STRIDE-based Methodologies for Threat Modeling of Industrial Control Systems: A Review

Olaf Saßnick, Thomas Rosenstatter, Christian Schäfer, Stefan Huber
Josef Ressel Centre for Intelligent and Secure Industrial Automation
Salzburg University of Applied Sciences
Salzburg, Austria
{olaf.sassnick, thomas.rosenstatter, christian.schaefer, stefan.huber}@ fh-salzburg.ac.at

***Abstract*—Industrial Control Systems (ICS) and Operational Technology (OT) in general are facing significantly increasing numbers of cyber attacks. Hence, threat identification is of utmost importance for their security architecture. The STRIDE methodology is well known for threat identification in the software domain, yet in recent years it has also been applied in other domains, such as Internet of Things, automotive or ICS. But OT domains are fundamentally different to IT by exhibiting unique characteristics such as high reliability, strict safety requirements or unique physical attack risks. Threat assessment thus needs to be adapted. This paper reviews STRIDE-based threat modeling approaches in that respect and provides a first step towards the overarching goal of establishing a common STRIDE-based methodology for threat modeling for ICS.**

***Index Terms*—Stride, ICS, IIoT, Threat Modeling**

I. Introduction

Historically, Industrial Control Systems (ICSs) used to form isolated networks that were often limited by a slow but reliable bus system. The paradigm shift towards more intelligent sensors and actuators, however, allows new possibilities to control, monitor, manage and optimize an ICS. But these opportunities also require the previously isolated networks to become open, to foster the so-called IT-OT convergence, and possibly be connected to the internet, becoming the Industrial Internet of Things (IIoT). This is the turning point in which cyber security has become essential to protect the ICS and ultimately ensure its intended purpose, such as the manufacturing of products or critical infrastructure operation.

Not only have standardization bodies like NIST identified the need for security in ICS [1], but attack statistics from recent years also demonstrate this necessity. Among the prime threats that occurred between July 2021 and July 2022 were ransomware attacks, malware, threats against data, and supply chain attacks [2]. The industrial sector was even the prevalent target of ransomware attacks between May 2021 to June 2022 according to the *ENISA Threat Landscape for ransomware attacks* report [3] with 27.8% out of all 623 incidents. These numbers also indicate that the ICS may actually not even be the prime target, but only the means to attack their customers or society.

Threat modeling is typically performed in the design phase to identify the threats against the system under consideration, rate them, and determine countermeasures. STRIDE [4], a widely-used methodology for threat analysis, was originally developed by Microsoft as part of their Secure Software Development Lifecycle [5]. The STRIDE threat model comprises six threat types: spoofing, tampering, repudiation, information exposure, denial of service, and elevation of privilege. Over the years STRIDE got extended and adapted but its usage always starts with the analysis of a certain model representing the system, for instance Data Flow Diagrams (DFDs). Once the threats for the assets in the system model are identified by means of STRIDE they may be further rated for prioritization and then mitigated by a variety of countermeasures.

Although STRIDE was developed for software, it was later also found to be applicable in other domains. In particular, STRIDE was also applied to Operational Technology (OT) systems, including automotive, IoT and ICS. This happened partly also due to extended connectivity and the increased use of software in these systems. At the same time, however, the physical aspect of the systems adds a new dimension to threat modeling including functional safety. Hence, existing approaches are being modified. For precisely these reasons, the extended use of STRIDE in OT and the significantly different attack surface, we investigate the use of STRIDE. This work summarizes in which domains STRIDE was used and discusses various published extensions of STRIDE.

Our research focus is how STRIDE can be used in threat modeling in ICSs, however we include also other OT areas with similar challenges in our initial search. We identify the following as the main challenges for ICS in threat modeling:

- Modeling of the physical attack surface is required (e.g., the interaction with human operators)
- Threat consequences can be physical and non-physical (e.g., functional safety)
- The lifecycle of devices need to be considered (e.g., during maintenance or reconfiguration additional connectivity is present)

Contribution. In this paper we show how the threat model STRIDE is being used in OT. STRIDE is of interest for its wide use in many industries. It has been used and adapted in several ways to accommodate the needs of a particular domain. The aim is to (i) provide an overview how STRIDE was modified to fit certain domains and how it was used in those domains and (ii) to identify relevant challenges and their

©2024 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works.
O. Saßnick, T. Rosenstatter, C. Schäfer, S. Huber, "STRIDE-based Methodologies for Threat Modeling of Industrial Control Systems: A Review," *in 2024 IEEE 7th Industrial Cyber-Physical Systems Conference (ICPS2024)*, IEEE 2024, *in print*.

potential solutions when applying STRIDE in ICSs.

II. Background

The RAMI 4.0 model [6] is the de facto model used to describe Industry 4.0. This reference architecture describes industrial machinery in three dimensions. One axis represents the hierarchy levels according to its functions, e.g., from product, field device to connected world. The other axis describes the products lifecycle and value stream. The horizontal axis, the *layers* dimension, decomposes the machine into its properties ranging from asset, integration to functional and business. This reference model allows users to have a common way to discuss and design complex automation system also involving many different actors and vendors. The model also highlights the far reaching potential of OT by not only considering the automation systems isolated from the entire process. NIST also started to investigate cyber securtiy for OT systems and published the NIST 800-82r3 [1], *A Guide to Operational Technology (OT), Security*. This document emphasizes the importance of OT security by highlighting that many OT-based systems are also belonging to critical infrastructure, e.g., food and agriculture, healthcare, transport systems, and energy. The NIST guidelines also support users in establishing OT security in an organization through guidance in the various processes, from setting up a cyber security program to defining a cyber security architecture.

