Product-Line Engineering for Smart Manufacturing: A Systematic Mapping Study on Security Concepts

Richard May, Alen John Alex, Rakky Suresh and Thomas Leich
Harz University of Applied Sciences, Wernigerode, Germany
{*rmay, u36903, u36912, tleich*}*@hs-harz.de*

Keywords: Security, Configurable Systems, Product-Line Engineering, Smart Manufacturing, Systematic Mapping Study.

Abstract: The growing configurability of smart-manufacturing software systems (SMSS) introduces a variety of security concerns. Although there is an ever-increasing risk for exploiting configuring-caused issues, there is currently no overview of research on security within SMSS, especially those based on product-line engineering (PLE). To address this gap, we employed a systematic mapping study of 43 publications (2014–2023) related to the intersection of security, SMSS, and PLE. Besides an overview of what properties have been researched, we identified nine literature gaps to guide future research. Overall, there is a need for more research on PLE security concepts in SMSS. Current approaches often address security as a separate requirement rather than integrating it into the PLE framework or mapping it to the unique properties of SMSS. Concrete security concerns are typically hardly described, which may have fatal consequences in safety-critical systems.

1 INTRODUCTION

In the past few years, smart manufacturing (SM) has emerged as a novel approach that embraces the convergence of advanced technologies, e.g., based on machine-learning-driven data analytics (Kusiak, 2018). This paradigm shift transcends traditional manufacturing methods, transforming factories into adaptive ecosystems that seamlessly integrate automated, data-driven production processes (Qu et al., 2019). SM supports the increase of functions and their configurations, making smart-manufacturing software systems (SMSS) variant-rich and highly complex (Fischer et al., 2023). Product-line engineering (PLE) is an established approach for developing and maintaining such configurable software systems (Uysal and Mergen, 2021). Specifically, PLE enables the creation of product families (i.e., variants) with shared functionalities (i.e., features), optimizing development efficiency and reducing costs (Apel et al., 2013). Configurability is becoming increasingly important for SMSS, which often require configuration to accommodate different production lines or product variants (Uysal and Mergen, 2021). However, the growing variability of SMSS presents several unique challenges, particularly in terms of system security (Kenner et al., 2021). Precisely, the more configurable systems are, the greater the risk of potential (mis)configurations or (unintended) feature interactions, leading to vulnerable bugs or even system failure (May et al., 2024).

PLE in the context of SM has already been addressed by research, e.g., Heikkilä et al. (2016) analyzed how to deal with configurability in robot systems and Fischer et al. (2021) investigated cyber-physical systems configuration testing. However, we miss a systematic overview of existing research – especially how they handle security. We aim to address this gap by employing a systematic mapping study to analyze existing literature (2014–2023) and investigate: (1) *to what extent the properties of configurability and security are covered by research* and (2) *which properties are underexplored and thus need more research.* In this context, our contributions are:

- An overview understanding of current research regarding security in the context of PLE and SMSS.
- A discussion of which properties have been adequately covered or need more research.
- An open-access replication package.[1]

2 BACKGROUND

Next, we address preliminary knowledge on *configurable systems*, *SM*, and *security*.

[1] https://doi.org/10.5281/zenodo.10653363

May, R., Alex, A., Suresh, R. and Leich, T.
Product-Line Engineering for Smart Manufacturing: A Systematic Mapping Study on Security Concepts.

In *Proceedings of the 19th International Conference on Software Technologies (ICSOFT 2024)*, pages 323-330
ISBN: 978-989-758-706-1; ISSN: 2184-2833

Configurable Systems. A configurable system is a software platform containing sets of reusable features that can be enabled, disabled, or adjusted to configure platform variants (Apel et al., 2013). PLE is an established approach for managing configurable software, incorporating concepts such as feature modeling (Meinicke et al., 2017) to facilitate maintenance or flexibility (van der Linden et al., 2007). There are three common verification strategies: product-based (i.e., code or abstraction analysis on each configuration), feature-based (i.e., analysis of each feature), and family-based (i.e., analysis of a meta system) (Thüm et al., 2014). Configurable systems usually rely on the classification by their projection space, including problem space (i.e., domain abstraction to identify requirements), solution space (i.e., implementation and product derivation), and their connection through a mapping in which appropriate features are derived (Meinicke et al., 2017).

Smart Manufacturing. SM aims to be highly integrated within software and hardware, giving a high degree of productivity, flexibility, and configurability (Kusiak, 2018). It points towards intelligent, interacting systems, primarily based on data-driven technologies and the Internet-of-Things (IoT) which is a bridge between the cyber and physical worlds (Zheng et al., 2018). SM technologies are an essential part of Industry 4.0, aiming to transform traditional manufacturing into smart, network-driven, and nearly autonomous manufacturing (Tuptuk and Hailes, 2018). In general, the goal of SM is to meet the changing requirements and conditions in the factory, the supply network, and customer needs through real-time responses (Kang et al., 2016). In this way, the manufacturing industry aims to address the ever-increasing demands for individualization, quality improvement, and shorter time-to-market (Zheng et al., 2018).

