A method for threat modelling of industrial control systems

Lars Halvdan Flå and Martin Gilje Jaatun

SINTEF Digital, Trondheim, Norway
lars.flaa@sintef.no

Abstract. In this paper we propose a new method for threat modelling of industrial control systems (ICS). The method is designed to be flexible and easy to use. Model elements inspired by IEC 62443 and Data Flow Diagrams (DFD) are used to create a model of the ICS under consideration. Starting from this model, threats are identified by investigating how the confidentiality, integrity and availability of different functions in the ICS can be attacked. Finally, threats are prioritised and mitigations are proposed for those threats that are not accepted by the ICS owner. We briefly illustrate the use of the method on a simplified and fictitious power grid secondary substation case.

Keywords: Threat Modelling, Industrial Control System, IEC 62443, Cyber Security, Cyber Physical System

1 Introduction

The identification of threats to an Industrial Control System (ICS) is an important part of assessing the cyber security risk. We argue that the key to a successful method for identifying threats is to find an appropriate level of abstraction. A too detailed method will be resource demanding, while a method with too few details leaves threats unidentified.

In this paper we propose a method for performing threat modelling of ICS, and provide a brief example of the use of the method. The method draws inspiration from existing methods, such as STRIDE [16] and Cyber HAZOP [3], as well as the IEC 62443 standard on industrial control system security. The method is intended to facilitate a suitable level of abstraction, be flexible, and easy to understand. These are all properties that we regard as important for a threat modelling method.

The rest of the paper is structured as follows. Section 2 gives a brief overview of existing approaches to threat modelling of ICS. Section 3 presents the proposed method. Section 4 shows how the method can be applied to a fictitious power grid secondary substation. Section 5 discusses the different steps of the proposed method. Section 6 concludes the paper.

2 Background

In this section we give an overview of existing approaches for threat modelling of ICS or cyber physical systems (CPS).

Several contributions use some form of STRIDE [14, 16] to perform the threat modelling. STRIDE is an mnemonic for Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service and Elevation of Privilege. These categories indicate the types of threats which should be considered when analysing a system (originally software) for threats. This process is often supported by a DFD of the system. More recently, STRIDE has been applied to a broader context. Khalil et al. [11] propose a nine step threat modelling method where they adapt STRIDE to CPS. The method uses an enhanced version of DFD to create a model of the system, among other things introducing support for combining physical processes and software processes, similar to what we propose in our method. Threats are identified using STRIDE-per-element, and ranked based on their impact on different consequence categories. Kim et al. [13] propose a seven step method for threat modelling of an ICS. The system is modelled using standard DFD elements and trust boundaries. The trust boundaries appear in their example to group DFD elements according to physical equipment. Threats are identified using STRIDE and prioritised using DREAD. Another adaption of STRIDE to a cyber physical system is proposed by Khan et al. [12]. They advocate creating a data flow diagram per component in a system, identifying threats based on STRIDE, mapping threats to predefined consequences, and identifying vulnerabilities to plan for security controls. Jbair et al. [10] propose a five step threat modelling method for cyber physical systems. The method includes well known methods for identifying threats, among them STRIDE. It does however also include several other activities, including quantifying risk and describing threat actors. Their scope is therefore wider than what we propose in this paper. When it comes to application in industry, an interview study of 11 security professionals working with CPS security revealed that STRIDE was by far the most popular method for threat modelling [9].

We argue that the STRIDE method for threat modelling has some weaknesses, both generally and specifically related to its use on ICS. Sion et al. [15] claim that DFD, which STRIDE typically relies on, among others have an inability to model security controls and information on where systems are deployed. We furthermore argue that STRIDE may appear confusing as it mixes categories that directly violate security properties with categories which can be seen as a preparation for violating security properties One can for instance argue that spoofing in itself does not violate confidentiality, integrity and availability, but that it can be a prerequisite for violating all three.