OT security is different to IT security for many reasons, crucial ones in regard to threat modeling are detailed below:

Availability is of utmost importance as OT systems need to be operating 24/7. A halt in production or of the system's function, e.g., waste water treatment, needs to be meticulously planned. Sudden stops could lead to significant loss in revenue for production systems or even have a serious impact on society when considering critical infrastructure. OT consists of real-time systems which require time guarantees to operate, and interact with the physical world and with each other. STRIDE already includes the requirement of availability through the denial of service threat. We believe that availability and real-time requirements are also crucial to include in threat prioritization and risk assessment.

Functional Safety needs to be guaranteed in ICS due to the close operation of heavy machinery to operators. In other words, the risk of such hazardous situations has to be minimized. Therefore, functional safety standards, such as ISO 13849 [7], need to be followed and certified. This introduces additional challenges, security mechanisms may interfere with safety or may even require a re-certification. Other domains have similar challenges, like the automotive domain.

The *Lifecycle* of an ICS starts with the development, continues with maintenance and operation and ends with decommissioning. The setup comprising Programmable Logic Controllers (PLCs), actuators and sensors from various vendors, however, increases the complexity for modeling and planning the security lifecycle. Security updates are examples for maintenance, they require planning and understanding of each component and how they interact, such that costly downtimes are avoided or reduced to a minimum. Moreover, production lines will be reconfigured more often to provide custom-made products resulting in an accelerated lifecycle.

Physical Threats in ICS are extending the attack surface significantly. The large, complex and unique setup of each production line enables malicious actors to attack the system on various physical points, e.g., pretending to come from a contracted company to perform service updates or infecting the computers of the maintenance company. Next to the extended attack surface for entering the system, OT systems are also tightly connected to physical processes, like production. Attacks on such systems could cause a full production stop leading to an immense loss in revenue.

A. Threat Modeling using STRIDE

DFDs are most commonly used for threat analysis, they describe the system comprising four types: process, data flow, data store, and external entity. DFDs also allow to easily model trust boundaries used to separate untrusted/less trusted environments from the trusted. Shostack [4] also highlights that DFDs are mostly ideal for threat modeling as problems/threats typically follow the data flow. Once the model sufficiently describes the system, the practitioners can start the analysis using STRIDE.

There are two ways to perform a STRIDE analysis; following STRIDE-per-element or STRIDE-per-interaction. By using STRIDE-per-element experts analyze each component separately for security threats, whereas STRIDE-per-interaction, focuses on functions, processes and analyzes these interactions as whole. Initially, STRIDE-per-element was thought to be simpler as it is easier understood by beginners. Yet, it is more difficult to understand the system by considering the elements one by one. STRIDE-per-interaction addresses this shortcoming by considering the interaction between two elements in the form of tuples $<$*origin, destination, interaction*$>$ [4]. In contrast to this, an empirical study by Tuma et al. [8] has shown that STRIDE-per-element still yielded in a higher completeness of identified threats.

The next step, identifying mitigation techniques for each of the identified threats, is more open and may require additional support for finding suitable mitigation techniques. First, a systematic risk assessment can help in focusing on the threats that matter most. Second, a taxonomy or structure of mitigation techniques may help to select the best suitable technique. For instance, NIST SP 800-82r3 [1] provides further guidance for risk assessment and mitigation techniques.

III. Methodology

We conducted our research by following the reviewing process proposed by Snyder [9]. The review is motivated by the need to strengthen the awareness of security practices using STRIDE in ICS, desired by industry and academia. In our search conducted in October 2023, no other comparable work was found in the IEEE, ACM, Elsevier and Google Scholar databases.

In this review, we first define the research questions our review should cover and then we perform a semi-exhaustive search to find relevant publications and manually screen them based on defined inclusion/exclusion criteria (see Section III-B). The analysis of the identified relevant publications is shown in Section IV.

A. Research Questions

We have identified two main research questions to which this review should contribute. Overall, we are interested how STRIDE is used in the OT domain such that we can identify approaches that are also suitable specifically for ICS.

- **RQ.1** How is STRIDE used in the overall threat modeling process in the OT domain?
- **RQ.2** How is STRIDE modified to address ICS specific aspects?

RQ.1 explores the overall threat modeling process incorporating the STRIDE methodology, and domain. In *RQ.2* the focus is shifted to the specific requirements in ICS environments, such as functional safety, lifecycle considerations, and physical threats. We examine whether these ICS-specific aspects were taken into account and if such considerations led to modifications of the STRIDE approach.

B. Search Strategy

The results are collected from a selection of publication databases, namely, ACM Digital Library, IEEE Xplore, and Elsevier's ScienceDirect. For each database a search string was formulated to find any publication that has `Threat Model` or `Threat Analysis` in their title, abstract or as keywords. Additionally the term `STRIDE` had to appear at least once in the full-text. To narrow down our results to the relevant domains, the search was further refined by additionally demanding one of the following terms to be present in the title, abstract or as keywords (singular or plural): `cyber physical system`, `CPS`, `Industrial IoT`, `IIoT`, `Industrial Control System`, `ICS`, `OT`, `IoT` or `automotive`. The queries in all three databases resulted in an initial total of 140 publications[1].

A two-stage manual screening was performed to identify relevant literature. In the first stage, publications were excluded based on title and abstract. The second step included a full-text screening of the remaining papers. The inclusion criteria were that the publication must use the STRIDE model or an extension, moreover, the domain had to be within OT or generic such that it could potentially be applied in ICS. The full process was performed by two of the authors in order to circumvent a potential bias in the selection process. Furthermore, research centering around smart home was excluded, as well as publications focusing solely on network communication and software systems.

Ultimately, this resulted in a total of 39 publications from journals and conferences of which 29 were found in IEEE Xplore, 7 in the ACM Digital Library, and 3 in Elsevier's ScienceDirect. Figure 1 provides an overview of the year when the research publications were published. The publication year also shows how this field evolved over the past years. For instance, 24 of the papers were published from 2021 onwards and only 4 were published before 2018. It also has to be taken into account that the year 2023 has not ended as the databases were queried on 21. September 2023.