Security. As more manufacturers are transitioning to SM, the physical and cyber worlds are merging, leading to increasing system complexities and greater attack surfaces (Alani and Alloghani, 2019). So, achieving robust security oriented towards customer demands, policies, and legal regulations is crucial to mitigate threats (ISO/IEC 27000, 2018). Threats are adverse incidents that may have a negative impact on a system, e.g., vulnerability exploits. The likelihood and impact of these incidents is called a risk (ISO/IEC 27005, 2022). Typically, countermeasures (e.g., authentication) are implemented in the context of a defined strategy (i.e., pattern) to provide an appropriate security level. Such countermeasures are usually oriented towards the fulfillment of six essential security goals, including confidentiality, integrity, and availability (i.e., CIA triad), as well as accountability, authorization, and non-repudiation (i.e., goals of information security) (ISO/IEC 27000, 2018).

3 METHODOLOGY

To address our research objectives, we carried out a systematic mapping study (Petersen et al., 2015). The methodological steps are illustrated in Figure 1.

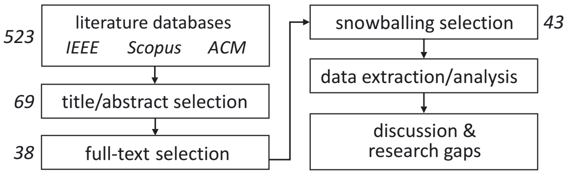

Figure 1: Overview of methodological research steps with numbers indicating the amount of selected publications.

3.1 Study Design

Databases and Search String. We relied on three databases: SCOPUS, IEEE XPLORE, and ACM DIGITAL LIBRARY and used the following search string:

*(“product*line*”) AND (“famil*” OR “config*” OR “variab*” OR “variant*” OR “feature” OR “model*”) AND (“secur*” OR “protect”) AND (“industry” OR “industrial” OR “manufactur*” OR “production” OR “cyber*physical”)*

Inclusion Criteria. We applied the following inclusion criteria (IC) to select relevant publications:

IC$_1$. The publication must have been published in the past decade (2014–2023), ensuring the topics included are fairly recent.

IC$_2$. The publication must be longer than three pages, ensuring that the literature included provides sufficient details.

IC$_3$. The publication must be a peer-reviewed book chapter, journal article, or conference paper to achieve a minimum quality of the publications included in our selection. We intentionally excluded review and/or overview studies.

IC$_4$. The publication must cover PLE approaches in the context SM as well as security concepts.

Data Extraction Criteria. To extract data valuable enough to achieve our research objectives, we created the following data extraction categories:

Publication including four criteria:

- *Publication year* of the contribution.
- *Contribution type*, i.e., a publication classification, including open items, method, model, metric, or tool (Engström and Runeson, 2011).

- *Perspective*, i.e., a decision whether the publication is focused on a security concept developed on PLE techniques or (static) security of an PLE-based system.
- *Fields*, e.g., robotics, manufacturing.

Configurable System including five criteria:

- *System focus*, i.e., a specification of what is actually configurable, including software, hardware, or both.
- *Evolution*, i.e., a description of evolutionary processes and issues, e.g., related to updates.
- *Verification strategy*, i.e., a method that is addressed in the publication, including feature-, product-, or family-based verification.
- *Projection space*, i.e., a classification into problem space, solution space, or mapping.
- *Tool*, i.e., if the publication mentioned any specific tool support for configuration.

Security including six criteria:

- *Standard*, e.g., ISO/IEC 27000 series.
- *Goals*, including confidentiality, integrity, availability (CIA triad), authorization, accountability, non-repudiation (information security), and other goals (e.g., authenticity).
- *Threats and risks*, i.e., threat- or risk-related security issues of configurable systems.
- *Vulnerabilities*, i.e., exploitable weaknesses.
- *Patterns*, i.e., concrete strategies to ensure system security.
- *Countermeasures*, i.e., mitigation techniques addressing threats, vulnerabilities, or risks to ensure security.

