Threat modelling of cyber-physical threats

Methodology for assessing threats associated with cyber-physical boundaries in systems

Niko Iskanius

Master's thesis
April 2024
Master's Degree Programme in Information Technology
Cyber Security

Jyväskylän ammattikorkeakoulu
University of Applied Sciences

Iskanius, Niko

Threat modelling of cyber-physical threats - Methodology for assessing threats associated with cyber-physical boundaries in systems

Jyväskylä: Jamk University of Applied Sciences, April 2024, 100 pages

Degree Programme in Information Technology, Cyber Security. Master's thesis.

Permission for open access publication: Yes

Language of publication: English

Abstract

Threat modelling of cyber-physical systems (CPS) is an extensively researched subject. While many traditional and modern frameworks have been successfully utilized for the task, the heterogeneity of industries and use-cases benefiting from cyber-physical capabilities of such systems is high. Easily adoptable, generic methodology cannot be identified from the current literature. Wide variety of frameworks are available, each with their own advantages and challenges.

The research set out to establish whether it is possible to formulate a general threat modelling approach and threat taxonomy capable to efficiently identify cyber-physical threat and support their analysis.

Constructive research method was utilized to analyze the current state of CPS system modelling and threat elicitation methods, comparing their efficiency with descriptive literature review. Set of requirements for the solution construct was formed based on the analysis. These requirements guided the development of a threat methodology combining system modelling, threat elicitation, threat analysis and validation steps, consolidated into a threat modelling process.

The thesis proposes an approach to identify cyber-physical boundaries (CPB) during system modelling phase. These boundaries are exploited as part of Attack Tree Analysis to elicit and analyze threats with effects traversing the CPB. Identified threats are compared to system's documented security context to improve accuracy of the analysis.

The research achieved a formalized process of eliciting cyber-physical threats in CPS. The approach enables flexible selection of frameworks for threat elicitation and analysis. The approach partially compensates limitations of Attack Tree Analysis by basing the analysis on CPB and exploiting attacker goal generation in the approach of Fault Tree Analysis. A generic attack taxonomy for CPS was not achieved during the research. Feasibility of such taxonomy, as well as testing feasibility of proposed methodology in practice was left for the future research efforts.

Keywords/tags (subjects)

attack tree analysis, cyber threat, cyber-physical threat, cyber-physical system, cyber security, industrial automation, threat modeling

Miscellaneous (Confidential information)

-

Kuvailulehti

Iskanius, Niko

Kyber-fyysisten uhkien mallinnus – metodologia järjestelmän kyber-fyysisiin rajapintoihin kohdistuvien uhkien arvioimiseksi

Jyväskylä: Jyväskylän ammattikorkeakoulu, Huhtikuu 2024, 100 sivua.

Tieto- ja viestintätekniikan tutkinto-ohjelma, kyberturvallisuus. Opinnäytetyö YAMK.

Julkaisulupa avoimessa verkossa: kyllä

Julkaisun kieli: englanti

Tiivistelmä

Kyber-fyysisten järjestelmien (CPS) uhkamallinnus on laajasti tutkittu aihe. Vaikka useita perinteisiä ja moderneja viitekehyksiä on käytetty tehtävässä menestyksekkäästi, kyber-fyysisiä järjestelmiä hyödyntävien teollisuudenalojen sekä käyttötapausten monimuotoisuus on suuri. Helposti käyttöönotettavaa, yleistä lähestymistapaa ei voida tunnistaa saatavilla olevasta tutkimuskirjallisuudesta. Laaja valikoima menetelmiä ja viitekehyksiä on saatavilla, kullakin omat vahvuutensa ja haasteensa.

Tutkimuksessa selvitettiin, onko mahdollista laatia yleiset uhkamallinnus- ja luokittelumenetelmät, jotka kykenevät tehokkaasti tunnistamaan kyber-fyysisiä uhkia ja tukemaan niiden analyysia.

Konstruktiivista tutkimusmenetelmää käyttäen tutkimus analysoi CPS-järjestelmien mallinnuksen ja uhkien tunnistamiseen käytettyjen menetelmien nykytilan, ja vertaili niitä kuvailevalla kirjallisuuskatsauksella. Analyysin pohjalta luotiin vaatimuslista ratkaisulle, jota käytettiin yleisen uhkamallinnusmenetelmän kehittämiseen. Menetelmä sisältää järjestelmän mallinnus-, uhkien tunnistamis- ja -analyysi-, sekä validointivaiheet, yhdistettynä uhkamallinnusprosessiksi.

Opinnäytetyössä ehdotetaan lähestymistapaa kyber-fyysisten rajapintojen (CPB) tunnistamiseksi järjestelmän mallinnusvaiheessa. Näitä rajapintoja hyväksikäytetään osana hyökkäyspuuanalyysiä (Attack Tree Analysis) sellaisten uhkien tunnistamiseksi ja analysoimiseksi, joiden vaikutukset ulottuvat CPB-rajapinnan yli. Uhkia verrataan järjestelmän turvallisuuskontekstiin analyysin tarkkuuden parantamiseksi.

Tutkimus onnistui formalisoimaan kyber-fyysisten uhkien mallintamisprosessin CPS-järjestelmiä varten. Lähestymistapa mahdollistaa joustavan viitekehyksien valinnan uhkien tunnistamiseksi ja analysoimiseksi. Hyökkäyspuumentelmän rajoituksia kompensoidaan osittain kohdistaen analyysi kyber-fyysiseen rajapintaan ja hyödyntäen hyökkääjän tavoitteiden määrittelyssä vikapuuanalyysin (Fault Tree Analysis) lähestymistapaa. Yleispätevää kyber-fyysisten uhkien luokittelumallia ei saavutettu tutkimustuloksena. Luokitteluviitekehyksen toteuttaminen, sekä opinnäytetyön ehdottaman lähestymistavan validointi käytännössä jätettiin tulevan tutkimustyön tehtäväksi.

Avainsanat (asiasanat)

hyökkäspuuanalyysi, kyberturvallisuus, kyber-fyysinen järjestelmä, kyber-fyysinen uhka, kyberuhka, teollisuusautomaatio, uhkamallinnus

Muut tiedot (salassa pidettävät liitteet)

-

Contents

Figures

Tables

1 Introduction

Conflicts and war are commonly associated with physical violence and the threat of destruction. In the wake of Russo-Ukrainian War, the reports of cyber warfare operations started pouring in in the beginning of the escalation in spring 2022. Prominent cyberattacks targeted e.g., energy sector (Finle, 2016), satellite terminals and telecommunication providers supporting more traditional military operations (Juutilainen, 2022, p. 19), to amplify effect of traditional warfare. Russo-Ukrainian War has extensively demonstrated the complex bi-directional relationship between cyber warfare and physical world; cyberattacks can result in physical damage, and events outside of the cyber domain can affect the information system’s security (Juutilainen, 2022, p. 62-64).

Cyber warfare and interstate conflicts are not the only avenue for cyber threats realizing into a physical world; Cyber-attacks causing direct or indirect have been reported for example against energy sector, (Shehod, 2016), nuclear enrichment facilities (Langner, 2013), nuclear power plants (Nirmal, 2020), and manufacturing facilities (Federal Office of Information Security, 2014). Security problems with potential to jeopardize safety of cyber-physical systems and their users or indirect stakeholders have been reported in, for example, car mounted systems (Foster, Prudhomme, Koscher, & Savage, 2015) and airplanes (Hollinger, 2018; Kumar & Xu, 2017). In 2023, research was published raising a concern that land-based satellite communication system’s software could be utilized to cause physical damage to human tissues (Argudo, & Mwana, 2023).

Threats have been identified and analyzed with structured methods for a long time. Threat modeling is an extensively used technique among system designers, architects, and developers to identify threats in a system design and address them in a structured manner. There are several methodologies, methods, and tools developed for the activity, with a goal to prevent critical software and engineering oversights (Shostack, 2014; Hussain, Kamal, Ahmad, Rasool & Iqbal, 2014; Shevchenko, Frye, & Woody, 2018a).

Field of cyber-physical systems is ever developing. Traditional threat modelling tools have proven successful in case-studies and practice, but generic approach to identify threats propagating between physical world and cyber domain has not been generally adopted. This is an interesting avenue for research.

1.1 Research motivation

Increasingly complex combinations of interconnecting systems are being constantly developed to serve new demands of evolving societies. Intelligence in form of computational power is progressively introduced into smart household utilities, medical instruments, smart clothing, and smart accessories, providing mobility among other benefits for their users.

On a larger scale, requirement of mobility can be imposed on an information system by the platform it is installed on, such as an autonomous ship, space rocket, satellite, unmanned aerial vehicle (UAV), unmanned surface vehicle (USV), or an autonomous automotive vehicle. It can also be a design requirement, such as in case of a surveillance truck, or a communication and information exchange system operated by an organisational headquarter of crisis management organisation or military unit. For cyber-physical systems which contribute to controlling or monitoring a physical process, such mobility can also be a requirement when discussing e.g. systems used for operating a vehicle. Fast-paced development and increasing applications of technologies, such as autonomous or semi-autonomous vehicles such as drones, cars, and maritime vessels, are making us increasingly dependent on such systems (Humayed, Lin, Li & Luo, 2017, p. 1803).

Cyber-physical system threats are extensively researched, for example by Shevchenko et al. (2018a). In addition, many traditional cyber security standards (Shevchenko et al., 2018a), frameworks and regulatory requirements do include a comprehensive approach to security including the aspects of physical domain threats and cyber-physical security (). Despite the fact, various industries are struggling in implementing effective methods and methodologies to address the cybersecurity challenges (Kumar & Xu, 2017; Greiman, 2023, p. 16; Jamil, ben Othmane & Valani, 2021), including model threats of information and cyber-physical systems. Some studies have concluded that industries where security design related processes are present, such as risk assessment during product life-cycle related processes, the application of the processes in practice is immature (Kumar & Xu, 2017). Other research has summarized that the methodologies utilized by target industries to identify cyber-physical threats and risks require further development to be effective (Ryon & Rice, 2018). Others have raised concerns that the used methodologies do not adequately consider the physical dimension of information and cyber-physical systems introduced by the developing technology (Aufner, 2019, p. 12; Shevchenko et al., 2018a, p. 6).

Threat modeling is a collection of techniques used to identify relevant threats and analyze their potential impact threats and vectors to determine the exposure of a target system. Various methodologies and tools are abundant, and studies have been conducted about the effectiveness of various approaches (Hussain et al., 2014, Shevchenko et al., 2018a) when assessing threats cyber-physical systems. Despite of the fact that successful combination exists, there is friction and low adaptability when implementing traditional methods to assess cyber-physical system (Shevchenko et al., 2018a, p. 7-10), and there is no structured approach to assess the threat of cyber-physical systems specifically (Jamil et al., 2021). Even when threat modeling methodologies as utilized, there are gaps which cause physical dimension threats not adequately addressed (Aufner, 2019, p. 11).

Jamil et al. (2021) in their recent interview of security experts concluded, that “the community should develop a knowledge repository of practical threats to CPSs”. This research analyzes threat modeling that has been previously performed in the context cyber-physical systems and aims to introduce a generic threat model for cyber-physical systems in respect of the threats with a dimension in physical domain with a goal of improving the effectiveness to identify and address threats specific to moving information systems. The thesis has been commissioned by Nixu Corporation Ltd., a Finland -based company focusing on holistic consultation in the field of cybersecurity.

1.2 Research objectives

The aim of this thesis is to improve the efficiency of identifying cyber-physical security threats in cyber-physical systems. This is achieved by proposing a threat modelling process combining methods and frameworks to 1) identify cyber-physical boundaries within a target system and 2) elicit cyber-threats that can cross the boundary (i.e., the cyber threat causing physical impact or a physical threat causing impact in an information system). The goal of the research is also to determine whether such generic approach applicable for wide variety of cyber-physical system is feasible.

The thesis bases its approach on more effective and comprehensive utilization of currently available threat modeling methodologies and methods, potentially contributing to decreasing the threshold of adopting such methodologies in various industries. Thesis may incorporate improvements to the approaches, embedded to the proposed threat modelling process.

As a result, produced generic threat modelling approach for cyber-physical systems can be used to generate scenario and system-specific threat models for target systems with varying degree of specialization. The proposed methodology can be developed further to cover more use-cases, for example to cover industry specific attack taxonomies, threat analysis methods or threat elicitation methods.

Primary target groups of this research are system and security architects, risk and threat management professionals, system designers and system developers. The goal is to provide a starting point for threat modeling systems with strong links to the physical world processes and events, such as cyber-physical systems in the energy industry and vehicles or information systems operated in physically harsh or hostile environments.

1.3 Scope and restrictions

The scope of threat modeling performed as part of this research is cyber threats with a dimension of physical domain, i.e., cyber-physical threats. Threats in scope are technical, i.e., each included threat shall have a capability to cause effect on or propagate effect through a digital system or cyber-physical system.

While the proposed methodology could be capable to elicit and analyze non-cyber-physical security threats, thesis does not cover these use-cases.

When utilizing and combining existing methods and frameworks for various parts of the threat modelling process, this thesis research does not aim to provide thorough guidance for utilization of each methodology. Rather the proposed methodology seeks to describe the general approach of using these frameworks as part of the proposed approach. Per contra, utilization of processes and templates unique to this thesis are described in detail.

The research focuses on the overall process, highlighting the capability to identify cyber-physical threats consistently and efficiently. Other aspects of the threat modelling process, e.g., threat prioritization, threat mitigation measures or validation of implementing such measures are only included to provide appropriate context. When applicable, such lack of detail or freedom of approach is highlighted in the methodology documentation.

1.4 Research problem

Following research questions have been formulated to achieve the research objectives outlined in chapter 1.2.

Primary research question **(RQ1)**: *“How can a generic threat modelling approach be produced to enable modeling of cyber-physical threats?”*

Secondary research question **(RQ2)**: “*Based on generic threat modelling approach, can a reference library of threat patterns or threat types be generated to support threat identification process for cyber-physical systems?*”

To be able to answer the primary research question, it must be understood what kind of boundary and interfaces are present between physical and cyber domain, what kind of threats are able to cross that boundary, and what capabilities and restrictions apply to the current tools and methodologies when identifying and addressing these types of threats.

In addition, to respond to the second research question, review of currently available threat pattern libraries and tools for threat identification should be conducted.

2 Research design

Thesis research is conducted applying constructive research methods, supported by literature review and construction of structured models which feasibility can be demonstrated in a pilot case-study. The construction of this thesis is a proposed threat modelling process, i.e., methodology, to identify cyber-physical threats.

Constructive research method combines utilization of deductive and inductive logic, transforming the research question based on theoretical framework into a generally applicable solution (Lehtiranta, Junnonen, Kärnä & Pekuri, 2015, p. 98). The process steps, as described by Kasanen, Lukka and Siitoinen (1993) and referred to by Kasanen et al. consists of the following steps as demonstrated in Figure 1.

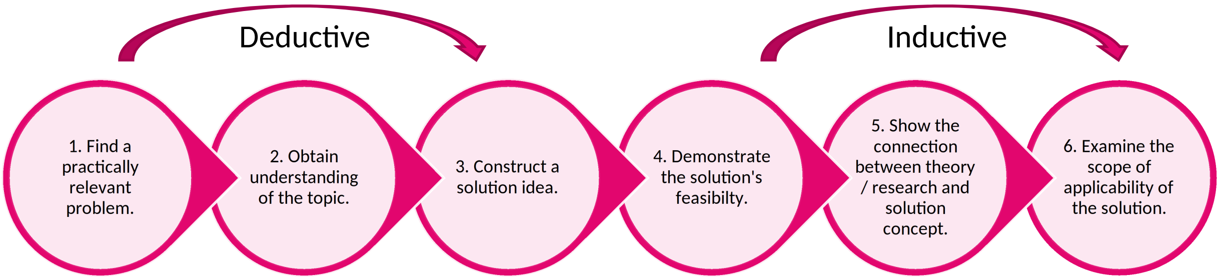

Deductive
Inductive
1. Find a practically relevant problem.
2. Obtain understanding of the topic.
3. Construct a solution idea.
4. Demonstrate the solution's feasibilty.
5. Show the connection between theory / research and solution concept.
6. Examine the scope of applicability of the solution.

Figure 1: Constructive research method (Kasanen et al., 1993; Lehtiranta et al., 2015, p. 98).

Justification of the research method selection is, that the method supports research goal of producing a concrete solution (i.e., a feasible construct) to solve a practical research question basing on pre-existing theoretical frameworks. In addition, the method is suitable for generating an outcome with generalized applications which can be utilized in and developed for wide variety of use cases.

The scope of this thesis does not include the demonstration of the solution’s feasibility. The construct is produced in a manner allowing utilization of the methodology, i.e., as part of a case-study. The process described in Figure 1 can be extrapolated into the research tasks presented in Figure 2.

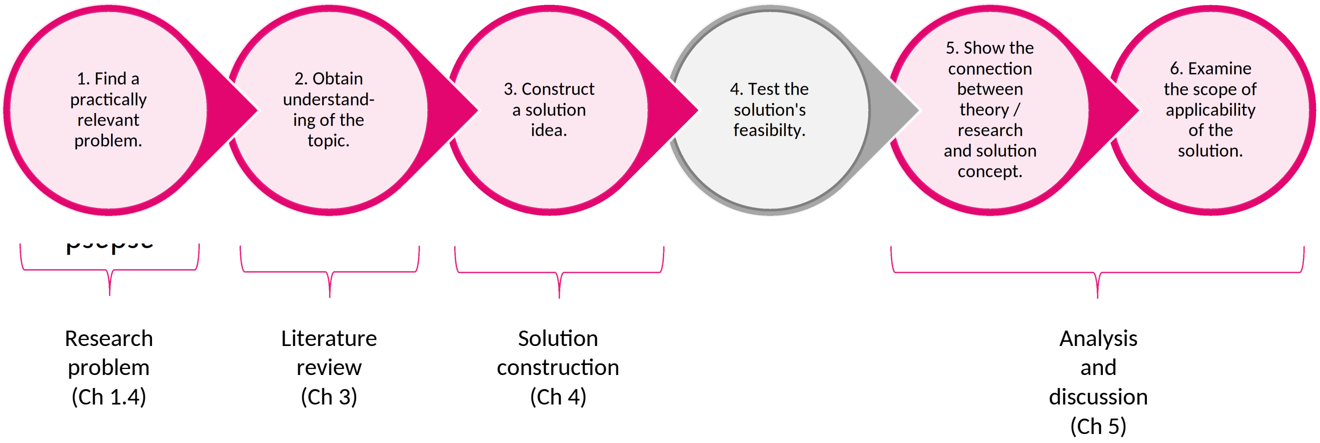

1. Find a practically relevant problem.
2. Obtain understand-ing of the topic.
3. Construct a solution idea.
4. Test the solution's feasibilty.
5. Show the connection between theory / research and solution concept.
6. Examine the scope of applicability of the solution.
Research problem (Ch 1.4)
Literature review (Ch 3)
Solution construction (Ch 4)
Analysis and discussion (Ch 5)

Figure 2: Research task outline considering constructive research method, relevant chapters embedded.

Statistical methods are not the primary focus of this research. Chosen methods are qualitative in nature and established in constructive research methodology.

2.1 Literature review

The research requires source material on various available threat modeling related methodologies, frameworks, models, and approaches to form its knowledge base. In addition, surveys and comparisons of the tools are required to establish current capabilities of the most common approaches used in the security industry.

Literary review focuses on examining previously used threat modelling frameworks for cyber-physical systems, threats with physical dimension currently considered in most common threat modelling frameworks, and supplementary sources for such threats from industry-specific frameworks and sources. In addition, understanding what physical attributes and parameters of a target system can factor into existence or feasibility of a threat provides necessary context for the threat analysis.

The results of literature review are presented in chapter 3.

2.1.1 Data gathering methodology

For data analysis constructive research methodology, especially for case-studies, suggests diverse types of triangulations. An especially significant method for this research is methodological triangulation, which can be used to compare methods and approaches. In addition, data triangulation can be used to compare data, such as threat lists or categorizations to form a common frame to support research tasks. (Yin, 2009, p. 130).

Analysis of previous research and studies are common in constructive research methodology (Yin, 2009, p. 56) and used in this research extensively when analyzing the results of the e.g., case-study. Approach and methodology selection also heavily relies on literature when such resources are available. Collected source material shall be categorized (Yin, 2009, p. 122) to establish the scope of their applicability, i.e., sources relating to threat modeling threats in the context of aerospace engineering may have different relevance for analyzed data point, than the same type of sources of different industry. Concept mapping may be used to support this activity, as described by Yin (2009, p. 122).

Descriptive literature survey is conducted as part of the research process to build a knowledge base of the relevant key concepts relevant for this research, i.e., to obtain the understanding on the topic as part of the constructive research method. Literature sources are used to document the chain of reasoning and basing the suggested constructs on theoretical and practical framework.

2.1.2 Data sources and keywords

Main tools used to gather literature is JAMK online library service Janet (Janet, n.d.) and Google Scholar (Google, n.d.). Following table presents used keywords for literature review based on main topics part of this research.

Literature type	*Description*	*Keywords and phrases, separated by comma*
Threat modelling framework methodologies and methods.	Material to deepen knowledge on subject matter and produce the basis for assessing and comparing different threat modeling approaches	(threat OR threat model), (“cyber threat” OR threat AND “analysis”), threat modelling
Cyber-physical system architecture and security	Material on current frameworks and standards on cyber-physical system architecture and security design.	“(cps OR “cyber-physical”) AND (“threat” OR “threat model), “(cps OR “cyber-physical”) and (“security” OR “design” OR “architecture” OR “development”), (“scada” OR “dcs” OR “autonomous vehicle”) AND (“threat” OR “threat model” OR “security”)
Physical security attributes, threa and security controls	Material to establish understanding on physical domain attributes, threats and related security controls relevant for information systems (IT or CPS)	“physical” AND (“security” OR “threat” OR “cyber”), “location” AND (“security” OR “threat” OR “cyberthreat”)
Industry-specific threat modeling methodologies not commonly used in cyber industry	Material for providing context on how industry specific development and maintenance processes deal with (cyber) threats, and to identify possible existing frameworks.	(“car” OR “maritime” OR “vessel” OR “ship” OR “airplane” OR “aircraft” OR ”spacecraft) AND (“cybersecurity” OR threat” OR “threat model”) AND (“standard” OR “framework” or “regulation” OR “method”), (“cyber-physical” OR “cps”) AND (“car” OR “maritime” OR “vessel” OR “ship” OR “airplane” OR “aircraft” OR ”spacecraft”)

Table 1: Literature types and used keywords and phrases during the literature review.

It should be noted that many sources used in the literature review were not part of the search results obtained utilizing the keywords presented in the previous table. As part of literature review, further sources were collected by e.g., inspecting the reference documents of the search results, point-like searches involving the subject matter keywords not specified in the above table or following the news and topical issues during the time of the research.

For standards and frameworks published by various authorities such as National Institute of Standards and Technology (NIST), International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC), material has been obtained directly from the publishing organization.

All news articles have been collected directly from the publishing news agency, blog or other publication channels.

2.2 Solution construct

Based on the literature review and preliminary research on relevant topics, solution idea to address defined research problems is constructed. The proposed solution utilizes threat modelling methods and frameworks selected based on data gathered during preliminary research. Solution is a threat modelling approach for identifying and analysis of cyber-physical threats.

2.2.1 Proposed solution

The proposed solution defines a process and tools for identifying cyber-physical threats within a cyber-physical system. The methodology is presented in chapter 4 and includes the following sections:

- Requirements for the methodology identified during literature review.
- Process and guidelines for modelling the target system in preparation of the threat modelling.
- Process for threat elicitation.
- Process for threat analysis.
- Description of the self-validation of the process.

Findings emerging during the solution construction are described in chapter 5, including the assessment of reliability of the results.

Conclusions, and future research and development recommendations are provided in chapter 6 as part of the conclusions.