[1]Search conducted on 21st September 2023

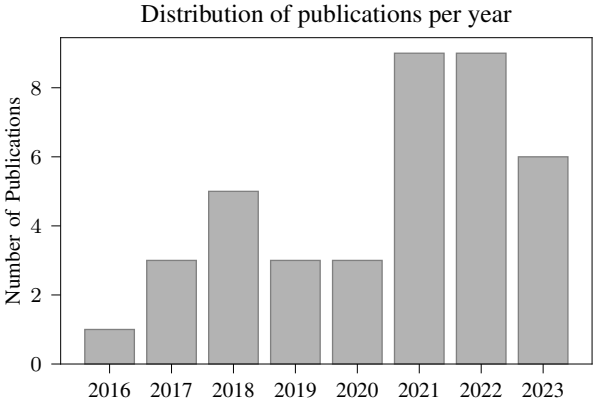

Figure 1. Number of publications per year ($n = 39$.)

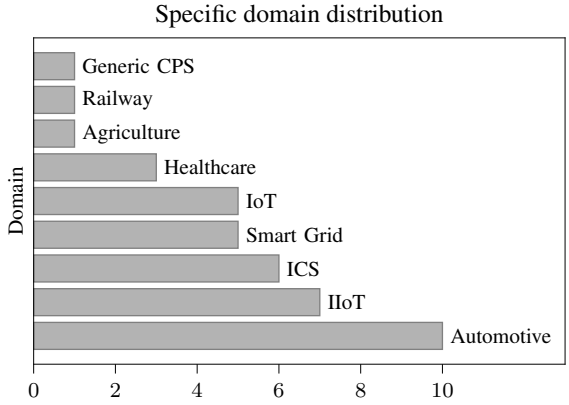

Figure 2. Number of publications per domain ($n = 39$).

IV. Results

In this section we first present in Table I an overview of the identified publications relevant to OT (see Section III). It shows the year of publication, the venue (7 journals, 28 conference and 4 workshop publications), the domain, and information about whether a STRIDE extension was proposed. Further, we include whether a DFD was used and whether a use case was included. Figure 2 presents a comprehensive overview of the different domains. Research in IIoT looked at industrial systems in a broader sense, e.g., smart manufacturing, and industry to cloud solutions. In contrast, literature identified as ICS focused on specific industrial systems, for instance waste water treatment or production lines.

Section IV-A addresses *RQ.1* by analyzing the threat modeling processes. *RQ.2* is examined in Section IV-B and IV-C.

Table I
OVERVIEW OF REVIEWED PUBLICATIONS USING STRIDE WITHIN THE OT DOMAIN.

Publisher	Year	Authors	Ref.	Venue	used STRIDE extension	DFD used	Use case included	Domain
ACM	2016	Islam et al.	[10]	Work.		√	√	Automotive
	2018	Monteuuis et al.	[11]	Work.	√			Automotive
	2019	Ankele et al.	[12]	Conf.				IIoT
	2020	Rak et al.	[13]	Conf.			√	Smart Grid
	2021	Li et al.	[14]	Conf.		√	√	ICS
	2022	Srikumar et al.	[15]	Conf.	√			IoT
	2023	Da Silva et al.	[16]	Conf.		√	√	ICS
Elsevier	2022	Sukiasyan et al.	[17]	Jour.			√	IIoT
	2023	Akkad et al.	[18]	Jour.			√	Smart Grid
		Khalil et al.	[19]	Jour.		√	√	Smart Grid
IEEE	2017	Khan et al.	[20]	Conf.		√	√	Smart Grid
		Ramis Ferrer et al.	[21]	Conf.				ICS
		Sandor and Sebestyn-Pal	[22]	Conf.		√		IoT
	2018	Cagnazzo et al.	[23]	Work.		√	√	Healthcare
		Furtado et al.	[24]	Conf.		√	√	Automotive
		Hagan et al.	[25]	Conf.				ICS
		Park et al.	[26]	Conf.		√	√	IoT
	2019	Leander et al.	[27]	Conf.		√		IIoT
		Tseng et al.	[28]	Jour.		√	√	Healthcare
	2020	Aigner and Khelil	[29]	Conf.			√	Automotive
		Danielis et al.	[30]	Conf.		√	√	IoT
	2021	Asif et al.	[31]	Conf.		√	√	Agriculture
		Cilleruelo et al.	[32]	Work.		√	√	Healthcare
		Flå et al.	[33]	Conf.		√	√	Smart Grid
		Girdhar et al.	[34]	Conf.		√	√	Automotive
		Hollerer et al.	[30]	Conf.	√			OT/IIoT
		Ruf et al.	[35]	Conf.			√	IIoT
		Strandberg et al.	[36]	Conf.			√	Automotive
		Zhang et al.	[37]	Jour.			√	Automotive
	2022	AbuEmera et al.	[38]	Conf.		√	√	IIoT
		Girdhar et al.	[39]	Jour.		√	√	Automotive
		Hollerer et al.	[40]	Conf.	√	√	√	ICS
		Kumar Kuri et al.	[41]	Conf.		√	√	Automotive
		Schmittner et al.	[42]	Conf.			√	IIoT
		Sheikh and Singh	[43]	Conf.		√		CPS
		Sindhwad and Kazi	[44]	Conf.				ICS
	2023	Castiglione and Lupu	[45]	Jour.				Railway
		Font et al.	[46]	Conf.		√	√	IoT
		Siddiqui et al.	[47]	Conf.		√	√	Automotive

In Section IV-B an overview is given on modifications of STRIDE, noting that only four out of 39 publications utilized or suggested modifications of STRIDE. Section IV-C details studies addressing OT- and more specifically ICS-relevant aspects.