3.2 Study Conduct

The search was performed by the first author on November 15th, 2023 and resulted in 523 publications after applying the selection criteria (489 after removing duplicates). By reading the titles and abstracts, a total of 69 publications was found. Then, the number of selected publications was reduced to 38 publications based on the full-texts, followed by a single pass of forward/backward snowballing, yielding five more publications (i.e., 43 publications in total). Next, the first author analyzed all selected literature. In this context, open-coding (i.e., labeling of data) and open-card-sorting methods (i.e., classification of recurring data into common themes) were applied. The second and the third author took random samples (five papers each) to verify the results. All analyzed data and interpretations were discussed until consensus was reached between all authors. In Figure 1, all methodological steps are illustrated.

4 RESULTS

In the following subsections, we describe the results classified according to our categories (cf. Table 1).

4.1 Publication

Publication Years. Starting in 2014 with two publications, the number remains constant between 2015 and 2018 (4.5 publications per year on average). There is a peak in 2019 with eight publications, followed by six publications per year in 2020 and 2021. Surprisingly, we found only two publications in 2022 and one publication in 2023.

Contribution Type. Most publications focus on open items (e.g., challenges). Methods and models are each described by 12 publications. In six cases, a concrete tool (e.g., framework) is proposed.

Perspective. We identified that the majority (37) is related to quite static security as part of the PLE while only in six publications configurable security mechanisms are described.

Fields. The application fields comprise diverse working areas and SM sub-fields. However, most publications (17) are focused on cyber-physical production systems. Ten publications are related to general manufacturing without further specifications. We identified seven more fields with less publications, including, e.g., robotics (4) and cloud manufacturing (3).

4.2 Configurable System

System Focus. Most publications (24) focus on software without considering any hardware components. 19 publications are related to software and hardware (e.g., cyber-physical production systems).

Evolution. About half of the publications (21) considered quite diverse evolutionary processes, e.g., feature interaction evolution. However, these are typically described in a rather superficial way.

Verification Strategy. 24 publications present information on verification, including feature-based (13), product-based (7), and both feature- and product-based (4). Interestingly, there was no information on family-based verification of any SMSS.

Projection space. We found that 17 publications relied on a mapping of the problem and the solution space. Furthermore, 15 publications covered the problem space and 11 publications the solution space.

Tool. Only 13 tools for supporting PLE or security management are applied, including FeatureIDE (3), HyperFlex Toolchain (2), and others (8) such as pure::variants. We highlight that there are current frameworks focusing on the field of cyber-physical

Table 1: Overview of the extracted data regarding publication, security, and configurable system.