2.2.2 Considerations on practical implementation

Assessing the solution should be conducted to verify and elaborate the analysis provided in this thesis. Constructive research method acknowledges that for complex problems and constructs built as a solution, “it is always difficult, if not impossible, to assess the practical adequacy of any new construction prior to its implementation” (Kasanen, et al., 1993).

Demonstration of the solution construct’s feasibility can be executed in a form of a case study not included in this thesis research. According to Oyegoke (2011, p. 585) pilot case study is a preferred method for testing a construct as part of constructive research method. According to Yin (2009, p. 18), “A case study is an empirical inquiry that investigates a contemporary phenomenon in depth and within its real-life context, especially when the boundaries between phenomenon and context are not clearly evident”. This definition accurately describes the premise set of the defined research questions. Yin also describes that case-study is suitable for the research when inquiry involves situation where there are “more variables of interest than data points”, multiple sources of evidence with data needing to be assembled and methodologically converged, and there are prior research or studies which can be used to guide collection of data and resulting analysis (2009, p. 18). In this research, it is expected that input variables and attributes for the analysis consisting of threats and their various attributes (risk factors) are abundant, whereas datapoints such as examples of previous similar exercise directly comparable to the study target will be scarce. Furthermore, a pilot case study is a preferred method for testing a construct as part of constructive research method according to Oyegoke (2011, p. 585).

Considering the previous justification, case-study is a recommended method for implementing the solution construct in practice.

2.3 Analysis and discussion

The observations and findings of case study can be used to develop and update the solution to better address the research objectives. Analysis aims to identify advantages and constraints of the solution idea, outlining the needs for future development and guidance for the results application to other use cases. Evaluation against the theoretical background is performed to link the results to their originating ideas and concepts.

Results are analysed and tied to theoretical background in chapter 5, including the analysis of solution's efficiency compared to other methodologies reviewed during this research.

2.4 Ethicality and reliability

The research will be conducted according to the Code of Responsible Research (CRC). Material collected for the literature review will be retrieved from only publicly available sources and cited in accordance with the APA7 reference system. The research shall not utilize illegally obtained source material, nor shall it contain classified information without the approval of the information owner (individual or organization). Hence, the research does not require signing non-disclosure agreements. Source material and references will be presented in a respectful manner. Where necessary, notes and comments originating from the thesis' author will be clearly separated from the source material.

Thesis may contain comments or contributions from individuals or non-literary sources. In such cases, permissions for quotation and paraphrasing will be collected from the persons in question prior to utilization of the material acquired in this manner. Thesis does not conduct structured non-literary data collection, such as interviews. Thesis shall not include any data considered sensitive in accordance with applicable privacy legislation and regulation.

The research shall follow a formal research process as described in the chapter 2 Research design to improve the research's reliability. As the thesis does not incorporate testing the feasibility of the proposed methodology, appropriate analysis must be conducted to outline challenges, restrictions and applicability of the methodology identified during the solution construct.

Thesis work is subjected to the commissioner’s feedback. All feedback shall be considered and when appropriate, corrections to approach and documentation of the methodology shall be implemented in cooperation with the commissioner.

3 Theoretical background

This research examines threats emerging from or affected by the physical domain targeting digital computer systems utilizing a structured approach, threat modeling.

Key areas of interest for the thesis research are threat modelling, i.e., a process of identifying, analyzing, and addressing cyber threats in information and cyber-physical systems, and examining the relationship of physical domain and cyber threats.

In the area of threat modelling, it is essential to identify commonly utilized frameworks and approaches used both in cyber security industry, and industrial sectors utilizing cyber-physical systems and components. Examples of such industries include energy, aerospace, maritime, land-based vehicular industries, and military industry.

Concerning cyber-physical, key issues to examine are the similarities and differences in identification and analysis in comparison with more traditional cyber-threats. It is necessary to understand what kind of threats or threat vectors reach physical dimension to identify patterns and trends that can be extrapolated into a generic threat model and as a result, produce concrete mitigation strategies for the target system.

Knowledge base is built on reviewing existing research on these fields to establish an understanding of the key topics described. Gathered data and related analysis is included in this chapter, under the following topics:

1. Threat Modelling (Chapter 3.1)
2. Cyber-Physical Systems (Chapter 3.2)
3. Cyber-Physical Threats (Chapter 3.3)

As part of this thesis research, it is essential to build understanding on how physical domain and cyber domain interact. This interaction is examined in the context of threat modeling, to enable the research to comprehensively to the defined research questions.

3.1 Threat modelling

Threat modeling is a structured approach to identify, analyze, and prioritize threats to an information system or organization.

National Institute of Standards and Technology ([NIST], 2020) defines threat modeling as a “A form of risk assessment that models aspects of the attack and defense sides of a logical entity, such as a piece of data, an application, a host, a system, or an environment” (p. 422). It is a process of analyzing a target entity to identify threats, designing, and implementing mitigative measures, validating that they are effective (Shostack, 2014, p. xxviii).

In cyber security industry framework, methodology and method are examples of terms often used interchangeably. This applies to threat modeling, where the same structured approach may be sometimes referred to as methodology, method, framework, or model. As a result, nonexpert readers may find it difficult to discover the appropriate resources to support their intended activities.

Threat modeling is not specific for cybersecurity, software architecture or software design only; It is a mindset which can be applied to anything, exemplified by Shostack (2014). This notion, at least in principle, implies that there are no restrictions to the threat types or scope of threat modeling process, unless such restrictions are applied by applied framework or its user.

To establish a common terminology across the research, thesis must adopt uniform terminology for interpretating the meaning of method, methodology and framework across the research paper.

3.1.1 Cyber threats

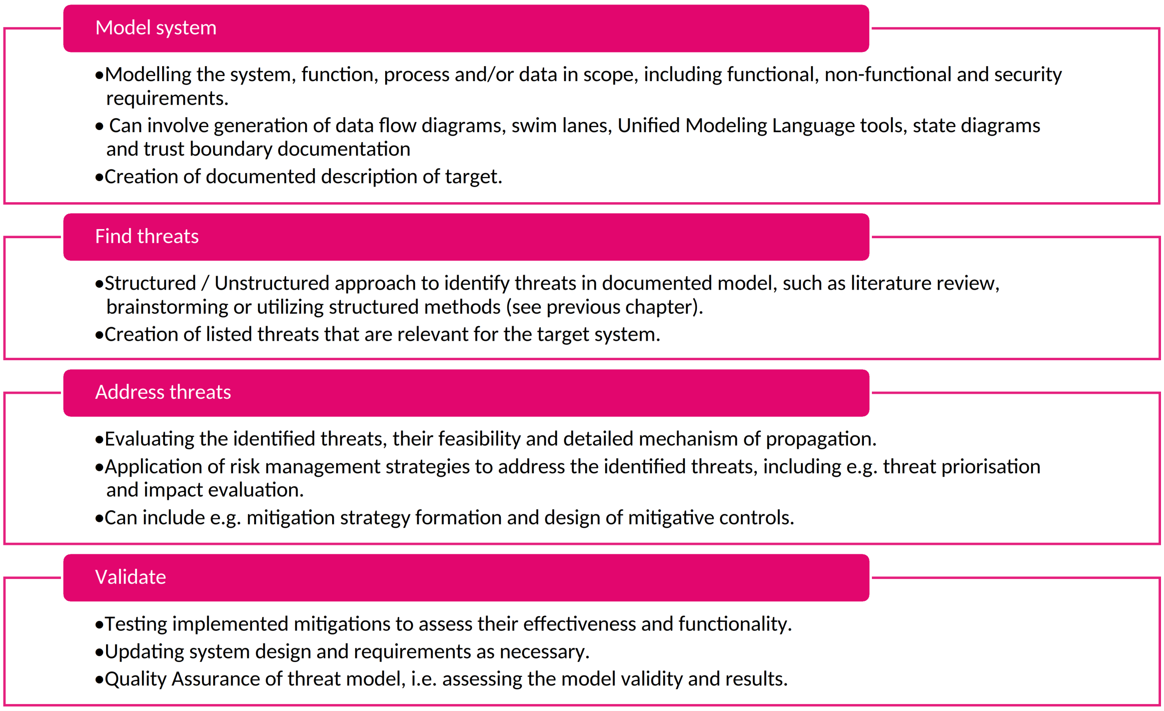
Threat is a “potential cause of incident, which may result in harm to a system or organization” (International Organization for Standardization [ISO], 2018). National Institute of Standards and Technology describes a threat in more detail, defining it as “any circumstance or event, which is capable of adversely impact organizational operations, organizational assets, individuals, stakeholders or the Nation through unauthorized access, destruction, disclosure, modification of information and/or denial of service” (NIST, 2020, p. 422).

The most common definitions include a single central theme, potential of harmful event caused by a combination of actor, error, and circumstances (ISO, 2018; NIST, 2020.). Threats can realize in various means; A subject causing the threat to realize may have malicious intent acting willingly and resulting in adversary action taking place in the system, against the data within the system, system owner or an indirect stakeholder. Unintentional human errors, errors in software or hardware, or events caused by occurrences and circumstances external to the system can lead to harmful results.

Systems are not static entities as their data, software, hardware, interconnectivity can vary over time. Correspondingly, the threats applicable for a given information system change with the system enabling, altering, and disabling threat vectors. Aside from the system’s own properties, changes can also occur in circumstances around or surrounding environment of the system, like changes to physical access control of the room the information system is in, the system’s own physical location.

3.1.2 Threat modelling process

Shostack (2014) describes a general threat modeling process a four-step exercise involving modeling the target entity or system, identifying the threats in the produced model, addressing the identified threats, and evaluating the effectiveness of the implemented measures.



Model system

- Modelling the system, function, process and/or data in scope, including functional, non-functional and security requirements.
- Can involve generation of data flow diagrams, swim lanes, Unified Modeling Language tools, state diagrams and trust boundary documentation
- Creation of documented description of target.

Find threats

- Structured / Unstructured approach to identify threats in documented model, such as literature review, brainstorming or utilizing structured methods (see previous chapter).
- Creation of listed threats that are relevant for the target system.

Address threats

- Evaluating the identified threats, their feasibility and detailed mechanism of propagation.
- Application of risk management strategies to address the identified threats, including e.g. threat priorisation and impact evaluation.
- Can include e.g. mitigation strategy formation and design of mitigative controls.

Validate

- Testing implemented mitigations to assess their effectiveness and functionality.
- Updating system design and requirements as necessary.
- Quality Assurance of threat model, i.e. assessing the model validity and results.

Figure 3: Process of threat modeling (Shostack, Chapter Introduction, 2014, p. 28-30, 44-52, 59-60 & 123-124)

The process steps described in Figure 3 are delineated from the four fundamental questions used to divide the goal of threat modelling into sub-activities which can be approached in a structured manner. While the tone of the questions described by Shostack describes a software design centric approach, the questions can simply be extrapolated for a more generic use-cases as described in Table 2.

Process step	*Shostack (2014, p. xxviii)*	*Generic use-case*	*Key deliverable*
Model system	What are you building?	What is the target system?	Description describing the system, e.g., Data Flow Diagram.
Find threats	What can go wrong with it once it is built?	What can go wrong?	List of security compromising threats.
Address threats	What should you do about those things that can go wrong?	How can identified threats be mitigated?	Analysis of the listed threats containing threat validity and proposed actions.
Validate	Did you do a decent job of analysis?	Can the results be trusted?	Amendments to previous deliverables, if applicable.

Table 2: Fundamental questions outlining the threat modelling process.

Shostack (2014) describes different approached to threat modelling considering different perspectives. Modelling can be conducted focusing on asset, attacker, or software. He further explains that different approaches examining the same target can lead to different results; Focusing assets do not directly yield information on how the asset may be compromised. Focusing on attacker can be hard, if motivation cannot be defined to identify otherwise applicable threat to target system. Shostack emphasises that approach should be selected to serve the goals set for the threat modelling; For example, software-oriented approach often results in best outcome when the goal is to improve software design. (p. 36-54, 56-57).

Generic process derived from the Shostack's approach presented in Figure 3 does not take into consideration what are the concrete methods and frameworks used within the process to identify, analyse, and produce the results of threat modelling. The process provides a skeleton approach including the tasks which can be used to define and manage activities to facilitate threat modelling and obtain the desired results effectively.

Efficiency and successful execution of threat modeling strongly relies on the documentation and understanding of the target system. Data Flow Diagrams (DFD), in addition to other documented logical descriptions of the system, are the primary target of examination for many methodologies, for instance STRIDE (Scandariato et al., 2015, p. 5; Khan et al., 2017, p. 2) and LINDDUN (LINDDUN, n.d.). Documentation is also required for the outcome of the process, such as identified, analyzed, and prioritized threats, risk analysis, in addition to assumptions and rationale contributing to the outcome to ensure that the process can be reproduced and re-evaluated e.g., when changes are introduced to the system (Yskout et al. 2020, p. 10).

3.1.3 Traditional Models and Methods

Examples of commonly recognized threat modeling methods and methodologies are STRIDE, Abuser Stories, T-MAP, LINDUNN, Fuzzy Logic, CORAS, Quantitative Threat Modeling (Hussain et al., 2014). Some of the methodologies are named after the mnemonics presenting their classification of the threats, for example software-focused STRIDE (Spoofing, Tampering, Repudiation, Information leakage, Denial of Service, Elevation of Privileges) and privacy threat-oriented LINDDUN (Linkability, Identifiability, Non-Repudiation, Detectability, Disclosure of Information, Unawareness, Non-Compliance).

STRIDE was originally developed by Microsoft as a tool to support threat identification. Its implementation is flexible and has no in-built process. An example implementation scenario is described by Scandariato, Wuyts and Joosen (2015, p.5-8), consisting of four distinct steps. Khan Mclaughlin, Laverty, and Sezer are using a five-step approach in their research (2017). These approaches are outlined in Table 3.

Process step	*STRIDE (Khan et al.)*	*STRIDE (Scandarito et al.)*	*LINDDUN (Linddun.org)*
Model System	1. Decompose system into components. 2. Plot Data Flow Diagram (DFD) for system components.	1. Model the system by means of a DFD. 2. Map the DFD elements to threat categories.	1. Define DFD.
Find Threats	3. Analyze Threats in DFD. 4. Identify vulnerabilities.	3. Elicit the threats. 4. Document the threats.	2. Map privacy threats to DFD elements. 3. Identify threat scenarios.
Address Threats	5. Plan mitigation strategies.	N/A	4. Prioritize threats. 5. Mitigate threats using PETS
Validate	N/A	N/A	N/A

Table 3: Methodology step comparison example with STRIDE and LINDDUN (Khan et al., 2017; Scandariato et al. 2015, LINDDUN, n.d.)

Validation of the threat modelling process described by Shostack is not a built-in feature for many of the commonly used approaches. Selected source material describes case-studies, where the methodology is used as one-off exercise. It should be noted that both validation of the implemented mitigative controls and the threat model itself are important steps of a comprehensive threat modelling process. Validation of the implemented corrections can be done e.g., with penetration testing, security testing and bug tracking. Validation of the threat model can be conducted during the threat modelling work or integrated into software and architecture design process to trigger the update of threat model every time a security critical change is introduced (Shostack, 2014, p. 195 - 202).

Assembling the steps of general threat modeling process into a structured approach can be achieved in diverse manners as demonstrated in Table 3. Some frameworks provide an approach including each step of the process (see Figure 3) while others are focused on introducing their indigenous or derived approach in more narrow scope of the process. STRIDE (Shostack, 2014, p. 64) and Attack tree (Ryon & Rice, 2018, p. 2-4) methodologies focus on threat identification and enumeration. As threat identification is just one step of threat modeling, further methods are required for effective threat mitigation and risk reduction. DREAD (another mnemonic for

"Damage"," Reproducibility", "Exploitability", "Affected Users" and "Discoverability") is a one example of method providing an approach to assess the probability and impact of the threat applicable to target system and can be used in conjunction with e.g., STRIDE identified threats (Shostack, 2008, p. 6-7).

Most popular methodologies have also generated variants, such as STRIDE-per-element, STRIDE-per-Interaction, DESIST, (Shostack, 2014, p. 79-85), and STRIDE Average Model (Hussain et al., 2014), facilitating modelling with different focus.

Other structured approaches to threat and risk assessment and analysis exist as well. Many safety-critical industries and system engineering performed in these industries rely on event driven assessment frameworks, in contrast with the software-centric approach of STRIDE and LINDDUN. In these approaches, the focus is to examine an event and its consequences, or its source. Some examples of methodologies with such techniques include Fault Tree Analysis, Event Tree Analysis, Cause Consequence Diagrams and Hazard-Barrier-Target model (de Ruijter & Guldenmund, 2014). Some of the threat modelling frameworks such as the examples mentioned by Shostack, Hussain et al. and Shevchenko et al., have been criticized for being prone to arduous implementation even when a successful combination of methodologies is discovered (Shevchenko et al., 2018a, p. 10).

Frameworks encompassing the entire treat modelling process include for example, Microsoft Security Development Lifecycle utilizing STRIDE by default, but supporting other frameworks as well (Microsoft, 2022). Another popular framework is PASTA, or Process for Attack Simulation and Threat Assessment. Both frameworks cater for the entire process described by Shostack (2014) illustrated in Figure 3.

PASTA framework heavily emphasizes validation of the model with attack simulations both to verify that the findings are feasible and provide input to help address the identified threats. It consists of seven stages combining into 21 activities. PASTA focuses on risk-centric, including activities like risk and impact analysis against the compliance and security requirements (Shevchenko, Chick, O'Riordan, Scanlon & Woody, 2018c).

3.1.4 Attack and Fault Trees

Wide success of Fault Tree Analysis used originally in safety analysis, identifying causal chains backwards from a single fault event utilizing binary logic, has led to development of Attack Tree Analysis by Bruce Schneier used in security related modeling of threat events and event causalities (Shostack, 2014, p. 86; Budde, Kolb & Soelinga, 2021, p. 457-458).

Attack Trees investigate the system's security by setting a goal for the attacker, extrapolating all identifiable routes to the goal through the system. Each node of the tree describes an action or activity by an attack leading towards the goal. Valuing each node can be used to assess the likelihood of the attack paths, for example identifying lowest resistant paths to the goal. IT can also help estimate the impact and cost of the attack, providing input for likelihood assessment. (Schneier, 1999; Saini, Duan, Paruchuri, 2008). Attack trees have also been criticized; For instance, Shostack (2014) notes that extensive attack trees are non-trivial to produce, and misidentifying the root nodes may lead to omission of entire attack groups (p. 99-100). He also states that attack trees as a method does not provide adequate tooling for scoping the problem (p. 100); While attack path is described, it is not easy to document what is occurring on the system level.

Budde, Kolb and Soelinga compared the fault tree commonly used for safety analysis and security-oriented attack tree approach while researching utilization of computational attack trees to calculate probable time consumer by the attacker. They deduced that both are using same static approach producing fundamentally different outcomes due to the difference in focus; Fault Tree analysis investigates probability of system failure, while Attack Tree analysis focuses on the probability of an attack. In their research, they have produced a model to combine the two approaches to reduce the effect of differences in approach, but they have also delegated the refinement of their method to future research (2021). Utilization of Attack Tree Analysis, as opposed to Fault Tree Analysis, requires deduction of attacker goals. Fault Tree, on the other hand, may require a deeper understanding of the system functionality for pinpointing the event chains occurring in the system after a failure.

Budde, Kolb and Soelinga (2021) also mention that Attack Trees and Fault Trees can be combined in various, for example for "modelling attackers that try to force a system failure" or by having attack tree structure branching from fault tree node or vice versa as made possible by Boolean-logic Driven Markov Processes (BDMP) formalism used in safety and security engineering. (p. 6)

3.1.5 Adversary Motive and Behavior Models and Methods

While not methodologies commonly used as part of the threat modelling to the process described in chapters, various structured methods developed to model a cyber-attack based on adversary motives and attack objectives should be mentioned in the context of threat identification and mitigation strategy formation.

One category of these models describes a process of cyber-attack conducted by an Advanced Persistent Threat (APT), i.e., "an adversary with sophisticated levels of expertise and significant resources" (NIST, 2011). Attack is dissected into phases or stages titled by many models as kill chains. These models are operational threat models (Shostack, 2014, p. 387), which show their approach around the adversary objectives, i.e., what actions the adversary must complete to fulfill the objective of an attack. Some examples of the kill chain models are Lockheed Martin Cyber Kill Chain (Lockheed Martin, n.d.), Hybrid Cyber Kill Chain, Unified Kill Chain and Mandiant attack life-cycle model (Lehto, 2022, p. 120-125).

Concept closely resembling kill chains called "threat genomics" has also been proposed, focusing on detectable changes in target system rather than examining threats as part of the attack process dissection (Shostack, 2014, p. 390-392), although the author argues that in practice differences of these approaches are covered by different categorization of techniques, especially if used in conjunction of frameworks such as attack libraries presented in following chapters.

Stochastic model-based methods e.g., applying discrete time Markov chain to produce probabilistic analysis on adversary behavior in a system (Oakley, Oprea & Tripakis, 2022) have also been used for threat modelling. Compared to the models based on adversary motives and objectives, these models use machine learning algorithms to compute behavioral probabilities. These methods are complex and current literature lacks the application of such techniques in practical use cases.

Attack -based models are widely used, for example PASTA encompassing the attacker perspective as part of its stages. They are popular among the security monitoring industry to analyze attack patterns, simulate adversary behavior to develop detection capabilities, and provide structural approach to forensic analysis and incident response. Although the originating objective of many of these models is to assist in post-compromise analysis and analyzing the threat actor itself (Lehto, 2022, p. 120-125), they can be used in threat modelling as well (Shostack, 2014, p. 388-390).

3.1.6 Attack Libraries, Taxonomies and Enumeration Methods

Attack libraries and other enumeration methods are used to assist in threat discovery during the threat modelling process.

An attack library is a list of commonly encountered threats, supplemented with information about e.g., threat's nature, common causes, and generic impact. They serve different target groups and provide a variable level of abstraction. In the most detailed form, these frameworks resemble checklists. On the other end, e.g., STRIDE can be classified as an attack library consisting of a collection of threat types which need to be interpreted into attacks during the threat modelling process (Shostack, 2014, p. 101-102). Shostack notes that while useful, attack libraries should not be solely relied on to avoid ignoring issues missing in the used library (2014, p. 103).

Numerous established attack libraries assist in identifying cyber threats by enumerating general or topical threats and threat actors. Examples of such frameworks are ISO/IEC 27005 (ISO, 2022b.), Common Weakness Enumeration (CWE) (Shevchenko et al, 2018c, p. 3) and MITRE knowledgebase for adversary attack and tactics (ATT&CK) (MITRE, n.d.a). MITRE has also produced an attack library for industrial control systems, expanding on threat types and categories specific to ICS and stripping the attack types not relevant for the type of systems (MITRE, n.d.b). For instance, two additional tactic categories have been introduced in ICS specific matrix, impair process control, and inhibit response function, not present in the more generically focused tactic matrix.

More specialized frameworks to threat identification have also been developed, for example Space Attack Research & Tactic Analysis (SPARTA) framework dedicated for classifying threat vectors and mitigation strategies for space-operated systems such as satellites (Aerospace Corporation, n.d.).