A. Threat Modeling using STRIDE

DFDs were the most common model used for threat modeling. More than half (23 of 39) of the reviewed publications were using DFDs. This observation also covers with Shostack [4] saying that they are in most cases ideal for threat modeling. The other models were often system models of the architecture in various abstractions, like describing the network components and how they are connected. Notably, a few publications used the STRIDE threat model to identify common threats, for example, by analyzing published attacks [36] or by using a threat analysis tool such as ThreatGet [42].

Comparing the specific STRIDE approaches utilized, we also observed that STRIDE-per-element was used for threat identification at most times. In cases the authors did not further specify taking the step of creating a DFD nor mention DFDs, we also assumed that they performed STRIDE-per-element directly on the system model. It may not be representative, but overall, STRIDE-per-element was more often used, likely also because it is easier to understand for beginners and has shown a higher level of completeness [8].

Concerning the further modeling process, how the threats are addressed or mitigated, we have not found a common methodology. Some followed the DREAD risk assessment model proposed by Microsoft. However, the Microsoft SDL team stopped recommending it since 2010, as they found that DREAD is fairly subjective leading to unusual results [4]. Other solutions, like Hagan *et al.* [25] propose using a set of access control policies instead of following guidelines to achieve the security requirements. Monteuuis *et al.* [11]

suggest in their risk analysis method *SARA* the use of attack trees to compute the risk ot the identified threats.

Most publications focused on their methodology and how to integrate it with other methods like previously explained. Exceptions are Da Silva *et al.* [16] and Flå *et al.* [33] who also developed an integration to existing software tool, i.e., a template for the Microsoft Threat Modeling Tool (MTMT) for ICS respectively smart grid systems.

B. Adaptations of STRIDE

Each of the six letters of the acronym STRIDE represents a threat category. By systematically and exhaustively considering each of the six categories for each element or interaction in the system model, we reduce the chance of overlooking threats. Hence, an obvious way to adapt STRIDE is to include further threat categories.

Monteuuis *et al.* [11] introduce STRIDELC. The motivation is to consider privacy issues and risks arising by processing incorrect data from trusted data sources. The added letters represent the additional threat categories *confusion* and *linkability*. Confusion describes the processing of authentic information, yet with incorrect content not reflecting ground truth. Incorrect data from a valid data source is being generated. Linkability is used describes public accessible data that can be used to de-anonymize the owner of the system.

Hollerer *et al.* [40] use STRIDE-LM, which was introduced by Muckin and Fitch at the Lockheed Martin Corporation [48]. LM stand for Lateral Movement, describing the expanding control over the target network beyond the initial point of compromise. However, this seems to form rather a threat consequence.

Srikumar *et al.* [15] propose STRIPED, where the letter *P* is added specifically to address physical attacks. The category is further divided into four sub-groups, namely device identity, device integrity, device lifecycle and device communication attacks. The main motivation is to raise the awareness for present physical access threats.

C. ICS Aspects

In the following, we highlight selected publications that specifically addressed ICS-specific aspects we described in Section II in order to contribute to *RQ.2*.

Safety. While more studies include safety considerations in the automotive domain, like [10], [11], [36], [39], a few also have done so in different domains and are therefor discussed more in the following.

Castiglione and Lupu [45] propose a methodology that combines a System Theoretic Process Analysis (STPA) with STRIDE to identify threats that can lead to accidents and hazards for a communication based train control system. By merging the results of the safety analysis with STRIDE threat modeling, they identify a set of vulnerabilities which ultimately can result in a safety critical attack.

Hollerer *et al.* [30] introduce a parallel approach, performing a HAZOP [49] analysis for safety threats and STRIDE-LM for security threats. Safety threats are evaluated based on the safety integrity levels introduced in IEC 61508. Security threats are assessed using the Common Vulnerability Scoring System (CVSS) and attacker modeling via Mitre Att&ck [50]. This results in an attack difficulty score, which is mapped to four security levels and is used to define system zones and conduits. The safety modeling results are used to reveal conflicts between safety and security, and in the final modeling step, the goal is to find solutions that satisfy both safety and security requirements.

Later, Hollerer *et al.* [40] compare STRIDE-LM and Failure-Attack-CounTermeasure (FACT) graphs [51] to highlight their differences. In an initial step the DFD of the system is created. In second step threats are identified with STRIDE by using MTMT. To include the safety modeling, for each object additional safety attributes are defined. The FACT graph represents a combination of a fault tree analysis and attack trees from the security domain. First a fault tree is built, leading to possible causes for a fault. Consequently, the possible causes are connected to attack trees. The authors note a high complexity for the resulting graphs and chose to split it into smaller layers.

Physical Threats. Many publications, like [16], [20], [23], [27], do not consider physical threats, reasoning that the physical part of their system is not susceptible to cyber attacks or clearly state that it is beyond the carried out work.

Others, like Khalil *et al.* [19], partially model physical attacks. Whenever a component is in an unsafe surrounding without protection, they consider accessible hardware interfaces, however disregard any kind of manipulation of the device sensing capabilities. They further note, that for the DFD creation process, no rules regarding physical system components were found, and therefore opted to include them, whenever it aided the overall system understanding. To make them distinguishable, they chose visually different connection types (analog/digital) and introduced the notion for physical processes.

In a similar fashion Schmittner *et al.* [42] add rules to a threat modeling tool, requiring access control for all kind of physical system management interfaces (e.g. HMI), otherwise listing an unauthorized physical access threat.

Casola *et al.* [52] add to the picture, that physical dependencies or characteristics might have an impact on relevant cyber threats, like a battery-powered device can be drained by increasing its power consumption, resulting in a DoS, which is not possible for an AC-powered device. Next to a dedicated ICS template for the Microsoft Threat Modeling Tool, they integrate Common Vulnerabilities and Exposures (CVEs) to MTMT and map them to STRIDE.

In the automotive domain, Kuri *et al.* [41] consider all kinds of physical threats regarding the sensing devices of modern connected vehicles and map them to the STRIDE categories. For example by clipping onto the sensor wires, arbitrary input data can be created. The threat categories elevation of privilege, spoofing and denial of service are assigned to the physical threats in their use case.

