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., 2021). 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). Building on our previous work by Schönig et al. (2022), which highlighted the potential of applying BPM concepts to IIoT security management, this paper addresses the challenges and intersections identified in that study. Using the IIoT security management process as a foundation, we illustrated how BPM methods can enhance IIoT security and discussed future challenges and areas for improvement. Since the publication of the initial paper, we have successfully resolved these challenges and addressed the open questions through the contributions presented in this paper.

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)*

[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

Hornsteiner, M., Koelbel, L., Oberhofer, D. and Schoenig, S.
A Reflection on Process-Oriented Industrial IoT Security Management.
DOI: 10.5220/0013163500003899

In *Proceedings of the 11th International Conference on Information Systems Security and Privacy (ICISSP 2025) - Volume 1*, pages 242-253
ISBN: 978-989-758-735-1; ISSN: 2184-4356

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 important 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 ensures 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.

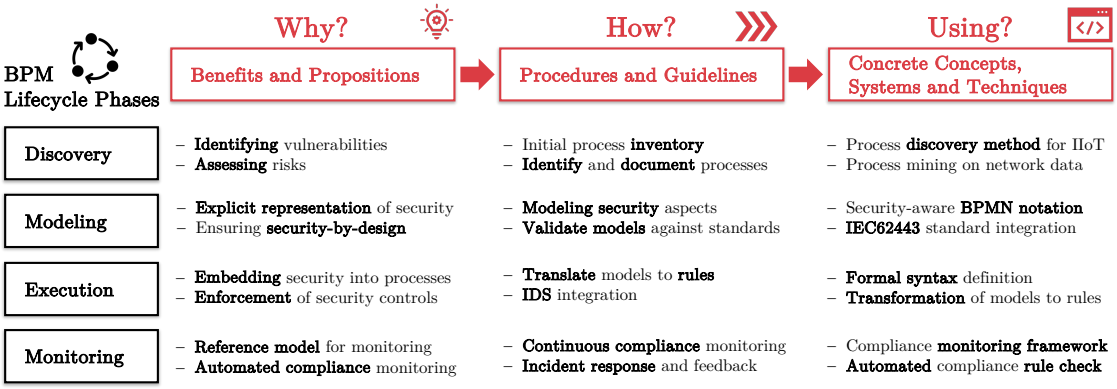

Figure 1: Overview of the presented process-centric IIoT security management framework.

- **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 struc-

tured 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 process 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 identify their 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 com-

munication 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 failsafe 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

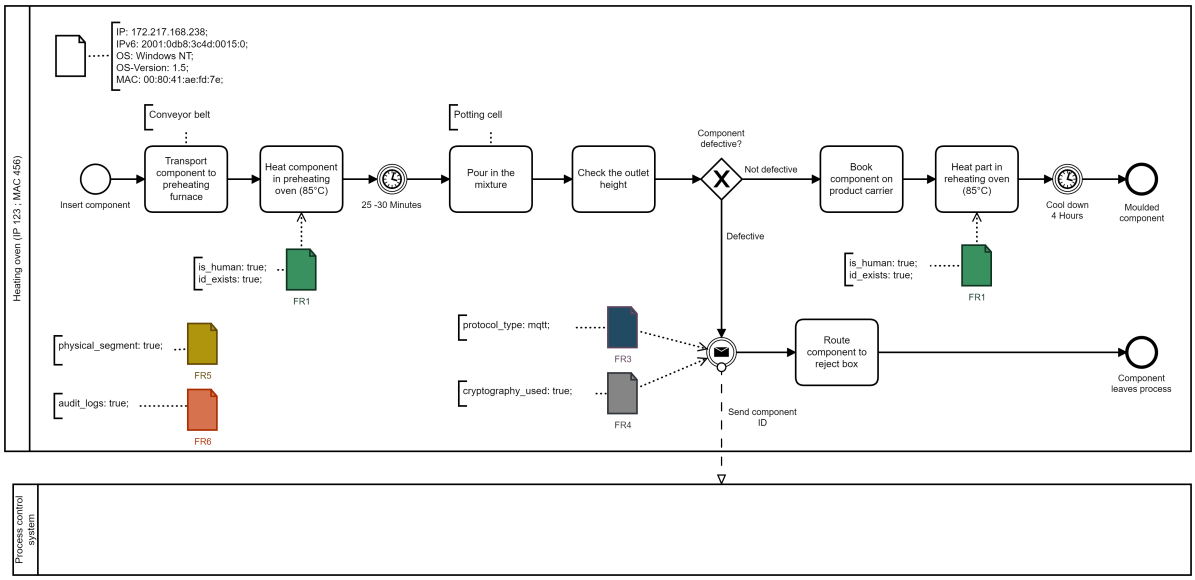

Figure 2: Use case for this paper: Industrial process for heating and filling components.