In comparison with MITRE's ATT&CK for ICS, several obscure techniques are described focusing on e.g., ground control stations and spacecraft communication, sensor tampering utilizing decoys, rendezvous, and proximity for initial access, and utilizing launch vehicle interface for lateral movement. Comparing the two frameworks, MITRE's framework seems to be a better match for generic purposes, SPARTA requiring more adaption although providing potential ideas for threat elicitation process for instance when assessing other vehicular systems (e.g., UAV, USV, UGV or semi-autonomous vehicles). For example, SPARTA includes many detailed techniques covered by MITRE in only superficially or not at all, such as uplink and downlink interception, proximity operations (i.e., threat actor is targeting onboard signal or network sensors and transmitters), side-channel attack and cross-link with compromised neighbor. Comparing the impact categories of both frameworks, differences in approach are the most evident SPARTA aligning its system impacts with military-oriented *destroy*, *disrupt*, *deny*, *degrade* (Laari, 2019) and *deceive*, supplemented by the outlier *theft*. MITRE on the other hand relies on more typical cybersecurity industry impact categorization containing damage, denial, loss and manipulation of various system attributes. SPARTA's impact categorization can be a tempting choice for special type of CPS used by military industry, such as weapon systems, navy vessels and aircraft. (Aerospace Corporation, n.d., MITRE, n.d.b) The author of the thesis argues, that in most civilian applications MITRE can cater to more variety of use-cases.

Frameworks to support formation of mitigation strategies, defence libraries, also exist. An example of such framework is MITRE D3DEND Matrix, at the time of research funded by Cybersecurity Directorate of the National Security Agency (MITRE, n.d.c). The framework's mitigation strategies are cross-referenced with MITRE's adversary technique and tactic knowledgebase, forming a comprehensive toolset for both threat identification and threat addressing.

Other tools providing aid for threat prioritization and impact assessment are also commonly used, such as Common Vulnerability Scoring System (CVSS) (Vallant, Stojanovic, Bozic & Hofer-Schmitz, 2021).

Benefits of the attack library and similar type of approaches include ease of adoption, as they can describe attacker behavior without the requirement of defining the attacker goals. This can be especially helpful for threat modelling participants who do not have a thorough understanding of cyber-attacks or attacker behavior in general. One of the challenges is utilizing a proper framework for the threat modelling target. As described in this section, various tools exist emphasizing distinct areas and attack types.

3.1.7 Application in Practice

Described methodologies have been in use for several decades, and case studies are prominently present in literature on the utilization of threat modelling methodologies. Selecting a proper methodology or a combination of methodologies for a given use-case can be tedious. As Shostack notes, “the right way to threat model is the way that empowers a project team to find more good threats against a system than other techniques that could be employed with the resources available” (2014, p. xxxi). Based on the Shostack’s review on various advantages and disadvantages of different approaches, Martins et al. (2015) argue that there is a strong motivation to favor software centric models, as the software is foundation of any applications (p. 115). Each framework has its merits and the existence of such a large variety of approaches to the task can make the selection of appropriate one challenging.

Other sources have been pointing out to the limitations of software-centric methodologies, either due to the lack of suitable abstraction of CPS to apply the model efficiently (see 3.2.1) or because the methodologies commonly utilized do not adequately address the physical domain of cyber-physical systems (Jamil et al., 2018). Threat modelling methodologies in the context of cyber-physical systems are examined in more detail in chapter 3.2.5.

When employed in practice, many methodologies have a risk to produce extensive output colloquially labeled as “threat explosion,” contributing to the resource intensiveness mentioned by Shostack. The term stands for a situation where resources of the threat modelling process are exhausted with overwhelming amount of resulting threats, exhausting the resources of the threat modelling process. For example, Scandariato et al. have noticed this tendency in STRIDE (2018, p. 16).

3.1.8 Current Research and Critique

In his article in December 2022, Shostack argues for methodologies with lower cost of adoptability and utilization, stating that simpler methods discussed in the article are more efficient in finding "light" flaws in system and require less a-priori knowledge of the system or expertise in the subject matter as opposed to more commonly used traditional methods. Shostack summarizes challenges on the current methodologies to be resource intensiveness, difficulties to adopt by non-security experts and systematic failure to identify certain types of threats, social threats in his example (p. 3). By introducing simpler methods for non-specialists to catch flaws discoverable with minimal system knowledge and security expertise, resources of security experts could be focused on hard-to-discover problems. (2022, p. 3-6)

Shostack is not the only one criticizing current methodology and their application in practice; Yskout, Heyman, Van Landuyt, Sion, Wuyts and Joosen reviewed 20 typical threat modelling related projects and available scientific evaluations and publications on threat modelling in practice, concluding that "threat modelling, as engineering discipline, is currently at a very low level of maturity" (p. 10). In their view, the literature on experience reports and industry-specific case studies is scarce as well as scientific evaluation of the available models. In their reviewed projects, highlighted issues included error-prone manual verification, ambiguity of risk assignment and threat prioritization, and over-reliance of expert knowledge. (2020, p. 10-11)

The issues of traditional methodologies described by Shostack in his article resemble observations made by e.g., Shevchenko et al. (2018a) and Jamil et al. (2021) about the challenges relating to threat modelling of cyber-physical systems discussed in following chapters in more detail. Furthermore, Shostack and Yskout et al. agree that current methods require a disproportionate amount of security expertise to be effectively utilized by non-experts (Shostack, 2022, p. 3; Yskout et al., 2020, p. 11). These challenges are not trivial to resolve. Shostack writes that mending these issues may call for a cultural change in the security industry (2022, p. 8).

3.2 Cyber-Physical Systems

Cyber-physical system (CPS) stands for a "a multi-dimensional complex system that integrates computing, network and physical environment, it connects sensors and actuators through wireless communication networks unifying the physical and cyber worlds" (Liu, Liyanage, & Sefanov, 2016). Systems with cyber-physical characteristics is adopted into use among various industries and field such as aerospace industry (Kumar & Xu, 2017), transportation and logistics, manufacturing, medical systems, as well as in critical infrastructure such as power grids, irrigation, and communication, civil infrastructure, defense systems and automation control and monitoring. (Gerla & Reiher, 2016; Guo, Li, K., Li, L., & Wang, 2022; Liu, Peng, Wang, Yao & Liu, Z., 2017, p. 37).

CPS are not the sole popular terminology strongly linked to information systems and physical world events. Internet of Things (IoT) is a term incorporating cross-disciplinary technologies, for example ubiquitous computing, embedded systems, and wireless sensor networks. Operational Technologies (OT) is commonly used when referring to industrial control systems (ICS), such as power plants and systems used for manufacturing processes (NIST, 2023). Both OT and IoT interface with physical worlds utilizing the same type of components and mechanisms as CPS, such as sensors to collect data from surroundings or actuators and programmable logic controller (PLC) to guide a physical process. In the case of OT, systems are often larger and more complex compered to IoT, incorporating large scale systems like distributed control networks (DCS) and supervisory control and data acquisition (SCADA) systems. Differentiating OT and IoT from CPS can be sometimes ambiguous depending on source, as terms are occasionally used interchangeably (NIST, n.d.). It can be argued that CPS may include OT and IoT devices or components, and referring to CPS in the context of many use cases including this research is sufficient to cover both.

In addition to CPS (including OT and IoT), traditional IT systems are linked to physical domain. Physical attributes such as location and presence in the physical world are examined in the following chapters. For now, it is sufficient to acknowledge that all described system types have are present in the domain of interest.

3.2.1 Architecture and Design

Some industries and sectors utilizing CPS falling under the specification of operational technologies (OT) have widely acknowledged modelling practices for various purposes. For instance, NIST guidelines document extensively on security related architectural model applicable for large, complex ICS, DCS and SCADA (2023, p. 10-32). Various tiered approaches exist for such systems, based on the type of the system in question. NIST guidelines, for instance, present three levels of architecture for industrial IoT (enterprise, platform, edge) (2023, p. 27) and four level architecture for building automation system (enterprise, supervisory, automation, field) (2023, p. 23).

Cyber-physical systems are a larger concept than OT, and various less established approaches for modelling them are available. One approach is exemplified by Humayed et al. (2017) by defining a general CPS to have three types of components: Communication, Computation and Control, and Monitoring and Manipulation. In this framework, the gateway between digital and physical world is provided by Monitoring and Manipulation components through sensors and actuators, while Computation and Control includes the logic and intelligence used to control the former. Communication components are responsible for facilitating the communique between the system and higher, or lower-level system and components. This categorization of components is non-exclusive in a sense that a single component may have multiple roles, e.g., a component can act as a communicator and an actuator at the same time. (p. 1804)

Liu et al. (2017) propose a different kind of abstraction, defining the three layers to be Physical System Layer, Information System Layer and User Layer. In their model, Information System Layer is responsible for processing and transmission of the data and User Layer provides a machine-to-human interface and safety protection mechanisms. Finally, the Physical Layer includes the components and sub-systems gathering and transmitting data and reacting to control signals to perform tasks required by a physical process. (p. 29) Notably, the model presented by Liu et al. does include human-machine interface omitted by Humayed et al.

Architectural models or abstraction methods described both by Liu et al. and Humayed et al. are not alone in their attempt to tame the complex landscape of CPS; Liu, Peng, Wang, Yao and Liu acknowledge the lack of unified approach to be a major obstacle in CPS development, attributing the issue to the fundamental differences in cultural and technical approaches between computer science theory and control theory, guiding theories of information technology and CPS development respectively (2017, p.36).

To enable communication between physical and cyber domain, CPS utilize open-source and proprietary protocols over both wire and wireless communication channels. These protocols are often application specific (Humayed, 2017, p.1804), contributing to their considerable abundance. Examples of common protocols include automation control protocols such as Modbus and Distributed Network Protocol (DNP3), Inter-Control Centre Protocol (ICCP) and IEC 61850 protocol for electric substation control (Alcaraz & Zeadally, 2013). Other cyber-physical system implementation, such as integrated medical devices, utilize low frequency electromagnetic bandwidths in inter-device communication. Regarding the heterogeneity of CPS systems, they often consist of proprietary components such as communication protocols, which can be challenging to defend within the security zone as noted by Alcaraz and Zeadally (2013).

The heterogeneity of CPS is noted as a challenge also by Humayed et al. (2017) in the context of security analysis, calling for a more suitable abstraction to facilitate efficient analysis (p. 1804). Variance in approaches to CPS architecture and approaches to their abstraction can be understood in the context of the variance of the systems under the umbrella of CPS terminology. Despite the lack of generalized approach to model such system characteristics specifically, tools and frameworks commonly used in threat modelling have been used in research and practice to identify and assess threats in CPS.

3.2.2 CPS development and security

Various surveys conducted on the security of CPS suggest that security in cyber-physical systems is often neglected in their design as the many systems have initially been designed to be isolated from external world (Humayed et al., 2017, p. 1824; Jamil et al., 2022, p. 1).

In software design and development, the physical dimension of security is not always considered for a variety of reasons. On the other hand, development of cyber-physical systems can overvalue the physical dimension at the cost of the cyber dimension. Liu et al. explain this with a cultural gap between developers of information systems and CPS (2017). One of the findings by Jamil et al. was that interviewed experts were struggling to utilize the experience they had obtained while threat modeling CPS in other use -cases outside of the domain of cyber-physical domain (2021, p. 2).

Lack of consideration regarding physical domain is not specific for CPS; Laeeq and Shamsi (2015) describe the lack of IoT security research to be a major risk to systems utilizing the type of components and security of the IoT is in “premature state”. While physical domain threats were not singled out as a type of threat, for example lack of secure architectural design, secure communication methods and protocols and unfiltered input data from perception layer components (Laeeq & Shamsi, 2015) will produce nonexistent mitigations rendering trivial cyberattacks and other types of threats more probable to realize. Since the research of Laeeq and Shamsi, several standards and frameworks addressing the security of IoT have been introduced to address the security and as a result cyberthreats, such as ETSI EN 303 645 describing baseline requirements for consumer IoT solution security (European Telecommunications Standards Institute, n.d.).

Martins et al. (2015) emphasize considering vulnerabilities of both cyber and physical components especially during design-phase noting the reduced overall costs (p. 114) compared to addressing the issues in the later stage of system lifecycle. Researchers such as Przybylski, Sugunaraj and Ranganathan (2023) also highlight the necessity of engineers to acknowledge that threats and attack surface can change depending on the current location and operational phase of the target system, such as spacecraft on a launchpad (p. 21). Another example is produced by the same research in the form of a satellite communicating with the payload carrying vehicle prior to deployment in their examples (p. 9). To adopt a more general approach on the topic, “specifics of CPS require focused attention not only on application and system software-related threats, but also on hardware and physical threats” (Shevchenko et al., 2018a, p. 6). Such methodologies have been researched, like described by Khalil et al. (2023).

Focusing on security to identify and address threats, physical or not, can be hard for nonexpert participants of the threat identification and assessment process, depending on selected approach of threat modeling (Shostack, 2014, p. 53-54), if such process is first implemented. Jamil et al. found out, that threat modeling processes involving subject matter experts, such as system operators, equipment suppliers and management, can provide valuable insights on the system itself, or its environment and related processes (Jamil et al. 2021).

Cybersecurity threats, which actualize through vulnerabilities in software, hardware, or processes, can be inherited by introducing existing technologies to new context, as described for example by Przybylski et al. (2023) regarding adoption of next-generation communication protocol in the context of aerospace engineering.

Several available research, for example those conducted by Aufner (2019), and Ryon and Rice (2018) have discovered, that practices of utilizing threat modeling or similar approach to identify and address threats are utilized in the field of CPS and IoT are immature. These observations combined with the fact that even suitable combination of methodologies is cumbersome to adopt into practice (Shevchenko et al., 2018a) underline the problem; Methodologies exist but they are impractical or hard to adopt in many cases.

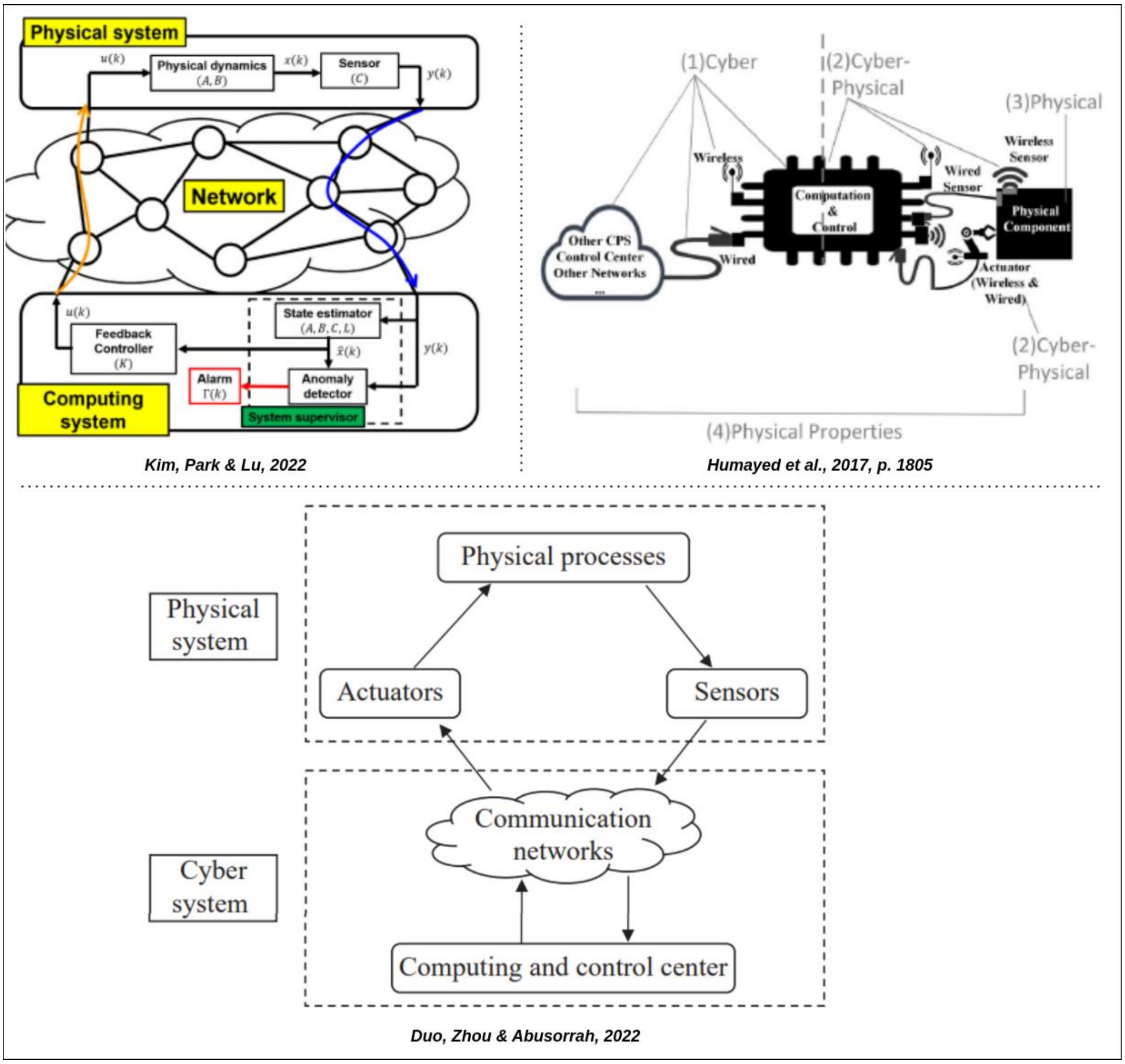
Some industry or system-type specific architectural design models do exist, EVITA project being one example of such frameworks. EVITA's proposes architectural design, threat, and risk management practices for designing safe automotive systems (EVITA, 2012).

3.2.3 Modelling of CPS

Modelling a generic CPS in a way suitable for assessing cyber-physical threats specifically is problematic as common architectural modelling concepts do not accurately describe the cyber-physical nature of the CPS, especially the interfaces between the domains. For example, DFD requirements and documentation practice does not identify cyber-physical boundaries within the system or between system and external entities. Humayed et al. (2017) have proposed an approach for dissecting a general CPS component into categories based on component's interactions for the purpose of threat modelling. Interactions of a component are described to be either cyber, cyber-physical or physical. As illustrated in Figure 4, this distinction allows to identify components that operate only in physical domain (physical), cyber domain (cyber), or act as an intermediary component between the two (cyber-physical), the latter two sharing some of the component level features. In practice this means, that component can be both cyber and cyber-physical, determining factor being the context of interaction with the external components. (p. 1804-1805)

Writer of this thesis notes, that while this approach does work on a higher level well, distinguishing the cyber, physical, and cyber-physical components may not be as unambiguous as expected. For example, what part of the components internal logic fall into which category in the cyber-physical boundary? On the other hand, this categorization can help to focus attention on certain system boundaries which convey interaction between cyber and physical domains.

Other takes exist as well under the research topic of CPS security. Duo, Zhou & Abusorrah (2022) do not identify cyber-physical components like Humayed et al. (2017) when making the distinction cyber and physical domain. Kim, Park, and Lu (2022) are providing yet another example of categorization used, when describing cyber-physical systems in the context of security. Both alternative modelling approaches are presented in Figure 4.



Kim, Park & Lu, 2022

Humayed et al., 2017, p. 1805

Duo, Zhou & Abusorrah, 2022

Figure 4: Various approaches to modelling CPS.

Assessing the security of CPS should consider system-specific requirements several requirements atypical for usual information systems. Real timeliness is often critical both for CPS's internal operation and its interaction with physical domain (Humayed et al., 2017, p. 1824, Liu et al. 2018, p. 30-31). Furthermore, connection to physical domain often emphasizes the system availability (NIST, 2023) over confidentiality and integrity when threats are analysed for impact. On various level of operations, differences affecting threat model of CPS are possible physical effects of misbehaving system, constrained resources, physically distributed system component location, different protocols for control and intra-process communication, and control logic atypical for traditional information systems. (NIST, 2023, p. 28-32)

3.2.4 Standards and Regulation

Physical aspects of security in traditional information systems are commonly part of its overall security posture also when considering an information. Requirements for implementing physical security controls exist as part of various standards and frameworks. Such recognized examples include ISO standard family which provide physical security related security controls for information systems (ISO, 2022a; 2022b.).

For cyber-physical systems, applicable standards and frameworks include for example standard family ISA 99/62443 or NIST special publications addressing security of operational technologies (OT) (International Society of Automation [ISA], n.d.; NIST, 2023). Many specialized standards considering industry specific system characteristics and requirements do also exist, for example NISTIR 8401 covering satellite ground-based infrastructure cybersecurity framework (Lightman, Suloway, & Brule, 2022).

Maritime industry has similar standards, such as United Requirement standards E26 and E27 covering maritime vessel cyber-resilience requirements for vessel and onboard systems (International Association of Classification Societies [IACS], 2022a; IACS, 2022b). These standards address the physical domain of cyber threats explicitly in several requirements, for example by requiring documentation of physical system layout (2022b, p. 6), network interface locations (2022a, p. 2), access control (2022a, p. 12) and wireless network related restrictions and hardening requirements (2022a, p. 13-14). To limit the impact of safety jeopardizing incidents, requirements such as falling back on minimal risk conditions are included in the framework (2022a, p. 20).

Gaps in various industries are present, such as Federal Aviation Administration (FAA) lacking guidelines and standards to assess cybersecurity risks and threats (Przybylski et al., 2023, p. 21)

Applicability of many requirements and regulations are limited to the country of origin or to the stakeholders of defined interest groups, and it is noteworthy that the maturity of industrial standardization, requirement frameworks and their implementation varies between countries, organizations, and industry sectors.

While many industries employ standards and other regulatory and statutory frameworks to guide the involved parties, application and maturity of the stakeholders is immature. Such statements have been issued for instance by Greiman (2023) regarding US energy sector's preparedness to secure its systems (p.106), recommending among other topics implementing security-by-design methodology into nuclear facility system design, with the support of quality assurance (p. 108). Implementing such recommendations into practice could include utilization of threat modelling methodologies as a tool, and threat assessment has gradually been introduced to the standard and guidelines over the years; For instance, International Atomic Energy Agency (IAEA) has added threat management into the computer security guidance for nuclear power plants (International Atomic Energy Agency [IAEA], 2022), greatly improving the previous version of the framework published in 2011 (IAEA, 2011).

Physical security is also extensively present in many government and regulatory cyber security related requirement frameworks, such as National Security Auditing Criteria of Finnish Government (Ministry of Foreign Affairs of Finland, n.d.). These requirements may be applicable to systems involving e.g., storing or processing information assigned a security classification according to local legislation or other regulatory frameworks. Such requirements and criteria aim to set an implementation baseline and do often require processes such as risk management and threat modelling to be applied on the target system as part of the auditing process. CPS rarely contain classified information, but this may be the case in some instances introducing another type of requirements to CPS threat modelling. This could be relevant when investigating cyber-physical threats, e.g., in the form of data exfiltration or data destruction achieved over cross-domain boundary.

3.2.5 Threat Modelling CPS

Most of the methodologies and approaches presented in the previous chapter have originally been designed for traditional information systems. However, their application to the context of

CPS has been targeted by some research, such as STRIDE (Khan, McLaughlin, Laverty & Sezer, 2017), Attack Tree (Ryon & Rice, 2018), STRIDE combined with STAMP/STPA (Kaneko, Takahashi, Okubo & Sasaki, 2018), and STRIDE combined with DREAD (Kim, K. H., Kim, K. & Kim, H.K., 2022) or CVSS (Dang, Khondoker, Wong & Kamijo, 2020) as risk rating method. Regardless of the available research, a consistent approach is yet to be adopted.

In 2021, Jamil, Othmane and Valali interviewed eleven security experts with experience on threat modeling cyber-physical systems. According to observed responses there currently is a lack of available methodology to address threat modelling challenges related to cyber-physical systems specifically (Jamil et al. 2021, p. 1), noted by Martins et al. as well (2015, p. 116).

Jamil, Othmane and Valali interviewed practitioners who utilized a varying methodology for threat and frameworks for threat identification, STRIDE being utilized by over half of the participants. PASTA, LINDDUN, DREAD and Attack Tree were also used, sometimes in combination of ISA/IEC 62443 and real-world experience for modelling zones and asset groups. Some participants opted for multiple methodologies in a single project for a more comprehensive list of threats. For risk assessment, used framework and tools varied from standard FAIR and Bug Bar to in-house tooling and processes. (2021, p. 1-6)

Some CPS specific attack taxonomies have been published in research, for example by Heartfield, Loukas, Budimi, Bezemskij, Fontaine, Filippoupolitis and Roesch (2018) whose extensive research inspected methods to identify, categorize and address cyber-physical threats against home automation systems. Their methodology relies heavily on home automation system specific attack vectors, protocols, and impact, and as such cannot be directly utilized to assess threats against a general CPS.