Finally, as previously mentioned in Section IV-B, Srikumar

et al. [15] proposed STRIPED. In the included use case, an aircraft inspection system is studied and 27 different physical threats are identified. While causing additional awareness, the category added to STRIDE for physical threats may be not required, as demonstrated by [41]. For instance, the sub-category of device identity attacks (e.g., sensor spoofing, hardware spoofing) can also be considered as spoofing in general and device communication channel attacks fall into the information disclosure category.

In summary, when including physical threats, a sensible approach seems to involve performing the STRIDE method twice, considering both roles of the system separately, from a cyber perspective and a physical perspective.

Lifecycle. Most of the studied publications omit the modeling of a lifecycle. It is mainly included in the automotive domain. For instance Islam *et al.* [10] map the different ISO 26262 lifecycle phases concept, product development and operational to adequate security measures. When modeling threats for ICSs with brownfield installations, the product concept and development phases may not be of great relevance. In that regard, Leander *et al.* [27] considered multiple scenarios reflecting different phases of the lifecycle. In one of their scenarios a pump device in a flow control loop needs to be replaced due to some malfunction. To manage the scenario, lifecycle entry and exit actions respectively for the old and new device are defined.

D. Challenges and Future Research Directions

While the number of publications on threat modeling processes utilizing STRIDE is increasing (Figure 1), open questions and challenges remain. Based on the studied publications (Table I), the following challenges have been identified:

Modeling of physical components. No standardized representations for physical components exist in a DFD. A common standard, which is widely known and accepted, is missing. Two studies [16], [33] contribute towards this goal by developing templates for MTMT. Notably, Khalil *et al.* [19] address this issue by using different notions for software-related and physical processes.

Level of detail. Current publications derive DFDs based on expert knowledge without a systematic approach to determine relevant security processes and entities. In such cases, the level of detail may vary, which can lead to too simplified DFDs, overlooking security-relevant information, or overly complex DFDs, which causes increased workload for subsequent process steps.

Scalability. Modeling systems with numerous entities in a single DFD becomes impractical. Questions arise regarding how to partition a DFD without losing security-relevant information and how to handle entities that are similar but not identical. While tools like MTMT automate the application of the STRIDE methodology, studies reveal that this automated approach easily generates a significant number of threats (for example, 879 in case of [40]), making manual processing afterwards cumbersome. Thus additional efforts need be directed towards reducing the amount of work for subsequent stages.

Usability. In the studied publications, the aspect of usability in the ICS domain was only investigated by Li *et al.* [14]. More specifically, they propose to additionally evaluate the usability of security mitigations. Their motivation has two aspects. Firstly, security measures should be efficiently implementable within a production environment, minimizing resource wastage. Secondly, security measures are naturally more likely to be followed, when they are designed to be user-friendly. A relatable example, mandating long auto-generated passwords results in handwritten sticky-notes, because they are hard to remember.

Future. The vision of highly-flexible smart manufacturing in contrast to the fast changing threat landscape and the efforts towards security-by-design indicate that threat modeling needs to result in a continuous process in the long run. It needs to become an integral part of a security-by-design architecture. In most of the reviewed publications, the threat modeling process was manually performed, which requires expert knowledge, involves manual decisions and substantial effort. Moreover, the **lifecycle** was mostly omitted.

There are endeavors to automate certain aspects (e.g., [53]), however for true continuity at manageable cost and at a flexible scale, a complete automation of the threat modeling process seems desirable. To achieve this, the entire threat modeling process needs to be more systematic and requiring less of expert knowledge. For instance, in [54] the security description of a full plant is formulated with AutomationML, which is generated from the existing artifacts, created during the design and engineering phase. Adding the vision of threat modeling being continuous, it could be adapted such that each device independently provides meta-data describing itself, contributing to a complete picture regarding the security of the plant. Consequently, a DFD can be auto-generated based on the interconnectedness and the provided meta-data of each device.

V. Related Work

Other works mainly focus on threat modeling concepts in general and how they are used, or perform threat modeling on a specific use case, however, to the best of our knowledge, we found no comparable work that investigates thoroughly the use of STRIDE in the OT domain.

Lohmann *et al.* [55] provide a systematic literature review on threat modeling concepts in general and also answer questions about the phases addressed according to the ISO 27005 risk management process. To find a general overview of the landscape within computer science, the authors in [55] only include journal publications with at least two citations. In our work, on the other hand, we want to explore a quite narrow area (OT domain), hence, we did not include such limitations, to not overlook any relevant publication. Benyahya *et al.* [56] review threat analysis and risk assessment methodologies for vehicles. They evaluate them with focus on highly connected and automated vehicles.

VI. Conclusion

In this study, we focused on the application of STRIDE when performing threat modeling of OT systems. The aim was to get an overview of the current state of the art and identify open challenges in the field of threat modeling for ICS. As other OT sub-domains face similar challenges, we consider all publications in the OT domain.

We defined research questions concerning the use of STRIDE in the OT domain. Most publications begin the threat modeling process by creating a DFD and subsequently performing STRIDE-per-element. For threat prioritization, various methods are applied, including DREAD, attack trees and CVSS. Overall, the automotive domain was the most dominant with 10 publications closely followed by IIoT and ICS with seven respectively six publications. The review also showed that working with STRIDE in the OT domain has significantly increased in the recent years.

To draw conclusions regarding threat modeling for ICS, specific aspects like physical threats, lifecycle, and safety were additionally studied across all publications. While a few works address the integration of safety and security for ICS directly (e.g., [30], [40], [45]), a systematic modeling approach for the lifecycle in STRIDE-based approaches was not found. Most reviewed works did not use an extension of STRIDE nor proposed a modification, only four out of the final set of 39 publications were using an extended STRIDE threat model.