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.

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. In the following, various scientific artifacts are introduced that 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.

To evaluate 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 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 no 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 their correct execution and continuous monitoring. The guiding research question 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 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 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.

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.*, 23(1):155–175.

Dumas, M., Rosa, M. L., Mendling, J., and Reijers, H. A. (2018). *Fundamentals of Business Process Management, Second Edition*. Springer.

Engelberg, G., Hadad, M., and Soffer, P. (2021). From network traffic data to business activities: A process mining driven conceptualization. In *Enterprise, Business-Process and Information Systems Modeling BPMDS*, volume 421, pages 3–18. 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 Lab ICS CERT*, 5.

Hadad, M., Engelberg, G., and Soffer, P. (2023). From network traffic data to a business-level event log. In *Enterprise, Business-Process and Information Systems Modeling - 24th International Conference, BPMDS*, volume 479, pages 60–75. Springer.

Hansen, H. R., Mendling, J., and Neumann, G. (2019). *Wirtschaftsinformatik (12. Aufl.)*. De Gruyter Studium.

Hornsteiner, M., Empl, P., Bunghardt, T., and Schönig, S. (2024). Reading between the lines: Process mining on OPC UA network data. *Sensors*, 24(14):4497.

Hornsteiner, M. and Schönig, S. (2023). SIREN: designing business processes for comprehensive industrial iot security management. In *18th International Conference on Design Science Research in Information Systems and Technology, DESRIST*, volume 13873 of *Lecture Notes in Computer Science*, pages 379–393. Springer.

Hornsteiner, M., Stoiber, C., and Schönig, S. (2022). Towards security- and iiot-aware BPMN: A systematic literature review. In *ICSBT*, pages 45–56. SCITEPRESS.

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. *CoRR*, abs/2410.11915.

Mendling, J., Reijers, H. A., and van der Aalst, W. M. P. (2010). Seven process modeling guidelines (7PMG). *Inf. Softw. Technol.*, 52(2):127–136.

Myers, D., Radke, K., Suriadi, S., and Foo, E. (2017). Process discovery for industrial control system cyber attack detection. In *ICT Systems Security and Privacy Protection*, volume 502 of *Advances in Information and Communication Technology*, pages 61–75. Springer.

Oberhofer, D., Hornsteiner, M., and Schönig, S. (2024). Process-aware security standard compliance monitoring and verification for the iiot. In *32nd European Conference on Information Systems ECIS*.

Palattella, M. R., Dohler, M., Grieco, L. A., Rizzo, G., Torsner, J., Engel, T., and Ladid, L. (2016). Internet of things in the 5g era: Enablers, architecture, and business models. *IEEE J. Sel. Areas Commun.*, 34(3):510–527.

Parker, S., Wu, Z., and Christofides, P. D. (2023). Cybersecurity in process control, operations, and supply chain. *Comput. Chem. Eng.*, 171:108169.

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 *Enterprise, Business-Process and Information Systems Modeling - 23rd International Conference, BPMDS*, pages 18–26. Springer.

Serror, M., Hack, S., Henze, M., Schuba, M., and Wehrle, K. (2021). Challenges and opportunities in securing the industrial internet of things. *IEEE Trans. Ind. Informatics*, 17(5):2985–2996.

Sisinni, E., Saifullah, A., Han, S., Jennehag, U., and Gidlund, M. (2018). Industrial internet of things: Challenges, opportunities, and directions. *IEEE Trans. Ind. Informatics*, 14(11):4724–4734.

Tange, K., Donno, M. D., Fafoutis, X., and Dragoni, N. (2020). A systematic survey of industrial internet of things security: Requirements and fog computing opportunities. *IEEE Commun. Surv. Tutorials*, 22(4):2489–2520.

van der Aalst, W. M. P. (2010). Process discovery: Capturing the invisible. *IEEE Comput. Intell. Mag.*, 5(1):28–41.

Wakup, C. and Desel, J. (2014). Analyzing a tcp/ip-protocol with process mining techniques. In *Business Process Management Workshop*, volume 202, pages 353–364.

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 Bussler, C. and Haller, A., editors, *Business Process Management Workshops, Revised Selected Papers*, volume 3812, pages 454–466.