Other findings by Jamil et al. included that the participants were emphasizing the challenge of validating the produced threat models aside from utilizing peer-evaluation and checklists, contributing to the fact that organizations do not update threat models after system modification as also noted by the Jamil et al. (2021, p. 2).

Some studies comparing various traditional methodologies of threat modeling utilized in the context of CPS have been performed. For instance, in 2018 Shevchenko, Frye and Woody compared threat modeling methods against a criterion of strengths and weaknesses, adoptability, tailor ability and applicability to cyber-physical systems. The evaluation targeted a list of methods and methodologies assembled by another study on the same year by the same research group with additional contributors (Shevchenko et al. 2018b). The study results released as whitepaper indicated, that based on the utilized evaluation criteria PASTA framework providing the overall process for threat modeling, augmented with STRIDE and LINDDUN methods for identification for threats matched best of the use case. (Shevchenko et al., 2018a; 2018b). The study provides many improvements suggestion to considered, should the recommended combination of methodologies be utilized. The suggestions include six additional documentation suggestions and 16 extra activities as well as four highlighted best practices (Shevchecnko et al., 2018a, p. 8-9). While the study and its results are important contributions in the field scarce with similar research, the author argues that changes are extensive and contribute to increased complexity. It is likely that re-evaluating the recommended combination of methodologies through the evaluation criteria utilized to produce the outcome would yield low scores in adoptability.

The amount of modification proposed by Shevchenko et al. (2018b) required to the available methodologies seem to corroborate the findings of Jamil et al., who highlighted the limitation of current approaches as a challenge; For example, STRIDE, focusing on threats of traditional information systems would yield deficient threat model for a CPS (2021). It can also be argued that limitations of these tools are transferrable to the methodologies derived from or building on them.

Validation of a threat model in the context of CPS has also been deemed difficult according to Jamil et al. (2021), who concluded that most study participants do not utilize quality assurance methods for validating the produced threat models (p. 8). This could be partially explained by the current practice of utilizing a combination of several methodologies across the industries, producing hard to validate results. There are methodologies with in-build validation, like PASTA recommended by Shevchenko et al. (2018a), but validation methods used by these frameworks (attack simulations in case of PASTA) may not be suitable for CPS. This highlights the urgency of appropriate threat modeling approach for CPS.

Jamil et al. also observed that methodology selection among the interviewees was directed by their background; participants with background in traditional IT tended to favor traditional frameworks like STRIDE and DREAD while participants with control system background opted for frameworks such as PASTA and STRIDE supplemented by failure mode analysis and asset criticality assessment (2021, p. 5). This observation hints of the same cultural difference in security-oriented thinking noticed and described by Liu et al. (2017, p. 36), but can also be interpreted as study participants resolving to known methods and approach, lacking a more appropriate alternative.

Khalil, Bahsi, Dola, Korõtko, McLauglin and Kotka (2023) also not, that not all proposed framework and tool combinations are valid for all stages of the CPS development and operational life cycle. They note that for example, CVSS focusing on deep technical details of a threat or vulnerability may not be assessable or comparable to the information available during the threat modelling of a system in development (p. 3).

Inspecting any given system's security requires detailed documentation on system behavior with dataflow diagrams (DFD), describing system's data and control flows, and trust-boundaries (Shostack, 2014, p. 5-6). Such documentation can be structured with various methodologies, for instance as described by Humayed et al. (2017). Shostack (2008) outlines four distinctive elements necessary for DFD: Process, Data Store, Data Flow and External entity (p. 3).

The process to produce the DFD for threat modelling varies too. For example, Khalil et al. (2023) outline the following process leading to the dataflow diagrams used as a basis for threat modelling a CPS.

Stage	*Stage description*	*Expected output*
Attack Taxonomy	Selection of appropriate taxonomy and categorization framework to identify threats suitable for the target system context.	Selected attack enumeration framework or customized adoption.
System asset identification	Identification of CPS components and assets, such as data stores, physical and software processes, measuring devices, and entities external to the system. Asset categorization may be aligned with normative dataflow diagram types.	Enumerated assets of CPS categorized according to types.
System information identification	Identification of CPS information and data content. Similarly, to asset identification, information is categorized into types based on their characteristics such as time-sensitivity.	Enumerated list of information asset types.
Dataflow Diagram (DFD)	Documentation of CPS, describing information asset and system assets relations in	Dataflow diagram(s) of CPS
Establish security context	Documentation of assumptions and system-specific criteria based on which the threat identification and assessment should be conducted. This context includes system characteristics such as the system's physical and virtual location.	Documented list of assumptions and system characteristics.

Table 4: System modelling process (Khalil et al., 2023, p. 6-10)

Approach suggested by Khalil et al. (2023) is systematic and in many parts typical for common threat modelling process. It highlights the definition of target's security context, as opposed to many other approaches considering this implicit or lacking it altogether, PASTA being one of the few exceptions.

3.3 Cyber-Physical Threats

Among cyber threats, physical threats are an acknowledged area of interest in systems with strong relation to physical world, such as ubiquitous and embedded computing platforms (Voeller, 2014), systems connecting multiple communicating physical devices such as sensors, and other cyber-physical systems (Pathan, 2016, Kim, Park & Lu, 2022). Voeller (2014) further states, that computer systems “are becoming more capable – and more vulnerable – as they are embedded more deploy into our environment”. For example, development of the connectivity in CPS, allowing increasingly complex and innovative use-cases, increase the vulnerability of to the CPS at the same time (Kim, Park & Lu, 2022). In addition to the system themselves, capabilities and sophistication of threat actors and tools used by them are increasing, as noted for example by Maglaras, Kantzavelou and Ferrag (2021).

Usually, one of the major goals of the attacker targeting cyber-physical systems is to cause physical damage to the system (Kim, Park & Lu., 2022, p. 1534), which is a lot more difficult for classic information systems without physical process interfaces. Examples of cyber threats with physical effects include the infamous case of Stuxnet targeting Siemens SCADA control software and causing physical damage to centrifuge of an Iranian uranium enrichment research (Langner, 2013). In 2016 US State Department researchers demonstrated on off-board hacking of Boeing 757, gaining remote access to airplanes systems with commonly available devices (Hollinger, 2018). Research have also found basis for suspecting that software vulnerabilities in e.g. ground-based satellite communication infrastructure could be exploited, potentially leading to physical harm to humans due to high-frequency radio bandwidth emission (Argudo & Mwana, 2023). Cyberattacks with physical destruction or operational disruption as a main objective has been used in military operations and are increasingly used in all types of hostile operations in conflicts of various by nation state actors and APTs (Alladi, Chamola & Zeadally, 2020; Finkle, 2016; Juutilainen, 2023).

In reviewed literature, cyber-physical threats causing effects in a target system caused by an event in a physical system component are more challenging to be found. In fact, they seem to be seldomly described as “cyber-physical”. Some cases which could fall under the term can be found in research, like attacks targeting autonomous vehicles LiDAR sensors, ultrasonic and infrared rangefinders, GPS receivers and inertial measurement units, affecting or disrupting the vehicles system functions (Wyglinski, Huang, Padir, Lai, Eisenbarth & Venkatasubramanian, 2013). Some classification of cyber-to-physical threats exist in the research. For instance, Yeh, Choi, Prelcic, Bhat and Heath classify threats against vehicular radar and dedicated short-range communication system (DSRC) into jamming, interference, and spoofing (2018).

3.3.1 Attack types

In many cyber-physical attack examples, damage is propagated via CPS into the physical world, more often than the other way around. There can be several reasons for this. One is, that such attacks are often categorized under something else than cyber-attack, for example misuse or functional restrictions of equipment (e.g., radar can only detect certain amount of target), equipment failure (e.g., PLC controlled pressure valve can only handle limited amount of pressure) or electronical warfare (e.g., jamming and decoys against system sensors). Some examples of attack types such as malicious insider, physical intrusion to equipment cabinet to access a system and evil maid attack are common types of cyber threats which are not categorized "cyber-physical." Yet another interpretation is that cyber-physical threats, when discussed in the research and public domain, emphasizes the physical consequences of the attack, rather than the nature of threat being transient between cyber and physical domain.

While examples cases of both types exist, threats propagating from cyber domain to physical domain seem to be more prominently presented in literature and public discourse. Despite the asymmetry, it can be established that threats emerging from cyber domain can affect physical domain, and vice versa, forming a bidirectional relationship between the domains.

It is also worth noting that occasionally, treating a cyber event as "cyber-physical threat" which should be included in the threat model may not be unambiguous as one might expect. For instance, USB letter bomb might not classify as cyber-physical threat even if the ignition utilizes a USB interface of a device (Radford, 2023), while social engineering an operator of an industrial process to perform inadvertently malicious actions causing physical destruction might. In another example, does bypassing airgap via payload delivered with spear phishing constitute cyber-physical, as the payload is moved across to the system by an unsuspecting proxy to CPS, even if the payload does not cause physical effects? When the attack results in physical damage or alteration of a physical process, cyber-physical attacks are easier to be classified as such, compared to the opposite scenario.

For this thesis, cyber-physical threats are defined to be threats propagating between the system components of different domain, excluding the threat actor from the consideration. I.e., threat actor accessing a physical interface of the of a device is not considered a cyber-physical threat. Practical utilization of this definition is demonstrated more thoroughly in chapter 4.3.3.

3.3.2 Attack categorization

Classification of cyber-physical threats and attacks has been part of many studies. In their paper describing data-driven approach to CPS threat identification utilizing network security monitoring, Kim et al. (2022) categorizes cyber-physical attacks against a CPS in three categories: attack-space, attack location and *stealthiness* [sic], which are further divided in sub-categories. In comparison to traditional cyber-attacks, attack location refers to the data manipulated by the adversary rather than the adversary compromised devices. The article justifies this definition by the prevalence of control signal and sensor input data modification as key enabler for cyber-attacks against CPS (p. 1543).

Many studies utilize generic threat categorization provided by the used threat modelling framework, e.g. STRIDE. Some studies have created their own, more cyber-physical focused threat categorization such as Khalil et al. (2023), defining preconditions and threat types for CPS.

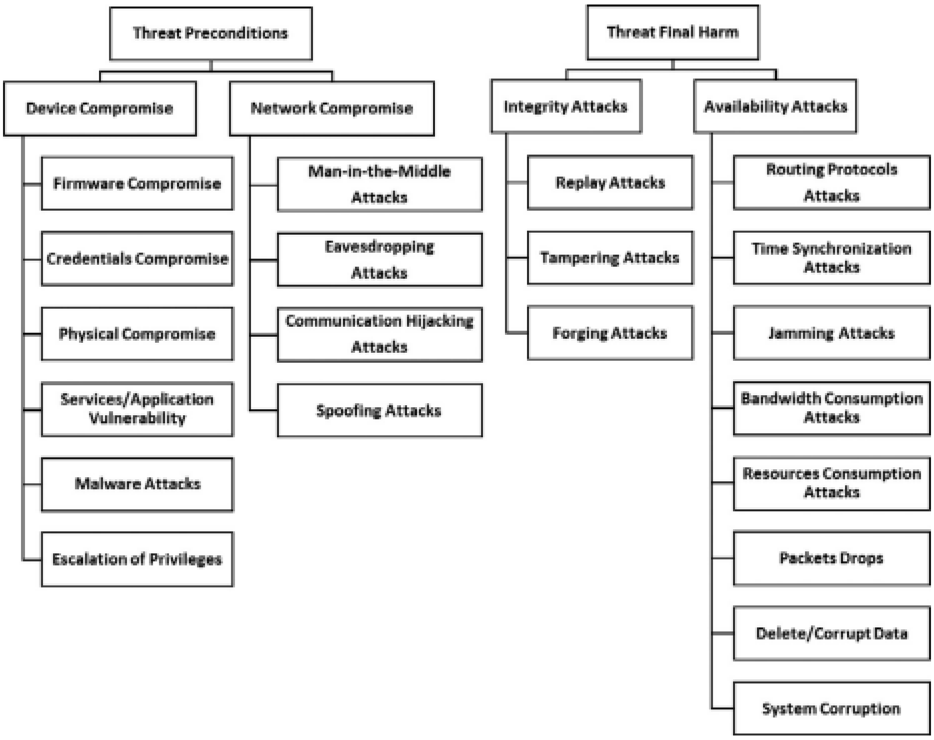


Figure 5: CPS threat pre-condition and attack type categorization (Khalil et al. 2023, p. 6)

Author of the theses argues however that threats are identifiable using various taxonomies, e.g., STRIDE –like threat categorization or attack libraries such as MITRE ATT&CK for ICS. CPS specific threat categorization itself does not provide crucial capability for threat elicitation process; The categorization can be seen as helpful convention that should be selected to best suit the context of the target system. Industry specific frameworks such as SPARTA should be used with care, when implementing in other use-cases than those of the original design purpose of such frameworks.

3.3.3 Effects of security context

System security context (Khalil et al., 2023) describes a system’s environmental characteristics, that may affect its overall security posture. For example, a locked door can be a part of a system's security context even though it does not belong to the system itself. It can involve the human-factor, for example identifying all legit operators of the system (system administrators, maintenance personnel, monitoring users) and potential adversaries (malicious insiders, external threat actors, etc.). In other words, security context records the assumptions that the threat model can be based on. According to Shostack (2014), such assumptions are vital to be recorded to avoid creating new issues in the form of unhandled security threats, improper security control implementation, false sense of security (p. 135). Shostack also suggests that impact of failed assumptions should also be considered to recognize what is the effect when reality does not correspond to the documented assumption (p. 135-136).

Security context may also include security controls in place to protect the system, either internal or external to the system itself. In the case of CPS, many such systems incorporate security instrumentation system (SIS) safeguarding the physical process by ensuring the process is ran within agreeable thresholds, returning it to safe state. For example, if process pressure, voltage or temperature rises above agreeable level, controller shutdown or other process restriction measures are implemented to avoid damage to equipment, surroundings and in many such cases, human health. SIS can be implemented either as a standalone, air gapped system outside of the control flow of the rest of the system, or it can be integrated. Typically, SIS is systems involved with chemical, nuclear or refinery processes. (NIST, 2023, p. 25)

For any physical entity, its *location* specifies the object's position in a reference coordinate system and an essential component of its security context. Changing the location also affects its security context, even if the change is temporary, also altering the system's threat model.

Examples of moving CPS involve various vehicular systems, such as airplanes, ships, UAV and USV, ground vehicles and spacecraft. Moving or changing location is not a typical attribute of vehicle-bound cyber-physical systems alone; Traditional information systems not involved with maintaining or observing physical processes can be moved as well, examples of such use cases including operational headquarters of distinct size military units, headquarters or bases of organisations participating in international crisis management operations or bases used for research.

Having dynamic environment is not CPS specific; Traditional IT systems can be mounted on or even be integrated as part of a moving platforms, such as trucks, ships, or airplanes. These systems can have various purposes, such as navigational operations, research data gathering, and various supporting systems for crew and/or passengers.

4 Proposed methodology

Solution construct proposes a framework to implement the threat modelling process described in chapter 3.1.2 containing steps of system modelling, threat identification, threat analysis and validation. Proposed solution allows iterative approach, i.e., enables re-evaluating the model's validity, and recommends documentation and tools for implementing each step.

The proposed approach focuses on identifying cyber-physical boundaries (CPB) in the target system, and investigating threats related to these boundaries.

A summary of the approach is presented in the following figure. It is aligned with common threat modelling approaches, proposing improvements to identify cyber-physical threats more efficiently.

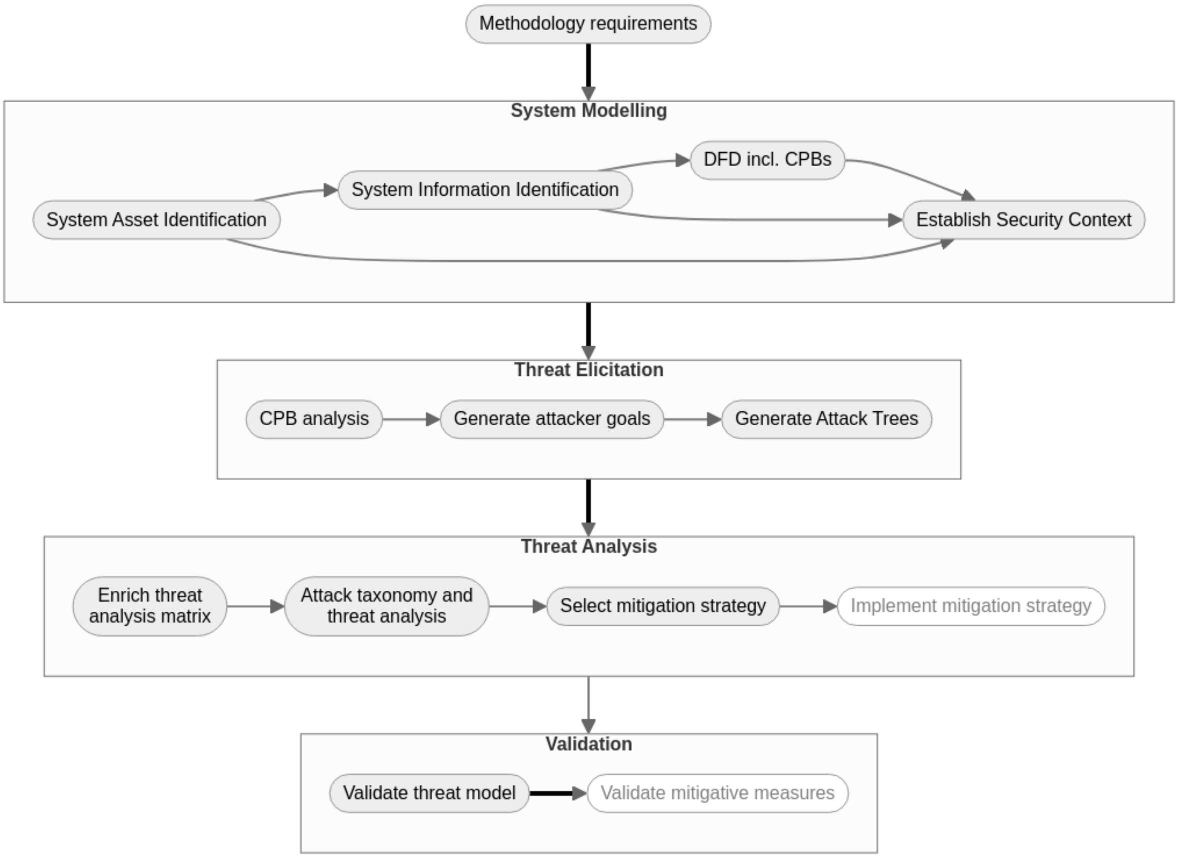

Methodology requirements
System Modelling
System Asset Identification
System Information Identification
DFD incl. CPBs
Establish Security Context
Threat Elicitation
CPB analysis
Generate attacker goals
Generate Attack Trees
Threat Analysis
Enrich threat analysis matrix
Attack taxonomy and threat analysis
Select mitigation strategy
Implement mitigation strategy
Validation
Validate threat model
Validate mitigative measures

Figure 6: Proposed approach for threat modelling cyber-physical threats in CPS.

The process holds similarity to the methodology proposed by Khalil et al. (2023), with added focus to cyber-physical boundary analysis which is analogous to the trust boundary analysis in the referred study.

4.1 Requirements for the methodology

Requirements for the threat modelling approach have been set to address the research objectives set for this thesis, presented in Table 5. Requirements were derived from the research objectives and the theoretical background presented in chapter Theoretical background3. Semantics used in the “Requirements” column adhere to the specification of RFC 2119 (Brader, 1997). Some requirements set for the methodology are defined as less restrictive, as they may be challenging to implement in practice, or their implementation may have limitations within the scope of the thesis research.

Requirement	Additional information	Rationale	Solution implementation
Must be applicable to a generic cyber-physical system.	I.e., produced model must utilize acknowledged CPS abstraction model (3.2.13.2.2).	Research objectives and problem (1.2, 1.4)	Solution implements expanded DFD model to pinpoint cyber-physical boundaries within the target system to facilitate analysis of event chains traversing this boundary. Solution implements modular tool and framework selection capable of fine-tuning the process.
Must be capable of identifying and support analyzing cyber-physical threats.	Models should also support cyber-only and physical-only threats.	Research objectives and problems (1.2, 1.4), Research scope (1.3).	Solution utilizes attack taxonomy suitable for CPS.
Should consider ease of adoptability as key criteria.	I.e., models must avoid proprietary methods and tools.	Adoptability is a widespread problem both in IT and CPS related methodologies. (3.1.8, 3.2.5)	Selected frameworks are selected based on literature review to support ease-of-adaption. Proposed framework aims to document in detail the steps to implement the approach in more specific use-cases
Should consider scalability as key criteria.	Upward and downward scalability, i.e., model must be lightweight for smaller target system (Yskout et al., 2020, p. 11). This implies that the model must be modular to support various levels of abstraction of the target system.	Common methodologies while comprehensive are laborious to implement in practice. (3.1.8, 3.2.5)	Solution documents requirements and guidance for upscaling the usage of approach to wider scope of target systems. Selected frameworks and tools are scalable.
Should implement semantics common both for CPS and IT industries when feasible.		Cultural difference in approaches between CPS and IT is seen to contribute to the lack of adoption and inefficient utilization of methodology (3.2.1, 3.2.5).	Selected frameworks should feature common terminology when feasible.
Should implement interchangeable attack taxonomy framework.	For example, selecting between attack tree and fault tree analysis should be possible.	Numerous studies have pinpointed that heterogeneity of CPS imposes challenges on selecting a suitable attack taxonomy. To future-proof the concept, proposed approach should be able to switch between attack taxonomies. (3.2.5)	The solution decouples threat identification from the analysis, enabling free selection of both threat elicitation and analysis methods. Validation framework is agnostic of the following methods.

Table 5: Requirements for a generic threat modelling approach for cyber-physical systems.

4.2 Framework for system modelling

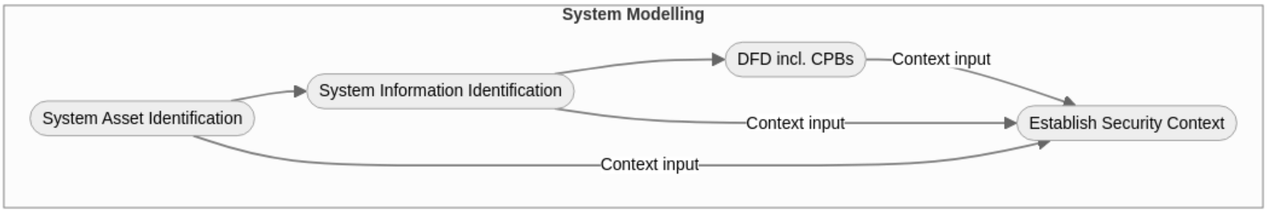

System Modelling
System Asset Identification
System Information Identification
DFD incl. CPBs
Context input
Context input
Context input
Establish Security Context

Figure 7: Process for system modelling a CPS.

To produce an assessable model of a target system, this thesis exploits the structured approach of Khalil et al. (2023) for modelling the system. In addition to asset and information identification present in their approach, to focus on cyber-physical threat identification it is necessary to pinpoint trust-boundaries and dataflows crossing cyber-physical domain, and system assets residing at this boundary, i.e. the cyber-physical boundaries. Humayed et al. (2017) propose dividing components in scope based on their interaction with other components. Each component represents one or more of the following interaction types: physical, cyber-physical, cyber. This distinction enables assessing a simple component from multiple perspectives, providing clear separation for modelling several types of threats. Duo, Zhou and Abusorrah provide a similar, more simplified, categorization of physical and cyber components.

