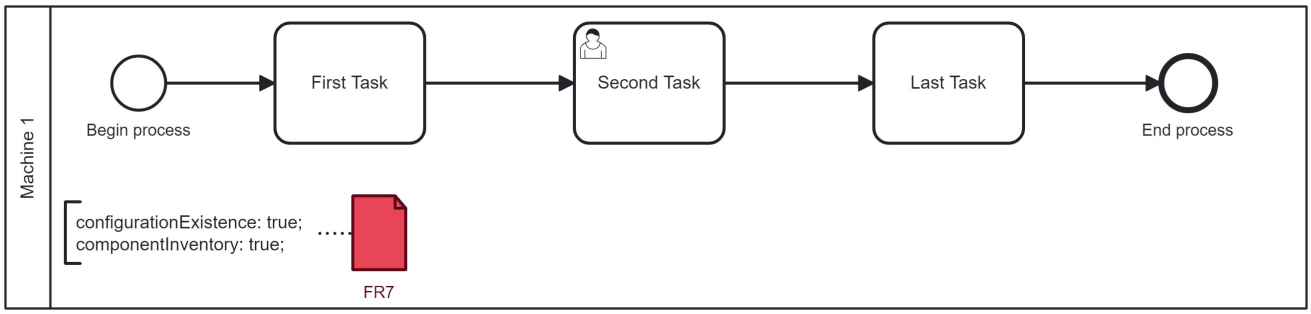


Fig. 5 Illustration how two controls from FR7 are attached to a resource presented by a lane.

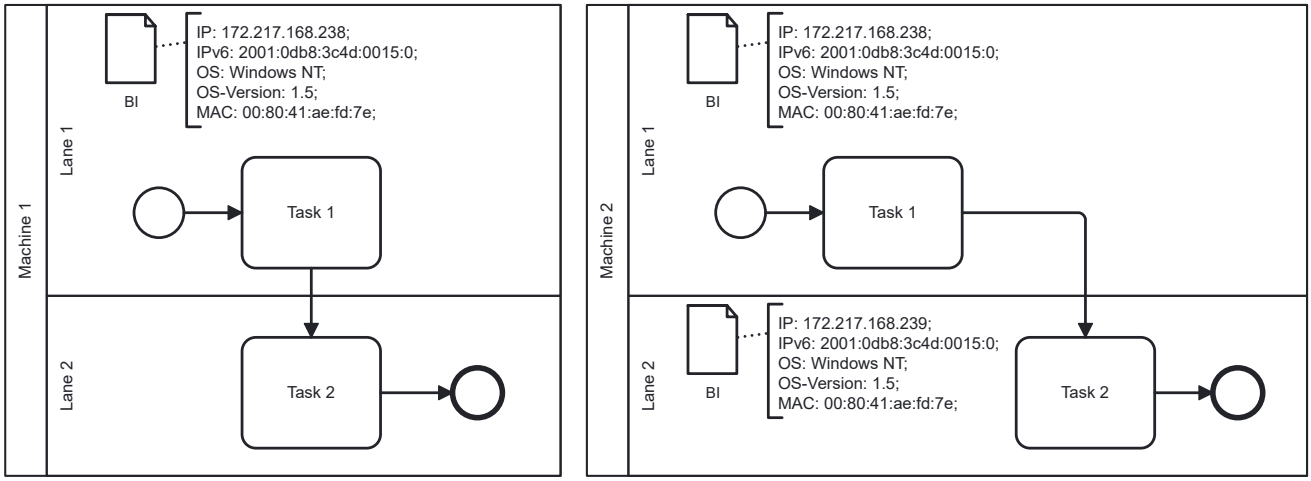


Fig. 6 Illustration how controls from different FRs are attached.

files using specific XML schemas, allowing syntax verification via regular expressions. Listing 1 provides an example of error detection and verification of modeled controls. Following these steps, the architecture should identify any non-compliance of modeled controls with the defined policies. Once verification is complete, the extracted controls and other relevant data can then be prepared for further processing. Finally, the information extracted from the XML is prepared in a machine-readable format that a subsequent system can use it. 1 provides an example of error detection and verification of the controls.

```
mixed_pattern = re.compile(
    r'^\s*\w+\s*:'
    r'\s*([\w.:]+|'
    r'\[\s*([\w.:]+\s*,\s*)*[\w.:]+\s*\])\s*$')
```

Listing 1: Regular expression to check the match of BPMN controls with defined controls.

6 Evaluation

In DSR, creating and testing a prototype is regarded as a sufficient form of evaluation, since it allows researchers to validate key design decisions, gather early feedback, and iteratively refine the artifact before full deployment. As Peffers et al. [37] point out, a prototype

helps demonstrate both the feasibility and utility of a design-science artifact in a realistic setting. In line with this principle, we developed a working prototype of our modeled controls framework and evaluated it using an industrial use case.

6.1 Practical Use Case

To evaluate the proposed concepts, they were applied to an industrial process provided by a well-established manufacturing organization, whose name cannot be disclosed for confidentiality reasons. The use case involves a process section where a component is transported into a heating oven and heated to 85°C. The heating process must be explicitly authorized by an employee. Following heating, a mass is added to the component, and the discharge height is measured. If the component is filled beyond the acceptable height, it is deemed defective. In such cases, a notification is sent to the Process Control System (PCS), indicating that the defective component, identified by its component ID, is exiting the process and will be sent to a reject box. If the component is not defective, it is transferred to a goods carrier and subsequently reheated to 85°C, which again requires employee approval. Afterwards, the component undergoes a cooling period of four hours. The use case contains FRs relevant to IEC 62443-3. The applicable FRs were identified in collaboration with process experts. Security-related controls were first collected and then mapped to the appropriate FRs. A corresponding control for each FR was defined, adhering to the specified syntax and value range. The relevant FRs and controls are outlined as follows:

FR1: When operating the oven, a person must explicitly authorize heating and have a organization-specific user ID, therefore `isHuman` and `idExists` must have the value `true`. This applies to both tasks where the oven is heated. These are therefore task contols.

FR3: The message the oven sends to the PCS must have the value `mqtt` for `protocolType`.

FR4: The message to the PCS must also be sent in encrypted form, therefore `cryptographyUsed` must be `true`.

FR6: The oven must keep a log showing which employees were logged in when, and which authorizations were given when. Therefore `auditLogs` must be `true`.

The model of the described process with FRs and controls can be seen in Figure 7.

6.2 Evaluation of Syntax and Modeling Policies

This section evaluates whether the developed artifact fulfills the design objectives set out in Section 4.2 and can answer the corresponding research questions. In order to evaluate the design objectives, *(I)* the implemented use case in Section 6.1 was considered and *(II)* the usability of the results was demonstrated using an analysis tool. The first design objectives for the artifact, to provide a *consistent syntax*, was implemented by defining syntax policies in Section 5.1. The syntax provides clear specifications how an control has to be named and written. The policies are standardized and without exception, so they can be applied universally. Users can therefore define controls themselves and integrate them into the existing application. The syntax is independent of the user group and can be used in different sectors and for different purposes. Examples used here for the application of IEC 62443-3 can also be transferred to other guidelines (e.g. NIS2). The syntax restricts the possible data types and provides precise information about the assignment of their values and the use of multiple values, there is no longer any ambiguity. The defined syntax was used in the use case in Section 6.1, whereby all possibilities for implementing the syntax were included. This section demonstrates that a seamless application is achievable, thereby meeting the first design objectives for a consistent and structured syntax in the formulation of controls. This consistency ensures applicability across diverse user groups and industry contexts. The second MR for the artifact, to provide *modeling rules*, was addressed by defining policies for grouping controls, as detailed in Section 5.3. These policies specify how defined controls can be mapped and utilized within a process, achieved by categorizing controls into three distinct groups, with each control assignable to at least one category. The categories are then modeled in alignment with the developed policies. In designing these policies, adherence to the standardized BPMN modeling conventions was ensured, allowing compatibility across any BPMN-supporting tools. The policies integrate the consistent syntax established in the first design objective and were demonstrated as universally applicable through their use in the case study presented in Section 6.1. The artifact effectively represents the necessary information in process models, fulfilling the second design objective.

6.3 Prototypical Implementation

The first two components of the artifact, the syntax definition and the policies for mapping compliance controls into the process model, satisfy the first two design

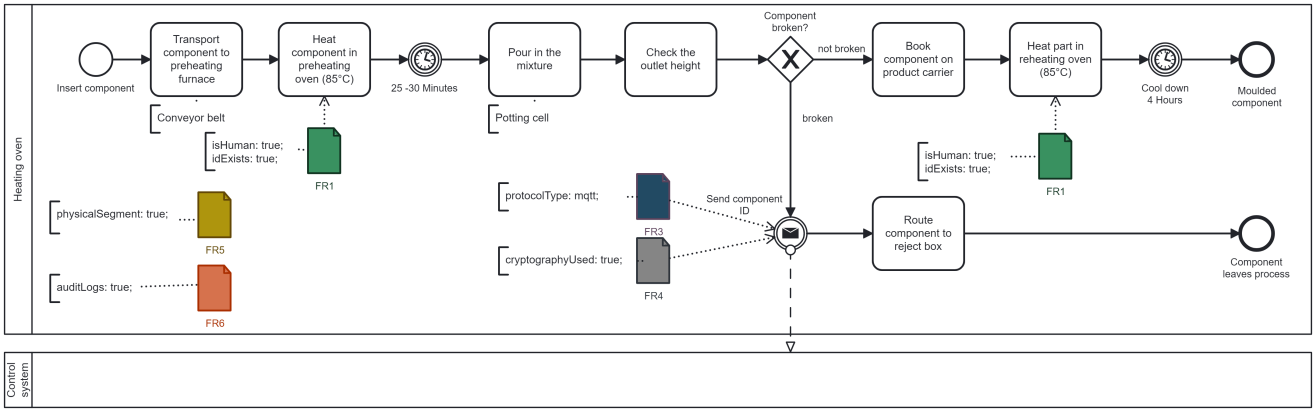


Fig. 7 Process for heating and filling components that must fulfill IEC 62443 controls.

objectives, as previously outlined. To further evaluate the artifact's capabilities in *Error Detection* and *Usability of Results*, a prototype has been developed that tests the syntax within a practical use case. This use case, termed compliance monitoring, involves network-based monitoring of security standards compliance [15]. In this context, the modeling syntax and associated policies are integrated into an existing monitoring solution, which is enhanced with an error detection module. Figure 8 illustrates the prototype architecture, implementing design objectives 1 through 4, accessible on GitHub[2].

In (1) and (2) the syntax is implemented into an actual BPMN process modeled within the tool Camunda[3]. The artifacts syntax definition uses lane annotations to display different controls, that can be used within the FRs of the IEC 62443 3-3 control catalog. Camunda allows for the export of the BPMN as the XML representation, which is used as the input for the main part of the artifact. Based on previous work, a python-based Parser was enhanced to be able to exclusively read the Syntax and modeling policies, defined in (1) and (2). This parser was also extended to fulfill (3), by implementing an error detection module, and (4), by connecting the new and improved parser to the original use case of compliance monitoring for further processing.

7 Conclusion

This paper presents a novel framework for integrating security controls in IIoT processes. Using the SIREN notation and the IEC 62443 standard as a basis, a formal syntax is developed that enables the systematic incorporation of security controls into process models. The key contribution is the modeling framework with formal syntax. The evaluation of the approach through a real-world use case demonstrates its practical applicability and effectiveness in enhancing process security. By embedding security controls during the process design stage and continuously monitoring compliance, this framework offers organizations a proactive tool to secure their industrial systems. Its adaptability across various industries makes it a solution for different security needs.

One promising avenue is the use of Large Language Models to further validate and refine security models. These could be employed to explain security controls in process models, evaluate compliance of processes with security standards, identify potential weaknesses, and suggest improvements, potentially leading to more efficient model adjustments and higher security standards. In conclusion, this research provides a robust foundation for managing security in IIoT environments. By integrating security by design, it offers a scalable solution that can be applied across industries, ensuring compliance with evolving cybersecurity controls and helping organizations mitigate the risks associated with increasingly interconnected industrial processes.

[2] https://github.com/mahopy/siren.exe
[3] https://camunda.com/download-camunda-7/

References

1. Maria Rita Palattella, Mischa Dohler, Alfredo Grieco, Gianluca Rizzo, Johan Torsner, Thomas Engel, and Latif Ladid. Internet of things in the 5g era: Enablers, architecture, and business models. *IEEE journal on selected areas in communications*, 34(3):510–527, 2016.
2. Emiliano Sisinni, Abusayeed Saifullah, Song Han, Ulf Jennehag, and Mikael Gidlund. Industrial internet of things: Challenges, opportunities, and directions. *IEEE transactions on industrial informatics*, 14(11):4724–4734, 2018.
3. Martin Serror, Sacha Hack, Martin Henze, Marko Schuba, and Klaus Wehrle. Challenges and opportunities in securing the industrial internet of things. *IEEE*

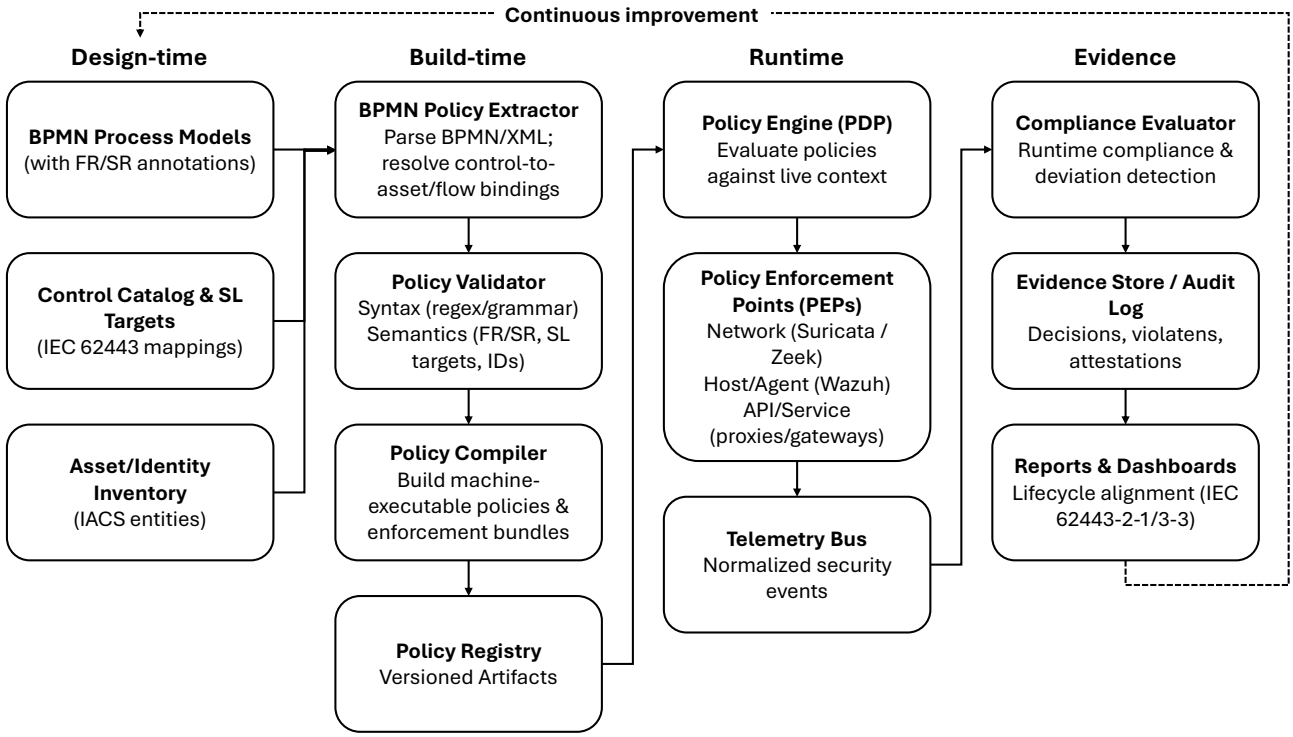


Fig. 8 End-to-end architecture of the lifecycle-aligned framework for specifying, validating, enforcing, and evaluating IEC 62443-based security controls.

Transactions on Industrial Informatics, 17(5):2985–2996, 2020.

4. Stefan Schönig, Markus Hornsteiner, and Christoph Stoiber. Towards process-oriented iiot security management: Perspectives and challenges. In *Enterprise, Business-Process and Information Systems Modeling*, pages 18–26, Cham, 2022. Springer International Publishing.
5. Lubna Luxmi Dhirani, Eddie Armstrong, and Thomas Newe. Industrial iot, cyber threats, and standards landscape: Evaluation and roadmap. *Sensors*, 21, 06 2021.
6. Koen Tange, Michele De Donno, Xenofon Fafoutis, and Nicola Dragoni. A systematic survey of industrial internet of things security: Requirements and fog computing opportunities. *IEEE Communications Surveys & Tutorials*, 22(4):2489–2520, 2020.
7. Ivan Cindrić, Marko Jurčević, and Tamara Hadjina. Mapping of industrial iot to iec 62443 standards. *Sensors (Basel, Switzerland)*, 25(3):728, 2025.
8. Nikita Bhardwaj and Peter Liggesmeyer. A runtime risk assessment concept for safe reconfiguration in open adaptive systems. In *International Conference on Computer Safety, Reliability, and Security*, pages 309–316. Springer, 2017.
9. Alessandro Di Pinto, Younes Dragoni, and Andrea Carcano. Triton: The first ics cyber attack on safety instrument systems. *Proc. Black Hat USA*, 2018:1–26, 2018.
10. Federal Bureau of Investigation and Cybersecurity and Infrastructure Security Agency. Triton malware remains threat to global critical infrastructure industrial control systems (ics). Technical report, Federal Bureau of Investigation (FBI) and Cybersecurity and Infrastructure Security Agency (CISA), 2022. Cybersecurity Advisory, March 25, 2022.
11. Markus Hornsteiner and Stefan Schönig. Siren: Designing business processes for comprehensive industrial iot security management. In Aurona Gerber and Richard Baskerville, editors, *Design Science Research for a New Society: Society 5.0*, pages 379–393, Cham, 2023. Springer Nature Switzerland.
12. Marlon Dumas, Marcello La Rosa, Jan Mendling, and Hajo Reijers. *Fundamentals of business process management*. Springer, 2018.
13. International Electrotechnical Commission. Understanding iec 62443. https://www.iec.ch/blog/understanding-iec-62443, 2021. Accessed: 2025-08-07.
14. International Electrotechnical Commission. IEC 62443-2-1:2024 — security program requirements for iacs asset owners, 2024.
15. Daniel Oberhofer, Markus Hornsteiner, and Stefan Schönig. Process-aware security standard compliance monitoring and verification for the iiot. In *ECIS 2024 Proceedings*, 2024.
16. Adam Shostack. *Threat modeling: Designing for security*. John wiley & sons, 2014.
17. Mike Da Silva, Maxime Puys, Pierre-Henri Thevenon, Stephane Mocanu, and Nelson Nkawa. Automated ics template for stride microsoft threat modeling tool. In *Proceedings of the 18th International Conference on Availability, Reliability and Security*, ARES '23, New York, NY, USA, 2023. Association for Computing Machinery.
18. Eric J Byres, Matthew Franz, and Darrin Miller. The use of attack trees in assessing vulnerabilities in scada systems. In *Proceedings of the international infrastructure survivability workshop*, volume 202. Lisbon, 2004.
19. Peter Maynard, Kieran McLaughlin, and Sakir Sezer. Decomposition and sequential-and analysis of known cyber-

attacks on critical infrastructure control systems. *Journal of Cybersecurity*, 6(1):tyaa020, 2020.
20. Otis Alexander, Misha Belisle, and Jacob Steele. Mitre att&ck® for industrial control systems: Design and philosophy. Technical Report 01ADM105-OT, The MITRE Corporation, 2020. Approved for Public Release. Distribution unlimited.
21. William Young and Nancy Leveson. Systems thinking for safety and security. In *Proceedings of the 29th annual computer security applications conference*, pages 1–8, 2013.
22. International Electrotechnical Commission. IEC 62443-4-1:2018 — secure product development lifecycle requirements, 2018.
23. National Insitute of Standards and Technology. The nist cybersecurity framework (csf) 2.0. NIST Cybersecurity White Paper (CSWP) 29, National Institute of Standards and Technology, Gaithersburg, MD, 2024.
24. OASIS Standard. extensible access control markup language (xacml) version 3.0. *A:(22 January 2013). URl: http://docs. oasis-open. org/xacml/3.0/xacml-3.0-core-spec-os-en. html*, 2013.
25. Open Policy Agent Project. Open policy agent (opa). https://www.openpolicyagent.org/docs/latest/, 2025. Accessed: 2025-08-07.
26. Ali M. Hosseini, Thilo Sauter, and Wolfgang Kastner. Integrating security into industrial control system architecture based on iec 42010. In *2024 IEEE 29th International Conference on Emerging Technologies and Factory Automation (ETFA)*, pages 1–8, 2024.
27. Ali M.Hosseini, Wolfgang Kastner, and Thilo Sauter. Ontology framework supporting security-by-design of industrial control systems. *IEEE Transactions on Industrial Informatics*, PP:1–10, 01 2025.
28. Arthur Amorim, Trevor Kann, Max Taylor, and Lance Joneckis. Towards provable security in industrial control systems via dynamic protocol attestation. In *2024 Annual Computer Security Applications Conference Workshops (ACSAC Workshops)*, pages 120–132, 2024.
29. Ruggero Lanotte, Massimo Merro, and Andrei Munteanu. Runtime enforcement for control system security. In *2020 IEEE 33rd Computer Security Foundations Symposium (CSF)*, pages 246–261, 2020.
30. Achim D Brucker, Isabelle Hang, Gero Lückemeyer, and Raj Ruparel. Securebpmn: Modeling and enforcing access control requirements in business processes. In *Proceedings of the 17th ACM symposium on Access Control Models and Technologies*, pages 123–126, 2012.
31. Curtis L. Maines, David Llewellyn-Jones, Stephen Tang, and Bo Zhou. A cyber security ontology for bpmn-security extensions. In *2015 IEEE International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing*, pages 1757–1764. IEEE, 2015.
32. Curtis L. Maines, Bo Zhou, Stephen Tang, and Qi Shi. Adding a third dimension to bpmn as a means of representing cyber security requirements. In *2016 9th International Conference on Developments in eSystems Engineering (DeSE)*, pages 105–110, 2016.
33. Florian Gallik, Yusuf Kirikkayis, and Manfred Reichert. Modeling, executing and monitoring iot-aware processes with bpm technology. In *2022 international conference on service science (ICSS)*, pages 96–103. IEEE, 2022.
34. Sonja Meyer, Andreas Ruppen, and Carsten Magerkurth. Internet of things-aware process modeling: Integrating IoT devices as business process resources. In *Lecture Notes in Computer Science*, volume 7908 LNCS. Springer, 2013.
35. Alan R Hevner, Salvatore T March, Jinsoo Park, and Sudha Ram. Design science in information systems research. *MIS quarterly*, pages 75–105, 2004.
36. Henry Haverinen, Tero Päivärinta, Jussi Vänskä, and Henry Joutsijoki. Information-centric adoption and use of standard compliant devsecops for operational technology: From experience to design principles. In *Software Business*, pages 400–415, Cham, 2024. Springer Nature Switzerland.
37. Ken Peffers, Marcus Rothenberger, Tuure Tuunanen, and Reza Vaezi. Design science research evaluation. In *Design Science Research in Information Systems. Advances in Theory and Practice - 7th International Conference, DESRIST 2012, Las Vegas, NV, USA, May 14-15, 2012. Proceedings*, volume 7286, pages 398–410, 05 2012.