Furthermore, we believe that the detailed approach taken by STRIDE can cause the number of threats to become high and therefore resource demanding to handle. Holik et al. [4] identify 92 threats to a digital secondary substation using STRIDE, although this number also greatly depends on the Microsoft Threat Modelling Tool template [2] used to perform the threat modelling. Regardless, the number of threats is likely to become significant for complex systems, especially if detailed DFD are created for all software processes present in all devices.

Other methods for identifying cyber threats to ICS exist, but they typically do so without referring to the term threat modelling. One class of such methods are safety related methods which have been adopted to security, for instance STPA-Sec [17] and Cyber HAZOP [3]. STPA-Sec takes a more top-down approach and starts with organisational purposes and goals, and ends up with identifying scenarios which may violate security requirements [17]. Cyber HAZOP is inspired by the original Hazard and Operability Analysis (HAZOP) method, which combines guide words (e.g., more, less, low, high) and process parameters (e.g., flow, pressure) to aid in the identification of dangerous situations. The team performing the assessment would then typically consider different part of the process and investigate what the effects of deviations such as ”more flow, less flow, low pressure, high pressure” could be. Cyber HAZOP, as described by Risktec [3], adapts this method to security. Instead of considering different parts of the process, the method first considers the organisation as a whole, and then individual zones and conduits. For zones, cyber guide words can for instance be ”Engineering Workstation”, or ”Control Server”, and cyber parameters can for instance be ”Execution”, ”Initial Access”, or ”Persistence”. For conduits, the only cyber guide word is data, while security parameters are ”Confidentiality”, ”Integrity” and ”Availability”. The Cyber HAZOP then creates deviations such as ”Engineering workstation - Execution” or ”Data - Integrity”. According to the authors, this can in turn be used to reason about consequences of such deviations, but also about vulnerabilities and security controls.

While STPA-Sec can be used to identify security relevant scenarios, we argue that a greater level of detail is needed to reason about how an attacker may cause such scenarios. Cyber HAZOP has similarities with our method in that it also appears to consider zones and individual components, such as an engineering workstation, and through their use of guide words. This is particularly true for how Cyber HAZOP treats conduits, where violations of confidentiality, integrity and availability is considered for the transmitted data. However, we argue for the need to establish a more detailed context for evaluating threats (e.g., which ICS functions rely on which devices, or what does the ICS function control), along with standardised elements for expressing this context. According to the authors in [3] ”A CyHAZOP will identify areas where more detailed investigations around controls and vulnerabilities should be undertaken”, and we intend, among other, that our proposed method can aid in this more detailed investigation of an area.

The method proposed in this paper allows for a relatively detailed modelling of an ICS, giving the team performing the threat modelling a good foundation for discussing methods for attack and consequences. However, by identifying threats at the level above individual processes and data flows, we believe the method also results in a manageable number of threats.

3 Threat modelling method

In this section we propose a threat modelling method for ICS. The method consists of three main steps: creating a model of the system, identifying threats, and evaluating threats. The goal of the method is to give a prioritised list of threats in need of mitigation, given the state of the ICS under consideration.

3.1 Creating a model of the system

The method starts with creating a model of the industrial control system under consideration. The model is built using the seven model elements: ICS function (which internally consists of a set of software processes and data flows), standalone security control, host device, network device, embedded device, external entity and zone. These elements are shown in Fig. 1 and described as follows:

ICS function: Inspired by the definition of an application in IEC 62443-4-2 [6]: *"one or more software programs and their dependencies that are used to interface with the process or the control system itself [...])"*. The ICS function performs a function in the ICS, and is implemented with potentially distributed software processes and the communication between these processes. The communication between these processes is modelled with data flows. However, we do not explicitly model the software dependencies.

Standalone security control: This element represents security controls that are implemented outside of ICS functions. Examples include VPN, IDS, and firewalls. Security controls implemented in ICS functions, such as for example application level authentication, is modelled as an attribute of the relevant ICS function.