4.2.1 Methodology selection

The combination of the three approaches can be done by expanding the asset identification matrices with information extrapolated from the identification process. For system assets, information is attached to the asset description on the nature of components interaction with other components i.e., is the component of physical, cyber-physical, or cyber in nature. For information assets, data flows included in the DFD should indicate whether the connection is physical, cyber-physical or cyber in nature. This information can be added to the information asset matrix to guide the threat assessment to the components of interest i.e., those residing between cyber and physical domains.

Depending on the level of abstraction, it may be useful to describe the component as cyber-physical over more precise cyber or physical. More detailed distinction can be made in more detailed inspection of the subcomponents. On a higher level it is enough to notice, that a component is cyber-physical and hence, may contain dataflows of interest when the target is to identify cyber-physical phenomena. In more detailed analysis, it is needed to define subcomponents into cyber or physical to provide distinct lines between the two.

Figure 8 illustrates the dissection of the CPS high-level component identification into more details diagram.

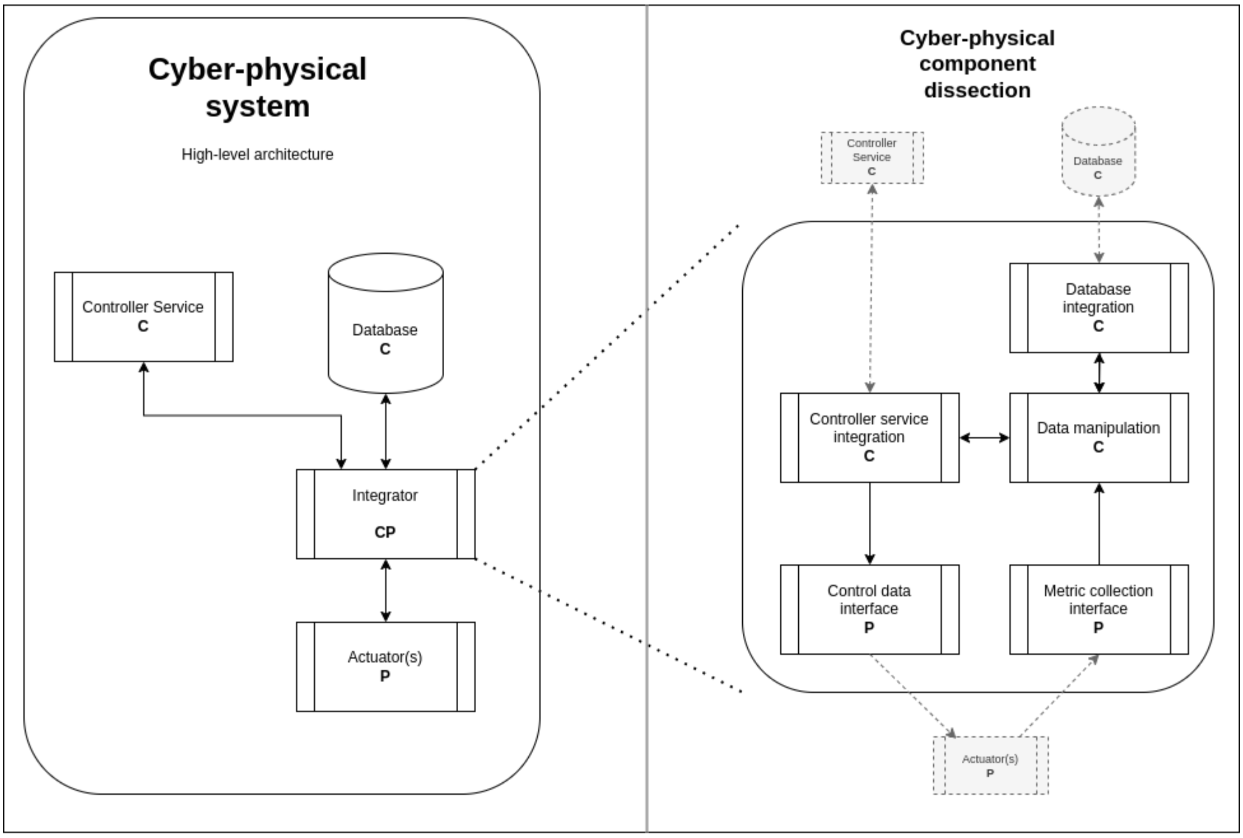


Figure 8: Dissecting cyber-physical components for DFD.

4.2.2 System and information assets

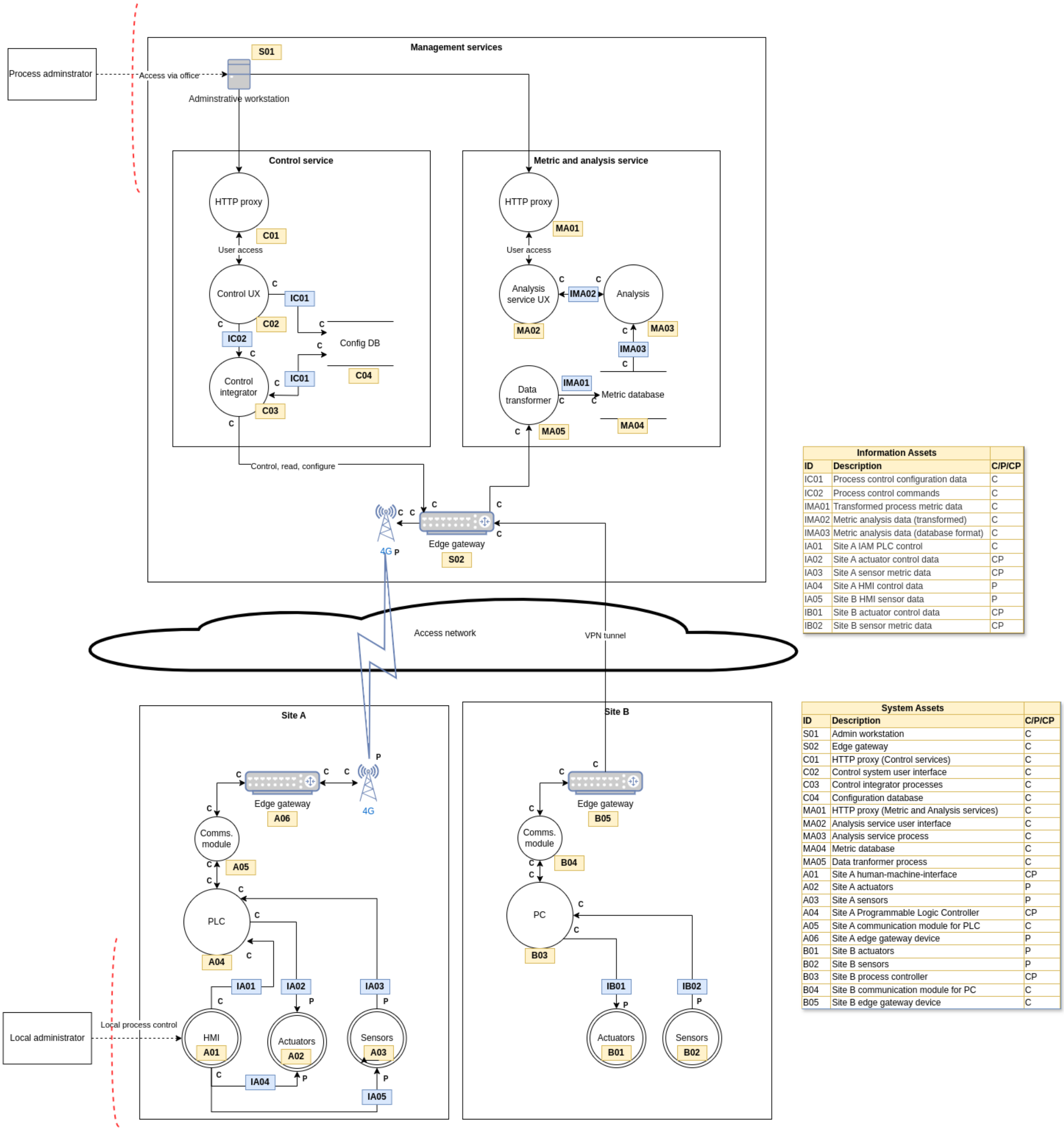
System assets and information assets are collected adapting a model described by Khalil et al., both types of assets in their own matrices. Information can be gathered from system documentation, workshops, interview sessions and other expert dialogue.

Data matrices for both types of asset information are described in Appendix 1, detailing their usage and references to source material used as a basis of their structure.

4.2.3 Dataflow diagrams

Considering the necessity to have distinct assets in various categories, DFD should also reflect these notions. Each dataflow describing information assets will include a type of connection defining whether the connection endpoint of the flow is physical or cyber. Connection is cyber-physical if connector endpoints are of several types. To make the distinction clearer, such classification is added as a note to each system asset node (process, external entity, data storage) to indicate the same distinction. It should be noted that system assets should not be classified as cyber-physical. If such a necessity arises, more details need to be added to the DFD or another more detailed version for the specific component should be drawn.

Following example dataflow diagram presents dataflow diagram of a demonstrative system featuring simplified distributed control system architecture utilizing edge gateways for connecting the process control of remote sites to centralized management services. The diagram features system and information asset labels and cyber-physical boundary representation as per above description.



Information Assets		
ID	**Description**	**C/P/CP**
IC01	Process control configuration data	C
IC02	Process control commands	C
IMA01	Transformed process metric data	C
IMA02	Metric analysis data (transformed)	C
IMA03	Metric analysis data (database format)	C
IA01	Site A IAM PLC control	C
IA02	Site A actuator control data	CP
IA03	Site A sensor metric data	CP
IA04	Site A HMI control data	P
IA05	Site B HMI sensor data	P
IB01	Site B actuator control data	CP
IB02	Site B sensor metric data	CP

System Assets		
ID	**Description**	**C/P/CP**
S01	Admin workstation	C
S02	Edge gateway	C
C01	HTTP proxy (Control services)	C
C02	Control system user interface	C
C03	Control integrator processes	C
C04	Configuration database	C
MA01	HTTP proxy (Metric and Analysis services)	C
MA02	Analysis service user interface	C
MA03	Analysis service process	C
MA04	Metric database	C
MA05	Data tranformer process	C
A01	Site A human-machine-interface	CP
A02	Site A actuators	P
A03	Site A sensors	P
A04	Site A Programmable Logic Controller	CP
A05	Site A communication module for PLC	C
A06	Site A edge gateway device	P
B01	Site B actuators	P
B02	Site B sensors	P
B03	Site B process controller	CP
B04	Site B communication module for PC	C
B05	Site B edge gateway device	C

Figure 9: Example of a simplified dataflow diagram with asset identification information. Adapted from NIST guidelines (2023, p. 10 - 32)

In the presented example the level of abstraction is high. This means, that not all the details necessary for instance to identify system or information assets, such as sub-processes, internal logic, configuration data, system logs and other internal data of each process is possible from this diagram alone. Referring to the chapter 4.2.1, more detailed diagram is required for each node for precise assessment. Overly abstract diagrams reduce the quality and reliability of the threat elicitation and consecutively, threat analysis.

4.2.4 System security context

System security context (Khalil et al., 2023) is defined with the information derived from the documented DFD and discussion with system owner, system specialists and security experts. Security context is essential to guide the threat modelling to address valid threat scenarios. It includes the assumptions against which the threat modelling is executed, for example main threat actor if such can be identified, physical location and security controls external to the system but affecting the systems security, identified trusted entities such as system admins or system operators, and security controls which can be expected to be in place such as firewalls and other security device (p. 4). Security context is not limited to these and can be anything relevant to the threat analysis. It should be updated during the threat modelling process as needed, as described later as part of the validation framework.

System security context and related assumptions should be documented. This methodology provides a template presented in Appendix 2, which should be expanded based on target system design, implementation and requirements.

4.3 Framework for threat elicitation

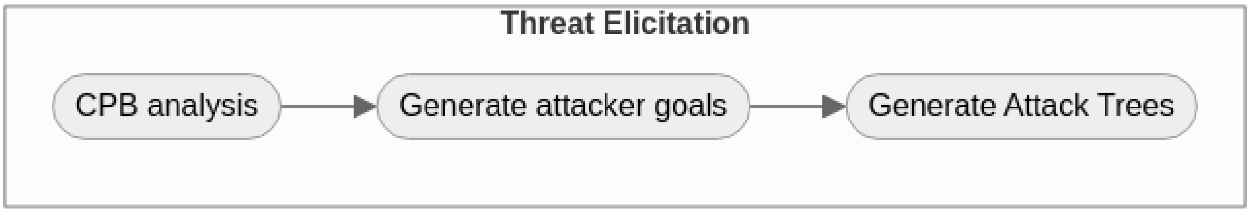


Figure 10: Threat elicitation process.

Threat modelling methodologies for traditional information systems have been extensively researched and applied in practice (chapter 3.1), although criticized by many sources for modeling threats both in traditional information systems (Shostack, 2022; Yskout et al., 2020) and cyber-physical systems (Martins et al., 2017, Jamil et al. 2020). Successful application of various combination of methodologies is tedious (Shevchenko et al. 2018a) and prone to many issues (Shostack 2022; Yskout et al, 2020, Jamil et al. 2020, Shevchenko et al., 2018a). For CPS, no common framework exists (Jamil et al., 2020, Martins et al., 2015). Literature provides no obvious choice for a methodology while providing many concerns and presenting various issues with the existing ones.

4.3.1 Methodology selection

Considering the examples of cyber-attacks with physical effects in the section 3.3 Cyber-Physical Threats, pre-emptively identifying such interaction between cyber and physical domain is not trivial. For example, origin of the physical effect of a cyber event may not necessarily origin from the cyber-physical component. Attacker actions in cyber domain may eventually lead to a physical effect. For instance, ransomware attack propagating through an ICS system may cause physical damage, even when the attack vector has not crossed CPB of a system. Rather, the effect of an attack does cross the boundary instead of the attack itself. This makes it hard to identify comprehensively cyber-to-physical effects utilizing attack libraries. Such like MITRE ATT&CK or SPARTA on identified cyber-physical components will not yield desired results unless such tools are used to evaluate the system as whole. When focus is to identify cyber-physical event chains specifically, using these methods can divert attention from the pertinent threats.

Khalil et al. (2023) suggest that based on their findings, to increase the methodology's ease of adoption the threat elicitation should be done prior to analysis of threat consequences (p.14). This may be true for STRIDE and similar mnemonic –type approaches utilized in their research and several studies related to CPS have proven their worth. Utilizing these types of models do not focus on cyber-physical attack chains per se, while they can be utilized in analogous manner focusing the analysis on the edges of cyber-physical boundary.

Attack trees, on the other hand, provide an effective method to trace events through the system, making it easier to pinpoint event chains across desired checkpoints, i.e. CPBs in this situation. Fault Tree Analysis would also be a suitable candidate, making it possible to track event chains starting from the defined consequences as opposed to Attack Tree Analysis starting from the defined attacker goal. When the assessment focus is to inspect the interaction between cyber and physical domain, this thesis proposes the usage of Attack Tree Analysis on CPBs documented in the DFD of the system.

Attack trees provide built-in approach to evaluate the tree nodes' value to assess e.g., monetary impact or attack likelihood with cost/benefit analysis (Schneier, 1999; Saini et al., 2008). Nodes can be valued by other attributes to calculate different dimensions of the attack, like exemplified by Budde et al. (2012) whose approach focused on investigating probable time consumed by an attacker to perform the attack. Proposed framework does not implement such an approach to avoid unnecessary strong coupling of threat elicitation framework and threat analysis framework; Node valuation can be implemented using the proposed methodology, if cost/benefit analysis or similar approach is deemed suitable analysis tool for the purpose of modelling the target system.

For this thesis approach, Attack Tree Analysis and resulting diagrams are convenient way to illustrate when attack crosses the CPB, making it more obvious where the transition between domains occur. This illustration works both for attack origin and attack consequence. Aside of Fault Tree Analysis, this is not as well presented by other well-established methods like STRIDE.

The critique of attack trees not being able to provide tools for scoping described in chapter 3.1.4 is partially compensated in by the proposed methodology with focus on the cyber-physical boundary elements of the system. Methodology does not however remove the inherent problems of the used framework and tends to produce a great deal of work when attack trees are generated for increasing amount of attacker goals in complex systems.

4.3.2 CPB analysis

Assessment focuses on event chains of a cyber-attack traversing the CPB, enabling the threat elicitation and further down the process design and implementation of security controls on mitigative measures on identified threats.

For threat elicitation, it is necessary to first examine the system asset nodes in DFD residing in CPB, along with their neighbouring nodes. This identification can be done by enumerating dataflows with two distinct types of endpoints; All dataflows which are classified as cyber-physical should act as a starting point for analysis, producing more at least on Attack Tree Analysis.

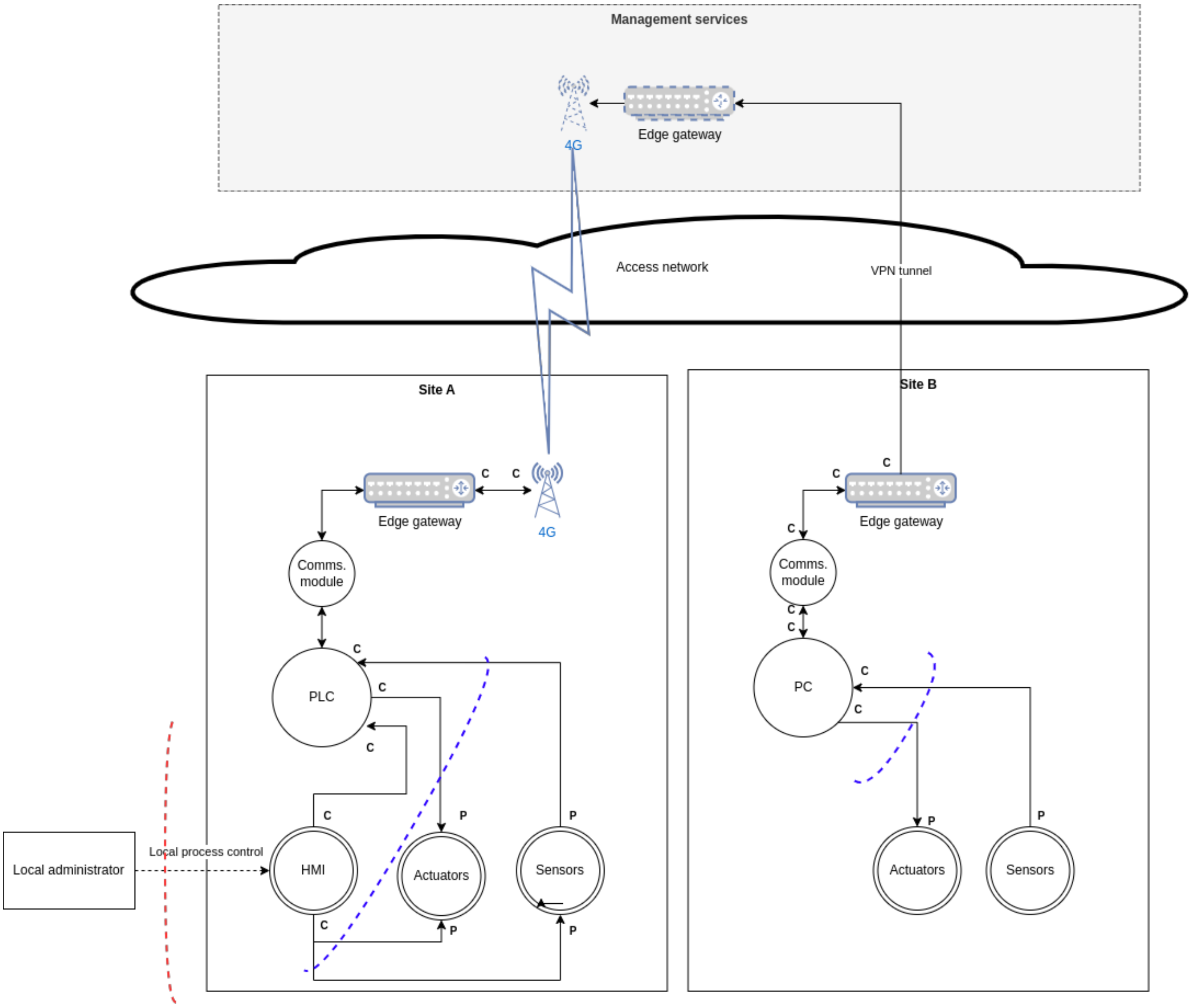


Figure 11: Example on CPB labels on a dataflow diagram *(Red = trust boundary, Blue = cyber-physical boundary)*

4.3.3 Attacker goal generation

In Attack Tree Analysis, threat elicitation is initiated by defining attacker goals. Considering the identified cyber-physical boundaries in previous step, two types of approaches should be used when selecting these objectives. Elicitation of cyber-physical threats based on attacker goals relies in this thesis' definition of cyber-physical threats described in chapter 3.3.1.

For event chains where consequences are expected to be physical, attack goal should be selected to match the functionalities and capabilities of DFD nodes in physical category. Particularly, inspecting the physical (*P type)* component's capabilities, feasible physical effects can be enumerated; For instance, actuator is only capable of controlling a small subset of mechanical components. In this scenario, attacker goal is equal to the undesired physical effect of a system.

Identifying how a physical component can misbehave can help to determine potential attacker goals.

Examples of attacker goal with a physical effect are e.g., inject malicious parameters to process control traffic or change configuration parameters controlling process safety thresholds.

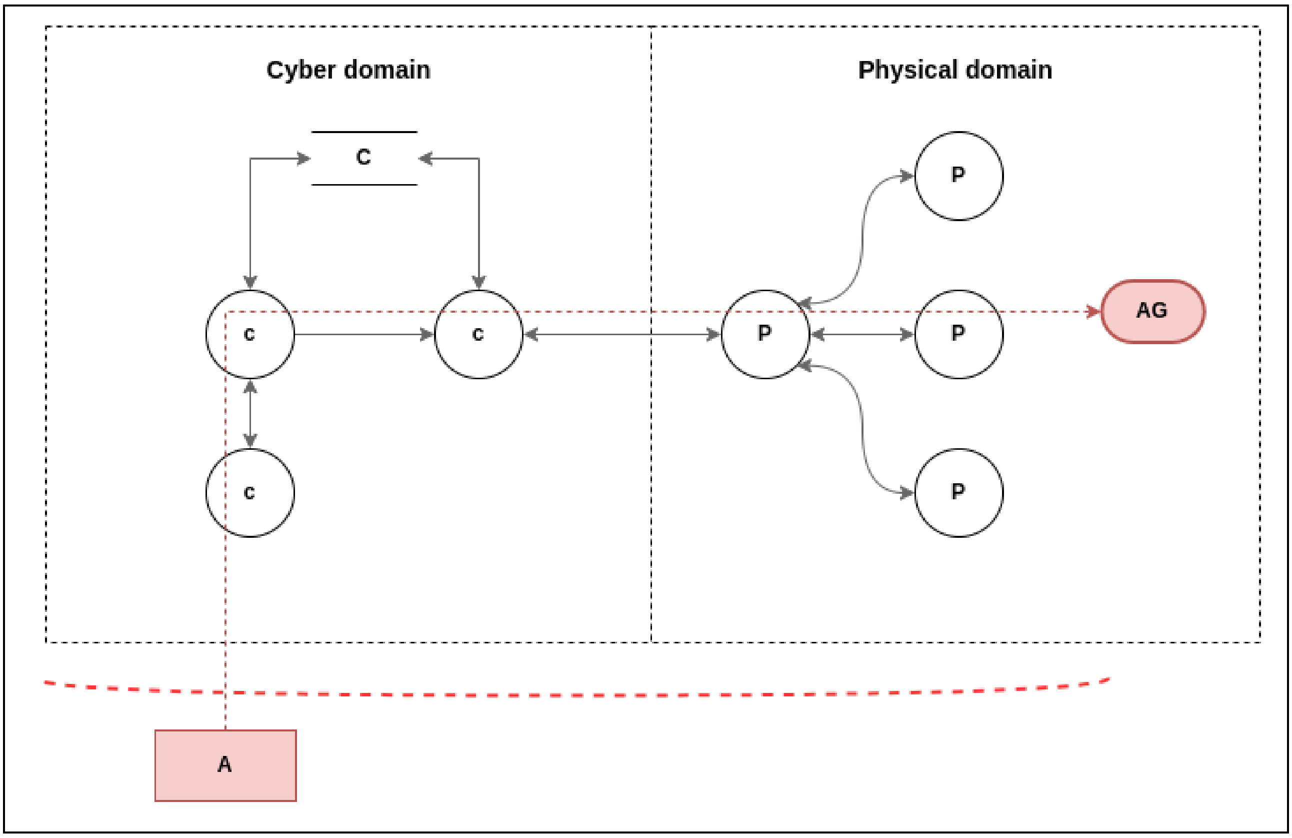


Figure 12: Simplified example cyber to physical attack *(C = Cyber, P = Physical, A = Attacker, AG = Attacker Goal, Red line = Trust Boundary)*.