P4: Process-Aware Security Standard Compliance Monitoring and Verification for the IIoT

Status	Published
Date of Submission	16 November 2023
Date of Acceptance	28 February 2024
Date of Publication	30 April 2024
Conference	European Conference on Information Systems
Location	Paphos, Cyprus
Period	13.06.2024 - 19.06.2024
Authors Contribution	Daniel Oberhofer 45% Markus Hornsteiner 45% Stefan Schönig 10%
Full Citation	Oberhofer, D., Hornsteiner, M., Schönig, S. (2024). Process-Aware Cybersecurity Standard Compliance Monitoring and Verification for the IIoT. In: *Proceedings of the 32nd European Conference on Information Systems (ECIS)*. 1.
Artifact	`https://github.com/DanielOberhofer/Compliance_Monitoring_with_Zeek`

Conference Description: The theme of ECIS 2024, the 32nd European Conference on Information Systems, is "People First: Constructing Digital Futures Together." The theme of the conference underscores the imperative that technological progress should be intrinsically linked to the betterment of human lives and inclusivity through cooperative efforts.

In an era of unprecedented technological strides, the conference seeks to explore how we can actively shape the evolving technological landscape while harmonizing innovation with societal well-being. Bringing together a diverse cohort of scholars, the conference intends to forge a collective path toward a digitally empowered future that resonates with human aspirations and addresses pressing challenges.

PROCESS-AWARE SECURITY STANDARD COMPLIANCE MONITORING AND VERIFICATION FOR THE IIOT

Completed Research Paper

Daniel Oberhofer, University of Regensburg, Regensburg, Germany, daniel.oberhofer@ur.de
Markus Hornsteiner, University of Regensburg, Regensburg, Germany, markus.hornsteiner@ur.de
Stefan, Schönig, University of Regensburg, Regensburg, Germany, stefan.schoenig@ur.de

Abstract

The distinct security challenges and characteristics inherent in Industrial Automation and Control Systems (IACS) within the Industrial Internet of Things (IIoT) have driven the adoption of security standards. Adhering to these standards mandates continuous and automated monitoring of Security Requirements (SRs) specific to the standard. This paper proposes a Security Compliance Monitoring and Verification (SCMV) framework that describes the key components and interactions for ongoing compliance assessment. The modular framework allows extensions or modifications of individual components. In addition, we demonstrate the potential of SCMV through the integration of process-related information, in particular BPMN annotations. This integration improves the visibility of the implemented security measures, enabling a comprehensive approach to achieving full compliance with security standards.

Keywords: Industrial IoT Security, Compliance Monitoring, Compliance Verification, Security Monitoring, Business Process Management and Notation.

1 Introduction

As an effect of the fourth industrial revolution, also referred to as Industry 4.0 (I4.0), new challenges in securing industrial facilities arise (Serror et al., 2021). The I4.0 concept describes the conjunction of the Internet of Things (IoT) paradigm with cyber-physical systems (CPS), leading to increased complexity in services and overall system infrastructure (Rubio et al., 2017; Shaaban, Kristen, and Schmittner, 2018). The Internet of Things can be divided into the consumer IoT and Industrial IoT (IIoT) (Bandyopadhyay and Sen, 2011). As the consumer IoT focuses on improving the quality of life for consumers by interconnecting smart devices with user environments, the IIoT connects industrial assets with information systems and business processes (Palattella et al., 2016; Sisinni et al., 2018). A significant part of the I4.0 paradigm is represented by the introduction of CPSs, which replace Programmable Logic Controllers (PLC) (Kopetz and Steiner, 2022). CPS connect these PLCs to the internet, enabling efficient communication between the physical components and their digital counterpart (Sisinni et al., 2018). The increased connectivity between operational technology (OT) and information technology (IT) systems leads to a gradual merging of IT and OT, disbanding the previously hierarchical structure of isolated industrial networks (Cruz et al., 2015; Rubio et al., 2017; Serror et al., 2021).

Categories of OT-based systems are supervisory control and data acquisition (SCADA) systems, industrial control systems (ICSs), and industrial automation and control systems (IACSs)(Conklin, 2016). These previously isolated OT systems face an increased interconnection and standardization (Rubio et al., 2017). An example of this standardization is conventional networking technology based on TCP/IP instead of proprietary vendor protocols (Shaaban, Chlup, et al., 2022; Zhou et al., 2015). Because of that process, industrial networks face an increasing amount of IT-based security vulnerabilities (Shaaban, Kristen,

and Schmittner, 2018). In addition to that, security functionalities of OT devices are often deprecated or missing, as their design was created for efficiency and longevity and not with security in mind (Conklin, 2016). Exchanging devices and components with weak security functionalities might also not be possible in every scenario and at all times, as it could disturb the continuous operation of the IACS (Shaaban, Kristen, and Schmittner, 2018).

The described increase in interconnection and standardization interacts with and elevates the unique characteristics of IIoT systems, making the implementation of a segregated and secure IIoT network architecture more difficult (Serror et al., 2021). Some of these characteristics are IIoT networks being at a larger scale than traditional enterprise networks, running without interruptions for a longer period, and focusing on safety more than security (Serror et al., 2021). Furthermore, the damage created by incidents affects the physical world with CPS, making a secure and safe architecture important (Conklin, 2016). Because of these characteristics, the prioritization of the well-known security objectives confidentiality (C), integrity (I), and availability (A) shift within the CIA triad. In traditional enterprise IT systems, confidentiality is the most critical requirement, as an interruption of business processes caused by availability issues does not have the same ramification of loss as it would have in OT systems (Conklin, 2016). On the contrary, in OT systems, the focus is on availability, followed by integrity, and last, confidentiality (Tange et al., 2020). As these systems keep getting more connected to the internet with enterprise IT and business processes aligned to the OT, integrity and confidentiality gain importance within the IIoT security requirements (SRs) (Tange et al., 2020). This leads to the necessity for an IIoT domain-specific requirement spectrum (Tange et al., 2020).

Security risks and characteristics of IACSs result in the requirement of a holistic cybersecurity concept, which integrates the principles of the IIoT into industrial security conception. Such a concept should also include a detailed domain-specific definition of IIoT SRs (Sadeghi, Wachsmann, and Waidner, 2015). A well-accepted cybersecurity standard for IACSs is provided by the IEC 62443 standard. Within the IEC 62443, an IACS life cycle is defined, which includes the continuous specification, design, and implementation of security functionalities (Kobes, 2016). This iterative and repeating process of implementing IEC 62443 specific security level measures (SLMs) to match the security level target (SL-T) with a sufficient achieved security level (SL-A) is a challenging task for asset owners (Kobes, 2016). The concepts of the work at hand rely on the principles of the IEC 62443 but can be adapted to arbitrary standards. Automatic and continuous standard compliance requires the monitoring of the implemented security requirements as well as the verification of the targeted compliance status (Bicaku, Zsilak, et al., 2022; Julisch, 2008).

With the described problem in mind, the work at hand presents the design of a *Security standard Compliance Monitoring and Verification* (SCMV) framework and process definition. Comparable systems are already in practical use but lack a specific domain definition in research. While some studies address general standard compliance, they lack a specific focus on the IIoT domain. As a second contribution, we highlight the potential of process-related information for such systems. This is also a novel approach of combining Business Process Management (BPM) with security standard compliance, which was motivated in research, but has not been adapted into a concrete security monitoring domain like compliance monitoring (Schönig, Hornsteiner, and Stoiber, 2022). We build on results of our previous research project SIREN and utilize the Business Process Model and Notation (BPMN) extension presented there to model security measures of the IEC 62443 (Hornsteiner and Schönig, 2023). The presented framework can be used to implement a system that continuously and automatically checks the compliance of an IIoT system to the SRs of an arbitrary security standard and incorporates existing process knowledge as a data source. Our work answers the following research questions:

- RQ1: How can process-related attributes be used to improve security standard compliance and the underlying process in the IIoT?
- RQ2: Which components would the design of a SCMV framework include?

The work is structured as follows: in Section 2, related work and the background in security monitoring is described. Followed by Section 3 in which the methodical approach based on Design Science Research (DSR) is explained. This is followed by Section 4, where the design for the SCMV framework is discussed in detail. After that, the usage of the framework is demonstrated in Section 5 by describing an implemented prototype. The design of the SCMV framework is then evaluated in Section 6, followed by a final conclusion in Section 7.

2 Background and Related Work

2.1 IIoT network monitoring

In this paper, we propose the domain of SCMV within the IIoT, leveraging well-established network monitoring techniques. As network monitoring is one of the two main parts of SCMV, we present different categories of monitoring techniques that are commonly used in research. Security Monitoring techniques in OT or IT networks can be categorized into active, passive, and hybrid systems. Passive monitoring approaches avoid creating network overhead, relying solely on monitoring network traffic within existing communications (Nicholson, Janicke, and Cau, 2014). This can be implemented by installing additional hardware or enhancing existing sniffing capabilities of system components (Raposo et al., 2018). Active monitoring solutions, on the other hand, distinguish themselves by generating additional network load (Nicholson, Janicke, and Cau, 2014). In addition to the network load, active monitoring utilizes component or node resources for detecting abnormal behavior (Raposo et al., 2018). Recognizing that entirely passive systems can only partially detect some threats, a combination of passive and active approaches is also discussed, categorized as hybrid monitoring systems (ENISA, 2016; Jardine et al., 2016).

2.2 Related work

The concept of SCMV is based on industry observations with a limited existing research base. While some studies address general standard compliance, they lack a specific focus on the IIoT domain. Furthermore, this paper proposes the SCMV framework as an entirely new artifact and incorporates process modeling with the BPMN as a novel approach. In the subsequent section, we discuss related work and its influence on the SCMV architecture. This aims to provide information on existing research endeavors, offering context for the contributions of our work within the domain of SCMV for the IIoT.

Ullah, Ahmed, and Ylitalo (2013) highlight challenges faced by automated security compliance tools in cloud environments, including the need to formalize external requirements, the lack of guidance in standard requirement descriptions, the necessity to identify and extract verifiable data, and the overarching goals of ensuring the security and integrity of audit data. The authors emphasize key components essential for such systems: a data collection engine, a verification engine, and a user interface for presenting audit data. Although their focus is on enterprise tools connected to a cloud-hosted system, these components are adaptable to the IIoT domain.

Cheng et al. (2018) emphasize the need to apply compliance to SRs and automate the verification process, highlighting the manual nature of compliance audits. Using ontology-based natural language processing, they extract SRs from standard definitions and implement verification through PowerShell audit scripts. While their primary focus is on extracting requirement concepts, their approach underscores the call for continuous, automated monitoring of standard compliance, as provided by SCMV.

Fenz and Neubauer (2018) also introduce an ontology-based methodology for standard compliance verification, employing the ISO 27002 standard as an example. This compliance verification system relies on a semantic knowledge base combined with reasoning engines, automatically deriving the compliance status of a system based on the inventory of implemented security measures and company assets. The inventory requires manual registration through a user interface, and the reasoning engine interprets the general description in a machine-readable manner. It's noteworthy that their work presents a

distinct approach to standard compliance compared to the monitoring-centered approach proposed in this paper. They utilize manual input descriptions of an asset inventory, a process that could potentially be overwhelmed by the existence of BPMN attributes. Despite these differences, their approach highlights the importance of translating imprecise descriptions of SRs into measurable indicators for automated machine verification of compliance status.

Kulik, Tran-Jorgensen, and Boudjadar (2019) describe the verification of IEC 62443-3-3 SRs by formalizing the behavior and requirements of cloud-connected SCADA systems. Their formalization includes labeled transition systems to model component behavior and the individual formalization of security properties with mathematical models. Finally, they evaluate the models using example requirements by elevating the formalization into a machine-readable format. Their paper shows a mathematical approach to compliance verification but only focuses on three requirements of the IEC 62443 standard, and their approach using the TLC model checker lacks scalability (Kulik, Tran-Jorgensen, and Boudjadar, 2019).

Bicaku, Tauber, and Delsing (2020) propose an architecture comparable to our approach on SCMV for the IIoT. They discuss the current state-of-the-art in standard compliance monitoring, highlighting the challenges introduced by the integration of big data analysis, cloud computing, and I4.0 technologies into industrial processes. The complexity of balancing security aspects in IIoT systems is underscored, especially as organizations implement security standards heavily reliant on integrating standard compliance into the security process. The authors recommend the adoption of the proposed architecture to facilitate continuous verification of standard compliance in the IIoT, aiming for increased efficiency. The proposed architecture utilizes active network monitoring techniques involving agents deployed on targeted systems. Acknowledging the potential impracticality of such an approach in IIoT systems due to unique availability requirements, it is not recommended to rely solely on active monitoring techniques.

In their most recent work, Bicaku, Zsilak, et al. (2022) expand on their previous framework and adapt it to service-oriented systems. They identify that compliance issues can lead to the missed potential of interoperability and standardization in IIoT systems, especially impacting service-oriented infrastructures. With their process definition, they support understanding and finding the cause of non-compliance to security standards. We enhance this process by adding the aspect of continuous compliance and including process-related information.

In conclusion, existing research in the field of applying security standards in IIoT addresses only a few aspects of our understanding of the research field. In order to delineate the boundaries and introduce the field of SCMV, it is necessary to take a comprehensive approach.

3 Research Methodology

3.1 Structure

Structure and research methodology adhere to the principles of Design Science Research (DSR) as proposed by Peffers, Tuunanen, et al. (2007). Specifically, a design-centered approach has been employed. This choice was influenced by the existence of comparable implementations of the proposed artifact already in practical use. However, a formal definition in the research context aims to distinguish compliance-oriented monitoring systems from general security architectures. With this focus on the SCMV domain, we lay a foundation for broader research and improvement of domain-specific components. Figure 1 illustrates the five steps used to organize the design of the artifact based on DSR principles. It also describes the development of the artifact presented in this paper.

The first step includes the description of the problem, motivating researchers to solve an identified problem with the intent to justify the value of the proposed solution, as discussed in Section 1 (Peffers, Tuunanen, et al., 2007). Revisiting this includes that a continuous process verifying the achieved status of the standards SRs is a complex task and not yet defined in research. Aligned with the second DSR step, we break the solution approach of our artifact down based on defining Meta Requirements (MRs) in

Subsection 3.2. This step allows the connection in between the problem described within the introduction and RQs and specifies it into a set of objectives, which the artifact should solve. By extending the research base in this field, the complex security standard compliance process can be improved. By quantifying the problem to solution connection with the MRs, we can later evaluate our design and link it to the proposed RQs. The next DSR step is described in Section 4 and includes the actual design of the artifact, which is the main contribution of this work. To further improve the ability to communicate the design process of the artifact and connect it with the objectives of the solution, we used concepts of design theory based on Heinrich and Schwabe (2014), which is discussed in more detail in the next section. With our artifact, we propose a new framework that connects BPMN information with a layered structure describing the necessary components of SCMV systems. In addition to that, the SCMV process is redefined as part of the artifact to further highlight the process-related potential. The following two steps of the DSR process are the demonstration of the usage of the artifact and then the evaluation of the artifact by comparing it to observed results with the previously defined objectives (Peffers, Tuunanen, et al., 2007). As shown in Figure 1, we combined both steps by demonstrating the framework's adaption and evaluating based on a prototype (Peffers, Rothenberger, et al., 2012).

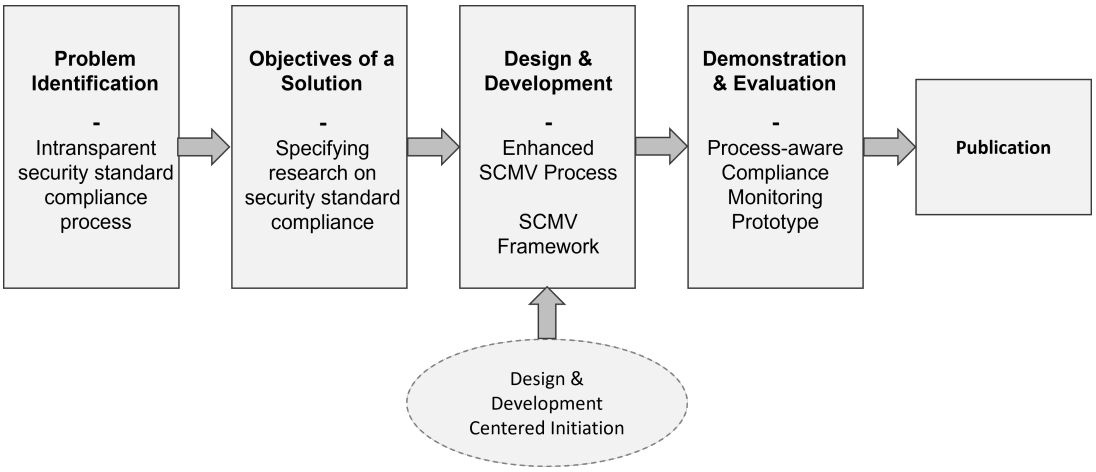


Figure 1. Applied methods of design science research by Peffers et al. (2012)

3.2 Design principles

By choosing the design-centered approach, we further structure the objective and design phases by creating a set of MRs and Design Principles (DPs) (Heinrich and Schwabe, 2014). This helps to further specify the contribution of the artifact and ensure that all existent knowledge bases are included in the design itself. Not only does it improve the quality of the artifact evaluation, but it helps the traceability of the design process, as it aligns the artifact to the central components of design theory (Gregor, Jones, et al., 2007).

Heinrich and Schwabe (2014) state, that *meta-requirements are just refinements to the solution objectives*. Based on the problem solution objectives deriving the problem discussion and the RQs in Section 1, we specify the following MRs: (1) The artifact should define necessary components of a SCMV system to achieve better understanding and delimitation in research, (2) The artifact should incorporate and highlight process-related information and present its impact on other design components, (3) The artifact should be based on properties of the IIoT to achieve a domain specification for the IIoT.

As discussed before, the design-centered approach was chosen based on the fact that systems checking compliance with security standards are already implemented in practice but lack scientific attention and definition. The properties of such systems were investigated and published in the form of a extensive market study by Oberhofer, Hornsteiner, and Schönig (2023). By combining the results of that market study with the theoretical findings we presented in Subsection 2.2, it was possible to extract a set of

Design Requirements (DRs) for the design of the artifact. The first three DRs were extracted from the market study, where different techniques of compliance monitoring are described based on existing industry solutions (Oberhofer, Hornsteiner, and Schönig, 2023). This includes the passive monitoring of a collection of network traffic attributes for compliance reasons (DR 1), the usage of static network component characteristics (DR 2), e.g. configuration files, and incorporating expected values (DR 3), e.g. asset inventory data, into the compliance monitoring process. DR 4 was included based on Schönig, Hornsteiner, and Stoiber (2022) and introduces the process attributes to the design. Another DR derived from the market study is DR 9. In there the findings suggest, that there are industry solutions providing automatic compliance verification functionalities, which would align with the overall IIoT goal of automating processes. The other DRs, were extracted from related work and introduce the findings described in Subsection 2.2 to the design.

Figure 2 shows the different DRs, their connection to the knowledge base, their derivation into a set of DPs, and finally, how they are implemented within the design of the artifact. The third DP does not directly lead to an implemented layer, as it only influences the monitoring layer to allow possible enhancements with active components and the extraction layer to allow standard-specific components. With that, we achieve a modular structure that is open for improvement and, therefore, is mutable by design (Gregor, Jones, et al., 2007). The other DPs were used to derive the main layers of the framework, as they have influenced the individual layer components.

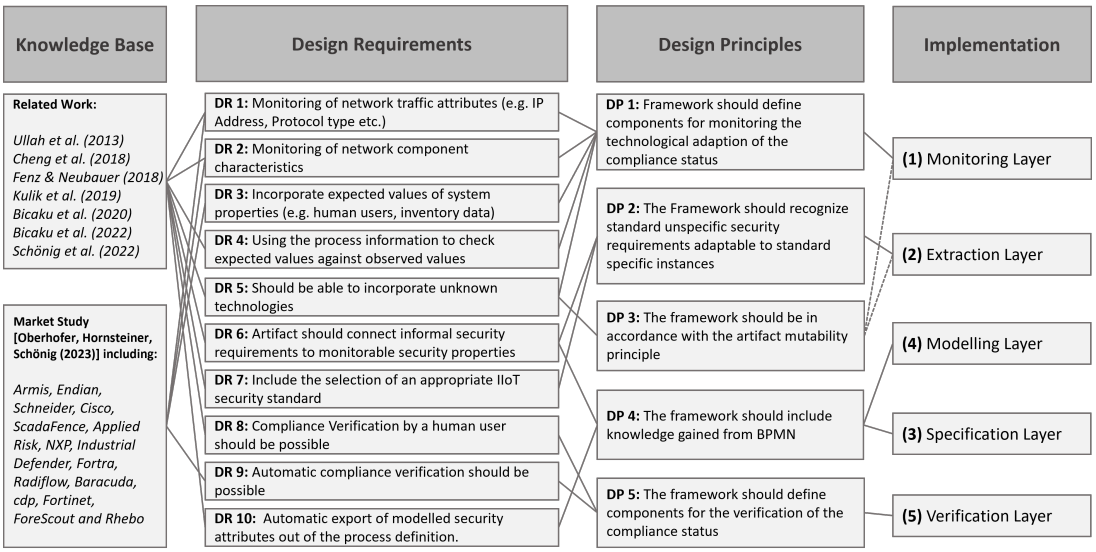


Figure 2. Realisation of Design Theory to the Design process of the artifact development

4 Designing a SCMV Framework

Security standards delineate a set of SRs for information systems at a general level. Conforming to these requirements and providing evidence of such conformity constitute security compliance (Julisch, 2008). This definition is further broadened to encompass measurable indicators depicting the evidence (Bicaku, Tauber, and Delsing, 2020). Standard compliance monitoring and verification can be viewed as a process aimed at understanding why a system, service, or device deviates from the requirements outlined in a security standard (Bicaku, Zsilak, et al., 2022). Importantly, this process is not confined to a single point in time but extends throughout the entire life cycle of the compliant system, necessitating continuous monitoring of compliance (Bicaku, Zsilak, et al., 2022). Consequently, by combining security compliance, compliance monitoring, measurable indicators, continuity, and compliance verification, we create the domain of SCMV.

Through the creation of an artifact designed for IIoT security standards, we establish a foundation for enhancing the overall security standard application process. While our focus is on adapting the IEC 62443 standard, particularly aligning with its IACS life-cycle, our proposed artifact is adaptable to any IIoT security standard or framework sharing a similar requirement concept.

Before developing the artifact, we formulated a set of DPs to effectively communicate our approach and align it with the existing knowledge base. Based on this, we developed the comprehensive SCMV framework, presented in Figure 4.

