Towards Design Patterns for Production Security

David Hoffmann[‡] Stefan Biffl[†§] Kristof Meixner[*†] Arndt Lüder[‡§]
[*]Christian Doppler Laboratory SQI, [†]Inst. of Information Sys. Engineering, TU Wien, and [§]CDP, Austria
E-Mail: [first].[last]@tuwien.ac.at
[‡]Institute of Ergonomics, Manufacturing Systems and Automation, Otto-von-Guericke U., Germany
E-Mail: [first].[last]@ovgu.de

***Abstract*—In Production System Engineering (PSE), domain experts aim at effectively and efficiently analyzing and mitigating information security risks to product and process qualities for manufacturing. However, traditional security standards do not connect security analysis to the value stream of the production system nor to production quality requirements. This paper aims at facilitating security analysis for production quality already in the design phase of PSE. In this paper, we (i) identify the connection between security and production quality, and (ii) introduce the Production Security Network (PSN) to efficiently derive reusable security requirements and design patterns for PSE. We evaluate the PSN with threat scenarios in a feasibility study. The study results indicate that the PSN satisfies the requirements for systematic security analysis. The design patterns provide a good foundation for improving the communication of domain experts by connecting security and quality concerns.**

***Index Terms*—Industrial information security, PSE, PPR**

I. Introduction

The development of Cyber-Physical Production Systems has lead to an increased focus on research related to security in Production System Engineering (PSE), as the convergence of Information Technology (IT) and Operational Technology (OT) lead to a broader attack surface for cyber-attackers [1]. Approaches, such as the VDI guideline 2182 [2] and the IEC 62443 standard [3], aim at mitigating Cyber-Physical System (CPS) security threats effectively and efficiently [4] by integrating IT-security methods into OT-based PSE.

However, the efficiency of these methods is disputed, as current research shows that the high complexity of these approaches leads to high effort for companies to analyze their security needs [1], [4]. As the implementation of the required security countermeasures is a collaborative effort of domain experts from mechanical, electrical, and software engineering, the resulting security model needs to be connected to knowledge in these disciplines [5].

Weippl and Kieseberg [1] therefore suggest quality engineering as a connection point between these domains and security, as PSE concerns the creation of a product-quality oriented value stream. [6]. As Meixner *et al.* [7] pointed out, specific design patterns in PSE can facilitate designing production system capabilities based on the required product qualities. As the successful implementation of security requirements describes the security capabilities of the production system [3], we consider adapting the concept of reusable design patterns to production security.

In this paper we (i) identify the connection between security and production quality with security as a part of the overall quality function of industrial products, and (ii) introduce the Production Security Network (PSN) to efficiently derive reusable security requirements for PSE. The remainder of this paper is structured as follows: Section II summarizes related work on industrial security analysis and on security by design. Section III motivates the research question and approach. Section IV introduces the PSN solution approach. Section V introduces an illustrative use case and identifies requirements for reuse of security knowledge in PSE. Section VI reports on a feasibility study to evaluate the PSN capabilities and discusses current results and limitations of the research. Section VII concludes and outlines future work.

II. Related Work

Industrial security analysis. Industrial security refers to the protection of technical systems in production, manufacturing and logistics from unknown attacks and disturbances [3]. The scope of industrial security concerns production systems, their control and network components, sensors, actors, and the services connected to the systems [2]. Domain-specific standards like the IEC 62443 [3] provide a variety of security properties and requirements for network-based assets. Furthermore, they provide concepts like security levels to specify the security capabilities of a system. These standards apply established IT-security principles like defense in depth or security goals to facilitate structuring the work packages required for implementing security.

However, as Weippl and Kieseberg [1] and Tuma *et al.* [4] point out, the mapping of IT-security principles to OT-based production systems and assets is difficult for manufacturing domain experts, as the security principles are not well aligned common PSE concepts. In PSE, choosing the right components with the right configuration in order to produce the right product is the foundation for designing an efficient production system [6], [8]. A modular approach for defining the right security configuration for assets can follow the Baseline Protection Catalog (BPC) [9], which provides modular building blocks for common system assets. Hoffmann [10] specifies building blocks that are relevant for Industrial Control Systems (ICS) assets and maps them to relevant concepts like the standardized security level.

However, no queryable knowledge base for such buidling blocks yet exists, that can be leveraged during design time of PSE. In this paper, we build on such blocks to create a knowledge base from existing standards and store the created

assets with their properties in a queryable graph database as a foundation to provide standardized information on common ICS assets.