Based on the results, five challenges that need particular attention were identified; namely the modeling of physical components, the level of detail used for the analysis, scalability, modeling of the lifecycle, and the usability of security mitigations in ICS.

For the future, given the increasing frequency of cyber attacks on ICS and considering the simultaneous ongoing initiatives for a highly-flexible smart manufacturing, the threat-modeling processes need to become less time-consuming, consequently moving towards a higher level of automation.

References

[1] K. Stouffer, M. Pease, C. Tang, *et al.*, "Guide to operational technology (OT) security," National Institute of Standards and Technology, Sep. 2023. DOI: 10.6028/NIST.SP.800-82r3.

[2] *ENISA threat landscape 2022: July 2021 to July 2022*, eng. Heraklion: ENISA, 2022, OCLC: 1370608603.

[3] *ENISA threat landscape for ransomware attacks*, eng. Heraklion: ENISA, 2022, OCLC: 1347439621.

[4] A. Shostack, *Threat modeling: Designing for security*. John Wiley & Sons, 2014.

[5] M. Howard and S. Lipner, *The security development lifecycle*. USA: Microsoft Press, 2006.

[6] M. Hankel and B. Hankel. "The reference architectural model industrie 4.0 (RAMI 4.0)." Accessed: 2022-09-26. (2015), [Online]. Available: https://www.zvei.org/en/press-media/publications/the-reference-architectural-model-industrie-40-rami-40.

[7] International Organization for Standardization (ISO), "ISO 13849-1:2023 – Safety of machinery — Safety-related parts of control systems — Part 1: General principles for design," Standard, 2023.

[8] K. Tuma and R. Scandariato, "Two architectural threat analysis techniques compared," in *Software Architecture: 12th European Conference on Software Architecture, ECSA 2018, Madrid, Spain, September 24–28, 2018, Proceedings 12*, Springer, 2018, pp. 347–363.

[9] H. Snyder, "Literature review as a research methodology: An overview and guidelines," en, *Journal of Business Research*, vol. 104, pp. 333–339, Nov. 2019. DOI: 10.1016/j.jbusres.2019.07.039.

[10] M. M. Islam, A. Lautenbach, C. Sandberg, and T. Olovsson, "A risk assessment framework for automotive embedded systems," in *Proceedings of the 2nd ACM International Workshop on Cyber-Physical System Security*, Xi'an China: ACM, May 2016, pp. 3–14. DOI: 10.1145/2899015.2899018.

[11] J.-P. Monteuuis, A. Boudguiga, J. Zhang, H. Labiod, A. Servel, and P. Urien, "SARA: Security automotive risk analysis method," in *Proceedings of the 4th ACM Workshop on Cyber-Physical System Security*, Incheon Republic of Korea: ACM, May 2018, pp. 3–14. DOI: 10.1145/3198458.3198465.

[12] R. Ankele, S. Marksteiner, K. Nahrgang, and H. Vallant, "Requirements and recommendations for IoT/IIoT models to automate security assurance through threat modelling, security analysis and penetration testing," in *Proceedings of the 14th International Conference on Availability, Reliability and Security*, Canterbury CA United Kingdom: ACM, Aug. 2019. DOI: 10.1145/3339252.3341482.

[13] G. Salzillo, M. Rak, and F. Moretta, "Threat Modeling based Penetration Testing: The Open Energy Monitor Case study," in *13th International Conference on Security of Information and Networks*, Merkez Turkey: ACM, Nov. 2020. DOI: 10.1145/3433174.3433181.

[14] K. Li, A. Rashid, and A. Roudaut, "Vision: Security-usability threat modeling for industrial control systems," in *Proceedings of the 2021 European Symposium on Usable Security*, Karlsruhe Germany: ACM, Oct. 2021, pp. 83–88. DOI: 10.1145/3481357.3481527.

[15] K. Srikumar, K. Kashish, K. Eggers, *et al.*, "STRIPED: A threat analysis method for IoT systems," in *Proceedings of the 17th International Conference on Availability, Reliability and Security*, Vienna Austria: ACM, Aug. 2022. DOI: 10.1145/3538969.3538970.

[16] M. Da Silva, M. Puys, P.-H. Thevenon, S. Mocanu, and N. Nkawa, "Automated ICS template for STRIDE Microsoft threat modeling tool," in *Proceedings of the 18th International Conference on Availability, Reliability and Security*, Benevento Italy: ACM, Aug. 2023. DOI: 10.1145/3600160.3605068.

[17] A. Sukiasyan, H. Badikyan, T. Pedrosa, and P. Leitao, "Secure data exchange in industrial Internet of Things," *Neurocomputing*, vol. 484, pp. 183–195, May 2022. DOI: 10.1016/j.neucom.2021.07.101.

[18] A. Akkad, G. Wills, and A. Rezazadeh, "An information security model for an IoT-enabled smart grid in the Saudi energy sector," *Computers and Electrical Engineering*, vol. 105, p. 108 491, Jan. 2023. DOI: 10.1016/j.compeleceng.2022.108491.

[19] S. M. Khalil, H. Bahsi, H. O. Dola, T. Korõtko, K. McLaughlin, and V. Kotkas, "Threat modeling of cyber-physical system - a case study of a microgrid system," *Computers & Security*, vol. 124, p. 102 950, Jan. 2023. DOI: 10.1016/j.cose.2022.102950.

[20] R. Khan, K. McLaughlin, D. Laverty, and S. Sezer, "STRIDE-based threat modeling for cyber-physical systems," in *2017 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe)*, Torino: IEEE, Sep. 2017. DOI: 10.1109/ISGTEurope.2017.8260283.

[21] B. Ramis Ferrer, S. O. Afolaranmi, and J. L. M. Lastra, "Principles and risk assessment of managing distributed ontologies hosted by embedded devices for controlling industrial systems," in *IECON 2017 - 43rd Annual Conference of the IEEE Industrial Electronics Society*, Beijing: IEEE, Oct. 2017, pp. 3498–3505. DOI: 10.1109/IECON.2017.8216592.