Host device: Inspired by the definition in IEC 62443-4-2 [6]: *"general purpose device running an operating system [...] capable of hosting one or more software applications, data stores or functions from one or more suppliers"*. It typically has a human-machine interface (i.e., keyboard and mouse) and does typically not have a real time scheduler.

Network device: Inspired by the definition in IEC 62443-4-2 [6]: *"device that facilitates data flow between devices, or restricts the flow of data, but may not directly interact with a control process"*. It typically runs an embedded OS or firmware and is configured through an external interface.

Embedded device: Inspired by the definition in IEC 62443-4-2 [6]: *"special purpose device designed to directly monitor or control an industrial process"*. Examples include Programmable Logic Controllers

(PLCs), field sensors, actuator devices, and safety instrumented system controllers. It is typically configured through an external interface, and typically has a real time scheduler.

Zone: Defined in IEC 62443-3-3 [8] as *"grouping of logical or physical assets that share common security requirements"*. We use the zone to aid the threat modelling process in managing complexity and to help prioritise the threat modelling effort. More critical zones may for instance be threat modelled in a more detailed way then less critical zones.

External Entity: This elements represents and actor outside the control of the ICS asset owner, for instance a company doing system maintenance.

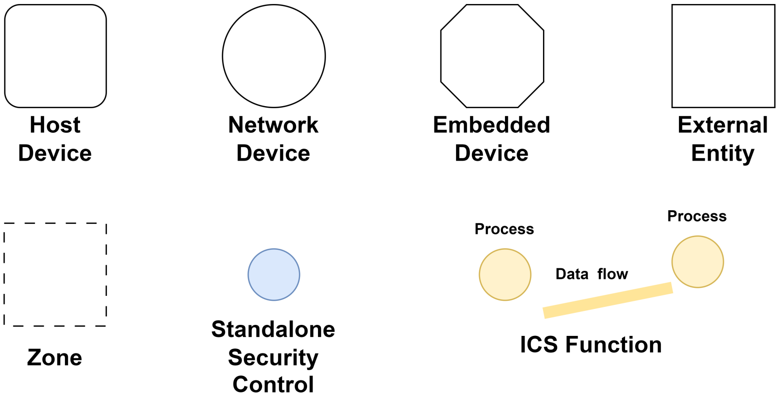

Fig. 1: The seven model elements of the proposed method.

These seven elements can be assigned a set of attributes. As examples, an ICS function may have an attribute such as "Implements authentication", or a firewall may have the attribute "Only allows inbound and outbound traffic over the protocols X and Y". However, we leave to the team performing the threat modelling to decide exactly what attributes they consider interesting and necessary.

3.2 Identify Threats

The second step of the proposed method is the identification of threats. Inspired by how HAZOP analysis uses guide words to detect potential dangerous conditions related to safety, we define a set of guide questions to aid in the identification of threats, listed in Table 1. These guide questions are grouped according to the well-known categories of integrity, availability and confidentiality.

The identification of threats is structured according to ICS functions. This means that the method considers everything needed to realise the function under consideration, instead of focusing on individual processes or data flows. During the threat identification process, threats that can be the answer to any of the guide questions should be listed.

Table 1: Threat Guide Questions.

Integrity	– How can an attacker send false data to any of the processes that are part of the ICS function, or tamper with legitimate data being sent from any of the processes that are part of the ICS function? – How can an attacker program/change logic (e.g., trip values, set points) in any of the processes that are part of the ICS function?
Availability	– How can an attacker deny the arrival of data sent between the processes that are part of the ICS function? – How can an attacker deny the service of the processes that are part of the ICS function? – How can an attacker deny the service of the devices involved in realising the ICS function?
Confidentiality	– How can an attacker obtain sensitive information from the ICS function?