The second core concept of this work involves the integration of BPMN and annotated security attributes into the artifact. This integration depicts the domain specification of SCMV to the IIoT, as it is based on the process-based nature of these systems, which is a result of the described alignment of business processes and operational processes. By incorporating data from such sources throughout the design process, embedding it within the framework, and examining its impact on SCMV processes, we aim to underscore the potential uncovered through our research.

4.1 SCMV process

Understanding the underlying process of SCMV systems allows for the development and description of interactions between different components within the framework. Bicaku, Zsilak, et al. (2022) proposed a process comprising five phases: (1) Requirements Gathering, (2) Standard Identification, (3) Measurable Metrics, (4) Standard Compliance Verification, and (5) Standard Compliance Result. Utilizing this as a foundation, we enhance it with two concepts. The first involves a continuous compliance approach, as outlined in specific standards like IEC 62443, which includes the repeated definition of the SL-T followed by checking the currently achieved SL-A of the system (Kobes, 2016). The second aspect we introduce is to demonstrate the impact of BPMN attributes on improving the individual phases, explained in more detail in Subsection 4.2. Figure 3 illustrates the adapted continuous SCMV process and the process relation discussed in Subsection 4.2.

In the first phase of the SCMV process, a collection of security requirements, or even the standard itself, is gathered (Bicaku, Zsilak, et al., 2022). The origin and form depend on the security standard, such as in the IEC 62443 context, where it is a collection of informally described security requirements in the form of SL-T (Kobes, 2016). The second phase involves constructing a portfolio of Security Compliance Indicators (SCIs) based on the previously gathered SRs portfolio. This step is necessary as the informal SRs must be transformed into a collection of measurable indicators usable within the monitoring phase to create a monitoring specification (Bicaku, Tauber, and Delsing, 2020). For example, this includes defining attributes like required protocol types or the necessity of encryption. The next step involves monitoring the defined SCI set by collecting process evidence within the IACS and comparing it with the expected values defined in the SCI portfolio. This step, though not explicitly mentioned in other research, is proposed as a monitoring phase within the SCMV process, given its central role in defining specific components. As part of the verification aspect of SCMV, phases four and five are required to calculate and present the results of the verification (Bicaku, Zsilak, et al., 2022). This verification includes a metric to ratify the current compliance status. In the end, based on the verification results, the SL-A can be derived. The continuous nature of the SCMV process is explained based on the IACS life-cycle of the IEC 62443, which defines the SL-T concept as the starting and the SL-A concept as the endpoint of the process. As a result, the defined process is repeated based on either a change in the SL-A or the SL-T, producing continuity. As a result of this section, we obtain an enhanced process, which we define as the SCMV process. This definition is used in Subsection 4.2 to show the impact of BPMN information on SCMV.

4.2 Process-oriented SCMV

Recent research has delved into process-oriented IIoT security management, aiming to enhance IIoT security by incorporating established methods, concepts, and principles from BPM. Especially the

connection in between executing process models for security process monitoring and the transfer to using them for security process audits, has been highlighted (Schönig, Hornsteiner, and Stoiber, 2022). In view of the identified potential, we assume that the application of BPM concepts to the SCMV process can be beneficial. This proposition aligns with the goal of simplifying the overall standard adaptation process, where continuous compliance plays a central role in the IACS life cycle (Kobes, 2016).

The primary process modeling language considered for the integration is BPMN, the de-facto standard for process modeling (Dumas et al., 2018). In order to be able to represent the IEC 62443-specific attributes in BPMN, we use our contributions from our work (Hornsteiner and Schönig, 2023), in which we have extended BPMN with IEC 62443 attributes. Here we also present a parser that reads the content of the BPMN model and converts it into a format that can be further processed. To structure the adaptation of BPM to SCMV, we define three categories of security-related process attributes: (1) Entity, (2) Communication, and (3) System. In this context, an entity refers to an IIoT device with an IP address. The second category encompasses communication attributes, representing properties of connections between two entity activities, always involving the transfer of information over a communication medium. Examples include the requirement for encrypted communication or the expected protocol type of the network session. The third category includes system attributes, describing the overall system structure, such as the count of unique entities in the system. Figure 3 illustrates the enhanced SCMV process, showcasing the investigated impact of the extracted Entity, Communication and System attributes on the individual phases.

Implementing security aspects as BPMN attributes from the start of the SCMV process can improve and automate the first phase of the SCMV process, as it is not necessary to manually define the SL-T but derive it from the BPMN diagrams. In the second phase, these attributes can be used to build the SCIs and to include the expected process behavior represented by the BPMN annotations. Within the third phase, the actual values of the attributes can then be used to monitor the live process realization. As the process phases are all represented by the different layers of the SCMV framework, BPMN attributes can be used as a central source of information in such a system. The potential highlighted through the provided examples showcase the impact of BPMN on the process. Based on that, we integrated BPMN into our proposition of a SCMV framework.

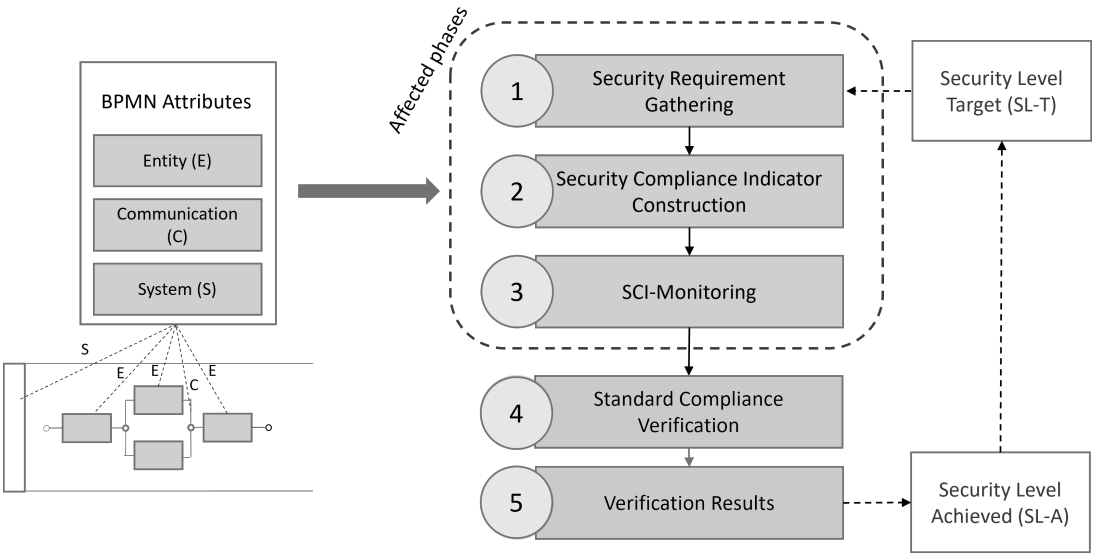


Figure 3. The extended SCMV process in the context of the IEC 62443 security standard and the affected phases by the BPMN attributes.

4.3 SCMV framework

Figure 4 delineates the envisioned SCMV framework, featuring six main components: (1) Extraction Layer, (2) Specification Layer, (3) Monitoring Layer, (4) Verification Layer, (5) Modelling Layer, and (6) Process Layer. In accordance with the established design principles, these layers amalgamate essential components to formulate a comprehensive definition of an SCMV system. Each layer corresponds to specific steps within the overarching SCMV process, demonstrating close interrelation while also capable of being perceived as discrete entities that receive input and yield output. Consequently, an implementation of an SCMV system utilizing this framework may merge components from various layers into a unified service or create distinct services for each layer.

Layers (5) and (6) do not serve as central layers, furnishing mandatory components to the SCMV system. Instead, they contextualize two data sources, namely BPMN attributes and live process data, in relation to the other layers. The Modelling Layer signifies the impact of BPMN attributes, aligning with the process-related SCMV process discussed in Subsection 4.2. On the other hand, the Process Layer delineates all data-producing components of the IACS process, serving as the framework entry point. In the following, we discuss the framework's central layers and delineate their constituent components.

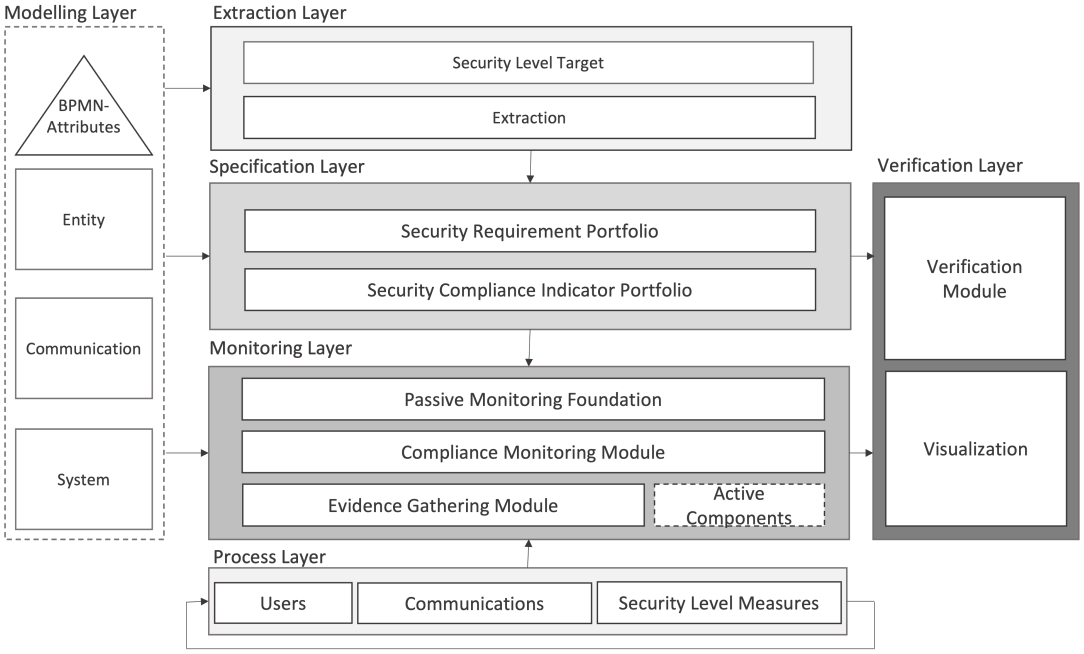


Figure 4. A layered SCMV framework and the possible impact points of using BPMN attributes

The first layer, designated as the Extraction Layer, encompasses all tasks associated with the extraction of SRs from the security standard. In most standards, the provided SRs are presented in an informal text-based description, rendering them impractical for machine-based interpretation. The execution of components within this layer can exhibit variability and may encompass manual extraction and transfer of requirements by human operators, or it can be achieved automatically through more intricate measures. Technological solutions with promise for this layer include ontology-based approaches or machine learning-based text recognition, with a focus on the extraction and formal definition of SRs from security standards (Cheng et al., 2018; Fenz and Neubauer, 2018).

The second layer of the SCMV framework is constituted by the Specification Layer, which comprises two distinct modules. These encompass the formulation of a system-specific set of SRs and, subsequently, the translation of these SRs into a portfolio of SCIs. The initial module of this layer explicates the imperative of selecting a unique set of requirements tailored to the specific use case. Within the context of IEC 62443, this materializes in the form of the SR portfolio, further refining the output of the extraction layer to align

with the SL-T of the IACS. In accordance with this target, not all requirements are deemed necessary for implementation within the system, and this module facilitates their exclusion. Analogous to the first layer, this task continues to rely on human expertise, with a human expert selecting the requirements for the SL-T. More complex techniques, such as the automated creation of requirement portfolios, are beyond the scope of this paper but represent possible future work. In essence, the tasks undertaken in this layer bear similarities to those in the extraction layer, yet they diverge by furnishing a higher level of system specification as compared to the standard specification addressed in the first layer.

The third primary constituent of the SCMV framework is the Monitoring Layer, encompassing all tasks associated with the monitoring of SCIs and the active monitoring of the live process. It constitutes the third phase of the SCMV process. Implicit in the term SCMV itself, the monitoring aspect assumes a pivotal role within the framework, a feature observed in analogous frameworks as well (Bicaku, Tauber, and Delsing, 2020). As previously highlighted regarding the unique demands on availability in the IIoT, this realization is embodied in the monitoring layer. By employing passive monitoring techniques to monitor compliance with as many SRs as possible, the impact on the performance of the IACS is minimized. This foundation allows for potential expansion by integrating active monitoring components, thereby establishing a hybrid approach to achieve broader SR coverage. In addition, the compliance monitoring module serves as a hub where the observed evidence is compared to the expected evidence defined by the SCI. The aforementioned observed evidence is gathered by an Evidence Gathering Mechanism or Module, which is tasked with collecting, filtering, and potentially storing evidence attributes (Bicaku, Tauber, and Delsing, 2020). This evidence includes all types of information generated by the underlying processes of the system.

The Verification Layer is the last mandatory segment of the SCMV framework and comprises two integral components: (1) the Verification Module and (2) the Visualization Module. The Verification Module analyses the output of the Compliance Monitoring Module and determines the actual compliance status of the system with the selected security standard. In the context of IEC 62443, this would manifest itself in the SL-A and the subsequent comparison with the SL-T. The second component, visualization, takes the compliance logs and the results of the Verification Module and presents them in a visual format so that humans can interpret the compliance status. Such a module could take various forms, including the display of generated audit logs or a compliance dashboard with various statistics and charts.

5 Demonstration

The utilization of the artifact is demonstrated through the development of a prototypical SCMV system, implementing each layer proposed in the SCMV framework. While the framework is adaptable to any IIoT security standard, its development is based on the IEC 62443 standard. Consequently, the construction of our SCIs draws upon the corresponding SRs outlined in document 3-3 of the standard (IEC, 2009). Furthermore, in alignment with the research questions, we underscore the potential of leveraging process-based information for the SCMV process. This is realized through the development of a research prototype focusing on SRs that benefit from such attributes.

5.1 SCIs for a specification-based IIoT security monitoring

Presently, the implementation of both the Extraction Layer and the Specification Layer still necessitates human involvement. The technical implementation falls beyond the scope of this work, as it would include extracting text-based SRs from the standard into a machine-readable format.

The IEC 62443 3-3 standard describes a comprehensive list of 51 security requirements, many of which include requirement enhancements for higher security levels. For the purposes of this demonstration and to reduce complexity, an abbreviated list of 25 requirements has been derived, omitting the requirement enhancements as some of them require monitoring functions beyond the scope of passive monitoring.

Based on this, a portfolio of SCI was created that defines concrete, observable properties for security requirements. A subset of the SCI portfolio is shown in Table 1. As an illustrative example, expected values for process attributes such as IPs, ports, and protocols of process participants can be used to check a basic level of identification and access control.

SCI-ID	SR	SCI	Attributes
SCI 1	1.1, 1.2, 1.6, 1.13	Foundational Identification and Access Control for System Users	IPs, Ports, Protocols
SCI 6	2.4	Restriction of Mobile Code	Protocol Type, File hash
SCI 14	4.1	Confidentiality in untrusted networks	Protocol, IP

Table 1. Example for the SCI-Portfolio linking security requirements to observable network attributes

5.2 Implementation

Figure 5 provides an overview of the various tools utilized for the SCMV prototype. The prototype is based on the SCMV framework, embodying the functionalities of each layer. As shown in the prototype overview, all the layers — Process, Modelling, Specification, Extraction, Monitoring, and Verification — are implemented. These layers are functioning independently of one another, with information exchange being the sole point of interaction. This modular approach to the layered structure of the framework provides developers the flexibility to exchange or customize layers autonomously from the remaining components. The technological implementation that characterizes the use of the SCMV framework for each layer is described below and can be accessed in the provided repository[1].

Each of the prototypes layers is encapsulated in a Docker[2] container, which enables uniform deployment on a single machine. Consequently, the prototype could be installed on a centralized network component, such as an IACS, with access to the entire network in a real-world scenario without the need for complex system modification.

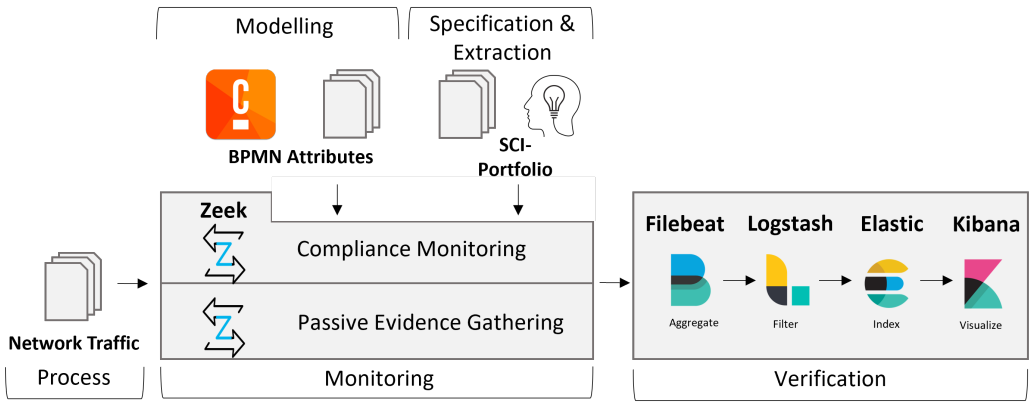


Figure 5. Components of a prototypical implementation of Compliance Monitoring with the SCMV framework

The Process Layer is represented by the monitored network traffic, which could either be in the form of a file containing documented network traffic or a connection to a network interface accessing the live network. As the prototype was intended to demonstrate the different components and not to evaluate

[1] github.com/DanielOberhofer/Compliance_Monitoring_with_Zeek
[2] docker.com

efficiency in a real practical deployment, we relied on previously recorded data. This pcap file of an open-source dataset contains monitored network traffic including several industry protocols and utilities[3].

The Modelling layer is implemented by creating a BPMN diagram in Camunda[4] and parsing security-related annotations via XML into an input readable by the Monitoring layer. These annotations are categorized into three variations. The first encompasses the modeling of the general properties of an entity, such as the IP address and the corresponding security level. The second describes modeled security properties in relation to the SRs, for instance, whether the entity is a human actor. The third category delineates properties of communications, such as the expected protocol used for data exchange.

The Monitoring layer is realized utilizing the open-source network monitoring tool Zeek[5]. While originally designed as an intrusion detection system, Zeek features an extensive scripting language that allows configuring built-in monitoring scripts to generate compliance-related logs. This streamlined the development process, enabling the amalgamation of multiple components of the monitoring layer into a single platform based on existing Zeek scripts. The Evidence Gathering module is represented by Zeeks' built-in network monitoring events, and the Compliance Monitoring module is facilitated by custom scripts that generate compliance-related logs.

The specification and Extraction layers are not implemented but are based on the manual selection of relevant SRs. This resulted in an extract of 25 SRs that benefitted from the input of the Modeling Layer. On this basis, we created the SCI portfolio manually and integrated it into the configuration of the Monitoring Layer. The prototype receives input from the BPMN diagrams, extracting expected values for related communications and entities. It then compares this information with the gathered network traffic, generating an output that reflects the live compliance status of the system. The structure of the custom scripts is informed by the knowledge derived from the SCI portfolio of the Specification Layer. This knowledge establishes a connection between actual monitorable properties in the network traffic and the informally described SRs of the security standard. These logs subsequently serve as input for the Verification layer.

For the Verification layer, an Elastic Stack[6] is utilized for aggregating, filtering, indexing, and visualizing the generated logs. The current implementation of the Verification Layer focuses on the visualization aspect using dashboards generated with boolean-type fields for each of the monitored SRs. This visualized output provides a human user with the means to verify the real-time compliance status of the monitored system.

6 Evaluation

This section evaluates if the proposed artifact provides a viable solution to the problems accompanying security standard compliance. As proposed by (Peffers, Rothenberger, et al., 2012) and demonstrated in Section 5, a prototype is used for that evaluation. To further structure our argumentation, we revisit the MRs presented in Subsection 3.2 representing the objectives of the SCMV artifact. By answering the MRs we can evaluate the quality of our framework. If the MRs (1) and (3) are present in the design, an answer to RQ was implicitly provided, through the introduction of the frameworks components. Accordingly the second MR (2) is related to the second RQ, and discusses the connection of business processes and their attributes to the contribution.

The first meta requirement derived was: *(1) The artifact should define necessary components of an SCMV system to achieve better understanding and delimitation in research*.

In practice, systems that monitor compliance with security standards are usually deployed as part of

[3] https://github.com/automayt/ICS-pcap
[4] camunda.com
[5] zeek.org
[6] elastic.co

general security architectures that implement measures to fulfill the SR and subsequently verify their implementation status. As a result, compliance-related systems are not clearly differentiated from other forms of monitoring systems, such as intrusion detection systems. In order to achieve full compliance with security standards and improve the process of compliance, an artifact that highlights this delineation by defining the components of the SCMV was required. With the prototype, it was possible to demonstrate an example of the implementation of each of the SCMV architecture components. Each of the components is dependent on the other and is required for the prototype to produce an output comparable to Figure 6. Such an output can be seen as the implementation of the verification part of SCMV, which depicts the end of the process. The start of the process is represented by a BPMN diagram, which works the same as a SL-T, initiating the process. With the demonstration, we were able to achieve a full process implementation, producing a valid output depicting the SL-T. Because of that, we can infer that the defined components in the SCMV framework are necessary for a system deployed in practice, spanning the whole SCMV process, and therefore, we contribute a delimitation of compliance monitoring systems to other monitoring systems and the artifact provides an answer to the first MR.

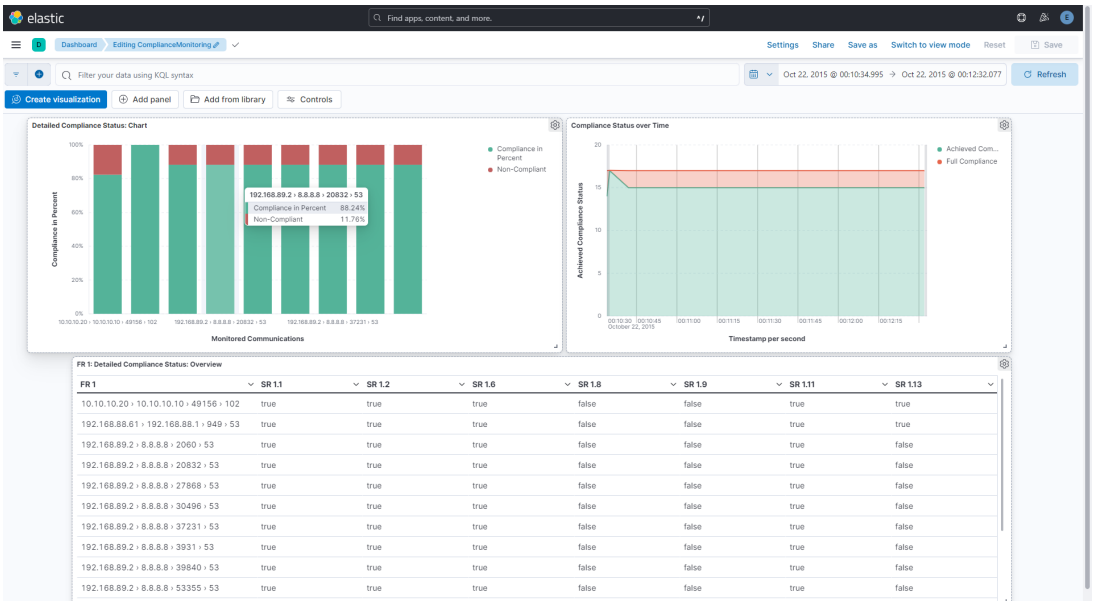


Figure 6. Example for a Compliance Dashboard visualization with Kibana

The second meta requirement was: *(2) The artifact should incorporate and highlight process-related information and present its impact on other design components*

We were able to highlight the impact of process-related information on the framework within the prototypes' concept by including the modeling layer as a central part. The BPMN attributes were imported automatically into the Monitoring Layer based on an XML file and then used as counter values to the observed network traffic generated by reading an ICS pcap file with pre-recorded network traffic. This attribute parsing spares us from manually defining these values within the SCI portfolio and, therefore, has an imminent impact. Using the existing information within SCMV, as they are provided by the BPMN diagrams in form of System-, Entity- and Communication UML annotations, is therefore incorporated into the SCMV framework and demonstrated by the prototype. With the previously defined SCI portfolio, we were able to passively monitor compliance to 25 SRs. In combination with active monitoring techniques, process information could elevate the compliance monitoring capabilities even further.