Publication			Security											Configurable system			
Reference	Perspective	Field	Standard	Confidentiality	Integrity	Availability	Authorization	Accountability	Non-repudiation	Threats and risks	Vulnerabilities	Patterns	Countermeasures	System focus	Projection space	Verification	Evolution
Eichelberger et al. (2014)	S → PLE	GM	○	○	○	○	○	○	○	●	○	○	○	S	S	–	●
Gherardi et al. (2014)	S → PLE	R	○	○	○	●	●	○	○	●	○	○	●	S	M	–	○
Smiley et al. (2015)	S → PLE	IA	○	●	○	●	○	○	○	○	○	○	●	S	M	F	●
Vogel-Heuser et al. (2015)	S → PLE	GM	○	○	○	●	○	○	○	○	○	○	○	S/H	P	F	●
García et al. (2015)	S → PLE	ERP	○	○	○	○	○	○	○	○	○	○	○	S	M	–	●
Galindo et al. (2015)	S → PLE	GM	○	○	○	○	○	○	○	●	○	○	●	S	P	–	●
Arrieta et al. (2015)	S → PLE	CPPS	○	○	○	○	●	○	○	○	○	○	○	S	M	–	○
Kokaly et al. (2016)	S → PLE	GM	●	○	○	○	○	○	○	○	○	○	○	S/H	P	F	●
Etigowni et al. (2016)	PLE → S	CPPS	○	●	●	○	●	○	○	●	○	●	●	S	M	–	○
Heikkilä et al. (2016)	S → PLE	R	○	○	○	○	○	○	○	●	○	○	●	S/H	S	–	○
Feldmann and Vogel-Heuser (2017)	S → PLE	GM	○	○	○	○	○	○	○	●	○	○	○	S	P	–	●
Larrucea et al. (2017)	S → PLE	IN	○	○	●	○	○	○	○	●	○	○	●	S/H	M	P	○
Young et al. (2017)	S → PLE	A_1	○	●	○	○	○	○	○	●	○	○	○	S	P	F	○
Seidl et al. (2017)	S → PLE	GM	○	○	○	○	○	○	○	●	○	○	○	S	P	–	●
McGee et al. (2017)	S → PLE	IA	○	○	○	○	○	○	○	●	●	○	○	S	P	F	○
Jalil and Bakar (2017)	S → PLE	ERP	○	○	○	○	○	○	○	●	●	○	●	S	M	P	○
Krieter et al. (2018)	PLE → S	CM	○	●	●	○	○	○	○	●	○	○	○	S	P	P	●
Brugali and Hochgeschwender (2018)	S → PLE	R	○	○	○	●	○	○	○	●	○	○	○	S/H	S	–	○
Zhang et al. (2018)	S → PLE	CM	○	○	○	○	○	○	○	●	●	○	●	S/H	S	F/P	●
Islam and Azim (2018)	S → PLE	CPPS	○	●	●	○	●	○	○	○	○	○	○	S/H	S	F	●
Shaaban et al. (2019)	PLE → S	CPPS	●	●	●	○	●	○	●	●	●	●	○	S	S	P	○
Hajri et al. (2018)	S → PLE	A_1	○	●	○	○	○	○	○	●	○	○	○	S/H	M	F/P	●
de Oliveira et al. (2019)	S → PLE	A_2	○	○	●	●	○	○	○	●	○	○	○	S/H	M	P	○
Cañete (2019)	S → PLE	CM	○	○	○	○	○	○	○	●	●	○	●	S/H	S	F	○
Bennaceur et al. (2019)	PLE → S	CPPS	●	○	○	●	○	○	○	●	●	●	●	S/H	M	P	●
Ebnauf et al. (2019)	S → PLE	CPPS	○	○	○	○	○	○	○	○	○	○	○	S	S	–	○
Meixner et al. (2019)	S → PLE	CPPS	○	○	●	●	○	○	○	○	○	○	○	S/H	P	–	●
Daun et al. (2019)	S → PLE	GM	○	○	○	●	○	○	○	○	○	○	○	S	M	–	○
García et al. (2020)	S → PLE	R	○	○	○	○	○	○	○	●	●	○	●	S/H	P	–	●
Pett et al. (2020)	S → PLE	A_1	○	○	○	○	○	○	○	○	○	○	●	S/H	M	F/P	●
Meixner (2020)	S → PLE	CPPS	○	○	○	○	○	○	○	●	○	○	○	S	P	–	○
Cañete et al. (2020)	S → PLE	CPPS	○	○	○	○	○	○	○	●	○	○	○	S/H	M	–	●
Varela-Vaca et al. (2020)	PLE → S	CPPS	○	●	●	●	●	●	●	●	●	●	●	S	M	P	○
Bandyszak et al. (2020)	S → PLE	CPPS	○	○	○	●	○	○	○	●	●	●	○	S	M	F	○
Xiao and Li (2021)	S → PLE	CPPS	○	○	○	○	○	○	○	○	○	○	○	S	S	F/P	○
Varela-Vaca et al. (2021)	PLE → S	CPPS	●	●	●	●	●	○	○	●	●	●	●	S	S	F	○
Uysal and Mergen (2021)	S → PLE	GM	○	○	○	●	●	○	○	●	○	○	●	S	S	F	●
Fischer et al. (2021)	S → PLE	CPPS	○	○	○	●	●	○	○	●	○	○	●	S/H	P	–	○
Bressan et al. (2021)	S → PLE	GM	○	○	○	○	○	○	○	○	○	○	●	S/H	M	–	○
Capilla et al. (2021)	S → PLE	GM	○	○	●	○	●	○	○	●	●	●	●	S	M	F	●
Feichtinger et al. (2022)	S → PLE	CPPS	○	○	○	○	○	○	○	●	○	○	○	S	P	F	●
Vogel-Heuser et al. (2022)	S → PLE	CPPS	○	○	○	●	○	○	○	●	○	○	○	S/H	P	–	○
Fischer et al. (2023)	S → PLE	CPPS	○	○	○	●	○	○	○	●	○	○	●	S/H	P	F	●

General: ● Fulfilled ○ Not fulfilled **Perspective**: S → PLE: static security concept besides PLE, PLE → S: security concept based on PLE
Field: A_1: Automotive, A_2: Avionics, CM: Cloud manufacturing, CPPS: Cyber-physical production systems, ERP: Enterprise-resource planning
GM: General manufacturing, IA: Industrial analytics, IN: Industrial networks, R: Robotics
System focus: S: Software, H: Hardware; **Projection space**: P: Problem space, M: Mapping, S: Solution space; **Verification**: F: Feature-based, P: Product-based

production systems and security-configuration verification, namely CyberSPL (Varela-Vaca et al., 2020) and CARMEN (Varela-Vaca et al., 2021).

4.3 Security

Standard. There were four publications referencing standards, precisely NIST cyber-physical-systems program (2), IEC 62443 (1), and IEEE 1686 (1).