Another approach is required for event chains where the consequence, i.e. attacker goal, resides in the cyber domain should start by identifying the DFD nodes along the CPB, and generate attack goals related to these components. More focus can be attained by focusing on the node's functionality which has relations to the physical component. Further attack trees can be generated starting from that node to identify consecutive attacker actions more thoroughly. In this case, compromising a node at the CPB can be seen as a stepping stone for further compromise of the system. This approach aims to counteract the overwhelming number of potential attack paths in complex systems, where attacker goals may be hard to derive.

Examples of attacker goal used for identifying cyber-physical event chain where the consequence lies within cyber domain are e.g., corrupt database gathering metric data from physical sensors and saturate backend-service resources connected to physical components.

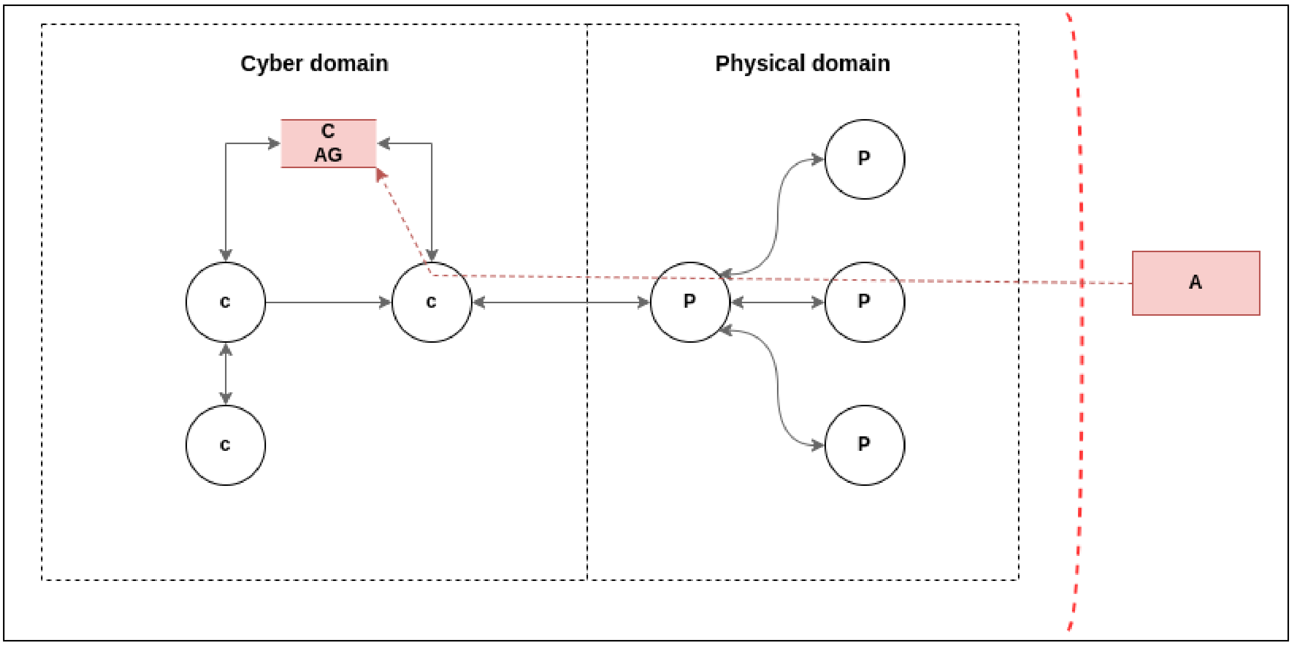
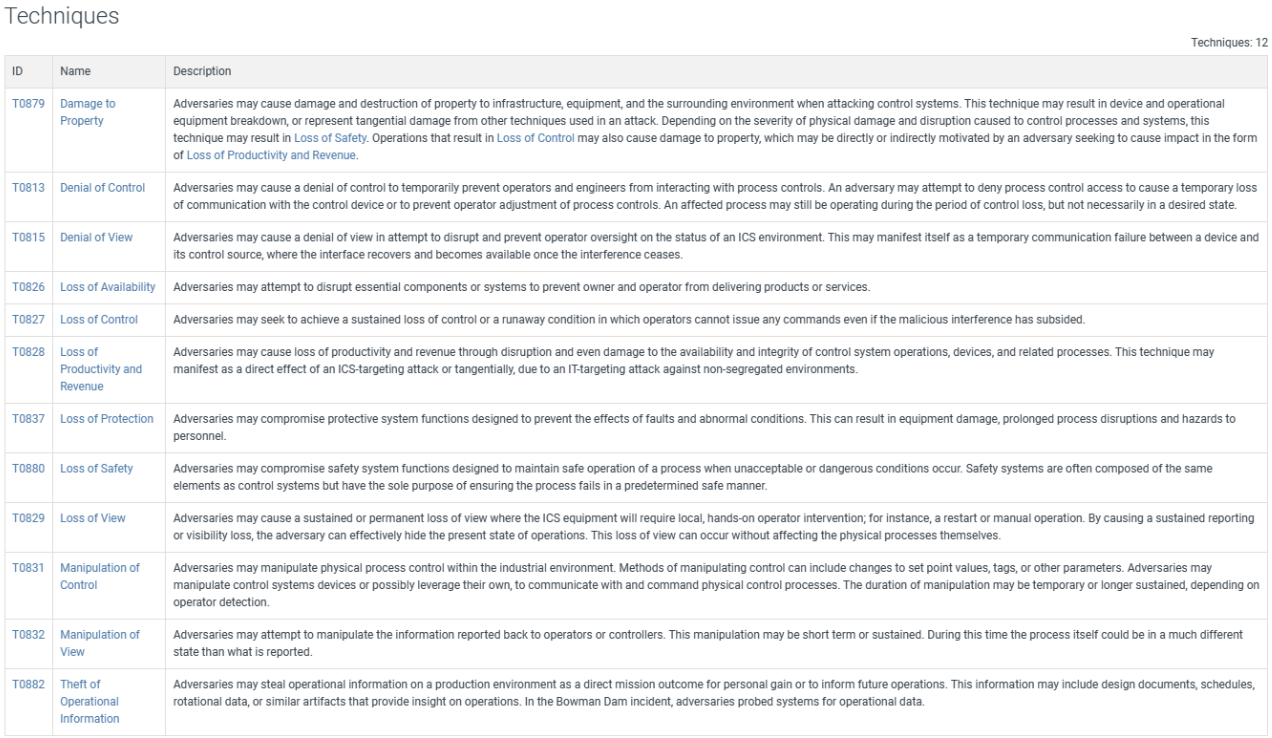


Figure 13: Simplified example physical to cyber-attack *(C = Cyber, P = Physical, A = Attacker, AG = Attacker Goal, Red line = Trust Boundary).*

Attacker goal generation is not trivial and considering the identified limitation of the attack tree analysis method presented in the chapter 3.1.4, scoping the issue can prove challenging. This is partially counter balanced by the focus to cyber-physical boundaries but should be kept in mind during the threat modelling assessment when determining whether all attacker goals have been identified. Threat modelling should be resumed when new attacker goals are identified.

One approach to generate attack tree is to exploit the selected threat taxonomy. For example, MITRE's framework provides a useful impact category, which can be iterated over the system component in question.



Techniques

Techniques: 12

ID	Name	Description
T0879	Damage to Property	Adversaries may cause damage and destruction of property to infrastructure, equipment, and the surrounding environment when attacking control systems. This technique may result in device and operational equipment breakdown, or represent tangential damage from other techniques used in an attack. Depending on the severity of physical damage and disruption caused to control processes and systems, this technique may result in Loss of Safety. Operations that result in Loss of Control may also cause damage to property, which may be directly or indirectly motivated by an adversary seeking to cause impact in the form of Loss of Productivity and Revenue.
T0813	Denial of Control	Adversaries may cause a denial of control to temporarily prevent operators and engineers from interacting with process controls. An adversary may attempt to deny process control access to cause a temporary loss of communication with the control device or to prevent operator adjustment of process controls. An affected process may still be operating during the period of control loss, but not necessarily in a desired state.
T0815	Denial of View	Adversaries may cause a denial of view in attempt to disrupt and prevent operator oversight on the status of an ICS environment. This may manifest itself as a temporary communication failure between a device and its control source, where the interface recovers and becomes available once the interference ceases.
T0826	Loss of Availability	Adversaries may attempt to disrupt essential components or systems to prevent owner and operator from delivering products or services.
T0827	Loss of Control	Adversaries may seek to achieve a sustained loss of control or a runaway condition in which operators cannot issue any commands even if the malicious interference has subsided.
T0828	Loss of Productivity and Revenue	Adversaries may cause loss of productivity and revenue through disruption and even damage to the availability and integrity of control system operations, devices, and related processes. This technique may manifest as a direct effect of an ICS-targeting attack or tangentially, due to an IT-targeting attack against non-segregated environments.
T0837	Loss of Protection	Adversaries may compromise protective system functions designed to prevent the effects of faults and abnormal conditions. This can result in equipment damage, prolonged process disruptions and hazards to personnel.
T0880	Loss of Safety	Adversaries may compromise safety system functions designed to maintain safe operation of a process when unacceptable or dangerous conditions occur. Safety systems are often composed of the same elements as control systems but have the sole purpose of ensuring the process fails in a predetermined safe manner.
T0829	Loss of View	Adversaries may cause a sustained or permanent loss of view where the ICS equipment will require local, hands-on operator intervention; for instance, a restart or manual operation. By causing a sustained reporting or visibility loss, the adversary can effectively hide the present state of operations. This loss of view can occur without affecting the physical processes themselves.
T0831	Manipulation of Control	Adversaries may manipulate physical process control within the industrial environment. Methods of manipulating control can include changes to set point values, tags, or other parameters. Adversaries may manipulate control systems devices or possibly leverage their own, to communicate with and command physical control processes. The duration of manipulation may be temporary or longer sustained, depending on operator detection.
T0832	Manipulation of View	Adversaries may attempt to manipulate the information reported back to operators or controllers. This manipulation may be short term or sustained. During this time the process itself could be in a much different state than what is reported.
T0882	Theft of Operational Information	Adversaries may steal operational information on a production environment as a direct mission outcome for personal gain or to inform future operations. This information may include design documents, schedules, rotational data, or similar artifacts that provide insight on operations. In the Bowman Dam incident, adversaries probed systems for operational data.

Figure 14: MITRE's Impact category techniques (MITRE, n.d.b)

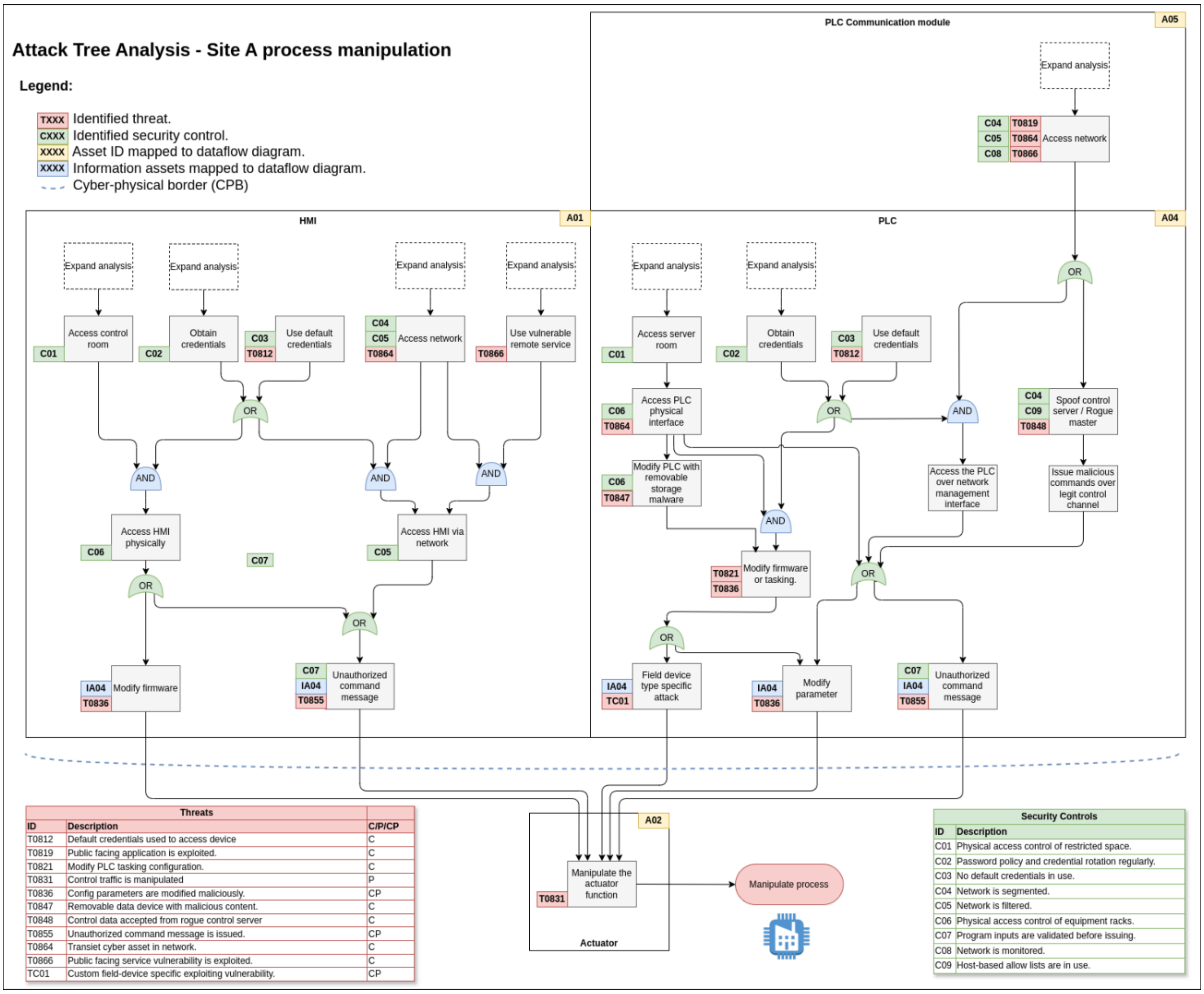
4.3.4 Attack tree generation

A single attack tree diagram should contain only one attacker goal, i.e. physical consequence, or attacker target in cyber domain. As a note, this methodology does not restrict the scope of the Attack Tree Analysis. Method can be used to inspect the security threats in a more general manner.

Each attack tree starts with definition of the root node (Shostack, 2014, p. 89), i.e. attacker goal in the context of this methodology. Following figure shows an example of an attack tree, where attacker attempts to manipulate a physical process. Asset boundaries have been highlighted in the diagram for clarity, as well as cyber-physical boundary identified during the CPB analysis.

Brainstorming and different structured approaches can be used to derive attack trees (Shostack, 2014, p. 89). Simplifying the analysis of each node when generating the attack tree, guiding questions to help threat elicitation process are 1) what attacker must do to proceed towards selected goal, 2) what conditions or node functionality enables the attacker to achieve this, and 3) what controls or conditions disables the attacker from proceeding? In attacker-centric models eliciting the attacker actions may be a challenge and prone to bias (Shostack, 2014, p. 40-41). To counteract this, it may sometimes be helpful to concentrate on the capabilities and limitations of the system function rather than the attacker actions. For example, instead of asking “what an attacker must do to achieve A?,” question can be reformed as “what must happen in the system component in order to enable A?”, followed by the analysis whether the pre-requisite of event A is in control of an attacker. This type of approach is more analogous to Fault Tree Analysis.

For this methodology, it is important to identify assets related to each node (system asset or information asset, i.e. dataflow) represented in the dataflow diagram. This makes it possible to investigate, which threats cross the CPB. Equally important topic of interest are the possible security controls already in place within the design or system in operation, to avoid planning duplicate mitigation and increasing the workload of already tedious task. Attack trees can be generated with various tools. Format of the attack tree can be presentative for human audience, or more structured to allow programmatic analysis (Shostack, 2014, p. 90-94).



Threats		
ID	**Description**	**C/P/CP**
T0812	Default credentials used to access device	C
T0819	Public facing application is exploited.	C
T0821	Modify PLC tasking configuration.	C
T0831	Control traffic is manipulated	P
T0836	Config parameters are modified maliciously.	CP
T0847	Removable data device with malicious content.	C
T0848	Control data accepted from rogue control server	C
T0855	Unauthorized command message is issued.	CP
T0864	Transiet cyber asset in network.	C
T0866	Public facing service vulnerability is exploited.	C
TC01	Custom field-device specific exploiting vulnerability.	CP

Security Controls	
ID	**Description**
C01	Physical access control of restricted space.
C02	Password policy and credential rotation regularly.
C03	No default credentials in use.
C04	Network is segmented.
C05	Network is filtered.
C06	Physical access control of equipment racks.
C07	Program inputs are validated before issuing.
C08	Network is monitored.
C09	Host-based allow lists are in use.

Figure 15: Example of Attack Tree Analysis with CPB, asset labels, identified threats and identified security controls. Stucture aligned with DFD described in Figure 9

Each identified threat with effects propagating over CPB are deemed as cyber-physical and marked *CP* respectively in the matrix. Used approach is comparable to the implementation of taxonomy classification of Heartfield et al. (2018), by categorizing the impact on the system to be either cyber or physical.

When relevant, identified security controls should be included in the attack tree diagram and threat analysis matrix under the proper threats. Security controls can be brought up by the documented security context, or during the discussion while generating the attack tree diagram with experts and system owner.

4.4 Framework for threat analysis

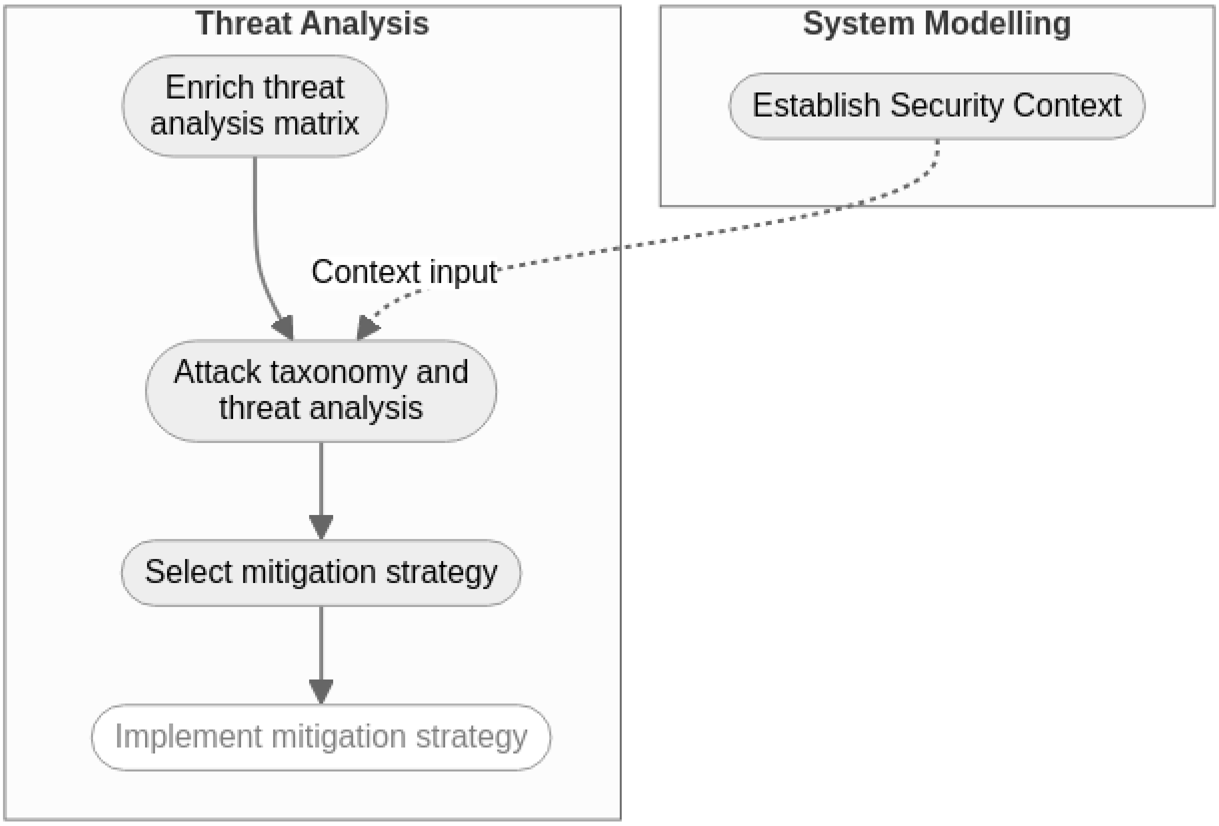

Threat Analysis
Enrich threat analysis matrix
Context input
Attack taxonomy and threat analysis
Select mitigation strategy
Implement mitigation strategy
System Modelling
Establish Security Context

Figure 16: Threat analysis process for identified attack paths and vectors.

After the threat elicitation is completed, each threat in the threat analysis matrix can be independently analysed and proper actions taken to process them according to system's requirement and design.

4.4.1 Methodology selection

Threat analysis is an important part of threat modelling process and presented here to demonstrate, that proposed methodology can be used as part of a practical assessment. Generic template for analysis is provided (Appendix 3), this section describing its utilisation during threat modelling process and key steps to achieve of handling the elicited security threats.

Attack libraries such as MITRE ATT&CK for ICS or SPARTA can be used to provide the attack taxonomy. Utilization of such frameworks should be carefully implemented and aligned with the level of detail available to the assessment to avoid imposing detailed technical analysis. For this thesis, MITRE ATT&CK for ICS is used as a tool to enrich the threats identified with Attack Tree

Model. MITRE’s framework is not perfect match for CPS threat analysis, as CPS incorporate a much larger set of systems than ICS alone. The frameworks extensiveness and otherwise general approach to process control provide a consistent template for threat analysis, which can be supplemented by other frameworks or system specific analysis.

As the threat elicitation is decoupled from the analysis, frameworks of attack taxonomy and threat analysis can be changed to framework more suitable for the target system’s context.

4.4.2 Threat taxonomy and analysis

MITRE ATT&CK for ICS described in previous chapters is one of the most extensive purpose-built attack library frameworks for ICS systems and by extension, CPS. This attack library tool contains kill-chain type of representation of various attack tactics, techniques, and categorization, which can be used to further increase the details of the findings.