The third meta requirement was: *(3) The artifact should be based on properties of the IIoT to achieve a domain specification for the IIoT*

The artifact fulfills the MR based on two aspects: (1) The defined structure of the SCMV process and,

therefore, the SCMV framework is based on principles of the IIoT standard IEC 62443 and general requirements on IIoT systems. This IACS-specific security standard includes domain-specific SRs and proposes the continuous aspect of standard compliance. This continuation is incorporated into the SCMV framework in the form of the SL-T as a starting point and the SL-T as the ending point of the process. Furthermore, the main property of IIoT systems is the importance of availability, recognized in the Monitoring Layer, where a passive monitoring component was chosen as the foundation. This allows the SCMV to fulfill the general availability requirements of IIoT systems. (2) The incorporation of BPMN attributes as a data source for the SCMV framework benefits from the process structure of industrial systems, with expected and cyclic network traffic. By highlighting and including the potential of process-related information in SCMV, a specification to the IIoT domain was possible.

Even though the MRs are visible in the artifact and we were able to demonstrate the framework with our prototype, open questions remain that need to be addressed in future research. The necessity for active monitoring components to span a relevant amount of security requirements, was only recognised and not implemented in the framework. Introducing active monitoring to the IIoT requires specific techniques, that respect the availability properties of such systems. This limitation is represented by the prototype, where we were able to only monitor 25 SRs with the passive monitoring foundation. Future work should improve the detail of the active monitoring part within the Monitoring Layer, as we were only able to recognise the necessity, but not to describe the specific properties.

7 Conclusion

In conclusion, this paper introduced a comprehensive framework for SCMV and demonstrated its practical implementation through a prototype, effectively realizing all layers and components. The adoption of a methodological approach rooted in DSR and DPs facilitated the integration of insights from industry practices and pertinent literature into the framework's design. Our proposed layered approach for the SCMV framework not only defined essential components but also delimited its scope from other monitoring domains, providing an answer to RQ2.

This contribution enables future research to target specific components or layers for enhancing SCMV by integrating with other research domains, incorporating emerging technologies, and advancing the overall automation of the standard compliance process. A pivotal aspect of this research was the integration of process-related information in the form of BPMN attributes, marking the second significant contribution. Our investigation into the impact of such information on the SCMV process led to its seamless integration as an additional layer in the SCMV framework.

The practical implementation of various SCMV layers not only validated the theoretical framework but also showcased the intricate interactions among its components. Specifically, the ability of the prototype to extract expected values from BPMN diagrams and monitor compliance to 25 SRs solely based on that information provided a tangible demonstration answering RQ1. This demonstration substantiated the assertion that process-related information, when integrated into an SCMV system, enhances overall security standard compliance.

In essence, this paper establishes a robust research foundation for the domain of SCMV in the IIoT. The potential for future work lies in further research endeavors aimed at improving and automating the various layers of the framework, ensuring its continued relevance and effectiveness in addressing evolving security challenges.

References

Bandyopadhyay, D. and J. Sen (2011). "Internet of things: Applications and challenges in technology and standardization." *Wireless personal communications* 58, 49–69.

Bicaku, A., M. Tauber, and J. Delsing (2020). "Security standard compliance and continuous verification for Industrial Internet of Things." *IJDSN* 16 (6), 155014772092273. DOI: 10.1177/1550147720922731.

Bicaku, A., M. Zsilak, P. Theiler, M. Tauber, and J. Delsing (2022). "Security Standard Compliance Verification in System of Systems." *IEEE Systems Journal* 16 (2), 2195–2205. DOI: 10.1109/jsyst.2021.3064196.

Cheng, D. C., J. B. Villamarin, G. Cu, and N. R. Lim-Cheng (2018). "Towards end-to-end continuous monitoring of compliance status across multiple requirements." *International Journal of Advanced Computer Science and Applications* 9 (12).

Conklin, W. A. (2016). "IT vs. OT Security: A Time to Consider a Change in CIA to Include Resilienc." In: *HICSS*. IEEE. DOI: 10.1109/hicss.2016.331.

Cruz, T., J. Barrigas, J. Proenca, A. Graziano, S. Panzieri, L. Lev, and P. Simoes (2015). "Improving network security monitoring for industrial control systems." In: *2015 IFIP/IEEE International Symposium on Integrated Network Management (IM)*. IEEE. DOI: 10.1109/inm.2015.7140399.

Dumas, M., M. La Rosa, J. Mendling, H. A. Reijers, et al. (2018). *Fundamentals of business process management*. Vol. 2. Springer.

ENISA (2016). "Communication network dependencies for ICS/SCADA Systems."

Fenz, S. and T. Neubauer (2018). "Ontology-based information security compliance determination and control selection on the example of ISO 27002." *Information & Computer Security* 26 (5), 551–567. DOI: 10.1108/ics-02-2018-0020.

Gregor, S., D. Jones, et al. (2007). "The anatomy of a design theory." In: Association for Information Systems.

Heinrich, P. and G. Schwabe (2014). "Communicating nascent design theories on innovative information systems through multi-grounded design principles." In: *Advancing the Impact of Design Science: Moving from Theory to Practice: 9th International Conference, DESRIST 2014, Miami, FL, USA, May 22-24, 2014. Proceedings 9*. Springer, pp. 148–163.

Hornsteiner, M. and S. Schönig (2023). "SIREN: Designing Business Processes for Comprehensive Industrial IoT Security Management." In: *DESRIST 2023*. Vol. 13873. LNCS. Springer, pp. 379–393. DOI: 10.1007/978-3-031-32808-4_24.

IEC (July 2009). *Cybersecurity for Operational Technology in Automation and Control Systems*. Standard. Geneva, CH: International Electrotechnical Commission.

Jardine, W., S. Frey, B. Green, and A. Rashid (2016). "Senami: Selective non-invasive active monitoring for ics intrusion detection." In: *Proceedings of the 2nd ACM Workshop on Cyber-Physical Systems Security and Privacy*, pp. 23–34.

Julisch, K. (2008). "Security compliance: the next frontier in security research." In: *Proceedings of the 2008 New Security Paradigms Workshop*, pp. 71–74.

Kobes, P. (2016). *Guideline Industrial Security: IEC 62443 is easy*. 2nd Edition. VDE Verlag. ISBN: 978-3-8007-5305-5.

Kopetz, H. and W. Steiner (2022). "Internet of Things." In: *Real-Time Systems*. Springer International Publishing, pp. 325–341. DOI: 10.1007/978-3-031-11992-7_13.

Kulik, T., P. W. V. Tran-Jorgensen, and J. Boudjadar (2019). "Compliance verification of a cyber security standard for Cloud-connected SCADA." In: *GIoTS 2019*. IEEE. DOI: 10.1109/giots.2019.8766363.

Nicholson, A., H. Janicke, and A. Cau (2014). "Position paper: Safety and security monitoring in ics/scada systems." In: *ICS-CSR 2014*, pp. 61–66.

Oberhofer, D., M. Hornsteiner, and S. Schönig (2023). *Market Research on IIoT Standard Compliance Monitoring Providers and deriving Attributes for IIoT Compliance Monitoring*. arXiv: 2311.09991.

Palattella, M. R., M. Dohler, A. Grieco, G. Rizzo, J. Torsner, T. Engel, and L. Ladid (2016). "Internet of Things in the 5G Era: Enablers, Architecture, and Business Models." *IEEE Journal on Selected Areas in Communications* 34 (3), 510–527. DOI: 10.1109/jsac.2016.2525418.

Peffers, K., M. Rothenberger, T. Tuunanen, and R. Vaezi (2012). "Design science research evaluation." In: *DESRIST 2012, Las Vegas, NV, USA, May 14-15, 2012. Proceedings 7*. Springer, pp. 398–410.

Peffers, K., T. Tuunanen, M. A. Rothenberger, and S. Chatterjee (2007). "A design science research methodology for information systems research." *Journal of management information systems* 24 (3), 45–77.

Raposo, D., A. Rodrigues, S. Sinche, J. Sá Silva, and F. Boavida (2018). "Industrial IoT monitoring: Technologies and architecture proposal." *Sensors* 18 (10), 3568.

Rubio, J. E., C. Alcaraz, R. Roman, and J. Lopez (2017). "Analysis of Intrusion Detection Systems in Industrial Ecosystems." In: *ICETE*. SCITEPRESS. DOI: 10.5220/0006426301160128.

Sadeghi, A.-R., C. Wachsmann, and M. Waidner (2015). "Security and privacy challenges in industrial internet of things." In: *Proceedings of the 52nd Annual Design Automation Conference*. ACM. DOI: 10.1145/2744769.2747942.

Schönig, S., M. Hornsteiner, and C. Stoiber (2022). "Towards Process-Oriented IIoT Security Management: Perspectives and Challenges." In: *Enterprise, Business-Process and Information Systems Modeling*. Springer International Publishing, pp. 18–26. DOI: 10.1007/978-3-031-07475-2_2.

Serror, M., S. Hack, M. Henze, M. Schuba, and K. Wehrle (2021). "Challenges and Opportunities in Securing the Industrial Internet of Things." *IEEE Transactions on Industrial Informatics* 17 (5), 2985–2996. DOI: 10.1109/tii.2020.3023507.

Shaaban, A. M., S. Chlup, N. El-Araby, and C. Schmittner (2022). "Towards Optimized Security Attributes for IoT Devices in Smart Agriculture Based on the IEC 62443 Security Standard." *Applied Sciences* 12 (11), 5653. DOI: 10.3390/app12115653.

Shaaban, A. M., E. Kristen, and C. Schmittner (2018). "Application of IEC 62443 for IoT Components." In: *Developments in Language Theory*. Springer International Publishing, pp. 214–223. DOI: 10.1007/978-3-319-99229-7_19.

Sisinni, E., A. Saifullah, S. Han, U. Jennehag, and M. Gidlund (2018). "Industrial Internet of Things: Challenges, Opportunities, and Directions." *IEEE Transactions on Industrial Informatics* 14 (11), 4724–4734. DOI: 10.1109/tii.2018.2852491.

Tange, K., M. D. Donno, X. Fafoutis, and N. Dragoni (2020). "A Systematic Survey of Industrial Internet of Things Security: Requirements and Fog Computing Opportunities." *IEEE Communications Surveys & Tutorials* 22 (4), 2489–2520. DOI: 10.1109/comst.2020.3011208.

Ullah, K. W., A. S. Ahmed, and J. Ylitalo (2013). "Towards Building an Automated Security Compliance Tool for the Cloud." In: *2013 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications*. IEEE. DOI: 10.1109/trustcom.2013.195.

Zhou, C., S. Huang, N. Xiong, S.-H. Yang, H. Li, Y. Qin, and X. Li (2015). "Design and Analysis of Multimodel-Based Anomaly Intrusion Detection Systems in Industrial Process Automation." *IEEE Transactions on Systems, Man, and Cybernetics: Systems* 45 (10), 1345–1360. DOI: 10.1109/tsmc.2015.2415763.

P5: Reading between the Lines: Process Mining on OPC UA Network Data

Status	Published	
Date of Submission	22 May 2024	
Date of Acceptance	06 July 2024	
Date of Publication	11 July 2024	
Journal	Sensors	
Authors Contribution	Markus Hornsteiner	50%
	Philip Empl	30%
	Timo Bunghardt	10%
	Stefan Schönig	10%
Full Citation	Hornsteiner, M., Empl, P., Bunghardt, T., Schönig, S. (2024). Reading between the Lines: Process Mining on OPC UA Network Data. *Sensors*, 24(14), 4497.	
DOI	10.3390/s24144497	
Artifact	`https://github.com/philipempl/opcua-mining`	

Journal Description: Sensors is an international, peer-reviewed, open access journal on the science and technology of sensors. Sensors is published semimonthly online by MDPI.

sensors

MDPI

Article

Reading between the Lines: Process Mining on OPC UA Network Data

Markus Hornsteiner, Philip Empl, Timo Bunghardt and Stefan Schönig *

Faculty of Informatics and Data Science, University of Regensburg, 93053 Regensburg, Germany; markus.hornsteiner@ur.de (M.H.); philip.empl@ur.de (P.E.); timo-bunghardt@t-online.de (T.B.)
* Correspondence: stefan.schoenig@ur.de

Abstract: The introduction of the Industrial Internet of Things (IIoT) has led to major changes in the industry. Thanks to machine data, business process management methods and techniques could also be applied to them. However, one data source has so far remained untouched: The network data of the machines. In the business environment, process mining, for example, has already been carried out based on network data, but the IIoT, with its particular protocols such as OPC UA, has yet to be investigated. With the help of design science research and on the shoulders of CRISP-DM, we first develop a framework for process mining in the IIoT in this paper. We then apply the framework to real-world IIoT network traffic data and evaluate the outcome and performance of our approach in detail. We find tremendous potential in network traffic data but also limitations. Among other things, due to the dependence on process experts and the existence of case IDs.

Keywords: process mining; industrial IoT; business process management; industry 4.0

Citation: Hornsteiner, M.; Empl, P.; Bunghardt, T.; Schönig, S. Reading between the Lines: Process Mining on OPC UA Network Data. *Sensors* **2024**, *24*, 4497. https://doi.org/10.3390/s24144497

Academic Editor: Joaquin Ordieres Meré

Received: 22 May 2024
Revised: 2 July 2024
Accepted: 6 July 2024
Published: 11 July 2024

1. Introduction

Industrial Internet of Things (IIoT) technologies have ushered in a new era of manufacturing and industrial processes, offering unprecedented levels of connectivity, automation, and data-driven decision-making. In the heart of these dynamic ecosystems lies the seamless exchange of information among interconnected devices, sensors, and control systems [1]. This intricate web of interactions, facilitated by standard industrial communication protocols such as OPC UA (Open Platform Communications Unified Architecture) [2] and MQTT (Message Queue Telemetry Transport), generates vast volumes of network data, which, until recently, remained an untapped resource for unraveling the underlying operational intricacies [3,4].

In this paper, we delve into the realm of process mining as a transformative approach to extract invaluable insights from collected network data in IIoT environments. Process mining, a field at the confluence of data science, machine learning, and process management, refers to the automated discovery, monitoring, and improvement of process models from event data of IT systems [5]. Event data are used in the research area of process mining to generate and compare process models automatically with the help of process mining algorithms. Event information can be generated by classical IT systems as well as by employees using smart devices, (production) machines, and sensors [6–8]. IT systems within an organization create, for example, records of activities performed, messages sent, or transaction data. These event data are compiled into event logs and form the starting point for process mining algorithms.

Using network data to discover business processes is an emerging research area that has recently garnered significant attention [9–12]. Integrating process mining with network data in IIoT environments has the potential to revolutionize industrial operations by providing a data-driven perspective for optimizing processes, enhancing decision-making, and unlocking the full potential of IIoT technologies [13]. This paper thoroughly investigates this innovative intersection, exploring its theoretical foundations, practical

implementation, and transformative impact on industrial operations. It addresses the following research question: "How to mine operational processes from OPC UA network traffic data?" To the best of our knowledge, our approach is the first to focus on rule-based process mining using real-world OPC UA network data. We outline the essential steps to transform unstructured and raw network data into an event log suitable for process mining, with a particular emphasis on collecting, preprocessing, and analyzing network data from IIoT environments. This involves addressing the challenges and complexities associated with handling large-scale, heterogeneous data sources. Through a real-world use case, we demonstrate the practical application of our approach, showcasing how it can generate actionable insights that lead to significant operational improvements. In summary, our contributions are as follows:

- We introduce a novel approach to generate event logs from OPC UA packets for use in process mining.
- We implement a proof-of-concept based on our approach, demonstrating the performance and quality of the process models derived from the generated event logs.
- To the best of our knowledge, we are the first to apply process mining on real-world network traffic data, rather than simulated data, illustrating how this approach can produce actionable insights that translate into operational benefits.

The paper is structured as follows: in Section 2, we present essential basics and related literature on process mining and network traffic data. This is followed in Section 3 by our method to discover business processes in the IIoT. In Section 4, we present the implementation of the method, which we apply to a real-world use case in Section 5. We evaluate and discuss our method in Section 6 regarding performance and quality and conclude the paper in Section 7.

2. Background and Related Work

2.1. Process Mining and Network Event Data

Event data, generated during business process execution, include details on activities, their sequence, timestamps, and contextual information. Event data are derived from systems like databases, software applications, or sensors and are the foundation for process mining. By combining data mining, machine learning, and process management techniques, process mining analyzes and visualizes event data to reconstruct and model organizational processes. It identifies inefficiencies, bottlenecks, compliance issues, deviations, and improvement opportunities. Process mining relies on event logs as its core input, forming the basis for analyzing and optimizing processes. Network data are precious for process mining due to various reasons:

- Rich Information Source: Network data contain information generated by interconnected devices and systems. They capture interactions and communications between entities, providing a detailed record of activities and their sequence.
- Granularity and Detail: Network data often offer granular insights into the flow of activities and dependencies among different elements within a system. This information can be valuable for reconstructing processes accurately.
- Real-Time and Continuous Data: Networks generate real-time data as activities occur, offering a current and comprehensive view of ongoing processes. This real-time feature allows for immediate analysis of deviations or inefficiencies.
- Comprehensive Coverage: Network data often cover various activities, including structured and unstructured data, allowing for a holistic view of processes.
- Interconnection of Systems: In many cases, processes are interconnected across various systems or devices. Analyzing network data helps understand the interactions and dependencies among these systems, offering insights into end-to-end processes.

Network data, though rich, can be complex and varied, requiring specialized expertise for effective preprocessing, analysis, and interpretation in process mining. Regarding the

IIoT, OPC UA is a widely used communication protocol in industrial automation, which is discussed in the following.

2.2. OPC UA Protocol

OPC UA (Open Platform Communications Unified Architecture) is a machine-to-machine communication protocol that is widely used in industrial automation systems. It provides a framework for secure and reliable data exchange between various devices and applications in a networked environment. OPC UA supports multiple data encoding formats to represent information during communication. These formats include binary, JSON (JavaScript Object Notation), and XML (eXtensible Markup Language). Each format has its own characteristics and usage scenarios. Binary encoding is preferred for performance-critical applications with limited bandwidth, while JSON and XML are used in web-based and interoperable systems where human readability and compatibility are crucial.

Table 1 provides an overview of the OPC UA packet structure. OPC UA can establish secure channels to ensure data confidentiality and integrity (A). Messages are either encapsulated within this channel or directly transmitted over the network. The message header contains crucial details such as type, size, and encoding (B). The message body holds the actual content, varying by message type (C). OPC UA defines a set of services that allow clients and servers to interact (D). These services are transmitted via the message body and provide functionality for various operations, such as reading and writing data, subscribing to events, browsing the server's address space, and managing sessions.

Table 1. OPC UA Packet Structure.

Secure Channel Layer (A)	**Optional**
Message Header (C)	fixed size
Message Type	4 bytes
Message Size	4 bytes
Secure Channel ID	4 bytes
Security Flag	4 bytes
Additional Header	variable size
Message Body (D)	variable size
ReadRequest/ReadResponse (E)	variable size

Every OPC UA handshake follows the request and response pattern, as shown by the read operation in Table 2. Besides the requested (e.g., NodesToRead) or transmitted data (e.g., Results), OPC UA packets carry the request handle located in the header, a unique identifier assigned to a client's request message when communicating with a server. It correlates a request (see Table 2a) and a response (see Table 2b) within a session. The request handle serves three main purposes. First, it allows the client to match the response received from the server to the original request. Second, OPC UA supports asynchronous communication, where a client can send multiple requests to a server without waiting for responses. Third, in case of errors or exceptions during processing, the server includes the request handle in the error response.

Table 2. Request and Response Headers. (**a**) OPC UA Read Request; (**b**) OPC UA Read Response.

(**a**)	
Request Header	
Type ID	4 bytes
Request Handle	4 bytes
Timestamp	8 bytes
NodesToRead	variable
(**b**)	
Response Header	
Type ID	4 bytes
Request Handle	4 bytes
Timestamp	8 bytes
Results	variable

2.3. Related Work

Process mining is an analytical discipline that aims to discover, monitor and improve real-world processes by extracting knowledge from event logs available in today's information systems [14]. It bridges the gap between data-centric analysis techniques such as machine learning, data mining and business process management. By leveraging event logs, process mining provides insights into actual process execution and enables organizations to improve efficiency, compliance and overall process performance [5]. One focus within this discipline is the identification and connection of new data sources for process mining as well as the processing and correlation of analyzed unstructured data and events. The aim is to exploit previously untapped potential. Examples of this include text data [15,16], time series [17], sensor data [18,19], or video data [20,21], or, as in this paper, network data. Network data for process mining is a burgeoning research area gaining significant attention (Table 3). Existing studies predominantly use simulated network data from tools like Wireshark (https://www.wireshark.org/ (acccessed on 10 June 2024)) and can be categorized into two event log generation techniques: rule-based and model-based. We explore related works organized by their event log generation techniques in the following.

Table 3. Related works on network data-based process mining.

Reference	Input Data	Log Generation	Automation	Model	IIoT
Wakup & Desel [11]	Simulated	Rule-based	◑	Petri net	
Engelberg et al. [9]	Simulated	Rule-based	◑	BPMN	
Hadad et al. [10]	Simulated	Model-based	◑	Event log	
Apolinário et al. [22]	Simulated	Model/rule-based	●	BPMN	
Lange & Möller [23]	Simulated	Model-based	●	BPMN	
Lange et al. [24]	Simulated	Model-based	●	BPMN	
Empl et al. [25]	Simulated	Rule-based	◑	Petri net	✓
Our paper	Real world	Rule-based	◑	BPMN	✓

◑ semi-automated; ● fully automated.