Goals. In the context of the CIA triad, confidentiality (9), integrity (9), and availability (16) are mentioned. Regarding information security, most publications refer to authorization (10). Only three publications consider non-repudiation (2) or accountability (1). Five other non-standardized goals are described, including reliability (6), authenticity (3), dependability (2), performance (2), and robustness (1).

Threats and Risks. We found that threats and risks are usually not described in detail. In general, issues that threaten the security of the SMSS are typically related to six categories: safety (13), communication (7), configurability (7), access (6), privacy (4), and trust (2). Note that publications may refer to more than one category. 12 publications do not mention any concrete threats or risks.

Vulnerabilities. The majority of the publications (32) do not consider vulnerabilities. However, in 11 cases, vulnerabilities that are closely related to threats and risks are mentioned, e.g., misconfigurations.

Patterns. There are eight publications that propose patterns that, however, vary greatly, e.g., due to different fields and use cases, including misuse cases (1) or access control patterns (1).

Countermeasures. We identified various mitigation techniques in 20 publications which we classified into four categories: access control (8), system or data isolation (6), general security analyses (3), and encryption mechanisms (2). Other countermeasures (5) include decentralization (1) or modularization (1).

5 DISCUSSION

In the following, we discuss our study results and derive nine **literature gaps (LG)** to be addressed in future research. We are aware that there are currently numerous approaches to dealing with security in SMSS that have little or no context to PLE – and thus usually also to configuring. Here, it should be investigated to what extent such approaches can be transferred to PLE. However, this would exceed the scope of our study.

5.1 Configurable Smart-Manufacturing Software Systems

Referring to the **publications years**, our results show that there is an awareness of SMSS security in the PLE community. However, this trend is decreasing since 2021. Interestingly, a significant number of open items as **contribution types** (e.g., challenges) were described until 2017, while more methods and models were published between 2018 and 2020. Since 2021, the focus has been much more on open items again. Specifically, current challenges arise mainly in the handling of complexities (e.g., time, configuration), variability (e.g., variant management), knowledge management and artificial intelligence, and (testing) agile requirements. Thus, (**LG1**) *there is a need for novel solutions (i.e., methods, models, tools that address the solution space) considering recent challenges of PLE-based SMSS during their development life cycle.*

While verification feature- and product-based **verification strategies** seem common for SMSS. So, (**LG2**) *there is a lack of family-based verification techniques* that could be used to assess secure functionalities across the entire product portfolio and identify potential vulnerabilities that may arise from evolving configurations. Note that despite its benefits, family-based verification faces challenges such as modeling the interactions between features and configurations, handling feature interactions, and efficiently verifying large product portfolios.

SMSS are constantly evolving, including changing requirements, features, and interactions, with increasingly automated evolutionary processes (Capilla et al., 2021). Although **evolution** is addressed in about half of the publications, more and deeper analyses are needed, especially since evolution is mostly described in a rather superficial way and handling configuration throughout updates is still highly challenging. Consequently, (**LG3**) *there is a need for concrete methodologies that can handle evolving configurations, feature interactions, and dependencies – without introducing new vulnerabilities (e.g., due to faulty system configurations).*

5.2 Security

Compliance with **security standards** can provide a baseline level of protection for SMSS. However, the consideration of general (e.g., ISO/IEC 27000 series) and domain-specific security standards (e.g., IEC 62443) is typically neglected in the PLE community, impairing the successful transfer of SMSS approaches into practice. We argue that (**LG4**) *there is a need for mapping security standards to the security engineering of the PLE framework.* We are aware that standard diversity means that it will hardly be possible to harmonize them in one single framework. Thus, we assume that either dynamic frameworks or several domain-dependent frameworks are required.

Surprisingly, the publications typically do not address **vulnerabilities**, although their management is an increasingly important field – especially in SMSS, where vulnerability exploits may have fatal consequences (e.g., system failure, reduced safety) (Yadav et al., 2022). Consequently, (**LG5**) *research is needed that focuses on detecting and managing vulnerabilities, especially in the context of the PLE framework.*

Specialized variability and security modeling **tools** are usually not mentioned by the publications. Although there are tools, e.g., in the context of verifying security configurations, (**LG6**) *there still seems to be a lack of appropriate tools for, as well as a lack of awareness in the community since existing tools are not or only rarely applied.* So, there is a need for accepted tool support that considers variable security concerns in the context of PLE activities that are relevant to security and the unique requirements of SMSS. Developing such tools may help automate security tasks, such as avoiding typical **threats and risks** in the context of system access or communication (cf. Figure 2). Such tools may also include the application of appropriate **security patterns** as con-

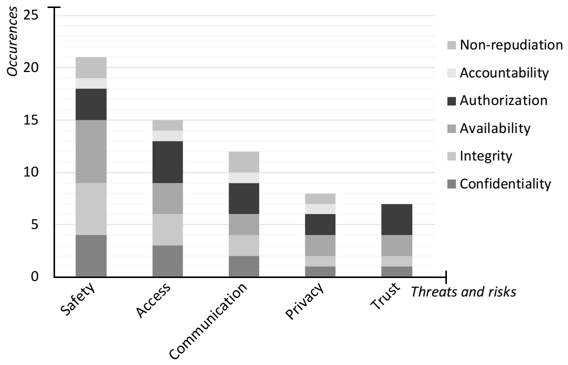

Figure 2: Distribution of security goals according to threats and risks (multiple goals or threats and risks per paper).

crete security strategies for configurable systems.