Template presented in Appendix 3 provides means to document threat details as they are identified using the Attack Tree Analysis. Suggested attack taxonomy can be used to enrich details on the threat, as well as define the impact of the threat when actualized. Impact may not be just the consequence defined by the attack goal, i.e. root node of an attack tree. Implications of succeeding attacker goal may exceed the actions taken on a single system component, for example losing control of a process component can cause monetary and reputational losses. Frameworks for analyzing these aspects of threats more thoroughly are available, such as DREAD (Kim et al., 2022; Martins et al., 2015) and CVSS (Dang et al. 2020; Martins et al., 2015) which can be used at this stage of the process.

4.4.3 Security context analysis

When analysing the identified threat, it is important to reflect the analysis against system’s security context. For example, is something a threat viable if currently implemented security controls are in place, Is the identified threat in the scope of the assessment or is the threat non-addressable due to the functional requirements of the system? This reflection is critical to the planning of proper mitigation strategy.

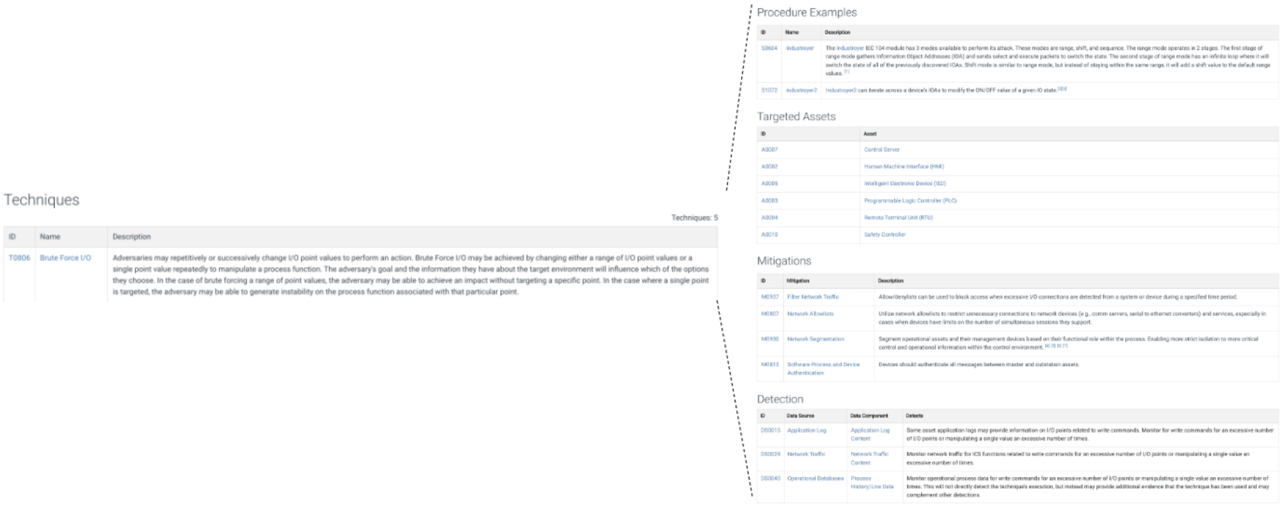
Each threat in threat analysis matrix should be compared to the security context record and verified, whether any assumption is relevant for the analysed threat in question. Analysis of threats may yield more information which may be necessary to be added to security context. Separate field has been reserved for this analysis in the template proposed in Appendix 3.

This analysis should be recorded to threat analysis matrix to the appropriate field for each threat, where relevant to provide insight into proper mitigation strategy selection.

4.4.4 Select mitigation strategies

After the analysis is completed and details have been included in the threat analysis matrix in (Appendix 3) mitigation can be designed for each threat (i.e., attack path) individually. More than one mitigation can be implemented against a single threat. Appropriate mitigations can be divers, and proposed methodology of this thesis does not provide a process for designing mitigations or threat prioritization based on e.g., risk scoring. As a summary, traditional risk management strategies include avoiding, addressing, accepting, transferring, and ignoring the risk (Shostack, 2014, p. 167 - 169), addressing the risk being the one including designing of security controls or applying the changes to design to mitigate the threat (p. 169 - 176). Appropriate strategy should be utilized in the context of target system.

MITRE’s ATT&CK for ICS provides technical mitigation strategies and attack detection guidelines for each technique, providing insight on what can be done to prevent and detect such attacks within a target system, exemplified by Figure 17.



Techniques

Techniques: 5

ID	Name	Description
T0806	Brute Force I/O	Adversaries may repetitively or successively change I/O point values to perform an action. Brute Force I/O may be achieved by changing either a range of I/O point values or a single point value repeatedly to manipulate a process function. The adversary's goal and the information they have about the target environment will influence which of the options they choose. In the case of brute forcing a range of point values, the adversary may be able to achieve an impact without targeting a specific point. In the case where a single point is targeted, the adversary may be able to generate instability on the process function associated with that particular point.

Procedure Examples

ID	Name	Description
S0604	Industroyer	The Industroyer IEC 104 module has 3 modes available to perform its attack. These modes are range, shift, and sequence. The range mode operates in 2 stages. The first stage of range mode gathers Information Object Addresses (IOA) and sends select and execute packets to switch the state. The second stage of range mode has an infinite loop where it will switch the state of all of the previously discovered IOAs. Shift mode is similar to range mode, but instead of staying within the same range, it will add a shift value to the default range values. [1]
S1072	Industroyer2	Industroyer2 can iterate across a device's IOAs to modify the ON/OFF value of a given IO state.[2][3]

Targeted Assets

ID	Asset
A0007	Control Server
A0002	Human-Machine Interface (HMI)
A0005	Intelligent Electronic Device (IED)
A0003	Programmable Logic Controller (PLC)
A0004	Remote Terminal Unit (RTU)
A0010	Safety Controller

Mitigations

ID	Mitigation	Description
M0937	Filter Network Traffic	Allow/denylists can be used to block access when excessive I/O connections are detected from a system or device during a specified time period.
M0807	Network Allowlists	Utilize network allowlists to restrict unnecessary connections to network devices (e.g., comm servers, serial to ethernet converters) and services, especially in cases when devices have limits on the number of simultaneous sessions they support.
M0930	Network Segmentation	Segment operational assets and their management devices based on their functional role within the process. Enabling more strict isolation to more critical control and operational information within the control environment. [4][5][6][7]
M0813	Software Process and Device Authentication	Devices should authenticate all messages between master and outstation assets.

Detection

ID	Data Source	Data Component	Detects
DS0015	Application Log	Application Log Content	Some asset application logs may provide information on I/O points related to write commands. Monitor for write commands for an excessive number of I/O points or manipulating a single value an excessive number of times.
DS0029	Network Traffic	Network Traffic Content	Monitor network traffic for ICS functions related to write commands for an excessive number of I/O points or manipulating a single value an excessive number of times.
DS0040	Operational Databases	Process History/Live Data	Monitor operational process data for write commands for an excessive number of I/O points or manipulating a single value an excessive number of times. This will not directly detect the technique's execution, but instead may provide additional evidence that the technique has been used and may complement other detections.

Figure 17: Example on MITRE ATT&CK for ICS mitigation and detection strategies for technique Brute Force I/O (MITRE, n.d.b)

As a footnote, ready-made standard mitigation technique libraries also exist, such as MITRE D3FEND. When utilizing MITRE ATT&CK or ATT&CK for ICS, technical security controls and mitigation measures can be cross-referenced and added to analysis, on top of the existing mitigation and detection suggestions provided by the MITRE frameworks themselves. It should be noted that the presented defense library is not CPS specific and may not cater to every mitigation scenario, requiring custom mitigation or other sources.

4.5 Framework for model validation

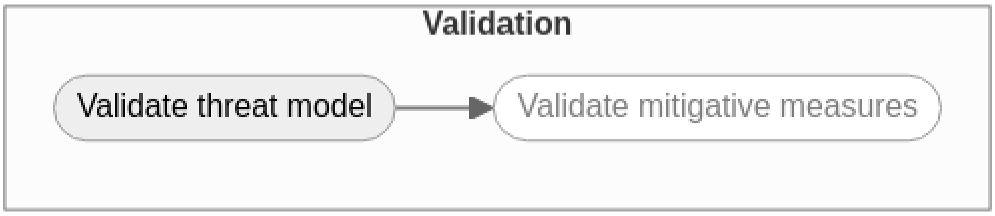
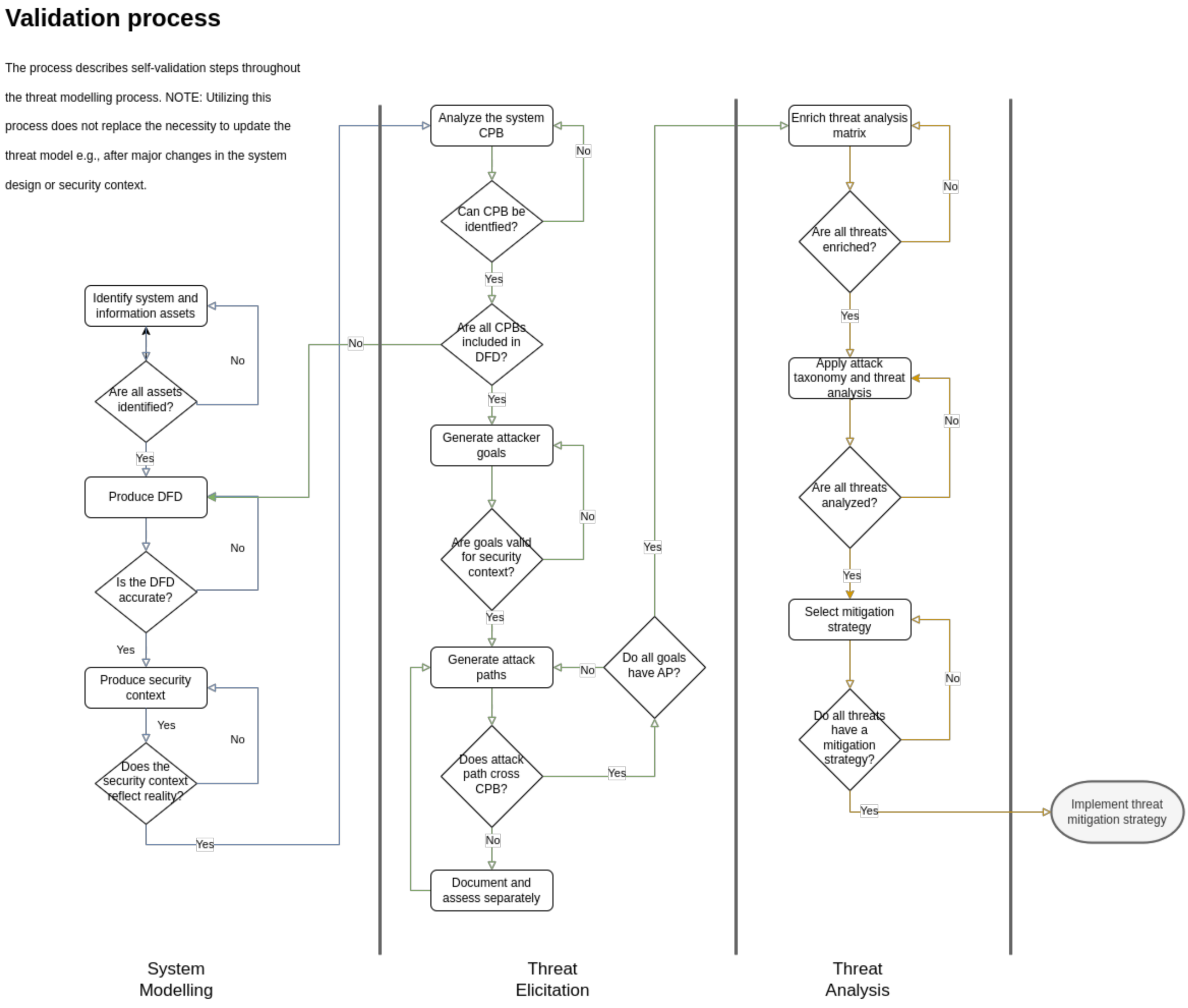


Figure 18: Steps to validate the threat model and corrective actions.

The aim of the model validation is to deduce whether the threat model accurately represents the system it was conducted for. According to Shostack (2014), validation of the produced threat model should be conducted to assess how well the designed model reflects reality. This can be done with constant re-evaluation cycle throughout the threat modelling process.

Iterative re-evaluation of the threat model is based on the approach used by Khalil et al. (2023), adapted for the process defined for this thesis. Self-validation is done as per described by the following figure.



Validation process

The process describes self-validation steps throughout the threat modelling process. NOTE: Utilizing this process does not replace the necessity to update the threat model e.g., after major changes in the system design or security context.

Identify system and information assets
Are all assets identified?
No
Yes
Produce DFD
Is the DFD accurate?
No
Yes
Produce security context
Yes
Does the security context reflect reality?
No
Yes
Analyze the system CPB
Can CPB be identfied?
No
Yes
Are all CPBs included in DFD?
No
Yes
Generate attacker goals
Are goals valid for security context?
No
Yes
Generate attack paths
Does attack path cross CPB?
Yes
No
Document and assess separately
Do all goals have AP?
No
Yes
Enrich threat analysis matrix
Are all threats enriched?
No
Yes
Apply attack taxonomy and threat analysis
Are all threats analyzed?
No
Yes
Select mitigation strategy
Do all threats have a mitigation strategy?
No
Yes
Implement threat mitigation strategy
System Modelling
Threat Elicitation
Threat Analysis

Figure 19: Self-evaluation cycle for the proposed approach

This thesis does not contain the validation process of implemented threat mitigation or other threat addressing actions. This must be done separately according to the change management or system design process of the target system in question.

5 Analysis and discussion

Following chapters describe observations and analysis of conducted research, divided in topical sections:

- Analysis of research problem and research design. (5.1)
- Observations during and after the solution construction. (5.2)
- Analysis on implementing the requirements set for the solution. (5.3)
- Analysis on reliability and applicability of the solution. (5.4)
- Analysis on research ethicality. (5.5)

5.1 Research objectives and methodology

Research was conducted to answer the question, *"(**RQ1)** How can a generic threat modelling approach be produced to enable modeling of cyber-physical threats?" and based on this, "**(RQ2)** can a reference library of threat patterns or threat types be generated to support threat identification process for cyber-physical systems?"* The thesis proposes a generic methodology to 1) identify cyber-physical boundaries within target system using conventional system modelling methods, 2) elicit cyber threats from target system which propagate their effect over the identified boundary and 3) provide tools and process for analyzing the elicited threats. Primary research question is addressed by the solution construct, i.e., proposed methodology.

Secondary research question of "**(RQ2)** *can a reference library of threat patterns or threat types be generated to support threat identification process for cyber-physical systems?*" is partially addressed by the solution construct, but not resolved in full. Various aspects of threat taxonomy and threat type categorization is discussed both in literature review (see 3.1 and 3.3), and solution construct (see 4.4). The proposed methodology does not however produce a generic threat taxonomy or categorization matrix, but rather provides an option to select the most suitable attack taxonomy for the purpose.

The methodology was formulated exploiting constructive research method, implementing steps based on method adapted from the processes of Kasanen et al. (1993) and Lehtiranta et al. (2015, p. 98), outlined in Figure 2. This thesis research omitted the demonstration of solution feasibility, i.e., the solution was not tested in practice. Decision of omission was based on the scope of the thesis, as well as challenges to find a representative test-case of cyber-physical system matching the schedule of the thesis.

The proposed methodology must be tested against in a real-life scenario to conclusively prove its validity, to refine the approach improving generic adoptability, and to identify limitations in the proposed approach. Furthermore, demonstrating a tangible use-case will with high confidence yield development suggestions and insights which cannot be attained in simulated scenario. Test-case study as described by constructive research method utilized in this thesis (see chapter 2) is recommended.

5.2 Observations

The main goal of threat modelling is to elicit relevant and feasible threats in target system to address the risks posed by those threats. Structured approaches serve to provide focus, and to provide consistent process for the assessment and analysis. The proposed solution aligns with general threat modelling process, combining frameworks to achieve the capability of identifying cyber-physical threats. Similarity of the approach can be assessed by comparing Figure 3 and Figure 6.

System modelling of a complex CPS is a tremendous task and many industries rely heavily on industry specific documentation requirements and approaches. A generic CPS modelling approach is hard to achieve, exemplified by Humayed et al. (2017) with alternative approaches presented by Kim et al. (2022) and Duo et al. (2022). In current situation, more efficient approach to implement the cyber-physical boundary analysis as part of dataflow diagrams required by the proposed solution would be to incorporate the necessary details to industry specific documentation convention, when the solution is applied in practice.

Regarding the definition of cyber-physical boundary in system as part of CPB analysis (4.3.2), defining such boundary may not be trivial. Proposed solution relies heavily on the CPB definition, but acknowledges that in some scenarios (e.g., proprietary vendor technology, licences and contractual requirements, lack of documentation or lack of expert information) needed information to accurately draw the boundary is not available. The definition of cyber and physical components can also be unambiguous in some cases. More refinement is required to accurately define the component classification and as a result, CPB in each scenario. For example, defining definition listing and examples on physical and cyber components can make the CPB analysis more approachable for threat modelling participants who have no previous experience in such exercise or CPB analysis.

Utilizing the Attack Tree Analysis for threat elicitation process is not without its limitations. As an attacker-oriented approach, several built-in limitations have been outlined in literature e.g., by Shostack (2014, p. 40-41). Setting of attacker goals may not be trivial for complex systems, especially of the threat actor cannot be narrowed down. Even when the attacker can be identified, in real life scenario attacker can be opportunistic and select a different goal than that chosen for the threat modelling scenario. This is a recognized weakness of the approach (Shostack, p. 41). Fault Tree Analysis on the other hand does not rely on attack goal definition like attack trees, making them less prone to guesswork and more focused on the systems capabilities. Similarly to Attack Tree Analysis, the method tends to be hard to scale especially in complex systems, but utilizing the focusing method provided by this methodology could be used in more restricted manner. Acknowledging these limitations, Fault Tree Analysis could make a good candidate for a threat elicitation method, especially among those participants and target groups more familiar with the methodologies used in security engineering.

Chapter 4.3.3 describing the goal generation provides an approach to counteract the challenge of setting relevant attacker goals, by focusing on components on cyber-physical boundary for physical-to-cyber (*consequence is in cyber domain)* threats, and physical component capabilities for cyber-to-physical threats (*consequence is in physical domain*). During the solution construct it was observed that cyber-to-physical threats are more challenging than their counterparts to identify using the proposed solution. This is interpreted to mean that the number of potential attacker actions on a node is higher than those of the capabilities of physical components. In other words, physical components in CPS operate usually small subset of actions, where cyber components often offer attacker various options to perform further steps. If MITRE ATT&CK for ICS is used as an input for ideas when defining attacker goals, impact category can provide insights especially for physical attack goals.

Properly selected threat taxonomy can help elicitation of threats and help the adoption of threat modelling approach, but generic taxonomies can yield similar results depending on the available details and expertise of the threat modelling participants. Proposed methodology uses MITRE ATT&CK for ICS as an example of generic attack taxonomy, but it may not be suitable for all use-cases; Care should be taken to avoid overreliance on attack taxonomies when utilizing them outside of the purpose for which they have been originally developed.

5.3 Requirement implementation

Requirements were set for the proposed methodology based on literature review defined in chapter 4.1 are analyzed under following sub-sections.

Selected frameworks are applicable for the CPS systems. The system modelling approach is based on previous research which has successfully utilized their approach for CPS (Humayed et al., 2017; Khalil et al., 2023). Attack Tree Analysis has also been used previously for CPS threat assessment (Shevchenko et al., 2018b). Selected frameworks are capable to identify cyber-physical threats, as well as cyber threats, including MITRE ATT&CK for ICS used for threat analysis. Threats in the physical domain are assessable from the point of view of physical system component capabilities, i.e. what can a malfunctioning or manipulated component achieve in the physical domain. This restricts the possible physical effects that need to be analyzed during the assessment.

The frameworks used as part of the solution are capable for assessing cyber-physical threats. For threats in the cyber-domain, many well-established frameworks are available, including the proposed MITRE attack library (MITRE, n.d.a; MITRE, n.d.b).

Methodology’s ease of adoption and scalability are more debatable issues. Scalability of the frameworks used in the methodologies is possible, although not without its problems. For instance, attack trees are notoriously laborious to produce and can take a lot of work. Dataflow diagrams, or other equivalent documentation of the target system may in many cases exist for other purposes, but documentation suitable for the threat modelling must be sometimes produced for the occasion specifically, increasing the workload of such assessment. Ease of adoption may be improved by the selection of Attack Tree Analysis as a threat elicitation framework, the method being based on Fault Tree Analysis and as such, more familiar to at least some industries utilizing CPS and employing safety engineering practices, such as OT. This only covers part of the field of CPS development and design, making the approach perhaps not as appealing to industries using different types of frameworks as part of their normal development and design processes. Requirement for ease of adoption and scalability should be considered only partially fulfilled by the current state of this methodology but can be somewhat counteracted with selecting different frameworks for threat elicitation.

Common semantics between IT and CPS industries is in moderately increase by the selection if industry-specific frameworks for the proposed methodology. As the approach aims to provide a generic approach, it is challenging to cater all industry specific lingo present under the umbrella of fields utilizing CPS. Especially for threat elicitation and analysis, common language is critical. Attack Tree Analysis is in many ways analogous to Fault Tree Analysis, which may help non-security experts with system design experience to adopt the approach. Used analysis framework (MITRE ATT&CK for ICS) provides an expandable baseline for discussing threat specifics with elements common to many types of CPS, although admittedly not applicable in all situations. In part, unrestrained selection of threat elicitation methodology enabled by the approach can help in more specific use-cases.

Lastly, the frameworks, such as threat elicitation method and threat analysis method are interchangeable within this methodology. For example, STRIDE or DESIST (Shostack, 2014, p. 79-85) can be used in the place of Attack Tree Analysis, if deemed more appropriate for the purpose. DREAD, CVSS (Martins, et al. 2015) or similar frameworks can be used for threat prioritization and risk analysis.

5.4 Reliability and applicability

Proposed methodology conforms to the accepted threat modelling process, incorporating the key steps for such activity. The approach of this thesis has been built on existing frameworks and as individual components of the process can be deemed as dependable. Security industry is constantly developing, and ample research material is available for various areas of interest, including cyber-physical system. The source material used for this thesis is but a minor scratch to the surface in a vast amount of available data. Bias in material selection or absence of critical source material used in the thesis is a risk that must be considered when reviewing and applying the proposed methodology in practice.

The key difference proposed in the thesis's approach compared to other reviewed methodologies lies on the consistent method to identifying cyber-physical boundaries during system modelling (chapter 4.2) and utilizing this information in the threat elicitation and threat analysis (chapters 4.3 and 4.4), as well as scoping the threat modelling process. Identifying the boundaries of cyber-physical interface is not trivial, and relying on the method included in the proposed methodology may yield varying results depending on the level of abstraction of the material and expertise available for modelling the target system.

Proposed methodology's selected framework for threat analysis presented in chapter 4.4.2 provides extensive template for analysing CPS specific threats but may not cater all types of CPS as well. For instance, systems like medical instruments and vehicle systems may find threat areas lacking from the framework, while the framework may contain some areas irrelevant to such systems. MITRE's framework has its merits in the case of generic CPS analysis, as it provides generic impact category which can be helpful for attacker goal generation and impact assessment regardless of the type of CPS in question.

Generic framework for CPS does not exist based on this thesis literature review and may not even be feasible considering the vast amount of variance of systems under the CPS terminology. Proposed methodology counteracts this by being agnostic of the threat taxonomy and analysis method; more suitable approach to the analysis can be selected when such is identified.

5.5 Ethicality

Thesis research has relied only on publicly available material and implemented according to Code of Responsible Research (JAMK, 2018). It does not contain any interviews, comments, or phrases from individuals outside of literary sources, or material sanctioned non-disclosure agreement. Author of the thesis has to the best of his ability cited the sources with respect. The author has considered that the security is a fast-developing area of research, and each of the referenced study is a product of its own time of publication. The research has not utilized artificial intelligence (AI) assisted tools, such as ChatGPT or OpenAI in any capacity.