Rule-based Techniques. Rule-based techniques transform captured network traffic into structured event logs through predefined rules, necessitating manual rule definition beforehand. For instance, Wakup and Desel [11] employ filter TCP dumps with predefined rules and use TCPLog2Eventlog for extraction. Engelberg et al. [9] focus on HR recruitment, applying the heuristic miner to capture network data for business processes. Apolinário et al. [22] introduce FingerCI, combining techniques for ICS model construction.

Model-based Techniques. Model-based techniques generate event logs or process models from network traffic data, requiring no human intervention through unsupervised learning. Hadad et al. [10] propose unsupervised learning for event log generation, ad-

dressing challenges in activity recognition from network data. Lange et al. [24] introduce MONA, deriving workflows directly from network data without generating event logs.

In contrast to papers that are not related to IIoT, our work contributes to explainable rule-based event log generation and process discovery, focusing on real-world OPC UA network data captured from a manufacturing company's end-of-line business process. Unlike Empl et al. [25], we investigate the OPC UA protocol instead of MQTT, utilize real-world network data, and do not alter the network traffic, as their approach requires a predefined trace identifier. Additionally, we generate event logs without isolating processes and derive processes without relying on inexplicable machine-learning techniques.

3. OPC UA Process Discovery Method

To address the lack of a structured approach for process discovery from OPC UA network data, we develop this method in this paper. Process discovery involves obtaining data from running processes, generating event logs, and mining processes from these logs [26]. The challenge lies in abstracting multiple low-level network events into a high-level event log [27]. Following the design science research approach by Hevner et al. [28], we develop an IIoT-specific artifact with CRISP-DM (Cross Industry Standard Process for Data Mining) [29], as illustrated in Figure 1. Further details on the individual phases follow.

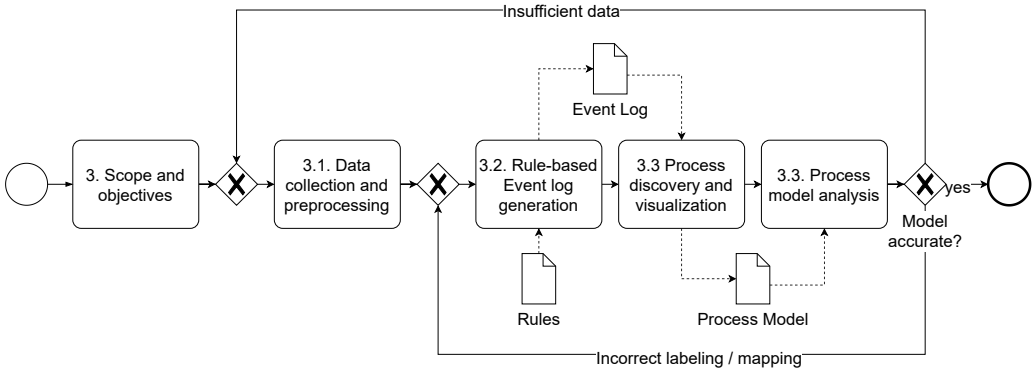


Figure 1. Generic process discovery approach in the IIoT.

Scope. Before starting, it is crucial to determine the scope: the target systems or components (which?), the technique, frequency, and timing (how?), the stakeholders (who?), and the desired outcome of the discovery (what for?). In addition, metrics must be defined to measure whether the scope has been achieved, e.g., which data should be used for the event log, or is there a process model to be compared against the output? The stakeholders involved should document and agree on these metrics to ensure the success [30].

3.1. Data Collection and Pre-Processing

Collect. Once the scope and objectives have been defined, we recommend using a passive data collection technique (network sniffing) instead of an active one, as it does not affect the operational processes and aligns with IIoT's high availability requirements. Passive recording is feasible using appropriate hardware (e.g., a switch with port mirroring) and software (e.g., Wireshark). Regardless of the hardware and software in use, the collected data's quality (e.g., completeness or encryption) is crucial. Competing with the large data volume, filtering rules (e.g., on ports) ensure alignment with the predefined scope, but when recording an initial snapshot, a full capture is recommended, pushing the understanding of the network further. Last, as the PCAP format might be difficult to handle, it can be transformed into human-readable formats (e.g., XML or JSON).

Understand. Before pre-processing the data, the data analyst must understand the data's context, e.g., by collecting additional information, such as existing process models, descriptions, expert interviews, asset inventories, or site visits. Afterward, it is crucial to understand the collected data [29]. In IIoT, this means gaining insights into the network

topology, IP addresses, ports or protocols. After resolving duplicates, the data analyst can dive deep into the structures of the packets to identify data of interest, such as the case ID for subsequent event logs. The visualization of information (e.g., social network diagram) can also be beneficial before data pre-processing.

Pre-processing. Network data are selected based on scope and objectives. Iteratively approaching the scope and objectives will lead to the desired outcome. Data analysts can assess the model's quality at each iteration by filtering less data and iteratively refining the selected data for the event log. Event log generation may involve aggregating multiple packets to form activities, especially in client-server architectures. In OPC UA, requests and responses can be matched using the so-called requestHandle (see Algorithm 1). The algorithm generates activities from low-level request-response events. Enriching activity names with human-readable labels ensures understandable process models. For example, if information on the function of a machine is available, replace the IP address and port with this information to increase readability.

Algorithm 1 Activity generation.

```
Require: opcua_packets
Ensure: matches
procedure MATCH_PACKETS(opcua_packets)
    req ← empty list
    res ← empty list
    for all packet in opcua_packets do
        ip ← packet.ipdst
        port ← packet.portdst
        time ← packet.time
        if packet.ttype == "MSG" then
            FIND_CONNECTION_TYPE(obj)
            if header then
                nodes ← GET_NODE_STRINGS
                if "RequestHeader" then
                    req.app(time,ip,port,nodes)
                else
                    res.app(time,ip,port,nodes)
                end if
            end if
        end if
    end for
    matches ← MATCH_REQUESTS(req, res)
    return SORT_BY_TIME(matches)
end procedure
```

3.2. Rule-Based Event Log Generation

After generating activities from filtered, aggregated, and labeled network packets, the next step is identifying each activity's process instance and generating an event log. Mandatory information of an event log includes the (1) case ID, (2) timestamp, and (3) activity name. The case ID is a unique identifier that identifies a process instance or a run and is assigned to all activities involved. Timestamps indicate the event's occurrence and provide information on sequential or parallel activities. While an event can have different activity names, non-uniqueness within the same process run is permitted. Optional information complements an event log, including information about the resource, e.g., the name of the actuator executing an activity. In the IIoT, we find physical processes and machines handing over products. We can refer to each product traveling through this process as a process instance, while a new process instance is created when it first appears in the network traffic. Each product has a unique identifier, ideal as a case ID. As not every packet carries the product identifier, pseudocode in Algorithm 2 details the event log generation

based on the case ID assignment. Automatically assigning activities ensures consistency over the process and the event logs. Experimenting with different case IDs (in the case of appropriate candidates) further allows the comparison throughout the event logs.

Algorithm 2 Event log generation.

```
Require: matches
Ensure: cases
procedure ADD_CASE_ID(matches)
    prod_id ← ITEM_ID
    ip_to_case_id ← empty dictionary
    cases ← empty list
    for all match in matches do
        time ← match.time
        ip ← match.ip
        port ← match.port
        nodes ← match.nodes
        case_id ← None
        for all node in nodes do
            if prod_id in node.keys() then
                case_id ← node(prod_id)
                ip_to_case_id[ip] ← case_id
                break
            end if
        end for
        case_id ← ip_to_case_id.get(ip)
        cases.app(time, ip, port, case_id)
    end for
    return cases
end procedure
```

3.3. Process Discovery, Visualization and Analysis

The derived event log is the basis for applying process mining techniques and enables identifying and visualizing processes and process instances. For example, process mining discovery techniques include heuristic, alpha, and inductive miners, which produce different outcomes (e.g., BPMN or Petri net). Each outcome, when visualized, shows different process perspectives. A direct follows graph creates an overview of process instances and dimensions (e.g., frequency or performance). The BPMN notation (and notably extended options with context-specific variables) focuses more on business processes [31].

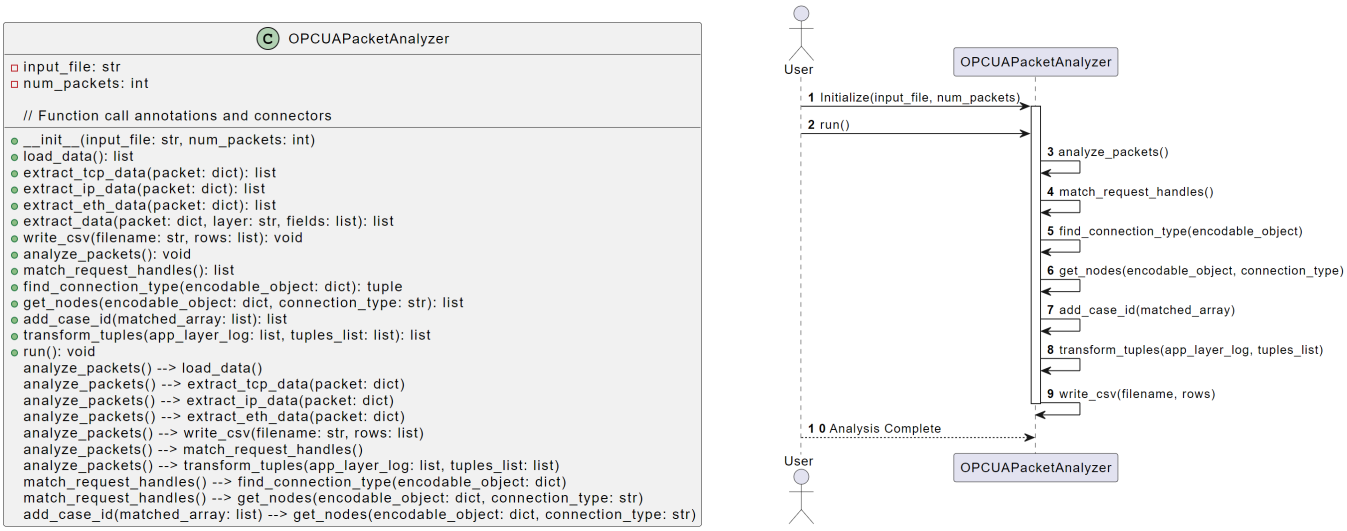
Data analysts can interpret the results regardless of the notation or process mining technique used. This way, deviations between the discovered and target processes can be identified, e.g., bottlenecks. Visualizations also help to uncover optimization potential. For informed decision-making, stakeholders can enrich the process models with expert knowledge if required. An inaccurate model (e.g., inadequate data or pre-processing) may result in returning to an earlier phase.

4. OPC UA Mining Implementation

This section introduces the Python implementation details of the event log generation using the OpcuaPacketAnalyzer class. This analyzes OPC UA network packets, extracting relevant information and generating event logs. The implementation is available on GitHub (https://github.com/philipempl/opcua-mining). It loads OPC UA data from a JSON file, extracts data from packets at various ISO/OSI layers, matches request/response handles in OPC UA packets, and generates CSV event logs. These event logs serve as the foundation for subsequent analysis.

4.1. Software Design

In Figure 2, we present a visual representation of the OpcuaPacketAnalyzer class structure and relationships (see Figure 2a). In the class diagram, we can derive the structure of the OpcuaPacketAnalyzer class, including its attributes and methods. The relationships between methods are depicted to provide a high-level overview of how they interact. A sequence diagram depicts the interactions and flow of control between objects and actors. In our case, we use a sequence diagram to illustrate how the OpcuaPacketAnalyzer class is invoked and how its methods interact (see Figure 2b). The sequence diagram shows the actions when users interact with the OpcuaPacketAnalyzer. The user initializes the class, runs the analysis, and triggers various internal methods to perform specific tasks, which we detail in the following.



(**a**) (**b**)

Figure 2. Implementation design of the OpcuaPacketAnalyzer class. (**a**) Class diagram. (**b**) Sequence diagram.

4.2. Implementation Details

We provide detailed explanations of key methods and functionalities of the OpcuaPacketAnalyzer class in the following:

Entrypoint. The analyze_packets() method is the entry point for event log generation, orchestrating data extraction, request handle matching, case ID assignment, and event log generation. It structures OPC UA packets for process mining and analysis.

Data Loading. The load_data() method loads OPC UA communication data from a Wireshark JSON file, ensuring availability for subsequent methods.

Data Extraction. Utilizing extract_tcp_data(), extract_ip_data(), and extract_eth_data(), this step extracts relevant data from packets at various ISO/OSI layers.

Request Handle Matching. The match_request_handles() method matches request handles in OPC UA packets, establishing relationships between requests and responses and creating activities.

Event Log Generation. The write_csv() method generates CSV event logs from extracted data for process mining or visualization.

Case ID Assignment. The add_case_id() method assigns case IDs to matched arrays of OPC UA packets based on keys, facilitating subsequent process mining techniques.

5. Use Case: End-of-Line Process

In this section, the methods from Section 3 to a real industrial use case are applied, demonstrating their application and relevance to OPC UA network data. We use the

OpcuaPacketAnalyzer class in a scenario involving an automotive supplier's end-of-line process, which includes robotic inspections, laser engraving, and cleaning. We examine each method phase and discuss appropriate measures. The dataset includes activities from four machines and a central process control system, providing a real-time process snapshot. The dataset comprises a total of 33 process instances, 30 of which are completed. A completed process instance signifies that the production of a part has commenced and reached a definitive conclusion. This conclusion can either indicate the completion of the entire process, resulting in a finished part or the termination of the process at an intermediate stage due to quality defects or other issues, leading to the ejection of the part. Our goal is to investigate the feasibility of mining this IIoT business process from OPC UA data.

5.1. Data Collection and Pre-Processing

Collect. We collect the data in real-time using a Raspberry Pi (https://www.onlogic.com/eu-en/computers/industrial/fanless/factor-200/) connected to the switch responsible for network communication. Using port mirroring, the Raspberry Pi captures and stores 30 minutes of network traffic in plain text on a USB hard disk. This created a snapshot of the network communication during live operation in PCAP format.

Understand. Initially, we attempted to read the PCAP file using pyshark (https://github.com/KimiNewt/pyshark), but faced limitations, such as no support for OPC UA. We then exported the network data with Wireshark to JSON, specifying relevant OPC UA service ports. The Wireshark OPC UA extension aids packet interpretation, enabling the creation of the network structure (see Figure 3a) for an overview. We identified the central network's IP address as .31 for the Process Control System (PCS) server. Among 24,445 OPC UA packets, we found 24,421 OPC UA message packets and 24 OpenSecureChannelRequest packets, which we did not further analyze. In total, 9244 packets have been sent by the PCS, the PCS has received 9247 packets, and 2965 were sent to the protocol server. The network data reveal that the PCS requests machine information through read and write requests. Publish and response packets lack production-relevant content, possibly due to an OPC PubSub-based notification system. Publish request packets originate from the PCS or the log system and are addressed to the cleaning, conveyor, and test systems, resulting in publish response packets. As the packet timestamps lack unique polling information, we exclude publish and subscribe packets from the event generation process.

(**a**) (**b**)

Figure 3. Representation of visualizations. (**a**) Network communication frequency based on IP addresses (green) and ports (grey). (**b**) Human-readable machine labeling of IP addresses.

Pre-processing. Following the contextual analysis of the packets, we initiate pre-processing. First, we exclude packets containing the protocol server and focus on OPC UA packets between machines and the PCS. We apply the request handle matching algorithm to create activities by aggregating OPC UA packets with matching request handle. For better

human readability, we assign labels using IP addresses with device type mapping (IP address:label). In Figure 3b, these labels, like .31:PCS server, serve as activity names in event logs, enhancing readability.

5.2. Rule-Based Event Log Generation and Process Mining

Next, we generate the event logs for the use case. We identify a product identifier (CanProduce.ITEM_ID) in the network traffic and use it as the case ID for the event log generation algorithm. The choice of case ID depends on the use case, which emphasizes the need to understand the data. The event log is then written to CSV files. After creating the event log, we apply process mining techniques. Appendix A shows the directly-follows graph of the event log. Since the alpha, heuristic and inductive miner use different algorithms, their results vary. Each process model has been evaluated for accuracy by process experts, with the result that all reflect reality to some degree. However, the process experts encounter difficulties when evaluating low-level network events.

6. Evaluation

As already shown that mining processes from OPC UA network data are feasible, we aim to assess the scalability and quality of our approach. To assess mining capabilities and model quality in the OPC UA context, we implement experiments within a Jupyter notebook, available on GitHub (https://github.com/philipempl/opcua-mining). Using a MacBook Pro 2021 with an Apple M1 Pro chip, 8 cores, and 16 GB of memory, we employ experiments on the OPCUAPacketAnalyzer class, analyzing OPC UA packets to generate event logs. This class extracts data from different ISO/OSI stack layers, generating logs for process mining algorithms. Performance evaluation involves generating event logs of varying sizes to understand scalability. Quality metrics such as replay fitness, precision, generalization, and simplicity gauge model performance. Collaboration with a process expert validates real-world accuracy and relevance, enriching results and fortifying practical implications.

6.1. Results

Event Log Generation Performance. Our experimental setup explores OPC UA packet processing performance by incrementally analyzing varying loads. Key metrics include time, CPU, and RAM usage. We start with 1000 packets, increasing by 1000 in each run until dataset exhaustion. Visualizing the results in Figure 4, packet analysis time shows a quadratic relationship with packet count, confirmed by a polynomial regression (black line). As expected, processing time increases with more packets. CPU and RAM usage (green and magenta lines) remain consistent, with occasional RAM spikes and steady CPU usage. Results indicate a significant computational demand increase with rising packet count. The polynomial regression in the experimental setup is as follows:

$$T(p) = 1.4840 \times 10^{-8} p^2 - 1.1514 \times 10^{-6} p + 0.0728$$

The polynomial regression trendline offers a predictive insight, where $T(p)$ is the time taken, and p is the number of packets, suggesting that for larger data sets, resource allocation should be planned judiciously to ensure optimal performance. For instance, generating an event log for 1,000,000 OPC UA packets requires approximately four hours, which is appropriate as it is the initial step towards process mining and deriving process models, which is relatively fast. The observed CPU/RAM usage trends further emphasize the importance of efficient resource management, when dealing with substantial packet loads.

Process Model Quality. Within our setting, we compare the quality of three process discovery algorithms, the Alpha miner, Heuristic miner, and Inductive miner, across varying dependency thresholds on our OPC UA data (see Figure 5). Therefore, we use established quality metrics: replay fitness, precision, generalization, and simplicity. Replay fitness measures how accurately the discovered model can reproduce the event log. Precision indicates how well the model represents the event log. Generalization measures how well

the discovered model can handle variations and unseen instances beyond the event log. Simplicity quantifies the level of complexity required by the model to represent the event log. In the following, we discuss those metrics.

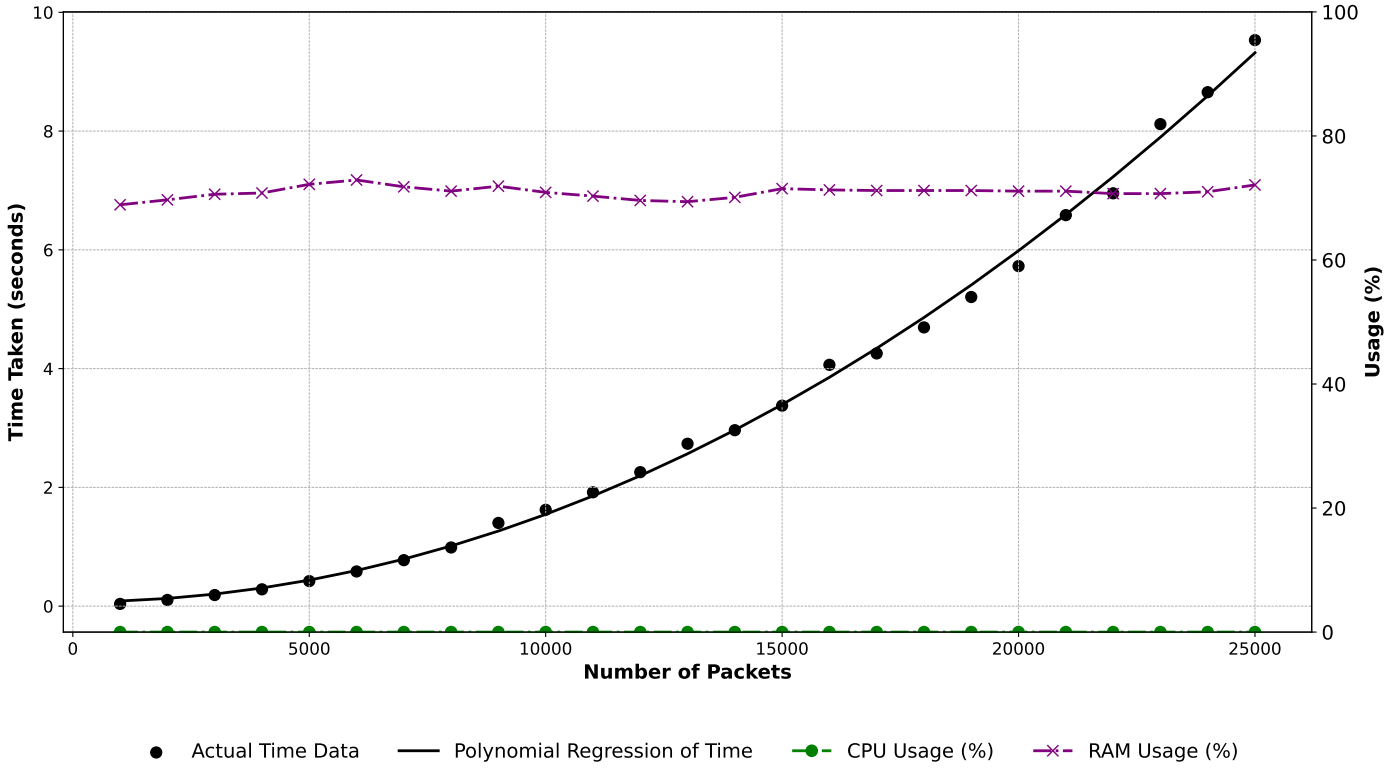
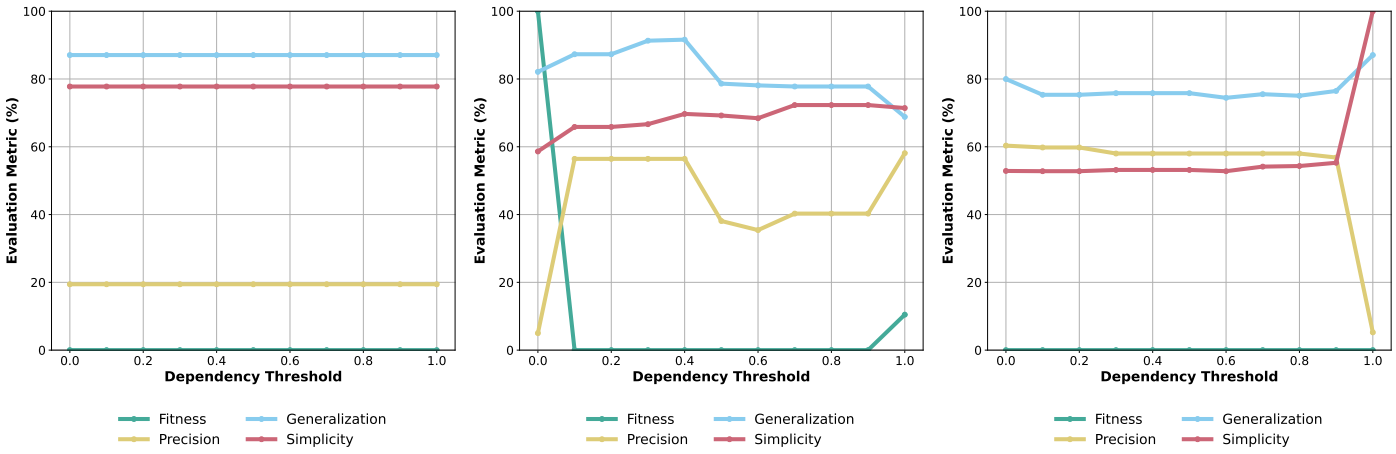


Figure 4. Performance analysis: time taken for analysis, CPU and RAM usage.