5.3 Security and Configurable Smart-Manufacturing Systems

Interestingly, most publications (88%) refer to SM **fields** which are highly dependent on hardware and software (e.g., cyber-physical production systems). However, most research (65%) focuses solely on software security although hardware security is equally important in SM, especially in the context of safety-critical systems. Thus, (**LG7**) *specifically interconnected hardware and software components with complex cross-dependencies in particular, require security mechanisms in comprehensive security management throughout domain engineering, security engineering, and application engineering*.

We identified that (**LG8**) *security in SMSS is typically addressed as a separate concern, rather than integrating it into the PLE framework or PLE-related activities for SMSS*. The approaches may lead to inflexible security countermeasures that cannot adapt to changing SMSS requirements and configurations. We argue, that this fact might be problematic because SMSS are constantly evolving due to new technologies, feature interactions, and changing business needs. Thus, traditional **security countermeasures** (e.g., mechanisms such as ownership and control) are hardly adequate (Uysal and Mergen, 2021). Continuous adaptive risk-based assessment and real-time decision-making enable appropriate adaptive responses at production level (i.e., cyber-physical processes) and business level (i.e., business processes).

The results show that availability and authorization are the most common **security goals**. This is not surprising, as both are essential for ensuring and controlling access to resources in SMSS. However, most goals are often overlooked in PLE-based SMSS approaches, despite their critical role in achieving a reliable security level by addressing common threats and risks (cf. Figure 2). To address this gap, (**LG9**) *the literature needs more compliant approaches to achieve standardized security levels in the context of the PLE-based system life cycles*.

5.4 Threats to Validity

There is an inconsistent level of detail as well as varying understandings of terms and concepts presented within the set of publications (e.g., system availability vs. security availability). Furthermore, some publications fulfill the extraction criteria from different perspectives and to varying extents, leading to potential risks for misinterpretations. The search string we created might not contain all the literature available which addresses security in SMSS, possibly affecting the external validity. To tackle the risk of misinterpretation, multiple researchers systematically investigated the publications and discussed the result until consensus on a decision was achieved. Moreover, besides relying on three well-known databases, we additionally performed a snowballing process. In this way, we were able to increase the first number of publications (38), making the extracted results more reliable and valuable.

6 RELATED WORK

We found related research within the field of PLE which (partly) covers several aspects regarding security or SMSS. Montagud et al. (2012) did a literature review (1996–2011) on quality attributes (i.e., including security) and measures for general PLE. Mahdavi-Hezavehi et al. (2013) presented a literature review (2000–2011) regarding variability in service-based software systems and considered security in a broad quality-related term. Geraldi et al. (2020) investigated publications related to the IoT and PLE (2006–2018), considering security as a non-functional requirement and manufacturing as an IoT application field. There is a systematic literature review by Uysal and Mergen (2021) (no restricted time frame) focusing on SM and the integration of PLE enterprise architectures. Security is described in the context of the (adaptive) risk and trust trend. In a mapping study conducted by May et al. (2022) security concepts for PLE-related data storages (2013–2022) are analyzed. They identified the manufacturing domain as one important domain when considering PLE and data storages.

We consider two studies as close to our work. Kenner et al. (2021) did a mapping study on PLE safety and security (2011–2020) and May et al. (2023)

focused on security in PLE-based safety-critical systems (2008–2022). Both publications share an approach similar to that of our work, which is why they served as a general orientation for our methodology. There are partly content-related similarities to our study (e.g., cyber-physical production systems), however, none of the publications is specifically focused on SM, distinguishing their insights from ours. We argue that our findings are of high value to the research community as we highlight unique insights based on a different body of knowledge.

7 CONCLUSION

We presented a systematic mapping study on the extent of security research in PLE-based SMSS. Specifically, we analyzed 43 publications and presented nine relevant literature gaps. We argue that there is high potential for research in terms of security within configurable SMSS. Publications often address security as a necessary but quite static feature that refers to the quality of SM systems. However, threats, risks, or vulnerabilities that may arise in configurable systems as well as related PLE activities are typically not further specified. We highlight that security in PLE-based SMSS seems underexplored, although there is a lot of literature related to security exclusively for SM (without any focus on PLE). There is great research potential regarding the investigation of software and hardware security as well as their cross-dependencies throughout configurations, harmonized mappings of security standards, and tools for managing threats, risks, and vulnerabilities in PLE-based SMSS.