3.3 Evaluate and mitigate threats

Starting from the identified threats, the team performing the threat modelling should make a prioritised list of threats. The criteria selected for prioritizing threats are left to the team performing the threat modelling. One approach is to compare the assumed consequence and likelihood of each threat against risk matrices defined by the team performing the threat modelling. Regardless of the method chosen, a justification for the priority of each threat should be provided.

Based on the list of prioritised threats, the threat modelling team should determine which of the threats can be accepted, and which require mitigation. Mitigating these threats may involve making changes to the ICS, including new standalone security controls or include/configure security controls in software implementing the different ICS functions. The details surrounding how each threat should be mitigated is left to the team performing the threat modelling.

4 Application to power grid secondary substation example

This section provides an example of how the proposed method can be applied to identify cyber security threats to a power grid secondary substation. We acknowledge that this is a simplified example with regards to the complexity of the ICS, the number of threats identified, and the evaluation of those threats.

4.1 Creating a model of the secondary substation

In Fig. 2, we illustrate how the elements can be used to create a model of a secondary substation being controlled from a control room. An ICS function monitors and controls a circuit breaker in the grid. Sensor readings are sent from the sensor to monitoring and control workstation, and control commands are sent from the workstation to the circuit breaker. Since equipment in the control room can interact with many secondary substations, this equipment is deemed to be more critical than the equipment in the secondary substation. Consequently, two different zones are established. In addition to devices, ICS functions, and zones, the example has a set of standalone security controls. The routers implement a VPN between them, in addition to running their own firewalls. The monitoring and control workstation in the control room runs an antivirus application and collects logs of events relevant for the cyber security of the workstation.

4.2 Identifying cyber threats to the secondary substation

Using the guide questions in Table 1, we identify cyber threats to the secondary substation. The identified threats are listed in Table 2, Table 3, and Table 4. The control room in this example is modelled as quite secure, based on the attributes and standalone security controls. Most of the threats are therefore identified in the secondary substation zone, which we assume does not enforce physical access control. To keep the number of threats low for the sake of simplicity, and to limit the number of false positives, we do not include threats which exploit vulnerabilities that are not included in the model. For our model, an example of such a threat would be: "An attacker may exploit a vulnerable configuration in the firewall to obtain access to the control room network", since this vulnerability is not included in the model.

4.3 Evaluating the identified threats to the secondary substation

In this section we prioritise the threats listed in Table 2, Table 3, and Table 4. As mentioned in section 3, our method does not mandate how this should be done, but leaves it to the team performing the threat