This threshold ranges from 0 to 1 and represents the minimum required dependency between activities to establish a causal relationship. Note, that the Alpha miner does not rely on dependency thresholds, resulting in horizontal lines. For the *Alpha miner* (Figure 5a), it consistently shows 0% fitness, indicating poor alignment with the event log. Precision, generalization, and simplicity metrics remain stable but at low values (19.4%, 87.1%, and 77.8%, respectively). This consistency indicates its limited adaptability. The *Heuristic miner* (Figure 5b) exhibits varied performance. At a threshold of 0, it achieves 100% fitness, declining sharply at higher thresholds. Precision peaks at 56.4%, with an upward trend in generalization. Simplicity fluctuates but remains within the mid-60% to mid-70% range. The *Inductive miner* (Figure 5c) shows intriguing results. At lower thresholds, it has 0% fitness, comparable to the Alpha miner. Precision starts at 60.3% and declines with higher thresholds. Generalization and simplicity fluctuate but within a tight range. In summary, the Heuristic Miner is highly adaptable but the Inductive Miner offers a balanced performance in precision, generalization, and simplicity. The Alpha miner, while stable, lacks alignment with the log. Considering these nuances is vital for selecting an optimal miner in practical applications.

Operational insights. We also gain insights from the continuous evaluation of processes through our industrial collaboration. An initial statement from the process expert is that "he would never have believed that we could get so close to the real process using only network data", which led to an internal rethink about the importance of network data for operational benefits. In addition, within the analysis of the network data, we identified further potential for process optimization. For example, in addition to OPC UA, we discovered that a server regularly searches for printers in the network, which reduced the performance of the network. There were also indications of typing errors in naming and variations in variables, which were identified.



(**a**) (**b**) (**c**)

Figure 5. Process discovery algorithms' quality with varying thresholds. (**a**) Alpha miner; (**b**) Heuristic miner; (**c**) Inductive miner.

6.2. Discussion

Limitations. While our research highlights the benefits of process mining in OPC UA network data, we acknowledge limitations that may impact the generalizability of our findings. First, our paper assumes the availability of network data in plain text. Encryption is sometimes used in real-life scenarios, which could conceal important information. Secondly, the method relies on a product ID for tracing and differentiating process instances. In cases of absent or inconsistent identifiers, mined process accuracy and completeness may be limited. Lastly, our dataset, covering only 32 unique process instances, may not represent the diversity of processes in more complex industrial settings, affecting the robustness and applicability of our insights.

Scientific Impact. In the evolving realm of process mining, our paper marks a paradigm shift, breaking away from conventional approaches. We pioneer the application of process mining to OPC UA data, showcasing its feasibility and effectiveness while highlighting key challenges, notably in data availability. This revelation emphasizes that datasets suitable for process mining are more extensive than previously believed. Our findings have broad applicability, such as in cybersecurity, where process models can enhance network intrusion detection or ensure compliance [31,32]. Last, our insights into OPC UA processes offer valuable nuances for future benchmarking studies.

Practical Impact. In the field of process mining, the decoding of OPC UA network data holds transformative potential for gaining insights into operational processes. Although our models currently have qualitative limitations, they already reflect real process behavior at the end of the production line. A larger volume of data would enable more meaningful models. While process experts are able to develop an understanding of the macro level, they may lack the granularity of network-level events. Accurately identifying process starting points is critical to aligning the mapped processes with the experts' understanding. Our 30-min capture shows that a one-week snapshot can reveal essential details for in-depth analysis. By bridging the gap between high-level process knowledge and complex network traffic patterns, organizations can realize the full potential of process mining.

In order to assess the accuracy of our process mining approach, we also collected the process manually by applying the methods of document analysis, interview and observation. To conduct this, we first examined two hours of available documents, then conducted a total of three interviews with two process experts over a total period of three hours and then observed the process on-site for two hours. We found that there was only a small difference between the manually recorded process and the real world, although this could be closed by the automatically recorded processes. Overall, however, it can be said that an automated survey has significant advantages over a manual one in terms of

effort and the associated costs. An automated recording and subsequent semi-automated investigation requires significantly fewer experts than interviews lasting several hours or an observation. In our opinion, an automated mining procedure and subsequent comparison by means of observation would be the most cost and effort-efficient way to survey processes in the IIoT.

7. Conclusions

Our research taps into the rich potential of network data in the IIoT, an area that has not been fully explored for generating event logs and uncovering business processes. To the best of our knowledge, we are the first to introduce a method that reveals IIoT processes based on (OPC UA) network traffic data. Our method not only advances academic research, allowing for more detailed comparisons and improvements (like benchmarking), but it also shows practitioners the real value of network traffic data. We developed an open-source prototype that represents a significant shift in process mining, offering a transparent and understandable way of mining OPC UA network data. Despite facing challenges like network encryption and working with a relatively small dataset, our findings are promising. They reveal that our process models accurately reflect a real-world use case at quite high quality with relatively good performance. In our discussion, we emphasize the importance of using larger datasets for more precise results. We are excited to follow future research in this area, confident that network traffic data are poised to unlock new opportunities in process mining and beyond.

Author Contributions: Conceptualization, T.B., P.E. and M.H.; methodology, P.E. and M.H.; software, T.B. and P.E.; validation, P.E. and M.H.; writing—original draft preparation, T.B., P.E. and M.H.; writing—review and editing, P.E., M.H. and S.S.; visualization, T.B., P.E. and M.H.; supervision, S.S.; project administration, M.H.; funding acquisition, S.S. All authors have read and agreed to the published version of the manuscript.

Funding: This work is funded by the "Bavarian Ministry of Economic Affairs, Regional Development and Energy" within the project Security Iiot pRocEss Notation (SIREN).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The datasets presented in this article are not readily available, as the data used was recorded in the real operations of an industrial company and its cybersecurity policies do not allow the publication of internal information. Nevertheless, all implemented artifacts presented in this paper are available on Github at https://github.com/philipempl/opcua-mining.

Conflicts of Interest: The authors declare no conflicts of interest.

Appendix A. Directly-Follows Graph of the End-of-Line Process

The directly follows graph (DFG) visualizes the sequence and frequency of events or activities in a given process. In this specific DFG, nodes represent distinct activities, such as *PublishRequest* and various *ReadRequest* operations with associated parameters. Directed edges between nodes signify the order in which these activities occur. For instance, an edge from *PublishRequest* to a *ReadRequest* indicates that the *PublishRequest* activity directly precedes the *ReadRequest* activity in the process sequence. Furthermore, numerical annotations on the edges, like 1588 or 1505, represent the sequence frequency, denoting how many times another directly followed one activity in the observed data. The nodes' parameters detail transferred data within the respective OPC UA tuples. This DFG provides insights into the common paths and patterns of the end-of-line process but is still cluttered.

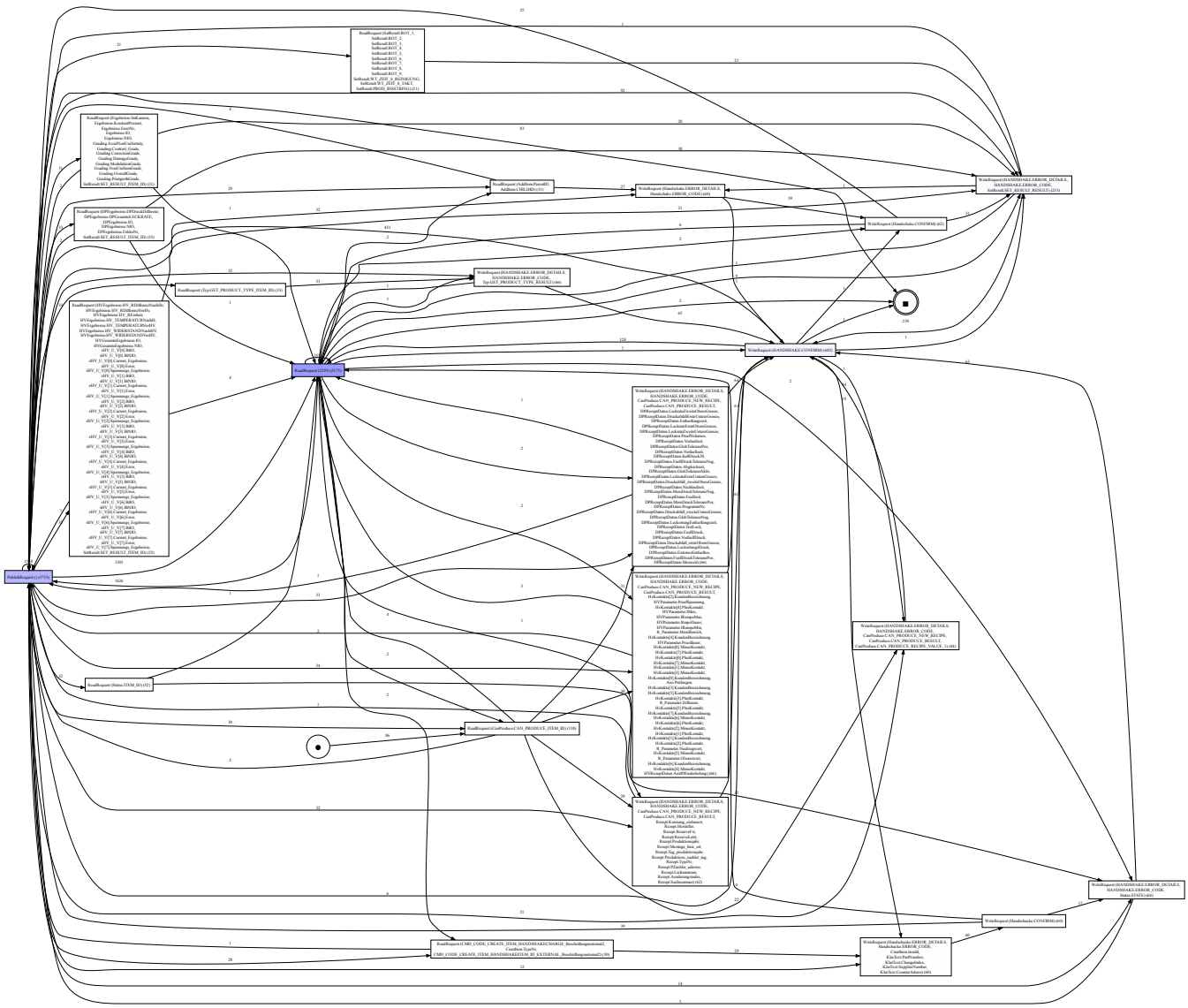


Figure A1. Cluttered directly-follows graph of the end-of-line process.

References

1. Boyes, H.; Hallaq, B.; Cunningham, J.; Watson, T. The industrial internet of things (IIoT): An analysis framework. *Comput. Ind.* **2018**, *101*, 1–12. [CrossRef]
2. Hästbacka, D.; Barna, L.; Karaila, M.; Liang, Y.; Tuominen, P.; Kuikka, S. Device status information service architecture for condition monitoring using OPC UA. In Proceedings of the 20th Conference on Emerging Technologies & Factory Automation, Luxembourg, 8–11 September 2015; pp. 1–7. [CrossRef]
3. Shin, S.J. An OPC UA-Compliant Interface of Data Analytics Models for Interoperable Manufacturing Intelligence. *IEEE Trans. Ind. Inform.* **2021**, *17*, 3588–3598. [CrossRef]
4. Schönig, S.; Hornsteiner, M.; Stoiber, C. Towards Process-Oriented IIoT Security Management: Perspectives and Challenges. In Proceedings of the Enterprise, Business-Process and Information Systems Modeling, Leuven, Belgium, 6–7 June 2022; pp. 18–26. [CrossRef]
5. van der Aalst, W.M. *Process Mining: Data Science in Action*; Springer: Berlin/Heidelberg, Germany, 2016. [CrossRef]
6. Bertrand, Y.; De Weerdt, J.; Serral, E. A bridging model for process mining and IoT. In Proceedings of the 3rd International Conference on Process Mining, Eindhoven, The Netherlands, 31 October–4 November 2021; Springer: Berlin/Heidelberg, Germany, 2021; pp. 98–110. [CrossRef]
7. Seiger, R.; Franceschetti, M.; Weber, B. An interactive method for detection of process activity executions from iot data. *Future Internet* **2023**, *15*, 77. [CrossRef]
8. Mangler, J.; Grüger, J.; Malburg, L.; Ehrendorfer, M.; Bertrand, Y.; Benzin, J.V.; Rinderle-Ma, S.; Serral Asensio, E.; Bergmann, R. DataStream XES extension: Embedding IoT sensor data into extensible event stream logs. *Future Internet* **2023**, *15*, 109. [CrossRef]

9. Engelberg, G.; Hadad, M.; Soffer, P. From network traffic data to business activities: A process mining driven conceptualization. In Proceedings of the International Conference on Business Process Modeling, Development and Support, Melbourne, Australia, 28–29 June 2021; Springer: Berlin/Heidelberg, Germany, 2021; pp. 3–18. [CrossRef]
10. Hadad, M.; Engelberg, G.; Soffer, P. From Network Traffic Data to a Business-Level Event Log. In Proceedings of the 2023 International Conference on Business Process Modeling, Development and Support, Zaragoza, Spain, 12–13 June 2023; Springer: Berlin/Heidelberg, Germany, 2023; pp. 60–75. [CrossRef]
11. Wakup, C.; Desel, J. Analyzing a TCP/IP-protocol with process mining techniques. In Proceedings of the International Conference on Business Process Management, Haifa, Israel, 7–11 September 2014; Springer: Berlin/Heidelberg, Germany, 2014; pp. 353–364. [CrossRef]
12. Ackermann, L.; Käppel, M.; Marcus, L.; Moder, L.; Dunzer, S.; Hornsteiner, M.; Liessmann, A.; Zisgen, Y.; Empl, P.; Herm, L.V.; et al. Recent Advances in Data-Driven Business Process Management, *arXiv* **2024**, arXiv:2406.01786.
13. Dunzer, S.; Zilker, S.; Marx, E.; Grundler, V.; Matzner, M. The Status Quo of Process Mining in the Industrial Sector. In *Innovation Through Information Systems. WI 2021*; Springer: Cham, Switzerland, 2021; pp. 629–644. [CrossRef]
14. van der Aalst, W.M.P. *Process Mining—Discovery, Conformance and Enhancement of Business Processes*; Springer: Berlin/Heidelberg, Germany, 2011. [CrossRef]
15. Banziger, R.B.; Basukoski, A.; Chaussalet, T. Discovering Business Processes in CRM Systems by leveraging unstructured text data. In Proceedings of the 2018 IEEE 20th International Conference on High Performance Computing and Communications; IEEE 16th International Conference on Smart City; IEEE 4th International Conference on Data Science and Systems (HPCC/SmartCity/DSS), Exeter, UK, 28–30 June 2018; pp. 1571–1577.
16. Chambers, A.J.; Stringfellow, A.M.; Luo, B.B.; Underwood, S.J.; Allard, T.G.; Johnston, I.A.; Brockman, S.; Shing, L.; Wollaber, A.; VanDam, C. Automated business process discovery from unstructured natural-language documents. In Proceedings of the Business Process Management Workshops: BPM 2020 International Workshops, Seville, Spain, 13–18 September 2020; Springer: Berlin/Heidelberg, Germany, 2020; pp. 232–243.
17. Fonger, F.; Aleknonyte-Resch, M.; Koschmider, A. Mapping Time-Series Data on Process Patterns to Generate Synthetic Data. In Proceedings of the Advanced Information Systems Engineering Workshops—CAiSE 2023 International Workshops, Zaragoza, Spain, 12–16 June 2023; Springer: Berlin/Heidelberg, Germany, 2023; Volume 482, pp. 50–61. [CrossRef]
18. Hemmer, A.; Abderrahim, M.; Badonnel, R.; François, J.; Chrisment, I. Comparative assessment of process mining for supporting IoT predictive security. *IEEE Trans. Netw. Serv. Manag.* **2020**, *18*, 1092–1103. [CrossRef]
19. Leotta, F.; Mecella, M.; Sora, D. Visual process maps: A visualization tool for discovering habits in smart homes. *J. Ambient Intell. Humaniz. Comput.* **2020**, *11*, 1997–2025. [CrossRef]
20. Knoch, S.; Ponpathirkoottam, S.; Fettke, P.; Loos, P. Technology-enhanced process elicitation of worker activities in manufacturing. In Proceedings of the Business Process Management Workshops: BPM 2017 International Workshops, Barcelona, Spain, 10–11 September 2017; Springer: Berlin/Heidelberg, Germany, 2018; pp. 273–284.
21. Kratsch, W.; König, F.; Röglinger, M. Shedding light on blind spots – Developing a reference architecture to leverage video data for process mining. *Decis. Support Syst.* **2022**, *158*, 113794. [CrossRef]
22. Apolinário, F.; Escravana, N.; Hervé, É.; Pardal, M.L.; Correia, M. FingerCI: Generating specifications for critical infrastructures. In Proceedings of the 37th ACM/SIGAPP Symposium on Applied Computing, Virtual, 25–29 April 2022; pp. 183–186. [CrossRef]
23. Lange, M.; Kuhr, F.; Möller, R. Using a deep understanding of network activities for workflow mining. In *KI 2016: Advances in Artificial Intelligence*; Springer: Berlin/Heidelberg, Germany, 2016; pp. 177–184. [CrossRef]
24. Lange, M.; Möller, R. Time series data mining for network service dependency analysis. In Proceedings of the SOCO'16-CISIS'16-ICEUTE'16, San Sebastián, Spain, 19–21 October 2016; Springer: Berlin/Heidelberg, Germany, 2017; pp. 584–594. [CrossRef]
25. Empl, P.; Böhm, F.; Pernul, G. Process-Aware Intrusion Detection in MQTT Networks. In Proceedings of the Fourteenth ACM Conference on Data and Application Security and Privacy (CODASPY '24), Porto, Portugal, 19–21 June 2024; p. 12. [CrossRef]
26. Cook, J.E.; Wolf, A.L. Automating Process Discovery Through Event-Data Analysis. In Proceedings of the 17th International Conference on Software Engineering, Seattle, WA, USA, 24–28 April 1995; pp. 73–82. [CrossRef]
27. Mannhardt, F.; de Leoni, M.; Reijers, H.A.; van der Aalst, W.M.P.; Toussaint, P.J. Guided Process Discovery—A pattern-based approach. *Inf. Syst.* **2018**, *76*, 1–18. [CrossRef]
28. Hevner, A.R.; March, S.T.; Park, J.; Ram, S. Design Science in Information Systems Research. *MIS Q.* **2004**, *28*, 75–105. [CrossRef]
29. Wirth, R.; Hipp, J. CRISP-DM: Towards a standard process model for data mining. In Proceedings of the 4th International Conference on the Practical Applications of Knowledge Discovery and Data Mining, Manchester, UK, 11–13 April 2000; Volume 1, pp. 29–39.
30. Mirza, M.N.; Pourzolfaghar, Z.; Shahnazari, M. Significance of Scope in Project Success. *Procedia Technol.* **2013**, *9*, 722–729. [CrossRef]
31. Hornsteiner, M.; Schönig, S. SIREN: Designing Business Processes for Comprehensive Industrial IoT Security Management. In Proceedings of the 18th International Conference on Design Science Research in Information Systems and Technology, Pretoria, South Africa, 31 May–2 June 2023; Springer: Berlin/Heidelberg, Germany, 2023; Volume 13873, pp. 379–393. [CrossRef]
32. Hornsteiner, M.; Stoiber, C.; Schönig, S. Towards Security- and IIoT-Aware BPMN: A Systematic Literature Review. In Proceedings of the 19th International Conference on Smart Business Technologies, Lisbon, Portugal, 14–16 July 2022; pp. 45–56.

P6: A Reflection on Process-oriented Industrial IoT Security Management

Status	Published
Date of Submission	22 October 2024
Date of Acceptance	04 December 2024
Date of Publication	03 March 2025
Conference	International Conference on Information Systems Security and Privacy
Location	Porto, Portugal
Period	20.02.2025 - 22.02.2025
Authors Contribution	Markus Hornsteiner 70% Linda Kölbel 10% Daniel Oberhofer 10% Stefan Schönig 10%
Full Citation	Hornsteiner, M., Kölbel, L., Oberhofer, D., Schönig, S. (2025). A Reflection on Process-Oriented Industrial IoT Cybersecurity Management. In: *Proceedings of the 11th International Conference on Information Systems Security and Privacy (ICISSP)*, pp. 242-253.
DOI	10.5220/0013163500003899

Conference Description: The International Conference on Information Systems Security and Privacy (ICISSP) is an event where researchers and practitioners can meet and discuss state-of-the-art research about the technological, social, and regulatory challenges that regard the security, privacy, and trust of modern information systems. The conference welcomes papers of either practical or theoretical nature, and is interested in research or applications addressing all aspects of trust, security and privacy, and encompassing issues of concern for organizations, individuals and society at large.

A Reflection on Process-oriented Industrial IoT Security Management

Markus Hornsteiner[a], Linda Koelbel[b], Daniel Oberhofer[c] and Stefan Schoenig[d]
University of Regensburg, Regensburg, Germany
{*markus.hornsteiner, linda.koelbel, daniel.oberhofer, stefan.schoenig*}*@informatik.uni-regensburg.de*

Keywords: Internet of Things, Process Management, IIoT Security

Abstract: The increasing adoption of the Industrial Internet of Things (IIoT) brings significant cybersecurity challenges due to the complexity and interconnectedness of industrial systems. This paper explores how business process management (BPM) can be applied to overcome these challenges by embedding security considerations into each phase of the BPM lifecycle: discovery, modeling, execution, and monitoring. Bringing together different research directions, including process mining, BPMN extensions and security compliance monitoring, this work provides a comprehensive overview of existing approaches to improve IIoT security. The paper presents opportunities for integrating security-aware processes into IIoT environments and provides insights into how organizations can use BPM to ensure continuous security enforcement and compliance. The study highlights current gaps and outlines opportunities for future development in the integration of BPM and IIoT security.