REFERENCES

Alani, M. M. and Alloghani, M. (2019). Security challenges in the Industry 4.0 era. *Industry 4.0 and Engineering for a Sustainable Future*.

Apel, S. et al. (2013). *Feature-oriented software product lines*. Springer.

Arrieta, A. et al. (2015). Cyber-physical systems product lines: Variability analysis and challenges. *Jornadas de Computación Empotrada*.

Bandyszak, T. et al. (2020). Orthogonal uncertainty modeling in the engineering of cyber-physical systems. *Transactions on Automation Science and Engineering*, 17(3).

Bennaceur, A. et al. (2019). Modelling and analysing resilient cyber-physical systems. In *SEAMS*. IEEE.

Bressan, L. et al. (2021). A variability modeling and transformation approach for safety-critical systems. In *VaMoS*. ACM.

Brugali, D. and Hochgeschwender, N. (2018). Software product line engineering for robotic perception systems. *International Journal of Semantic Computing*, 12(01).

Cañete, A. (2019). Energy efficient assignment and deployment of tasks in structurally variable infrastructures. In *SPLC*. ACM.

Cañete, A. et al. (2020). Supporting the evolution of applications deployed on edge-based infrastructures using multi-layer feature models. In *SPLC*. ACM.

Capilla, R. et al. (2021). On autonomous dynamic software ecosystems. *IEEE Transactions on Engineering Management*, 69(6).

Daun, M. et al. (2019). Using view-based architecture descriptions to aid in automated runtime planning for a smart factory. In *ICSA-C*. IEEE.

de Oliveira, A. L. et al. (2019). Variability management in safety-critical systems design and dependability analysis. *Journal of Software: Evolution and Process*, 31(8).

Ebnauf, M. et al. (2019). State-driven architecture design for safety-critical software product lines. In *ICOM*. IEEE.

Eichelberger, H. et al. (2014). EASy-producer: Product line development for variant-rich ecosystems. In *SPLC*. ACM.

Engström, E. and Runeson, P. (2011). Software product line testing–a systematic mapping study. *Information and Software Technology*, 53(1).

Etigowni, S. et al. (2016). CPAC: Securing critical infrastructure with cyber-physical access control. In *ACSAC*. ACM.

Feichtinger, K. et al. (2022). Industry voices on software engineering challenges in cyber-physical production systems engineering. In *ETFA*. IEEE.

Feldmann, S. and Vogel-Heuser, B. (2017). Interdisciplinary product lines to support the engineering in the machine manufacturing domain. *International Journal of Production Research*, 55(13).

Fischer, S. et al. (2021). Testing of highly configurable cyber-physical systems–A multiple case study. In *VaMoS*. ACM.

Fischer, S. et al. (2023). Testing of highly configurable cyber–physical systems—-Results from a two-phase multiple case study. *Journal of Systems and Software*, 199.

Galindo, J. A. et al. (2015). Supporting distributed product configuration by integrating heterogeneous variability modeling approaches. 62.

García, C. et al. (2015). A software process line for service-oriented applications. In *SAC*. ACM.

García, S. et al. (2020). Robotics software engineering: A perspective from the service robotics domain. In *ESEC/FSE*. ACM.

Geraldi, R. T. et al. (2020). Software product line applied to the internet of things: A systematic literature review. *Information and Software Technology*, 124.

Gherardi, L. et al. (2014). A software product line approach for configuring cloud robotics applications. In *CLOUD*. IEEE.

Hajri, I. et al. (2018). Change impact analysis for evolving configuration decisions in product line use case models. *Journal of Systems and Software*, 139.

Heikkilä, T. et al. (2016). Dealing with configurability in robot systems. In *MESA*. IEEE.

Islam, N. and Azim, A. (2018). Assuring the runtime behavior of self-adaptive cyber-physical systems using feature modeling. In *CASCON*. ACM.

ISO/IEC 27000 (2018). Information technology – Security techniques – Information security management systems. Standard, ISO.

ISO/IEC 27005 (2022). Information security, cybersecurity and privacy protection – Guidance on managing information security risks. Standard, ISO.

Jalil, D. and Bakar, M. S. A. (2017). Adapting software factory approach into cloud ERP production model. *International Journal of Computer Science and Information Security*, 15(1).