[22] H. Sandor and G. Sebestyen-Pal, "Optimal security design in the Internet of Things," in *2017 5th International Symposium on Digital Forensic and Security (ISDFS)*, Tirgu Mures, Romania: IEEE, Apr. 2017. DOI: 10.1109/ISDFS.2017.7916496.

[23] M. Cagnazzo, M. Hertlein, T. Holz, and N. Pohlmann, "Threat modeling for mobile health systems," in *2018 IEEE Wireless Communications and Networking Conference Workshops (WCNCW)*, Barcelona: IEEE, Apr. 2018, pp. 314–319. DOI: 10.1109/WCNCW.2018.8369033.

[24] M. D. Furtado, R. D. Mushrall, and H. Liu, "Threat Analysis of the Security Credential Management System for Vehicular Communications," in *2018 IEEE International Symposium on Technologies for Homeland Security (HST)*, Woburn, MA, USA: IEEE, Oct. 2018. DOI: 10.1109/THS.2018.8574206.

[25] M. Hagan, F. Siddiqui, S. Sezer, B. Kang, and K. McLaughlin, "Enforcing policy-based security models for embedded socs within the internet of things," in *2018 IEEE Conference on Dependable and Secure Computing (DSC)*, Kaohsiung, Taiwan: IEEE, Dec. 2018. DOI: 10.1109/DESEC.2018.8625140.

[26] W. Park, D. Choi, and K. Lee, "Threat analysis of Wi-Fi connected dashboard camera," in *2018 International Conference on Platform Technology and Service (PlatCon)*, Jeju: IEEE, Jan. 2018. DOI: 10.1109/PlatCon.2018.8472768.

[27] B. Leander, A. Causevic, and H. Hansson, "Cybersecurity challenges in large industrial IoT systems," in *2019 24th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA)*, Zaragoza, Spain: IEEE, Sep. 2019, pp. 1035–1042. DOI: 10.1109/ETFA.2019.8869162.

[28] T. W. Tseng, C. T. Wu, and F. Lai, "Threat analysis for wearable health devices and environment monitoring internet of things integration system," *IEEE Access*, vol. 7, pp. 144 983–144 994, 2019. DOI: 10.1109/ACCESS.2019.2946081.

[29] A. Aigner and A. Khelil, "A security qualification matrix to efficiently measure security in cyber-physical systems," in *2020 32nd International Conference on Microelectronics (ICM)*, Aqaba, Jordan: IEEE, Dec. 2020. DOI: 10.1109/ICM50269.2020.9331797.

[30] S. Hollerer, W. Kastner, and T. Sauter, "Towards a threat modeling approach addressing security and safety in OT environments," in *2021 17th IEEE International Conference on Factory Communication Systems (WFCS)*, Linz, Austria: IEEE, Jun. 2021, pp. 37–40. DOI: 10.1109/WFCS46889.2021.9483591.

[31] M. R. A. Asif, K. F. Hasan, M. Z. Islam, and R. Khondoker, "STRIDE-based cyber security threat modeling for IoT-enabled precision agriculture systems," in *2021 3rd International Conference on Sustainable Technologies for Industry 4.0 (STI)*, Dhaka, Bangladesh: IEEE, Dec. 2021. DOI: 10.1109/STI53101.2021.9732597.

[32] C. Cilleruelo, J. Junquera-Sanchez, L. de-Marcos, N. Logghe, and J.-J. Martinez-Herraiz, "Security and privacy issues of data-over-sound technologies used in IoT healthcare devices," in *2021 IEEE Globecom Workshops (GC Wkshps)*, Madrid, Spain: IEEE, Dec. 2021. DOI: 10.1109/GCWkshps52748.2021.9682007.

[33] L. H. Flå, R. Borgaonkar, I. A. Tøndel, and M. Gilje Jaatun, "Tool-assisted threat modeling for smart grid cyber security," in *2021 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)*, Dublin, Ireland: IEEE, Jun. 2021. DOI: 10.1109/CyberSA52016.2021.9478258.

[34] M. Girdhar, J. Hong, Y. Yoo, and T.-j. Song, "Machine learning-enabled cyber attack prediction and mitigation for EV charging stations," in *2022 IEEE Power & Energy Society General Meeting (PESGM)*, Denver, CO, USA: IEEE, Jul. 2022. DOI: 10.1109/PESGM48719.2022.9916914.

[35] P. Ruf, J. Stodt, and C. Reich, "Security threats of a blockchain-based platform for industry ecosystems in the cloud," in *2021 Fifth World Conference on Smart Trends in Systems Security and Sustainability (WorldS4)*, London, United Kingdom: IEEE, Jul. 2021, pp. 192–199. DOI: 10.1109/WorldS451998.2021.9514058.

[36] K. Strandberg, T. Rosenstatter, R. Jolak, N. Nowdehi, and T. Olovsson, "Resilient shield: Reinforcing the resilience of vehicles against security threats," in *2021 IEEE 93rd Vehicular Technology Conference (VTC2021-Spring)*, Helsinki, Finland: IEEE, Apr. 2021. DOI: 10.1109/VTC2021-Spring51267.2021.9449029.

[37] H. Zhang, Y. Pan, Z. Lu, J. Wang, and Z. Liu, "A cyber security evaluation framework for in-vehicle electrical control units," *IEEE Access*, vol. 9, pp. 149 690–149 706, 2021. DOI: 10.1109/ACCESS.2021.3124565.

[38] E. A. AbuEmera, H. A. ElZouka, and A. A. Saad, "Security framework for identifying threats in smart manufacturing systems using STRIDE approach," in *2022 2nd International Conference on Consumer Electronics and Computer Engineering (ICCECE)*, Guangzhou, China: IEEE, Jan. 2022, pp. 605–612. DOI: 10.1109/ICCECE54139.2022.9712770.