1 INTRODUCTION

The Industrial Internet of Things (IIoT) represents a paradigm shift in industrial environments, enabling increased connectivity, automation, and data-driven decision-making (Palattella et al., 2016; Sisinni et al., 2018). As organizations leverage IIoT technologies to enhance productivity and efficiency, they face unprecedented cybersecurity challenges, henceforth referred to as security (Serror et al., 2020). The interconnected nature of IIoT systems, often spanning legacy infrastructure, real-time operations, and diverse devices, creates a broad and dynamic attack surface. Securing these complex environments requires holistic approaches that go beyond traditional IT security frameworks and integrate security into business processes from the beginning - security by design. (Tange et al., 2020).

To address IIoT's unique security challenges, traditional controls can be complemented by process-centric approaches that consider the entire industrial lifecycle (Schönig et al., 2022). This paper explores how Business Process Management (BPM), a method traditionally used to improve organizational efficiency, can be adapted to enhance security in IIoT environments. BPM offers potentials to enhance IIoT security by providing a structured way to design, analyze, and monitor processes, enabling direct integration of security mechanisms (Oberhofer et al., 2024). By formalizing and visualizing security-aware workflows, BPM helps organizations understand device, data, and network interactions, ensuring security is embedded throughout the process lifecycle. By embedding process-centric security measures, organizations can define processes that are robust and adaptable to evolving threats (Schönig et al., 2022).

This work synthesizes existing approaches in the application of BPM to IIoT security management and describes a comprehensive framework summarized in Figure 2. The answered research questions and contributions of the framework therefore are threefold: We investigate *(i)* the benefits and propositions (*Why BPM is effective for IIoT security?*), *(ii)* the procedures and guidelines (*How to integrate and perform process-centric IIoT security management?*), and *(iii)* the concrete necessary concepts and techniques (*Using which technical tools and methods?*). By offering a structured overview of BPM methods applied to IIoT security, the aim is to provide both practitioners and researchers with an insight into how security can be systematically embedded in IIoT processes. Additionally, this synthesis highlights existing gaps in research and identifies opportunities for further development in this emerging field.

The structure of the paper is as follows: Section 2 provides background information on impor-

[a] https://orcid.org/0000-0002-8024-1220
[b] https://orcid.org/0009-0006-6907-2784
[c] https://orcid.org/0009-0008-9078-0149
[d] https://orcid.org/0000-0002-7666-4482

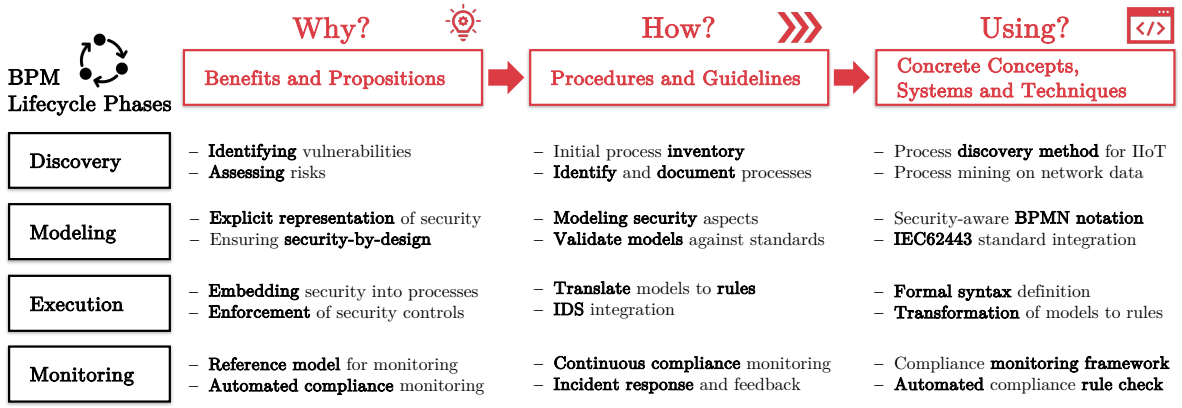


Figure 1: Overview of the presented process-centric IIoT security management framework

tant topics and describes the structure of the individual sub-areas. Section 3 introduces the overarching challenges of IIoT security and the benefits and propositions of BPM in addressing these challenges. Section 4 presents procedures and guidelines for applying BPM methods to IIoT security management. Section 5 delves into each phase of the BPM lifecycle, presenting concrete technical methods and approaches that can support IIoT security at each stage. Section 6 addresses open questions and possible future research approaches, followed by Section 7, which provides concluding thoughts and directions for future research.

2 BACKGROUND

2.1 Business Process Management

Business Process Management (BPM) encompasses all tasks and measures to make processes more efficient and effective (Hansen et al., 2019). BPM should serve as a decision-making aid for process improvement and support the management of organizations (Weske, 2012). In particular, the aim is to shorten throughput times, increase efficiency, save costs and minimize error rates, which then contributes to increasing competitiveness (Dumas et al., 2018; Bernardo et al., 2017). BPM is also seen as a strategy for gaining a competitive advantage, whereby numerous definitions exist (zur Muehlen and Ho, 2005).

2.2 Industrial IoT Security

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. In addition to the new opportunities offered by the IIoT, there are also new challenges. For example, the networking of industrial components opens up new opportunities for attackers to infiltrate, interrupt or maliciously modify processes (ENISA, 2018). One unique aspect of IIoT security is that, in contrast to IT security, it is primarily concerned with the security of OT and therefore availability (Tange et al., 2020). To ensure this, industry standards such as IEC62443 call for the *security by design* paradigm (IEC, 2009). This means that the security of processes and components must already be guaranteed during the design process. To consider security in industrial processes, there is a need for an inclusive modeling approach of security- and IIoT-aware processes (Schönig et al., 2022). In this paper, the term *security mechanisms* is used as an umbrella term to encompass a range of security-related concepts such as policies, rules, attributes, controls, protocols, measures, and requirements. These mechanisms represent various ways to address security concerns in IIoT environments. Additionally, *security controls* refers specifically to the concrete, actionable components within a system, such as access controls, data encryption, and network isolation, which are implemented to enforce security at different points in the process. By defining these terms upfront, the discussion of security in IIoT environments is streamlined, ensuring clarity when referring to different aspects of IIoT security throughout the paper.

2.3 Method

The discussion of the individual sub-areas presented in Section 5 follows a structured approach that en-

sures systematic identification of research gaps and artifacts aimed at addressing these gaps. The steps outlined below form the core methodology applied to each sub-area in Section 5, ensuring a consistent and rigorous approach across the entire study:

- **Definition of Research Questions** Each subarea begins with the identification and formulation of one or more research questions. These guide the exploration of specific challenges in that area and focus on how BPM can improve IIoT security. The research questions serve as the basis for the research and are aligned with the overarching objectives of this work.
- **Literature Review** If necessary, a suitable literature review is presented. This sets out the scientific basis for the problem and provides a comprehensive overview of the research area. This step ensures that all developments, trends and limitations in the literature are identified and lays the foundation for revealing research gaps.
- **Identification of Research Gaps** On the basis of the literature, one or more research gaps are identified and, in the following, approaches to closing them are presented. The identification of these gaps is critical, as it shapes the direction of the research and pinpoints the specific challenges that the developed artifacts must address.
- **Presentation of approaches** To address the research gaps, one or more artifacts are discussed, such as frameworks, models, methods, or tools. The artifact's development, presentation, testing, and evaluation are explained to determine its effectiveness in closing the research gap. This includes a critical evaluation of how well the artifact addresses the research gap and thus contributes to the expansion of knowledge in the field.

2.4 Effectiveness for IIoT Security

Contextual Awareness for Enhanced Security Traditional security measures like IDS and firewalls are essential, but their effectiveness improves significantly with a deeper understanding of the processes they protect (Parker et al., 2023). BPM provides this context by clarifying data flows, device interactions, and information exchange within the system, enabling more tailored security rules (Oberhofer et al., 2024). For instance, understanding device communication conditions allows for more precise monitoring and response mechanisms, resulting in stronger security.

Holistic Approach to Security Individual security tools often address specific threats but can overlook the broader context (Pulsipher et al., 2022). BPM offers a holistic approach by mapping system workflows and understanding process functions, enabling a comprehensive security strategy that integrates seamlessly with operations. This approach ensures security is proactive, not just reactive.

Adaptability in Dynamic Environments Industrial systems are dynamic, with constant changes in users, devices, and connections. Static security controls quickly become outdated, increasing vulnerability (Pulsipher et al., 2022). BPM keeps processes well-defined and current, allowing continuous adjustments to security mechanisms. This adaptability reduces the risk of legacy issues and maintains relevant, effective security over time.

Streamlined Compliance Management Standards like IEC 62443 require not only compliance but also proof over time (IEC, 2009). Integrating security into business processes simplifies traceability, allowing for continuous compliance management and streamlined audits. BPM ensures security measures can be verified throughout the process lifecycle, supporting long-term governance.

Proactive Security and Operational Continuity Security measures can sometimes disrupt operations unexpectedly (Goncharov, 2018). By incorporating security into process design, BPM aligns security mechanisms with operational needs from the start. This proactive approach prevents conflicts between security and functionality, ensuring that processes remain secure and fully operational, thus supporting both security and smooth business operations.

3 LEVERAGING BPM METHODS FOR IIOT SECURITY

To address IIoT's unique security challenges, traditional controls can be complemented by process-centric approaches that consider the entire industrial lifecycle (Schönig et al., 2022). BPM offers potential to enhance IIoT security by providing a structured way to design, analyze, and monitor processes, enabling direct integration of security mechanisms (Oberhofer et al., 2024). By formalizing and visualizing workflows, BPM helps organizations understand device, data, and network interactions, ensuring security is embedded throughout the process lifecycle.

This chapter explores how IIoT security can be supported by means of the four key phases of the pro-

cess lifecycle: process discovery, modeling, execution, and monitoring. Each phase offers opportunities to strengthen security by systematically integrating controls into the design, execution, and monitoring of processes.

3.1 Discovery

Process discovery identifies and documents existing processes in an IIoT environment, clarifying how devices, systems, and human operators interact (van der Aalst, 2010). This helps organizations create an accurate representation of workflows, serving as the foundation for modeling, execution, and monitoring phases. From a security perspective, process discovery is crucial for identifying vulnerabilities and gaps (Myers et al., 2017).

BPM-driven process discovery formalizes and maps as-is processes, capturing data flows between IIoT devices, systems, and control points. It identifies critical tasks, data exchanges, and supporting infrastructure. For example, process discovery can reveal how data flows from sensors to control systems and storage platforms. It also uncovers risks like unmonitored data flows, vulnerable connections, or legacy systems lacking security mechanisms.

BPM-driven process discovery helps create an inventory of IIoT assets and interactions (Hornsteiner et al., 2024), determining where to apply security controls. Understanding the process landscape allows teams to assess risks like unauthorized access or weak authentication, prioritizing security mechanisms during modeling and execution.

Insights from systematic process discovery also help understand operational disruptions, such as cascading effects from compromised devices. This supports proactive security mechanisms to guard against threats. For example, if a critical sensor is identified, additional monitoring or controls can be applied to protect multiple processes.

3.2 Modeling

Process modeling formally represents business processes using techniques like BPMN (Mendling et al., 2010). In IIoT security, this step is key to defining interactions between connected devices, data flows, and actors. Explicitly modeling these interactions provides a transparent and comprehensive view of the operational landscape, making it easier to identify vulnerabilities and enforce security mechanisms.

BPM methods provide a structured way to capture processes visually and formally. During modeling, critical security aspects - such as communication paths, data exchanges, and access control points - are mapped. For instance, BPMN diagrams can illustrate how data moves from servers to control systems and cloud storage. These workflows help security teams to identify vulnerable points, such as unauthorized data access or malicious device interactions.

Process modeling also allows the explicit representation of security mechanisms within the process. Controls such as data encryption, device authentication, or network segmentation can be integrated directly into the model, serving as templates for the security mechanisms used during real-time monitoring (Hornsteiner and Schönig, 2023). By incorporating security early in the modeling phase, organizations ensure that it becomes integral to process design rather than an afterthought.

BPM helps standardize and optimize interactions typical in IIoT, reducing ambiguity and ensuring consistent application of security across systems. Clear documentation of process flows and interactions in BPMN also improves communication between IT, OT, and security teams, fostering a shared understanding of system security requirements.

3.3 Execution

In the process execution phase, formally defined processes are executed in real-time using automation tools and systems. In IIoT environments, execution involves the interaction of multiple devices, sensors, and actuators, contributing to real-time operations of critical processes. This phase is crucial for security, as executing processes opens potential attack vectors like unauthorized device access, data manipulation, and network intrusion.

BPM enhances security during execution by embedding security mechanisms directly into executable processes. Formalizing workflows through model-based execution allows for the tight integration of security controls, such as authentication, authorization, and encryption-at the operational level (Hornsteiner and Schönig, 2023). For instance, BPM tools can enforce access controls for actors (e.g., machines or operators), ensuring that only authorized entities can trigger actions, thereby reducing the risk of unauthorized access.

BPM methods standardizes data flows and communication channels between IIoT devices. Modeling these interactions establishes clear security mechanisms for device communication. Such specifications mitigate risks like man-in-the-middle attacks or data tampering by enforcing secure communication protocols during BPM-driven executions.

Moreover, BPM-based execution frameworks can

incorporate real-time security monitoring as part of the process. Embedding security checks into executed workflows ensures continuous security assessment. For example, if a device behaves anomalously, predefined BPM rules can trigger alerts or initiate fail-safe protocols to mitigate potential breaches.

3.4 Monitoring

The process monitoring phase is an ongoing step to ensure the security and stability of IIoT environments. Here, defined processes are continuously monitored to ensure they conform to expected behaviors and security mechanisms. Effective monitoring is crucial for detecting anomalies, identifying threats, and responding to incidents in real time. In IIoT, where systems are distributed and interconnected, monitoring must be comprehensive and adaptive to detect deviations across diverse devices and networks.

BPM plays a key role by providing a reference model against which activities are monitored. BPM models serve as benchmarks for secure operations, enabling monitoring systems to track IIoT processes in real time by comparing actual interactions with expected behaviors (Oberhofer et al., 2024).

Aligning monitoring systems with BPM-based rules allows for targeted and efficient monitoring. Specific events and interactions - such as unauthorized communication or anomalously sensor readings - can trigger alerts. E.g., if the BPM model specifies that a sensor sends data only during a defined window, any communication outside of that window can be flagged for investigation. This reduces false positives and helps security teams focus on real threats.

BPM-driven monitoring also supports automated incident response. When an anomaly is detected, predefined actions - such as isolating devices, restricting access, or triggering emergency protocols - can be initiated automatically, reducing response time and mitigating impacts.

Beyond security, BPM-based monitoring aids in performance optimization and compliance. Continuous monitoring against the BPM model helps detect inefficiencies, enabling real-time adjustments to keep processes secure and aligned with operational objectives and regulatory requirements.

4 PROCEDURES AND GUIDELINES

The following section outlines a structured approach for organizations to leverage BPM techniques to enhance security in IIoT environments. By systematically integrating security considerations into each phase of the process lifecycle, the framework aims to help organizations better manage cyber risks in complex IIoT ecosystems.

4.1 Process Discovery

Objective: Identify and understand all processes in the IIoT environment, including potential security risks.

Step 1: Initial Process Inventory The first step in the framework is to conduct a comprehensive inventory of all IIoT-related processes within the organization. This includes identifying both business workflows and the technical processes that underlie IIoT operations. A combination of manual and automated methods is recommended for this phase. Manual methods can include interviews with stakeholders, document analysis, and workshops. Automated methods, such as process mining, can further assist in discovering workflows from system logs and network data.

By discovering these processes, organizations gain an understanding of how data flows between devices, systems, and users. This serves as the foundation for subsequent security analysis, providing a clear view of the overall operational landscape where security risks must be managed.

Step 2: Identify Security-sensitive points Once the process inventory is established, the next step is to identify security-sensitive points within each discovered process. These points are typically areas where data exchange occurs between devices, through communication channels, or at access points that could be targeted by attackers. It is critical to engage security experts during this step to conduct a thorough evaluation of potential vulnerabilities in these processes.

The identification of security-sensitive points allows organizations to focus their security efforts on the most critical areas of the process. For example, any communication between IIoT devices that involve sensitive or critical data must be carefully examined for vulnerabilities such as unencrypted transmissions, weak authentication, or insufficient access control.

Step 3: Document Security Requirements After identifying security-sensitive points, the next step is to document security requirements for each process, ensuring objectives like confidentiality, integrity, and availability are met. These requirements should align with standards like IEC 62443 and may include encryption, access controls, and data integrity checks. This structured approach integrates security mechanisms into the BPM cycle, providing a foundation for continuous compliance monitoring and proactive risk management in IIoT environments.

4.2 Process Modeling

Objective: Create security-aware models of the IIoT process using BPMN or similar modeling techniques.
Step 1: Modelling Security Aspects The next step involves process modelling notations like BPMN. Process knowledge from the previous phase is used to formally visualize and model workflows of the IIoT environment. Here, security mechanisms and controls are incorporated directly into the IIoT process models. This includes embedding components such as access control, data encryption, and communication monitoring into the process workflows. It is essential that these security controls are integrated in alignment with industry standards like IEC 62443 to ensure robust security coverage.
Step 2: Validate Models Against Security Standards Once the models are developed, they must be continuously validated against relevant security standards and organizational policies. This process should involve collaboration between business and security stakeholders to ensure that both operational efficiency and security requirements are met.

4.3 Execution and Enforcement

Objective: Ensure the secure execution of processes and real-time monitoring of compliance with security mechanisms.
Step 1: Translate Models into Executable Rules The first step involves translating security-aware BPMN models into executable rules that can be implemented by security systems, such as Intrusion Detection Systems (IDS) or firewalls. Tools or middleware should be used to convert the security attributes embedded in the BPMN models into enforceable policies that ensure processes adhere to the defined security requirements during execution. This step bridges the gap between formal process models and their real-world implementation in IIoT environments.
Step 2: Real-Time Monitoring and IDS Integration Once the processes are translated into executable rules, continuous monitoring is critical. This involves integrating with an IDS to track compliance with security mechanisms in real-time. The system monitors key aspects of the process execution, such as encrypted communications, access control enforcement, and potential suspicious network behavior. This ensures that any deviation from the modeled security requirements is detected and addressed immediately.
Step 3: Adapt to Dynamic Threats To maintain robust security, the system must be adaptable to evolving IIoT threats. Automated updates to security mechanisms should be enabled, allowing the system to respond to new threats as they arise. Leveraging AI and machine learning algorithms, the system can identify emerging attack vectors and adjust security controls in real-time, ensuring continued protection as the threat landscape changes.

4.4 Monitoring and Compliance

Objective: Continuously monitor process execution for compliance with security standards and respond to any violations or anomalies.
Step 1: Continuous Compliance Monitoring In this step, continuous compliance monitoring mechanisms are implemented to ensure scalability and adaptability in complex and heterogeneous IIoT environments. By incorporating machine learning techniques, the system can predict potential security violations or breaches before they occur, allowing for dynamic adjustments to compliance controls based on real-time network behavior.
Step 2: Incident Response and Feedback Loop When a security violation or anomaly is detected, predefined incident response workflows are triggered immediately. This step also establishes a feedback loop where insights gathered from continuous monitoring are fed back into the discovery and modeling phases. This iterative approach improves process security over time, enhancing overall system resilience against emerging threats.

5 CONCEPTS AND TECHNIQUES

In Section 4 we showed that BPM can also help to address challenges of security management in IIoT environments. BPM methods provide a systematic way to integrate security mechanisms such as policies, controls, and monitoring in the operational process lifecycle, ensuring that security is embedded from the outset rather than treated as an afterthought.

As IIoT environments and especially security aspects are typically not represented and supported in traditional BPM methods and systems, these require new and adapted concepts e.g., procedures, notations, systems and algorithms. Following the research methodology outlined in Section 2.3, we now address the key research gaps and highlight the latest scientific advancements that support the use of BPM technology for security management in IIoT scenarios. We again structure our findings according to the process lifecycle phases.

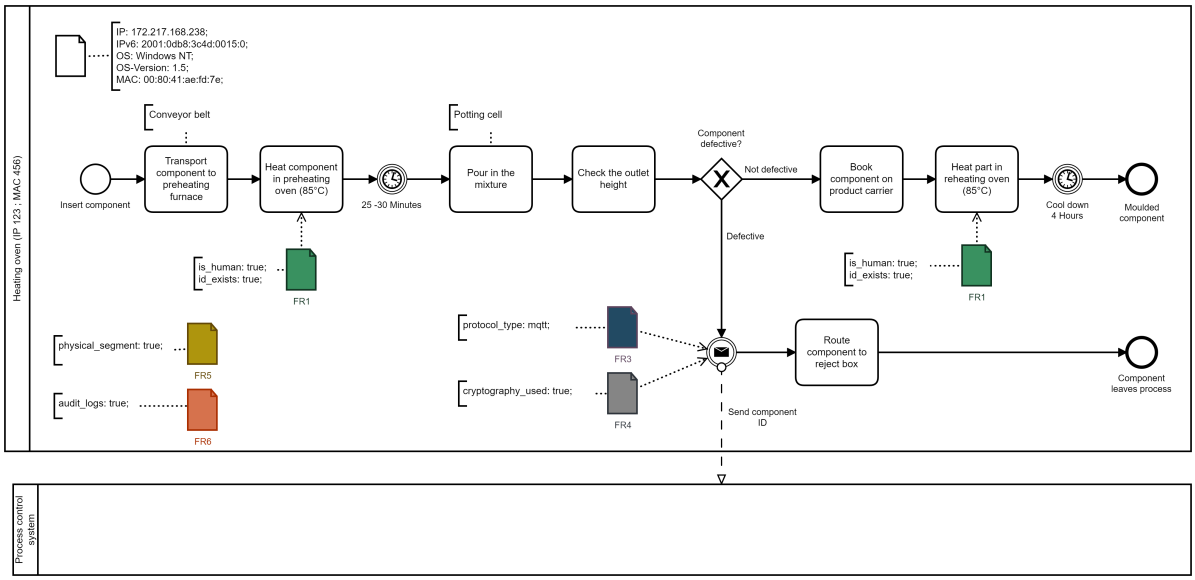


Figure 2: Use case for this paper: Industrial process for heating and filling components.

5.1 Real-World IIoT Process Use Case

In this section, each phase of the lifecycle is explained, including the corresponding questions, approaches, and artifacts, using the industrial process illustrated in Figure 2. This process is an excerpt from the real-world operations of an industry partner and was modeled using the framework presented in Section 4. Throughout the following, various scientific artifacts are introduced that can support each phase of the lifecycle.

In the process shown in Figure 2, a component undergoes several steps. First, the component is transported to a furnace for heating. After a specific time, the component is filled with a material, and the filling level is measured. If the filling exceeds a predetermined threshold, the component is deemed defective and rejected. The product ID of the rejected component is then transmitted to the process control system. If the component meets the required standards, it is transported to a second furnace for reheating, then cooled, and the process is completed.