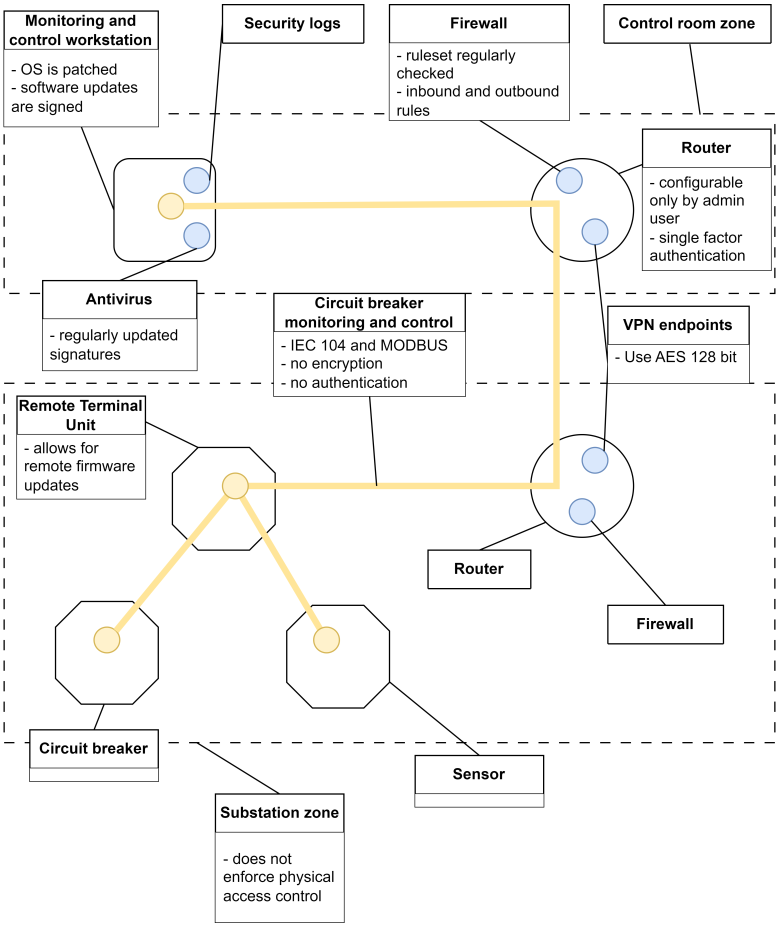
Monitoring and control workstation
- OS is patched
- software updates are signed
Security logs
Firewall
- ruleset regularly checked
- inbound and outbound rules
Control room zone
Router
- configurable only by admin user
- single factor authentication
Antivirus
- regularly updated signatures
Circuit breaker monitoring and control
- IEC 104 and MODBUS
- no encryption
- no authentication
VPN endpoints
- Use AES 128 bit
Remote Terminal Unit
- allows for remote firmware updates
Router
Firewall
Circuit breaker
Sensor
Substation zone
- does not enforce physical access control

Fig. 2: An example model of the control of a power grid secondary substation.

Table 2: Integrity related cyber threats to the secondary substation case.

How can an attacker send false data to any of the processes that are part of the ”circuit breaker monitoring and control” function, or tamper with legitimate data being sent from any of the processes that are part of the ”circuit breaker monitoring and control” function?

- I1: An attacker can get access to the secondary substation network and perform a man in the middle attack between the devices involved in the communication.
- I2: An attacker can get access to the secondary substation network, observe sequence numbers, and hijack the communication.

How can an attacker reprogram/change logic (e.g., trip values, set points) or otherwise attack the integrity of any of the processes that are part of the ”circuit breaker monitoring and control” function?

- I3: An attacker can target the supply chain to tamper with the integrity of the software.
- I4: An attacker can get access to the secondary substation and install malicious software on the devices in the secondary substation network.

Table 3: Availability related cyber threats to the secondary substation case.

How can an attacker deny the arrival of data sent between the processes that are part of the "circuit breaker monitoring and control" function?

- A1: An attacker can get access to the secondary substation network and flood the control room engineering workstation with IEC 104 packets.
- A2: An attacker can flood the control room and secondary substation routers with large amounts of traffic from an external network.
- A3: An attacker can change the policies for routing across the network between the control room and the secondary substation.

How can an attacker deny the service of the the "circuit breaker monitoring and control" function?

- A4: An attacker can target the supply chain for any of the software component which the "circuit breaker monitoring and control" function relies on.
- A5: An attacker can target the supply chain for software needed for the correct functioning of the devices on which the "circuit breaker monitoring and control" function relies.

Table 4: Confidentiality related cyber threats to the secondary substation case.

How can someone obtain sensitive information from the "circuit breaker monitoring and control" function?

- C1: An attacker can get access to the secondary substation networks, and sniff process parameters, commands and settings sent between the processes in the "circuit breaker monitoring and control" function.
- C2: An attacker can get access to the secondary substation and extract process parameters, commands and settings directly from the remote terminal unit, sensor, or circuit breaker.

modelling. In this simplified example, we prioritise the threats based on whether they have the potential to cause a blackout, whether they are scalable (meaning that they can affect several substations), and whether the attack can be executed without alerting operators. For each of these categories, we indicate whether the threat applies to it or not. Threats are then firstly prioritised according to whether they can cause a blackout, then according to whether they are scalable, and lastly according to whether the attack can be executed without alerting operators. The result is shown in Table 5. Regarding the threats to availability, we assume that a loss of availabilty can cause a blackout, but this may not be the case more generally.