Kang, H. S. et al. (2016). Smart manufacturing: Past research, present findings, and future directions. *International Journal of Precision Engineering and Manufacturing-Green Technology*, 3.

Kenner, A. et al. (2021). Safety, security, and configurable software systems: A systematic mapping study. In *SPLC*. ACM.

Kokaly, S. et al. (2016). Model management for regulatory compliance: A position paper. In *VaMoS*. ACM.

Krieter, S. et al. (2018). Towards secure dynamic product lines in the cloud. In *ICSE*. ACM.

Kusiak, A. (2018). Smart manufacturing. *International Journal of Production Research*, 56.

Larrucea, A. et al. (2017). Modular development and certification of dependable mixed-criticality systems. In *DSD*. IEEE.

Mahdavi-Hezavehi, S. et al. (2013). Variability in quality attributes of service-based software systems: A systematic literature review. *Information and Software Technology*, 55(2).

May, R. et al. (2022). A systematic mapping study of security concepts for configurable data storages. In *SPLC*. ACM.

May, R. et al. (2023). A systematic mapping study on security in configurable safety-critical systems based on product-line concepts. In *ICSOFT*. SciTePress.

May, R. et al. (2024). Vulnerably (mis)configured? Exploring 10 years of developers' Q&As on Stack Overflow. In *VaMoS*. ACM.

McGee, E. T. et al. (2017). Designing for reuse in an industrial internet of things monitoring application. In *WASCHES*. ACM.

Meinicke, J. et al. (2017). *Mastering software variability with FeatureIDE*. Springer.

Meixner, K. (2020). Integrating variability modeling of products, processes, and resources in cyber-physical production systems engineering. In *SPLC*. ACM.

Meixner, K. et al. (2019). Towards modeling variability of products, processes and resources in cyber-physical production systems engineering. In *SPLC*. ACM.

Montagud, S. et al. (2012). A systematic review of quality attributes and measures for software product lines. *Software Quality Journal*, 20.

Petersen, K. et al. (2015). Guidelines for conducting systematic mapping studies in software engineering: An update. *Information and Software Technology*, 64.

Pett, T. et al. (2020). Risk-based compatibility analysis in automotive systems engineering. In *MODELS*. ACM.

Qu, Y. J. et al. (2019). Smart manufacturing systems: State of the art and future trends. *The International Journal of Advanced Manufacturing Technology*, 103.

Seidl, C. et al. (2017). Challenges and solutions for opening small and medium-scale industrial software platforms. In *SPLC*. ACM.

Shaaban, A. M. et al. (2019). Ontology-based security tool for critical cyber-physical systems. In *Systems and Software Product Line Conference*. ACM.

Smiley, K. et al. (2015). Evolving an industrial analytics product line architecture. In *SPLC*. ACM.

Thüm, T. et al. (2014). A classification and survey of analysis strategies for software product lines. *Computing Surveys*, 47(1).

Tuptuk, N. and Hailes, S. (2018). Security of smart manufacturing systems. *Journal of Manufacturing Systems*, 47.

Uysal, M. P. and Mergen, A. E. (2021). Smart manufacturing in intelligent digital mesh: Integration of enterprise architecture and software product line engineering. *Journal of Industrial Information Integration*, 22.

van der Linden, F. J. et al. (2007). *Software product lines in action*. Springer.

Varela-Vaca, Á. J. et al. (2020). Definition and verification of security configurations of cyber-physical systems. In *ESORICS*. Springer.

Varela-Vaca, Á. J. et al. (2021). CARMEN: A framework for the verification and diagnosis of the specification of security requirements in cyber-physical systems. *Computers in Industry*, 132.

Vogel-Heuser, B. et al. (2015). Evolution of software in automated production systems: Challenges and research directions. *Journal of Systems and Software*, 110.

Vogel-Heuser, B. et al. (2022). Automation software architecture in cpps-definition, challenges and research potentials. In *ICPS*. IEEE.

Xiao, B. and Li, F. (2021). Knowledge-based formal modeling for CPPS in personalized intelligent manufacturing. In *DASC*. IEEE.

Yadav, G. et al. (2022). Vulnerability management in IIoT-based systems: What, why and how. In *Secure and Trusted Cyber Physical Systems: Recent Approaches and Future Directions*. Springer.

Young, B. et al. (2017). Product line engineering meets model based engineering in the defense and automotive industries. In *SPLC*. ACM.

Zhang, Z. et al. (2018). CMfgIA: A cloud manufacturing application mode for industry alliance. *The International Journal of Advanced Manufacturing Technology*, 98.

Zheng, P. et al. (2018). Smart manufacturing systems for industry 4.0: Conceptual framework, scenarios, and future perspectives. *Frontiers of Mechanical Engineering*, 13.