5.2 Manual Process Discovery in IIoT

In the context of IIoT, *how can manual process discovery methods be adapted to ensure comprehensive process identification for improved IIoT security?* Automated techniques are often favored for efficiency, but manual methods - including document analysis, observation, interviews, and workshops - remain vital for capturing nuanced, human-driven processes critical to IIoT security. However, *how can these manual techniques be systematically applied to IIoT*, where physical and cyber systems converge, creating unique operational complexities?

A review of existing literature (Kölbel et al., 2024) reveals that while manual discovery methods are well-studied in traditional business environments, structured approaches for IIoT environments are scarce. The integration of physical processes, real-time data, and machine interactions in IIoT presents challenges that generic manual methods do not adequately address. Literature emphasizes human-driven insights for identifying security-relevant processes, yet lacks an adaptable framework for IIoT.

The identified gap is the absence of a structured procedure for manual process discovery tailored to IIoT security management. Unlike traditional environments, IIoT involves complex cyber-physical interactions, making it difficult to capture all processes without a framework that considers specific IIoT characteristics, such as device communication, real-time data flows, and the physical-virtual interface. Current manual methods, used without adaptation, lead to potential security blind spots.

To address this, Kölbel et al. (2024) introduces a structured procedure for manual process discovery targeting IIoT environments. This framework adapts classic manual methods like document analysis, observation, and interviews to IIoT needs. For instance, document analysis emphasizes operating manuals and system logs highlighting device communication and data processing crucial for security.

The framework also proposes a mixed-method approach combining multiple discovery techniques for a

comprehensive IIoT overview. The evaluation shows the guidelines benefit both beginners, with step-by-step instructions, and experts, by ensuring consistent quality standards during process discovery.

This structured approach ensures accurate identification of critical processes in IIoT, providing a foundation for integrating security mechanisms throughout the process lifecycle.

Using the framework, initial process drafts (Figure 2) were discovered through a mixed-method approach: document analysis, followed by interviews, and observation. Security mechanisms were then added through expert interviews and document analysis. However, no structured approach currently exists for discovering these security mechanisms. Section 6 proposes future research to address this gap.

5.3 Process Mining IIoT Network Data

Process mining has become a powerful tool for discovering business processes from data logs, offering insights into operational efficiency and identifying bottlenecks. However, its application in the IIoT remains an emerging and unexplored area. This raises a key question: *How can process mining be effectively applied to real-world IIoT network data to enhance operational security and efficiency?* Given that IIoT environments generate vast amounts of network data, there is significant potential for uncovering detailed, security-relevant processes through process mining. The challenge lies in adapting existing techniques to deal with the complexities and scale of IIoT data while addressing real-world industrial applications rather than simulations.

A review of the literature highlights a growing interest in applying process mining techniques to network data, with a variety of approaches having been developed in recent years (Engelberg et al., 2021; Hadad et al., 2023; Wakup and Desel, 2014). Process mining on network data has shown promise in detecting anomalies, uncovering hidden processes, and optimizing operational workflows. However, as indicated in Hornsteiner et al. (2024), these studies focus on simulated environments or general network data, leaving a gap when it comes to applying these techniques to industrial network data. Industrial environments, with their complex interactions between physical devices, sensors, and control systems, pose unique challenges that are not yet addressed in existing work. Moreover, using real-world data for process mining introduces issues such as data heterogeneity, noisy logs, and the difficulty of capturing relevant events in a meaningful way for process discovery.

The primary gap identified is the *lack of process mining approaches applied to real-world industrial network data*. While several studies have demonstrated the viability of using network data for process mining, they rely on simulated data or simplified environments, which do not accurately reflect the complexity of industrial processes. Real-world IIoT network data is far more challenging due to the diversity of devices, the mix of machine-to-machine communications, and the variety of protocols involved. Furthermore, data from industrial environments often contains noise or irrelevant information, making it difficult to extract meaningful event logs for process discovery. This creates a significant gap between the potential of process mining in IIoT and its actual application in real-world scenarios.

To address this gap, Hornsteiner et al. (2024) introduces a novel approach based on actual industrial network environments, moving beyond previous studies that relied on simulated datasets. This shift provides an accurate representation of challenges and opportunities inherent in IIoT, e.g., handling large data volumes, dealing with noisy or incomplete logs, and identifying key security and operational events.

The approach begins by recording network data from an operational IIoT environment, which is then used to generate event logs from network traffic. These logs serve as the foundation for discovering actual process models, enabling businesses to visualize and analyze their workflows. The methodology considers the unique characteristics of IIoT systems - machine, sensor, and control system interactions - ensuring the process models are both accurate and actionable for improving security and operational efficiency.

The developed methodology outlines how raw network data is transformed into event logs, and how process mining is applied to uncover previously hidden processes. This approach not only addresses the research gap by applying process mining to real-world IIoT data but also provides organizations with a practical tool for gaining deeper operational insights. Evaluations have shown the approach to be effective in discovering operational processes, identifying inefficiencies, and detecting potential security risks in IIoT environments. Network data from IIoT systems is particularly valuable for capturing not only basic information such as IP addresses, protocols, or encryption methods, but also more detailed network characteristics, including device communication patterns. This insight can be used to segment the network and enhance overall security.

As an evaluation of the approach, the main control-flow dependencies of the process depicted in Figure 2 where automatically discovered based on analysing OPC-UA network data that has been

recorded before.

5.4 Modelling Security-Aware Processes

The second phase of the BPM lifecycle focuses on process modeling, where abstract representations of processes are defined using notations such as the de-facto standard BPMN. In the context of IIoT, the challenge arises of how BPMN can be adapted to not only model operational processes but also integrate security awareness. Specifically, the research question is: *How can BPMN be extended to model IIoT processes in a security-aware manner, ensuring that security requirements and rules are embedded in the process design and can be monitored for compliance throughout execution?*

A literate review by Hornsteiner et al. (2022) explores existing research on BPMN modeling in both IIoT and security contexts. This indicates that, although BPMN extensions exist that are specifically tailored for either IIoT or security, a comprehensive solution that fully integrates both domains has yet to be developed. Current approaches either focus solely on modeling IIoT operations without considering security, or address general security concerns without specific considerations of IIoT environments. This highlights a critical gap: existing BPMN frameworks lack the ability to model IIoT processes in a way that directly incorporates and enforces security measures.

The literature review identified two main gaps:

1. There is no unified framework that integrates both IIoT modeling elements and security concerns, which is crucial for securing complex IIoT environments. Existing BPMN extensions address either IIoT or security, but lack an integrated approach to cover both aspects effectively.
2. Although some BPMN extensions capture security mechanisms, they provide inadequate process monitoring solutions, lacking the continuous controls necessary for ensuring compliance and mitigating threats in real time during process execution.

These gaps highlight the need for a BPMN extension that models and enforces IIoT security mechanisms.

To address this gap, Hornsteiner and Schönig (2023) recently introduces SIREN, a BPMN extension specifically designed for modeling security-aware processes in IIoT environments. SIREN extends BPMN by incorporating elements based on the IEC 62443 standard, which is well accepted in the industrial security domain. These new elements allow modelers to define and visualize security controls alongside operational processes. For example, SIREN introduces symbols and annotations for specifying access control, data integrity, and encryption protocols that must be enforced during IIoT process execution.

In addition to providing a framework for security-aware modeling, SIREN also introduces an approach for monitoring compliance in real time. The approach ensures that security controls modeled in BPMN can be translated into monitorable rules, which are then implemented within network monitoring systems. This allows security teams to track whether processes adhere to the predefined security protocols and receive alerts if any violations occur. The combination of process modeling and continuous monitoring ensures that security is not just a design-time concern but is actively enforced throughout the execution phase of the process lifecycle.

The effectiveness of SIREN was successfully validated through several case studies in industrial settings like the process of Figure 2, demonstrating that it not only enables the clear and structured modeling of security concerns within IIoT processes but also facilitates real-time security monitoring. By providing both the tools to model and enforce security controls, SIREN fills the gap identified in the literature and offers a practical solution for organizations seeking to secure their IIoT operations comprehensively.

5.5 Executing and Monitoring Security-Aware IIoT Processes

Once processes have been discovered and modeled, the next challenge is ensuring both their correct execution and continuous monitoring. The research question guiding this phase is: *How can security-aware business process models in IIoT environments be executed and monitored to enforce security in real-time, ensuring compliance with standards like IEC 62443?* While it is possible to model security mechanisms in BPMN, the question remains how these models can be translated into enforceable, monitorable controls during execution.

The literature review of Hornsteiner et al. (2022) reveals that existing approaches focus on the visual representation of security mechanisms in BPMN but fail to address execution and real-time enforcement. BPMN extensions for specific contexts, such as data security, access control, or integrity, are widely discussed, but they stop short of bridging the gap to actual implementation within IIoT environments. Furthermore, existing work on real-time monitoring focuses heavily on traditional IT systems and does not fully explore cyber-physical interactions found in IIoT, where the complexity of connected devices and

networks poses additional security challenges.

Two major gaps emerge from the literature:

- **Modeling to Execution** There is a lack of approaches for translating security-aware BPMN models into executable processes that can be monitored in real time. While BPMN provides visual extensions to model security mechanisms, these are not operationalized into enforceable controls during process execution in IIoT environments.
- **Continuous Compliance Monitoring** Existing research on process monitoring tends to focus on IT systems or simulated environments, leaving out industrial network data and the complexities of real-world IIoT. Additionally, many approaches do not integrate continuous compliance monitoring mechanisms that ensure security policies, such as those defined by IEC 62443, are enforced throughout the process lifecycle.

To address these gaps, the development and application of the SIREN markup language and the Security Compliance Monitoring and Verification (SCMV) framework from Oberhofer et al. (2024) is proposed. SIREN, as depicted in Figure 2, allows security mechanisms, such as access control, encryption, and integrity, defined during process modeling to be embedded in BPMN models based on IEC 62443 standards. These mechanisms are then transformed into a set of actionable controls that can be monitored by an IDS, ensuring that processes are continuously monitored for compliance during execution.

The SCMV framework integrates real-time monitoring of these controls, ensuring that as processes execute, compliance with security standards is actively enforced. For instance, if the model specifies data encryption, the IDS monitors network traffic to ensure compliance with this requirement. Unauthorized access attempts or deviations from modeled behavior trigger alerts, enabling early detection of threats. This approach turns BPMN models from static representations into dynamic, enforceable security mechanisms that respond to evolving threats in real-time.

By embedding security in BPMN and leveraging the IDS to monitor execution, the framework ensures that IIoT processes maintain compliance with security requirements. This integrated approach closes the gap between modeling, execution, and continuous monitoring, providing organizations with a robust, scalable solution to secure IIoT processes in real-time.

6 CHALLENGES AND INTERSECTIONS

6.1 Procedure for developing security enhanced process models

Before the concepts developed and presented can be applied, the associated process model and the security requirements for the process must be known for the process under consideration. These are the fundamental basis of the concepts. A prerequisite for applying BPM in IIoT is discovering both, processes and their security requirements. Manual methods, such as interviews, observations, or workshops, are commonly used to discover process models, while automated methods like process mining can also be applied. However, none of these methods currently provide a structured approach for discovering security requirements within processes.

Future work should address developing methods for identifying security requirements in processes. Key questions include:

- Can security requirements be discovered in parallel with or integrated into process discovery?
- How can discovered security requirements be correctly assigned within models?
- Which manual or automated methods are suitable for security requirement discovery, and are new concepts needed?

Further research into process evaluation and security is needed to answer these questions.

6.2 Security-Aware Models for Holistic and Automated Risk Management

Security-aware process models can be used for automated security risk management, specifically supporting the interaction between the three steps: Risk Assessment, Risk Response, and Risk Monitoring. The concept of security requirements and the monitoring of their compliance can be integrated within the risk management process. Such security controls are discovered during the Risk Assessment, automatically implemented during Risk Response, and then monitored within the Risk Monitoring phase. This enables a holistic view of the risk management process, which is essential for end-to-end automation. Implementing this automation is a challenging task, dependent on future advancements. Particularly in the domain of IIoT, where security functionalities must not compromise system safety, automated, planned, and context-

oriented execution of security processes is more reliable than human interactions.

In Risk Assessment, security-aware process models define a catalog of security controls with their criticality, based on different standards, regulations, or laws. The process model acts as an output report of the Risk Assessment process and also serves as input for the second phase. Within the automated Risk Response, the machine-readable security control catalog is implemented and forms the basis for ongoing verification of the risk status within Risk Monitoring. Risk Monitoring benefits from security-aware process models in the form of compliance monitoring, as described in this work.

Another area where process models help improve automation within security risk management is the generalization of security controls. After security controls are discovered and integrated into process models, they need to be generalized to work with different security standards, regulations, or laws. This generalization can be achieved within the process models themselves by defining a common security-aware process language, for example, based on the common control framework, in combination with a mapping of specific security controls (e.g., IEC 62443 security requirements) to similar controls within other policies. The generalized controls displayed in the process models should be automatically transformed into policy-specific versions.

In conclusion, future work should aim to increase the automation of security risk management by implementing a holistic, process-centered approach that leverages the potential of integrating security-aware process models into the risk management lifecycle.

6.3 AI-based Model Explanation

The concepts in this paper are all designed for the application of security requirements. The results are, among other things, process models with security requirements. One problem that arises is the comprehensibility and readability of the models for people who are not familiar with the modelling language or who do not know the security requirements and their origin, or who have no background knowledge of IT security. Nevertheless, in order to define process models, security requirements and their origin understandable for 'non-experts', a way of explaining the process models is needed. One idea that is already being realised is the comparison of process models with security standards and norms using Large Language Models (LLM). To this end, models are translated into XMLs for readability by the LLMs. The objective is to enable LLMs to explain the models and the security requirements they contain. LLMs should assess whether modelled security aspects fulfil the requirements of selected standards and explain why these are or are not fulfilled. In addition, LLMs should make suggestions for improving the implementation to date. In order to obtain such a LLM-based explanation, research in the field of prompt engineering must be carried out and applied to corresponding example scenarios in the future.

7 CONCLUSION AND OUTLOOK

In light of growing security challenges in IIoT environments, this paper demonstrates the value of integrating security mechanisms across the entire lifecycle of BPM. By synthesizing various research streams, including manual and automated process discovery, security-aware modeling, execution and compliance monitoring, the paper provides a comprehensive insight for embedding security into IIoT processes. This approach not only strengthens the enforcement of real-time security, but also ensures continuous alignment with established standards such as IEC 62443. By incorporating these methods, organizations can achieve a more resilient IIoT infrastructure, where security is integrated into the core of process management and helps to mitigate risk in increasingly complex industrial systems. The presented research addresses critical gaps how security can be effectively modeled, executed, and monitored, and highlights the need for a holistic perspective when addressing security in the IIoT. The findings provide both researchers and practitioners with a structured path for applying BPM to industrial security, offering a unifying perspective that ties together several existing approaches. While this paper lays the foundation for embedding security into the BPM lifecycle for IIoT environments, it leaves open questions for future work that could further strengthen this integration. One important direction is to develop a structured approach to identifying security requirements. While methods for process discovery to identify business processes in the IIoT have been explored, there is a need for a dedicated framework that systematically reveals security requirements during the discovery phase and ensures that security risks are identified early in the process. Furthermore, future work should focus on advancing AI-driven and model-based security compliance assessment. By employing artificial intelligence and formal models, it is possible to enhance real-time monitoring and automatic compliance verification, especially in dynamic IIoT environments where threats develop quickly. AI techniques could

enable adaptive security mechanisms that respond to new threats and continuously optimize compliance monitoring, making security processes more scalable and adaptable. These advances could further close the gap between security modeling and real-time enforcement, ensuring that IIoT processes remain secure and compliant throughout their lifecycle, even as industrial environments become more complex.

ACKNOWLEDGEMENTS

This work is funded by the "Bavarian Ministry of Economic Affairs, Regional Development and Energy" within the project Security Iiot pRocEss Notation (SIREN).

REFERENCES

Bernardo, R., Galina, S. V. R., and de Pádua, S. I. D. (2017). The BPM lifecycle: How to incorporate a view external to the organization through dynamic capability. *Bus. Process. Manag. J.*

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

Engelberg, G., Hadad, M., and Soffer, P. (2021). From network traffic data to business activities: a process mining driven conceptualization. In *BPMDS*. Springer.

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

Goncharov, E. (2018). Challenges of industrial cybersecurity. *Kaspersky*.

Hadad, M., Engelberg, G., and Soffer, P. (2023). From network traffic data to a business-level event log. In *BPMDS*. Springer.

Hansen, H., Mendling, J., and Neumann, G. (2019). *Wirtschaftsinformatik*. De Gruyter.

Hornsteiner, M., Empl, P., Bunghardt, T., and Schönig, S. (2024). Reading between the lines: Process mining on opc ua network data. *Sensors*.

Hornsteiner, M. and Schönig, S. (2023). Siren: Designing business processes for comprehensive industrial iot security management. In *DESRIST*. Springer.

Hornsteiner, M., Stoiber, C., and Schönig, S. (2022). Towards security- and iiot-aware bpmn: A systematic literature review. In *ICSBT*.

IEC (2009). Cybersecurity for Operational Technology in Automation and Control Systems. Standard, International Electrotechnical Commission.

Kölbel, L., Hornsteiner, M., and Schönig, S. (2024). Guideline for manual process discovery in industrial iot. *Arxiv*.

Mendling, J., Reijers, H., and van der Aalst, W. (2010). Seven process modeling guidelines (7pmg). *Information and Software Technology*.

Myers, D., Radke, K., Suriadi, S., and Foo, E. (2017). Process discovery for industrial control system cyber attack detection. In *IFIP SEC*. Springer.

Oberhofer, D., Hornsteiner, M., and Schönig, S. (2024). Process-aware security standard compliance monitoring and verification for the iiot. In *ECIS*. AIS.

Palattella, M. R., Dohler, M., Grieco, A., Rizzo, G., Torsner, J., Engel, T., and Ladid, L. (2016). Internet of things in the 5g era: Enablers, architecture, and business models. *IEEE journal on selected areas in communications*.

Parker, S., Wu, Z., and Christofides, P. D. (2023). Cybersecurity in process control, operations, and supply chain. *Computers & Chemical Engineering*.

Pulsipher, D. W., Scott, A., and Reeb, F. (2022). An argument for a holistic approach to critical infrastructure security. *Intel Corporation*.

Schönig, S., Hornsteiner, M., and Stoiber, C. (2022). Towards process-oriented iiot security management: Perspectives and challenges. In *BPMDS*. Springer.

Serror, M., Hack, S., Henze, M., Schuba, M., and Wehrle, K. (2020). Challenges and opportunities in securing the industrial internet of things. *IEEE Transactions on Industrial Informatics*.

Sisinni, E., Saifullah, A., Han, S., Jennehag, U., and Gidlund, M. (2018). Industrial internet of things: Challenges, opportunities, and directions. *IEEE transactions on industrial informatics*.

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.*

van der Aalst, W. (2010). Process discovery: Capturing the invisible. *IEEE Computational Intelligence Magazine*.

Wakup, C. and Desel, J. (2014). Analyzing a tcp/ip-protocol with process mining techniques. In *International Conference on Business Process Management*. Springer.

Weske, M. (2012). *Business Process Management - Concepts, Languages, Architectures, 2nd Edition*. Springer.

zur Muehlen, M. and Ho, D. T. (2005). Risk management in the BPM lifecycle. In *BPM*.

Appendix
Curriculum Vitae

Markus Hornsteiner

Chair of Process-Based Information Systems
Faculty of Informatics and Data Science – Regensburg, Germany
mahopy • 0000-0002-8024-1220 • PqUBZtIAAAAJ

Education

PhD Student
University of Regensburg, *2022–2025*
Focus: IIoT Security

M.Sc. Business Informatics
University of Regensburg, *2019–2021*
Focus: Information Security

B.Sc. Business Informatics
University of Regensburg, *2015–2018*

Research Projects

IRAPS (2024-2026): Integration resilienter Arbeitswelten und IoT-gestützter Produktionssysteme für industrielle Anwendungen

SIREN (2023-2026): Security Iiot pRocEss Notation and Mining

INSIST (2021-2024): *INduStrial IoT Security Operations CenTer*

Teaching

Object Oriented Programming — **Professorship for IoT-based Information Systems**
Tutor *2022–2024*

Practice of IT security — **Chair of Information Systems IV**
Student Tutor *2020–2021*

Security Management — **Chair of Information Systems IV**
Student Tutor *2020–2021*

Publications

[1] Markus Hornsteiner, Sebastian Groll, and Alexander Puchta. "Towards a user-centric IAM entitlement shop - Learnings from the e-commerce". In: *13th International Conference on Security of Information and Networks*. SIN 2020. Merkez, Turkey: Association for Computing Machinery, 2021.

[2] C. Roth et al. "ROADR: towards road network assessment using everyone-as-a-sensor". In: *The 2nd International Conference on Distributed Sensing and Intelligent Systems (ICDSIS 2021)*. 2021.

[3] Markus Hornsteiner, Christoph Stoiber, and Stefan Schönig. "Towards Security-and IIoT-Aware BPMN: A Systematic Literature Review." In: *ICSBT*. 2022.

[4] Stefan Schönig, Markus Hornsteiner, and Christoph Stoiber. "Towards Process-Oriented IIoT Security Management: Perspectives and Challenges". In: *Enterprise, Business-Process and Information Systems Modeling*. Ed. by Adriano Augusto et al. Cham: Springer International Publishing, 2022.

[5] Markus Hornsteiner and Stefan Schönig. "SIREN: Designing Business Processes for Comprehensive Industrial IoT Security Management". In: *Design Science Research for a New Society: Society 5.0*. Cham: Springer Nature Switzerland, 2023.

[6] Daniel Oberhofer, Markus Hornsteiner, and Stefan Schönig. *Market Research on IIoT Standard Compliance Monitoring Providers and deriving Attributes for IIoT Compliance Monitoring*. 2023. arXiv: 2311.09991 [cs.CR].

[7] Lars Ackermann et al. *Recent Advances in Data-Driven Business Process Management*. 2024. arXiv: 2406.01786 [cs.DB].

[8] Markus Hornsteiner et al. "Reading between the Lines: Process Mining on OPC UA Network Data". In: *Sensors* (2024). ISSN: 1424-8220.

[9] Markus Hornsteiner et al. "Real-Time Text-to-Cypher Query Generation with Large Language Models for Graph Databases". In: *Future Internet* (2024). ISSN: 1999-5903.

[10] Linda Kölbel, Markus Hornsteiner, and Stefan Schönig. *Guideline for Manual Process Discovery in Industrial IoT*. 2024. arXiv: 2410.11915 [cs.SE].

[11] Daniel Oberhofer, Markus Hornsteiner, and Stefan Schönig. "Process-Aware Security Standard Compliance Monitoring and Verification for the IIoT". In: *ECIS*. AIS, 2024.

Talks and Presentations

Systematic Literature Review - the "Pythonic" way
lero.ie *2022*

Towards Process-oriented IIoT Security Management: Perspectives and Challenges
BPMDS Conference *2022*

Towards Security- and IIoT-Aware BPMN: A Systematic Literature Review
ICSBT Conference *2022*

Designing Business Process for Comprehensive Industrial IoT Security
SIREN Conference *2023*

Process-Aware SCMV for the IIoT
ECIS Conference *2024*