For this example, we assume that the ICS owner does not accept the threats that can cause a blackout affecting a larger portion of the grid. In accordance with the method, we therefore propose some mitigations for these threats, as shown in Table 6.

5 Discussion

In this section, we discuss the three phases of the method, along with more general considerations regarding the context in which the method can be used.

5.1 Creating the model

By basing some of the model elements on IEC 62443-4-2 [6], we ensure that the team performing the threat modelling can (1): easily evaluate the level of security of these elements simply by comparing the state of the element to IEC 62443-4-2 requirements, and (2): have a set of recognised requirements to increase the level of security, if the threat modelling process deems this necessary.

We furthermore note that the model creation step of the method can benefit from existing network diagrams of the ICS as a starting point. Creating various forms of network diagrams is already required by IEC 62443-2-1 [5] (Requirement 4.2.3.5). A zone and conduit drawing, required by IEC 62443-3-2 [7] (Requirement 4.7.4.1), can likely also be used as input to the threat modelling process. The same goes for asset inventories of hardware and software in an ICS.

The method we propose includes support for explicitly expressing security controls that are independent of ICS functions. To avoid that the model becomes overly complex, different types of controls are modelled with the same symbol, but with the possibility to add further details in the form of attributes.

As stated in section 3.1, we only give examples of attributes, but do not include a specific list of attributes for each element. This is because we anticipate that different use cases may have different needs in term of the number of attributes and the level of detail of the attributes. As

Table 5: List of prioritised threats

Threat	Blackout	Scalable	Undetectable	Justification
I3	x	x	x	The threat can modify software to open breakers at a specific time, modify status updates to operators to hide itself, and does scale to many substations.
A1	x	x		The threat can cause a blackout, does affect several substations, but is easily detectable.
A2	x	x		The threat can cause a blackout, does affect several substations, but is easily detectable.
A3	x	x		The threat can cause a blackout, does affect several substations, but is easily detectable.
A4	x	x		The threat can cause a blackout, does affect several substations, but is easily detectable.
A5	x	x		The threat can cause a blackout, does affect several substations, but is easily detectable.
I1	x		x	The threat can inject breaker commands, modify status data to operators, but does not scale beyond one substation.
I4	x		x	The threat can install software to open breakers at a specific time, modify status updates to operators to hide itself, but does not scale beyond one substation.
I2	x			The threat can inject breaker commands, but does not scale beyond one substation and is assumed to be less stealthy.
C1			x	The threat cannot cause a blackout, is only executed against one substation, but may not be detectable.
C2			x	The threat cannot cause a blackout, is only executed against one substation, but may not be detectable.

Table 6: Proposed mitigation for threats that are not accepted

Threat	Proposed mitigation
I3, A4, A5	Require suppliers to implement a information security management system and have it certified
A1, A2	Install routers who can handle the necessary amount of traffic.
A3	Implement two factor authentication for configuration of routers.

an example, a model of a remote access function from a vendor into an ICS with potential for major health, safety and environmental (HSE) consequences may require a high level of detail in its element attributes. A model of an ICS providing auxiliary functions with no potential for HSE consequences may require less detailed and numerous attributes.