Security patterns by design. A variety of domain-specific standards and methods are available to address potential security issues. The guideline VDI 2182 [2] formulates an iterative eight-step procedure model to systematically explore and assess threats to ICS and to formulate appropriate security measures. Cost-effective implementation of these measures requires their consideration early in production system design. The principle *Security-by-Design* [11] aligns well with the multi-disciplinary requirements of PSE: the precise definition of system requirements early on facilitates early verification and validation of the results [5]. This is especially important for security measures that require validation to mitigate possible threats efficiently [2]. To this extent, current research aims at establishing security as a quality requirement of production, expressed as IEC 62443 security levels [3].

Even though standards like the VDI 2182 [2] acknowledge the importance of security-by-design for efficient security implementation, they do not specify how to use this principle in PSE, as the procedure model is concerned with analyzing the security of existing system architectures [4], rather than designing a secure system architecture, which could yield a more effective and efficient approach [11].

To design a production system by reusing components that embody required quality aspects, Meixner *et al.* [7] recommend using design patterns. They analyzed in PSE recurring design patterns of products, processes and resources (PPR) [12], connected to fulfill specific needs and requirements, so called skills, to achieve sufficient process and product quality. However, they did not discuss how to include requirements and standards from domains like security as skills of the system in order to make these requirements reusable for PSE.

In this paper, we leverage PPR design patterns [7] and connect them to a standardized security evaluation as the security skill of a system, in order to establish design patterns for production security towards effective and efficient security analysis.

III. Research Question and Approach

In this paper, we use Design Science methodology [13] to investigate how to improve identifying necessary security requirements for reuse in PSE. Therefore, we (i) conducted a domain analysis in the automotive industry, (ii) condensed a representative use case, and (iii) extracted security requirements in regard to the value stream of the system. Considering identified gaps in the related work and requirements in PSE, we formulate the following research question: *What modeling approach can effectively and efficiently link security requirements in the form of reusable design patterns to the production requirements in PSE?*

Security standards provide various methods and concepts that help security experts in securing production systems. However, in order to integrate security into traditional PSE, security needs to be considered along the multidisciplinary design process of production systems [5].

To establish *Security-by-Design* for PSE, we establish security requirements in the design phase of PSE and integrate them into the design of products, processes and resources. Our contribution is the Production Security Network (PSN), a knowledge graph that connects products, processes and resources to standardized security requirements using a set of design patterns, based on established security concepts like the layered security approach [1] and security levels [3].

We derived a use case by investigating the production and security data of robot cells with the help of the IEC 62443 and BPC standards [3] [9] and validated the data with security and domain experts. With this data, we identified knowledge elements that represent abstract security-patterns for reuse. From these elements we build a condensed modeling approach as the basis for the PSN (see Fig. 1).

We evaluate the PSN in a feasibility study for the use case (cf. Section V). To this end, we use data from a sample *Car Body with Screwed-on Parts* on artifacts from the domain analysis. We investigate to what extent a secure system architecture can be derived by queries to the PSN.

IV. Solution Approach

To address the research question, we introduce the PSN approach that consists of (i) the PSN model that represents the elements required for building the knowledge base and (ii) the PSN method that results in a PSN model instance.

Fig. 1 shows the PSN model consisting of a Product-Process-Resource (PPR) model [1], [12] with associated skills (PPRS) [7], and the general security requirements and their classification [3]. Additionally, it shows the PSN method with its derivation and provision of a Security Level (SL) for the Product-Process-Resource-Skill (PPRS) model, bawed on novel Production Security Patterns (Px).

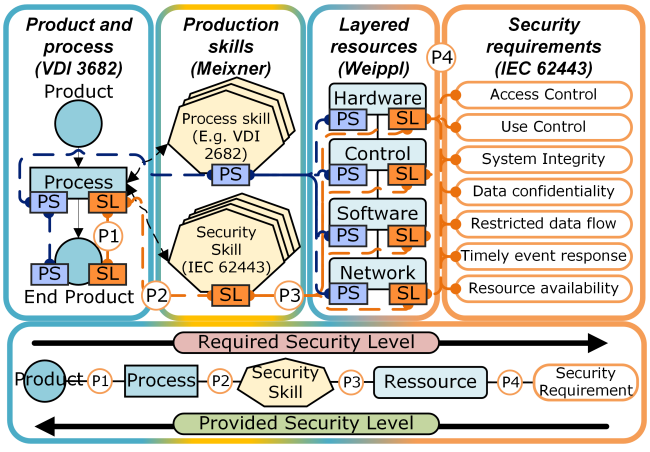

Fig. 1. Production Security Network (PSN) solution overview, based on VDI 3682 [12], IEC 62443 [3], PSE-skills [7] and layered security apporach [1]

PSN model. The PSN model consists of the following elements: **(i) Products** with certain characteristics, manufactured by specialized **(ii) Processes** [12] that fulfill the needs of the

production. **(iii) Process skills (PS)**, required for the successful operation of processes [7], e.g., a screwing skill, defined in the VDI 2862 standard [14], Layered **(iv) Resources** [1] with specific features that fulfill the skill requirements. **(v) Security skills** in the form of a SL, rooted in the basic PPRS model to define security needs of the system, and **(vi) Security requirements** for the resources, that need to be fulfilled to provide the needed security skill.