[39] M. Girdhar, Y. You, T.-J. Song, S. Ghosh, and J. Hong, "Post-accident cyberattack event analysis for connected and automated vehicles," *IEEE Access*, vol. 10, pp. 83 176–83 194, 2022. DOI: 10.1109/ACCESS.2022.3196346.

[40] S. Hollerer, M. Chabrova, T. Sauter, and W. Kastner, "Combined modeling techniques for safety and security in industrial automation: A case study," in *2022 15th International Conference on Security of Information and Networks (SIN)*, Sousse, Tunisia: IEEE, Nov. 2022. DOI: 10.1109/SIN56466.2022.9970541.

[41] S. K. Kuri, T. Islam, J. Jaskolka, and M. Ibnkahla, "A threat model and security recommendations for IoT sensors in connected vehicle networks," in *2022 IEEE 95th Vehicular Technology Conference: (VTC2022-Spring)*, Helsinki, Finland: IEEE, Jun. 2022. DOI: 10.1109/VTC2022-Spring54318.2022.9860359.

[42] C. Schmittner, A. M. Shaaban, and G. Macher, "ThreatGet: Ensuring the Implementation of Defense-in-Depth Strategy for IIoT Based on IEC 62443," in *2022 IEEE 5th International Conference on Industrial Cyber-Physical Systems (ICPS)*, Coventry, United Kingdom: IEEE, May 2022. DOI: 10.1109/ICPS51978.2022.9816864.

[43] Z. A. Sheikh and Y. Singh, "A Hybrid Threat Assessment Model for Security of Cyber Physical Systems," in *2022 Seventh International Conference on Parallel, Distributed and Grid Computing (PDGC)*, Solan, Himachal Pradesh, India: IEEE, Nov. 2022, pp. 582–587. DOI: 10.1109/PDGC56933.2022.10053332.

[44] P. Sindhwad and F. Kazi, "Exploiting Control Device Vulnerabilities: Attacking Cyber-Physical Water System," in *2022 32nd Conference of Open Innovations Association (FRUCT)*, Tampere, Finland: IEEE, Nov. 2022, pp. 270–279. DOI: 10.23919/FRUCT56874.2022.9953826.

[45] L. M. Castiglione and E. C. Lupu, "Which Attacks Lead to Hazards? Combining Safety and Security Analysis for Cyber-Physical Systems," *IEEE Transactions on Dependable and Secure Computing*, 2023. DOI: 10.1109/TDSC.2023.3309778.

[46] J. A. Font, J. Jarauta, R. Gesteira, R. Palacios, and G. López, "Threat models for vulnerability analysis of IoT devices for Manipulation of Demand attacks," in *2023 JNIC Cybersecurity Conference (JNIC)*, Vigo, Spain: IEEE, Jun. 2023. DOI: 10.23919/JNIC58574.2023.10205781.

[47] F. Siddiqui, R. Khan, S. Y. Tasdemir, *et al.*, "Cybersecurity engineering: Bridging the security gaps in advanced automotive systems and ISO/SAE 21434," in *2023 IEEE 97th Vehicular Technology Conference (VTC2023-Spring)*, Florence, Italy: IEEE, Jun. 2023. DOI: 10.1109/VTC2023-Spring57618.2023.10200490.

[48] M. Muckin and S. C. Fitch, "A threat-driven approach to cyber security," *Lockheed Martin Corporation*, 2014.

[49] T. Srivatanakul, J. A. Clark, and F. Polack, "Effective security requirements analysis: HAZOP and use cases," in *Information Security: 7th International Conference, ISC 2004, Palo Alto, CA, USA, September 27-29, 2004. Proceedings 7*, Springer, 2004, pp. 416–427.

[50] The MITRE Corporation, *MITRE ATT&CK*, https://attack.mitre.org/, 2023.

[51] G. Sabaliauskaite and A. P. Mathur, "Aligning cyber-physical system safety and security," in *Complex Systems Design & Management Asia: Designing Smart Cities: Proceedings of the First Asia-Pacific Conference on Complex Systems Design & Management, CSD&M Asia 2014*, Springer, 2015, pp. 41–53.

[52] V. Casola, A. D. Benedictis, C. Mazzocca, and R. Montanari, "Toward automated threat modeling of edge computing systems," in *2021 IEEE International Conference on Cyber Security and Resilience (CSR)*, Rhodes, Greece: IEEE, Jul. 2021, pp. 135–140. DOI: 10.1109/CSR51186.2021.9527937.

[53] V. Casola, A. De Benedictis, M. Rak, and U. Villano, "Toward the automation of threat modeling and risk assessment in IoT systems," *Internet of Things*, vol. 7, p. 100 056, Sep. 2019. DOI: 10.1016/j.iot.2019.100056.

[54] M. Eckhart, A. Ekelhart, and E. Weippl, "Automated security risk identification using automationml-based engineering data," *IEEE Transactions on Dependable and Secure Computing*, vol. 19, no. 3, pp. 1655–1672, May 2022. DOI: 10.1109/TDSC.2020.3033150.

[55] P. Lohmann, C. Albuquerque, and R. Machado, "Systematic literature review of threat modeling concepts," in *Proceedings of the 9th International Conference on Information Systems Security and Privacy*, Lisbon, Portugal: SCITEPRESS - Science and Technology Publications, 2023, pp. 163–173. DOI: 10.5220/0011783000003405.

[56] M. Benyahya, T. Lenard, A. Collen, and N. A. Nijdam, "A systematic review of threat analysis and risk assessment methodologies for connected and automated vehicles," in *Proceedings of the 18th International Conference on Availability, Reliability and Security*, ser. ARES '23, Benevento, Italy: Association for Computing Machinery, 2023. DOI: 10.1145/3600160.3605084.