5.2 Identifying threats

The method groups threats according to whether they violate confidentiality, integrity or availability. These categories were chosen as they are easily relatable and commonly understood. An alternative would have been to use STRIDE. However, we argue that STRIDE may appear confusing as it mixes categories that directly violate security properties with categories which can be seen as a preparation for violating security properties. While information disclosure, tampering, and denial of service map directly to violation of confidentiality, integrity and availability, this is not the case for spoofing, repudiation and elevation of privilege. Spoofing, the impersonation of someone or something else, does not in itself violate confidentiality, integrity and availability. But successful impersonation of a ICS operator may allow for both information disclosure, tampering and denial of service. A similar argument can be made for elevation of privilege. Repudiation can be defined as the possibility for an actor to deny having performed an action. Non-repudiation may have some relevance in the protection towards insider threats, and if logs are used to ensure non-repudiation, these may be useful for forensics after an incident. However, to avoid the method becoming too resource intensive, we choose to exclude repudiation threats.

As described in section 3.2, the ICS functions are what drives the threat identification phase. By doing so, the abstraction level of the method sits between ICS/CPS adaptations of STRIDE, which identifies threats to individual processes and data flows, and Cyber HAZOP, which models zones and conduits. We argue that considering individual processes and flows may result in an overwhelming number of threats, whereas considering only zones and conduits may hide important details of the system.

The method does not explicitly include a step for determining attacker tactics, techniques, and procedures as described in [10], or for establishing an attack taxonomy as in [11]. Instead we regard domain and cyber security knowledge as a prerequisite for identifying threats. A potential source of inspiration for this phase may be the MITRE ATT&CK Matrix for ICS [1].

As we do not strictly define what attributes should be included in a model, we also do not define detailed steps for how they should be included in the threat identification phase. One approach, as illustrated in the example in section 4.2, is to only take modelled vulnerabilities into account. Another approach may be to also consider potential vulnerabilities for more critical zones. This implies that threats exploiting vulnerabilities that may be present (but uncertain and not modelled as an attribute) are also included. These threats should then come in addition to those threats exploiting vulnerabilities expressed through attributes.

5.3 Evaluating threats

We do not specify how identified threats should be evaluated, beyond stating that they should be prioritised and that mitigation should be proposed for those who are not accepted by the ICS owner. We choose this approach to keep the method light weight and flexible. Different industries and environments may have different aspects which should be emphasised. Industries facing the risk of major accidents with loss of life may choose to have this as a specific focus when evaluating threats. There might also be differences as to how thoroughly this step should be carried out. As an example, assessment of an ICS in operation may require a more thorough approach than the first of several iteration in the design of a new ICS.

Regardless of the approach chosen, it should be performed by a team including both cyber security and domain specialists, in order to cover both the identification of threats and the process of determining potential consequences.

5.4 Use of the method in different contexts

We argue that the method is applicable both in the design phase and the operations phase of an ICS. In the design phase, the method can be applied without any security controls to provide input to what security controls should be included, and where they should be placed. In the operations phase, the method can offer insight into what threats face the ICS in its current state.

We furthermore argue that the method can be used in combination with more extensive risk assessment methods, for instance IEC 62443-3-2 on security risk assessment for system design. The first step of the detailed risk assessment for a zone, ZCR 5.1, requires the threats which can affect the assets in a zone or conduit to be listed. Threats are then used as inputs to the steps determining consequence and likelihood.

5.5 Limitations of the method and future work

A limitation of the method is its inability to contextualise how isolated threats can be combined into a larger attack (differently from how for instance the ICS Kill Chain models attacks). Another limitation of the methods is that it is heavily reliant on the knowledge and imagination of the team performing the threat modelling.

We plan to validate the method on a another case study from the smart grid domain. Furthermore, inspired by Microsoft Threat Modelling Tool and the OWASP Threat Dragon, we believe that the method can successfully be implemented in software, an advancement that likely will reduce barrier to use of the method. Furthermore, an implementation of the method in software can include measures to assist the user in managing complexity (for instance by introducing zones which can be collapsed or expanded, based on what zones the user is studying).

6 Summary and conclusions

In this paper we have proposed a new method for threat modelling of an ICS. The method is based on creating a model of the ICS, including both physical devices and software based functions, and on identifying threats violating the confidentiality, integrity and availability properties. We argue that the method allows for threat modelling at a suitable abstraction level, balancing the need for detail with the need for an efficient process.