PSN Design Patterns. In order to link these elements that represent the partial views of the stakeholders, we derived the following design patterns for production security, based on [7] and the communication with production and security stakeholders. **P1: Products and Process Pattern**. In PSE, specific processes manufacture products with specific qualities [7]. As the PSN aims at establishing security as a required property of the final product, the involved processes have to operate on at least the SL of the final product. **P2: Process and Skill Pattern.** Processes are linked to skills that provide functionalities required for successful process execution [7]. Therefore, the SL of the skill determines the SL of the process. **P3: Skill and Resource Pattern.** Resources implement the skills by forming functional units that depend on mechatronic components and automation devices [7] connected to software and network assets [1]. Therefore, the minimal SL of the required resources determines the SL of the skill. **P4: Resource and Security Requirements Pattern.** The SLs of the resources are associated with a set of security requirements belonging to a SL that can be mapped to basic types of PSE assets based on [9], [10], representing their secure usage. Therefore, the minimal SL of the unfulfilled security requirements determines the SL of a resource [3].

PSN method. To build the PSN model, the responsible process and security experts conduct the following steps. **Step 1: Scope the PPRS model.** First, the process experts scope the PPRS model from use case data to reflect production reality, resulting in a basic PPRS model [7]. **Step 2: Derive security requirements.** This step integrates security features with the basic PPRS model coming from Step 1, resulting in the derivation of security requirements to sufficiently secure the system. Therefore, production stakeholders select a target SL for production, e.g., based on recommendations of security experts and standards. With the help of the PSN design patterns (P1-P4), the target SL propagates through the elements of the PPRS model, resulting in the derivation of security requirements for the scope of the use case. **Step 3: Validate and verify SL implementation.** In this step, the security and process experts validate to what extent the derived security requirements can be implemented. The conditions and stakeholders for a successful implementation can be derived from security guidelines [9], [10]. SL validation checks whether a resource implements all requirements for the planned SL. In the same way, the validation checks the SLs of the security skill, processes, and the final product. Therefore, the SL of the product will be the minimal SL of the involved PSN elements. Finally, production and security experts iteratively assess the feasible product SL, considering improvements in the PSN.

V. Illustrative Use Case

This section introduces the use case *Car Body with Screwed-on Parts*. We condensed the use case from a domain analysis in the automotive manufacturing domain [7].

For our use case we observed a screwing operation with its screwing and inspection process to manufacture a product joined from its parts (cf. Fig. 2). The successful operation requires a screwing skill, which is extended by a security skill to achieve secure operation. To fulfill the screwing skill, the required resources for the screwing operation are chosen, e.g., the screwing unit, a PLC, an HMI to operate the unit, and a data server to store configurations. For the target security level, there is a list of security requirements. Due to lack of space, Fig. 2 focuses on selected requirements for the PLC. The use case assumes the requirements of SL 1 to be fulfilled, but for SL 2 to miss the requirement *Protection against malware*. According to the PSN method, the final product inherits the the minimal SL 1 from the PLC.

VI. Evaluation and Discussion

This section discusses the preliminary feasibility study of the use case and its contributions with a focus on the research question raised in Section III.

As a proof of concept, we used a part of the production system for the use case *Car body with screwed on parts* from the initial domain analysis [7] to design and instantiate the PSN in a graph database. The PSN was found easy to create by following the PSN method steps, iteratively expanding the included knowledge by discussing and validating the model with domain experts. To validate the functionality, we worked together with security experts to devise security attacks on the system, and countermeasures to mitigate the effects of these attacks. Then, we evaluated the required security level and queried the database to explore whether the right security information could be found. The query was able to identify countermeasures to overcome the attacks [10].

The PSN approach was well received by stakeholders, as the focus of security analysis worked well with the known PSE approach of deploying quality functions [6]. This makes the PSN more effective than the traditional approach of aiming for a system with maximum security, as the PSN focuses the efforts of the domain experts onto the value stream of production. Furthermore, querying the database is time and resource efficient, as it does not require the security experts to provide answers, as their knowledge is represented in the database with standardized information. This makes the PSN more efficient than the traditional approach of performing a security analysis for every system [2] by avoiding redundant data acquisition [4]. These capabilities indicate that security experts can utilize the PSN as a modeling approach in PSE to effectively and efficiently link security requirements of the system to the product-focused value stream of PSE, thereby answering the research question in Section III.

We go beyond the state of the art in PSE by providing a solution approach for the issues raised on how to integrate security with traditional PSE goals and methods [1], [4],