Acknowledgements

This work has been supported by WP2 of CINELDI – Centre for intelligent electricity distribution, an 8-year Research Centre under the FME-scheme (Centre for Environment-friendly Energy Research, 257626/E20). The authors gratefully acknowledge the financial support from the Research Council of Norway and the CINELDI WP2 partners.

References

1. Alexander, O., Belisle, M., Steele, J.: Mitre att&ck® for industrial control systems: Design and philosophy. The MITRE Corporation: Bedford, MA, USA p. 29 (2020)
2. Flå, L.H., Borgaonkar, R., Tøndel, I.A., Jaatun, M.G.: Tool-assisted threat modeling for smart grid cyber security. In: 2021 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA), pp. 1–8. IEEE (2021)
3. French, S.: Cyhazop – bringing cyber to the hazop. https://risktec.tuv.com/risktec-knowledge-bank/business-continuity-management/cyhazop-bringing-cyber-to-the-hazop/. Accessed: 2023-04-07

4. Holik, F., Flå, L.H., Jaatun, M.G., Yayilgan, S.Y., Foros, J.: Threat modeling of a smart grid secondary substation. Electronics **11**(6), 850 (2022)

5. IEC: Industrial Communication Networks - Network and System Security - Part 2-1: Establishing an industrial automation and control system security program. Geneva. International Electrotechnical Commission (2010)

6. IEC: Security for industrial automation and control systems. Part 4-2: Technical security requirements for IACS components. Geneva. International Electrotechnical Commission (2019)

7. IEC: Security for industrial automation and control systems. Part 3-2: Security risk assessment for system design. Geneva. International Electrotechnical Commission (2020)

8. IEC: Industrial Communication Networks - Network and System Security - Part 3-3: System security requirements and security levels. Geneva. International Electrotechnical Commission (2021)

9. Jamil, A.M., Ben Othmane, L., Valani, A.: Threat modeling of cyber-physical systems in practice. In: Risks and Security of Internet and Systems: 16th International Conference, CRiSIS 2021, Virtual Event, Ames, USA, November 12–13, 2021, Revised Selected Papers, pp. 3–19. Springer (2022)

10. Jbair, M., Ahmad, B., Maple, C., Harrison, R.: Threat modelling for industrial cyber physical systems in the era of smart manufacturing. Computers in Industry **137**, 103611 (2022)

11. Khalil, S.M., Bahsi, H., Ochieng'Dola, H., Korõtko, T., McLaughlin, K., Kotkas, V.: Threat modeling of cyber-physical systems-a case study of a microgrid system. Computers & Security **124**, 102950 (2023)

12. Khan, R., McLaughlin, K., Laverty, D., Sezer, S.: Stride-based threat modeling for cyber-physical systems. In: 2017 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe), pp. 1–6 (2017). https://doi.org/10.1109/ISGTEurope.2017.8260283

13. Kim, K.H., Kim, K., Kim, H.K.: Stride-based threat modeling and dread evaluation for the distributed control system in the oil refinery. ETRI Journal (2022)

14. Kohnfelder, L., Garg, P.: The threats to our products. `https://shostack.org/files/microsoft/The-Threats-To-Our-Products.docx`. Accessed: 2023-06-03

15. Sion, L., Yskout, K., Van Landuyt, D., van Den Berghe, A., Joosen, W.: Security threat modeling: are data flow diagrams enough? In: Proceedings of the IEEE/ACM 42nd International Conference on Software Engineering Workshops, pp. 254–257 (2020)

16. Swiderski, F., Snyder, W.: Threat Modeling. Microsoft Press, Redmond, WA (2004)

17. Young, W., Leveson, N.: Systems thinking for safety and security. In: Proceedings of the 29th Annual Computer Security Applications Conference, pp. 1–8 (2013)