References have been supplemented to tables and figures or their descriptive captions, where material is fully or partially generated using source material. Unreferenced content should be considered thesis author's extrapolation and analysis of referenced literature.

Thesis commissioner has been provided an opportunity to comment and affect the thesis content, all feedback cooperatively discussed, and corrections and adjustments implemented where necessary.

6 Conclusions

The thesis proposes a generic threat modeling process to identify cyber-physical threats, which is agnostic of the threat elicitation and threat analysis frameworks, addressing **RQ1**. The key to solution's approach is the identification of boundary between cyber domain and physical domain, and analyzing the threats that transcend between the two. Selected threat elicitation tool, Attack Tree Analysis, provides a convenient illustration and relatively effective way to observe threat propagation over the cyber-physical boundary. Similar results could be achieved e.g. by utilizing Fault Tree Analysis, which could be a viable candidate for threat elicitation of CPS. An interesting future research topic would be utilizing Attack Tree and Fault Tree Analysis in combination, for example by utilizing BDMP formalism as noted by Budde, Kolb and Soelinga (2021, p. 6).

The proposed solution for **RQ1** provides guidance on circumventing part of the inherent problems related to Attack Tree Analysis methodology, such as scoping the threats (by focusing on CPB) and attacker goal definition (by employing the goal definition based on component's functionality). The solution is recommended for threat modelling cyber-physical systems, when the focus of the assessment is on the interaction between physical domain and cyber domain components. The solution is not recommended for scenarios, where inspecting cyber-physical boundary is not in the scope of the assessment, as the approach will not provide additional value or insights compared to other available methodologies.

Cyber-physical threats are often described as threat with potential to cause physical damage, omitting the fact that threats may propagate from physical domain to cyber domain as well. This does not suggest that these types of threats are consistently left unidentified by the methodologies commonly in use for threat modelling of CPS. However, the author of the thesis suggests that physical-to-cyber threats should be included under the terminology more frequently, like they are addressed by the proposed solution **(RQ1)**.

This research did not fully address the secondary research **(RQ2)** question regarding generic threat taxonomy for cyber-physical threats. It is left for future research efforts to investigate whether such framework is feasible and producible in a way which can cater to need of heterogenous family of cyber-physical systems. For now, the thesis results propose case-by-case attack taxonomy selection for the purpose, MITRE ATT&CK for ICS being a formidable candidate for many use cases.

On a general note, threat modelling of cyber-physical systems, or any complex system for that matter, is a complex task to resolve and scaling the tools for the trade remains challenging. To counter the vast amount of work related to attack tree generation, investigating, e.g., artificial intelligence's capabilities to automate generation of attack trees based on structurally formatted dataflow diagrams with incorporated cyber-physical boundaries could provide a valuable tool for threat elicitation and analysis in complex systems in the future.

By developing the ways of modelling a system, it would be beneficial to produce a standard approach for modeling the interfaces between cyber and physical domains. Standardizing modelling of the CPB would benefit the industry by enabling development of automated tools for modelling, such as producing or evaluating the dataflow diagrams.

References

Aerospace Corporation. (n.d.). *Space Attack Research & Tactic Analysis (SPARTA).* Aerospace Corporation. Retrieved May 3, 2023 from https://sparta.aerospace.org/

Alcaraz, C., & Zeadally, S. (2013). Critical Control System Protection in the 21st Century. *Computer (Long Beach, Calif.)*, 46(10), 74-83. https://doi.org/10.1109/MC.2013.69

Alladi, T., Chamola, V., & Zeadally, S. (2020). Industrial Control Systems: Cyberattack trends and countermeasures. *Computer communications*, *155*, 1-8. https://doi.org/10.1016/j.comcom.2020.03.007

Allen, J. R., Hodges, F. B., & Lindley-French, J. (2021, April). *Future War and the Defence of Europe*. https://intersecmag.co.uk/wp-content/uploads/2021/05/016-018_Future_war_APR_FINAL_JDW.pdf

Argudo, A., & Mwana, G. N. (2023, March). Cyber-Physical Attack Using High Power RF in Havana, Cuba. In R. L. Wilson & B. Curran (Eds.), *ICCWS 2023 18th International Conference on Cyber Warfare and Security, 18(1), 7-18.* https://doi.org/10.34190/iccws.18.1.961

Aufner, P. (2019). *The IoT security gap: a look down into the valley between threat models and their implementation*. International Journal of Information (2020) 19:3-14. https://doi.org/10.1007/s10207-019-00445-y

Budde, C. E., Kolb, C. & Soelinga, M. (2021, August). Attack trees vs. fault trees: two sides of the same coin from different currencies. In A. Abate & A. Marin (Eds.). *Quantitative Evaluation of Systems. QEST 2021. Lecture Notes in Computer Science*, 12846. Springer, Cham. https://doi.org/10.1007/978-3-030-85172-9_24

Brader, S. (1997). *Key words for use in RFCs to Indicate Requirement Levels*. IETF Request for Comment Nr. 2119. Network Working Group. Retrieved May 10, 2023 from https://datatracker.ietf.org/doc/html/rfc2119

Dang, Q. A., Khondoker, R., Wong, K., & Kamijo, S. (2020). *Threat Analysis of an Autonomous Vehicle Architecture*. https://doi.org/10.1109/STI50764.2020.9350512

de Ruijter, A., Guldenmund, F. (2016). *The bowtie method: A review.* Safety Science, (88), 211-218. https://doi.org/10.1016/j.ssci.2016.03.001

Duo, W., Zhou, M., & Abusorrah, A. (2022). A Survey of Cyber Attacks on Cyber Physical Systems: Recent Advances and Challenges. *IEEE/CAA journal of automatica sinica*, 9(5), 784-800. https://doi.org/10.1109/JAS.2022.105548

European Telecommunications Standards Institute. (n.d.). *CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements.* ETSI Standard No. EN 303 645 V2.1.1. https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf

EVITA. (2012). *Project summary*. Sevent Research Framework Programme (2007-2013) of the European Community. European Union. https://evita-project.org/publications/EVITAD0.pdf

Federal Office of Information Security. (2015). *The State of IT Security in Germany 2014.* Bundesamt für Sicherheit in der Informationstechnik – BSI. Germany. Retrieved on May 3, 2023 from https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Securitysituation/IT-Security-Situation-in-Germany-2014.pdf?__blob=publicationFile&v=3

Finle, J. (2016, January 8). U.S. firm blames Russian 'Sandworm' hackers for Ukraine outage. *Reuters*. https://www.reuters.com/article/us-ukraine-cybersecurity-sandworm-idUSKBN0UM00N20160108/

Foster, I., Prudhomme, A., Koscher, K., & Savage, S. (2015*). Fast and vulnerable: A story of telematic failures*. In 9th {USENIX} Workshop on Offensive Technologies ({WOOT} 15). https://www.usenix.org/system/files/conference/woot15/woot15-paper-foster.pdf

Gerla, M. & Reiher, P. (2016). Securing the Future Autonomous Vehicle: A Cyber-Physical Systems Approach. In A. K. Pathan (Eds.), *Securing Cyber-Physical Systems* (chapter 7). Taylor & Francis https://doi.org/10.1201/b19311

Greiman, V. (2023, February). *Nuclear Cyber Attacks: A Study of Sabotage and Regulation of Critical Infrastructure.* In In R. L. Wilson & B. Curran (Eds.), *International Conference on Cyber Warfare and Security*, *18(1)*, *103-110*. https://doi.org/10.34190/iccws.18.1.1042

Google. (n.d.). *Google Scholar*. Google Inc. https://scholar.google.com

Guo, J., Li, K., Li, L. & Wang, J. (2022). Cyber-Physical System-Based Path Tracking Control of Autonomous Vehicles under Cyber-Attacks, *IEEE Transactions on Industrial Informatics*, 2022. https://doi.org/10.1109/TII.2022.3206354

Heartfield, R., Loukas, G., Budimir, S., Bezemskij, A., Fontaine, J. R., Filippoupolitis, A., & Roesch, E. (2018). A taxonomy of cyber-physical threats and impact in the smart home. *Computers & security*, 78, 398-428. https://doi.org/10.1016/j.cose.2018.07.011

Hollinger, P. (2018, October 17). *Can your flight be hacked?* The Financial Times. https://www.ft.com/content/2e416eca-4e3d-11e8-ac41-759eee1efb74

Hussain, S., Kamal, A., Ahmad, S., Rasool, G., & Iqbal, S. (2014). *Threat modelling methodologies: a survey*. Sci. Int.(Lahore), 26(4), 1607-1609.

Humayed, A., Lin, J., Li, F., & Luo, B. (2017). *Cyber-Physical Systems Security-A Survey*. IEEE internet of things journal, 4(6), 1802-1831. https://doi.org/10.1109/JIOT.2017.2703172

International Atomic Energy Agency. (2011). Computer Security at Nuclear Facilities. IAEA Nuclear Security Series No. 17. Retrieved May 4, 2023 from https://www.iaea.org/publications/8691/computer-security-at-nuclear-facilities

International Atomic Energy Agency. (2021). Computer Security for Nuclear Facilities. IAEA Nuclear Security Series No. 42-G. Retrieved May 4, 2023 from https://www.iaea.org/publications/13629/computer-security-for-nuclear-security

International Association of Classification Societies. (2022a). *UR 26 Cyber Resilience of Ships*. IACS Req. 2022. Retrieved May 3, 2023 from https://iacs.org.uk/download/14104

International Association of Classification Societies. (2022b). *UR 27 Cyber resilience of on-board systems and equipment*. IACS Req. 2022. Retrieved May 3, 2023 from https://iacs.org.uk/download/14105

International Organization for Standardization. (2022a). *Information security, cybersecurity and privacy protection — Information security management systems — Requirements* (ISO Standard No. 27001:2022). https://www.iso.org/standard/82875.html

International Organization for Standardization. (2022b). *Information security, cybersecurity and privacy protection — Guidance on managing information security risks* (ISO Standard No. 27005:2022). https://www.iso.org/standard/80585.html

International Organization for Standardization. (2018). *Information technology — Security techniques — Information security management systems — Overview and vocabulary* (ISO Standard No. 27000:2018). https://www.iso.org/standard/73906.html

International Society of Automation. (n.d*). List of All ISA Standards*. International Society of Automation. Retrieved March 10, 2023 from https://www.isa.org/standards-and-publications/isa-standards/list-of-all-isa-standards

Jamil, A., ben Othmane, L., & Valani, A. (2021). *Threat Modeling of Cyber-Physical Systems in Practice*. https://doi.org/10.1007/978-3-031-02067-4_1

JAMK. (2018, December 11). *Ethical Principles for JAMK University of Applied Sciences Approved by the Student Affairs Board on 11 Decem*ber 2018. JAMK University of Applied Sciences. Retrieved on April 8, 2024 from https://www.jamk.fi/fi/file/ethical-principles

Janet. (n.d.). *Jamk University of Applied Sciences Online Library*. Jyväskylä University of Applied Sciences (JAMK). https://janet.finna.fi

Juutilainen, J. (2022). *Cyber Warfare: A Part of the Russo-Ukrainian War in 2022*. Jyväskylä University of Applied Sciences [Master's thesis, JAMK University of Applied Sciences]. Theseus. https://urn.fi/URN:NBN:fi:amk-2022092620438

Kaneko, T., Takahashi, Y., Okubo, T., & Sasaki, R. (2018). Threat analysis using STRIDE with STAMP/STPA. In The international workshop on evidence-based security and privacy in the wild (p. 10-17). https://ceur-ws.org/Vol-2809/WESPr-18_02.pdf

Kasanen, E., Lukka, K., & Siitonen, A. (1993). The constructive approach in management accounting research. Journal of management accounting research, 5, 243. Retrieved May 4, 2023 from https://www.proquest.com/scholarly-journals/constructive-approach-management-accounting/docview/210177084/se-2

Khalil, S. M., Bahsi, H., Dola, H. O., Korõtko, T., McLaughlin, K., & Kotkas, V. (2023). Threat Modeling of Cyber-Physical Systems - A Case Study of a Microgrid System. *Computers & security*, 124, 102950. https://doi.org/10.1016/j.cose.2022.102950

Khan, R., McLaughlin, K., Laverty, D., & Sezer, S. (2017). *STRIDE-based threat modeling for cyber-physical systems*. https://doi.org/10.1109/ISGTEurope.2017.8260283

Kim, K. H., Kim, K., & Kim, H. K. (2022). STRIDE-based threat modeling and DREAD evaluation for the distributed control system in the oil refinery. *ETRI journal*, 44(6), 991-1003. https://doi.org/10.4218/etrij.2021-0181

Kim, S., Park, K., & Lu, C. (2022). *A Survey on Network Security for Cyber-Physical Systems: From Threats to Resilient Design*. IEEE Communications surveys and tutorials, 24(3), 1534-1573. https://doi.org/10.1109/COMST.2022.3187531

Kumar, S.A.P & Xu, B. (2017). Vulnerability for Security in Aviation Cyber-Physical Systems. *IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud)*, 145-150. https://doi.org/10.1109/CSCloud.2017.17

Laari, T. (Ed.). (2019). #kyberpuolustus [#cyberdefence]. Helsinki: Maanpuolustuskorkeakoulu.

Laeeq, K. & Shamsi, J. A. (2015). A Study of Security Issues, Vulnerabilities, and Challenges in the Internet of Things. In A. K. Pathan (Eds.), *Securing Cyber-Physical Systems* (chapter 8). Taylor & Francis https://doi.org/10.1201/b19311

Langner, M. (2013). *To kill a centrifuge*. The Langner Group. Retrieved May 2, 2023, from https://www.langner.com/wp-content/uploads/2017/04/To-kill-a-centrifuge.pdf

Lehtiranta, L., Junnonen, J., Kärnä, S. & Pekuri, L. (2015). The Constructive Research Approach: Problem Solving for Complex Projects. In B. Pasian, & R. Turner (Eds.). *Designs, Methods and Practices for Research of Project Management* (p. 95-106). Taylor & Francis Group. https://doi.org/10.4324/9781315270197-20

Lehto, M. (2022, March). APT cyber-attack modelling – building a general model. *ICCWS 2022 17th International Conference on Cyber Warfare and Security, 121-129*. https://doi.org/10.34190/iccws.17.1.36

Lightman, S., Suloway, T. & Brule, J. (2022). *Satellite Ground Segment – Applying the Cybersecurity Framework to Satellite Command and Control*. NIST Interagency Report 8401 (NIST IR). https://doi.org/10.6028/NIST.IR.8401

LINDDUN. (n.d.). LINDDUN Pro Privacy Engineering Framework. Retrieved May 8, 2023 from https://linddun.org/instructions-for-pro/

Liu, A., Liyanage, K. & Sefanov, A. (2016). ICT Modeling for Cosimulation of Integrated Cyberpower Systems. In A. K. Pathan (Eds.), *Securing Cyber-Physical Systems* (chapter 2). Taylor & Francis https://doi.org/10.1201/b19311

Liu, Y., Peng, Y., Wang, B., Yao, S., & Liu, Z. (2017). Review on Cyber-physical Systems. *IEEE/CAA journal of automatica sinica*, 4(1), 27-40. https://doi.org/10.1109/JAS.2017.7510349

Lockheed Martin. (n.d.). The Cyber Kill Chain. Retrieved March 10, 2024 from https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.htmlKill

Maglaras, L., Kantzavelou, I., & Ferrag, M. A. (2021). *Digital Transformation and Cybersecurity of Critical Infrastructures*. Applied sciences, 11(18), 8357. https://doi.org/10.3390/app11188357

Martins, G., Bhatia, S., Koutsoukos, X., Stouffer, K., Tang, C., & Candell, R. (2015*)*. Towards a systematic threat modeling approach for cyber-physical systems. *2015 Resilience Week (RWS).* 1-6. https://doi.org/10.1109/RWEEK.2015.7287428

Microsoft. (2022, August 25). *Getting started with the Threat Modeling Tool*. Retrieved May 8, 2023 from https://learn.microsoft.com/en-us/azure/security/develop/threat-modeling-tool-getting-started

MITRE ATT&CK. (n.d.a). *A knowledge graph of cybersecurity countermeasures*. MITRE Corporation. Retrieved March 9, 2023, from https://attack.mitre.org/

MITRE ATT&CK for ICS. (n.d.b). ICS Matrix. MITRE Corporation. Retrieved March 9, 2024, from https://attack.mitre.org/matrices/ics/

MITRE D3FEND. (n.d.c). *A knowledge graph of cybersecurity countermeasures*. MITRE Corporation. Retrieved March 9, 2023, from https://d3fend.mitre.org/

Ministry of Foreign Affairs of Finland. (n.d.). *Information security auditing tool for authorities – Katakri*. Finland. Retrieved May 2, 2023, from https://um.fi/information-security-auditing-tool-for-authorities-katakri

National Institute of Standards and Technology. (2023). *Guide to Operational Technology (OT) Security*. NIST Special Publication 800-82 Revision 3. https://doi.org/10.6028/NIST.SP.800-82r3

National Institute of Standards and Technology. (2020). *Security and Privacy Controls for Information Systems and Organizations*. NIST Special Publication 800-53 Revision 5. https://doi.org/10.6028/NIST.SP.800-53r5

National Institute of Standards and Technology. (2011). *Managing Information Security Risk – Organization, Mission and Information System View*. NIST Special Publication 800-39. https://doi.org/10.6028/NIST.SP.800-39

National Institute of Standards and Technology. (n.d.). *Cyber Physical Systems*. National Institute of Standards and Technology. Retrieved March 10, 2023, from https://www.nist.gov/itl/ssd/cyber-physical-systems

Nirmal, J. (2020, November 25). Breach at Kudankulam nuclear plant may have gone undetected for over six months: Group-IB. *The Economic Times*. https://economictimes.indiatimes.com/jobs/hr-policies-trends/why-creating-psychologically-safe-workplaces-is-crucial-for-overall-well-being/articleshow/99845384.cms

Oakley, L., Oprea, A. & Tripakis, S. (2022). Adversarial Robustness Verification and Attack Synthesis in Stochastic Systems. *In 2022 IEEE 35th Computer Security Foundations Symposium (CSF)*. 380-395. https://doi.org/10.1109/CSF54842.2022.9919660

Oyegoke, A. (2011). *The constructive research approach in project management research*. International Journal of Managing Projects in Business, 4(4), 573-595. https://doi.org/10.1108/17538371111164029

Radford, A. (2023, March 21). Journalist opens USB letter bomb in newsroom. *BBC.* https://www.bbc.com/news/world-latin-america-65026522

Ryon, L. & Rice, G. A. (2018). Safety-focused Security Risk Assessment of Commercial Aircraft Avionics. IEEE/AIAA 37th Digital Avionics Systems Conference (DASC). 1-8. https://doi.org/10.1109/DASC.2018.8569314

Pathan, A. K. (2016). *Securing cyber-physical systems.* Taylor & Francis. https://doi.org/10.1201/b19311

Przybylski, T., Sugunaraj, N., & Ranganathan, P. (2023). *A Whitepaper On Aircraft Communication Systems - Topologies, Protocols, and Vulnerabilities By Center for Cyber Security Research (C2SR)* [Whitepaper]. Journal of Network and Computer Applications. https://commons.und.edu/ee-stu/11/

Saini, V. K., Duan, Q., & Paruchuri, V. (2008). *Threat modeling using attack trees*. Journal of Computing Sciences in Colleges 23.4 (2008): 124-131. https://www.researchgate.net/publication/234738557_Threat_Modeling_Using_Attack_Trees

Scandariato, R., Wuyts, K., & Joosen, W. (2015). A descriptive study of Microsoft's threat modeling technique. Requirements engineering, 20(2), 163-180. https://doi.org/10.1007/s00766-013-0195-2

Schneier, B. (1999). *Attack Trees*. Schneier on Security. Retrieved March 12, 2024, from https://www.schneier.com/academic/archives/1999/12/attack_trees.html

Shehod, A. (2016). *Ukraine power grid cyberattack and US susceptibility: Cybersecurity implications of smart grid advancements in the US*. Working Paper CISL #2016-22. Cybersecurity Interdisciplinary Systems Laboratory, MIT. Retrieved May 3, 2023 from https://web.mit.edu/smadnick/www/wp/2016-22.pdf

Shevchenko, N., Frye, B. R. & Woody, C. (2018a) *Threat Modeling for Cyber-Physical System-of-Systems: Evaluation and Recommendations* (Accession No. AD1083907). Defense Technical Information Center. https://apps.dtic.mil/sti/pdfs/AD1084209

Shevchenko, N., Frye, B. R. & Woody, C. (2018b) *Threat Modeling for Cyber-Physical System-of-Systems: Methods Evaluation* (Accession No. AD1083907). Defense Technical Information Center. https://apps.dtic.mil/sti/citations/AD1083907

Shevchenko, N., Chick, T. A., O'Riordan, P., Scanlon, T. P. & Woody, C. (2018c). *Threat modeling: A summary of available methods* [Whitepaper]. Carnagie Mellon University Software Engineering Institute. https://resources.sei.cmu.edu/asset_files/WhitePaper/2018_019_001_524597.pdf

Shostack, A. (2008). Experiences Threat Modeling at Microsoft. MODSEC@ MoDELS, 2008, 35. Retrieved May 10, 2023 from https://adam.shostack.org/modsec08/Shostack-ModSec08-Experiences-Threat-Modeling-At-Microsoft-published.pdf

Shostack, A. (2014). *Threat Modeling: Designing for Security*. John Wiley and Sons.

Shostack, A. (2022, December). *Fast, Cheap and Good: Lightweight Methods Are Undervalued (Preprint)*. arXiv.org. https://doi.org/10.48550/arXiv.2301.03593

Vallant, H., Stojanović, B., Božić, J., & Hofer-Schmitz, K. (2021). Threat Modelling and Beyond-Novel Approaches to Cyber Secure the Smart Energy System. *Applied sciences*, *11(11)*, 5149. https://doi.org/10.3390/app11115149

Voeller, J. G. (Ed.). (2014). *Cyber Security*. John Wiley & Sons, Incorporated.

Wyglinski, A. M., Huang, X., Padir, T., Lai, L., Eisenbarth, T.R., & Venkatasubramanian, K. (2013). Security of Autonomous Systems Employing Embedded Computing an Sensors. *IEEE MICRO*, *33*(1), 80-86. https://doi.org/10.1109/MM.2013.18

Yeh, E., Choi, J., Prelcic, N. G., Bhat, C. R., & Heath, R. W. (2018). *Cybersecurity Challenges and Pathways in the Context of Connected Vehicle Systems* (Report No. D-STOP/2017/134). University of Texas at Austin. Data-Suppoerted Transportation Operations & Planning Center (D-STOP). https://rosap.ntl.bts.gov/view/dot/37194/dot_37194_DS1.pdf

Yin, R. K. (2009). Case study research: Design and methods (Vol. 5). Sage.

Yskout, K., Heyman, T., Van Landuyt, D., Sion, L., Wuyts, K., & Joosen, W. (2020). *Threat modeling: From infancy to maturity*. https://doi.org/10.1145/3377816.3381741

Appendices

Appendix 1. System and Information asset identification examples

The following table will be used to collect identified system assets and information assets. Asset category is either “System,” describing a system component or “Information” describing content of data flows. Asset types have been selected from common DFD elements used in threat modelling (Shostack, 2008, p. 3), contrary to the more specific categorization presented by Khalil et al. (2023) to reduce complexity and provide a more general approach. The right-most column describes the assets cyber-physical interaction according to distinction proposed by Humayed et al. (2017)

Asset Type	*Asset name*	*DFD Type*	*C/P/CP*
Process Type 1	Process 1	Process	C
	Process 2	Process	C
Process Type 2	Process 3	Process	CP
Process Type 3	Process 4	Process	CP
Data Store	Data store 1	Data Store	C
External Entity	External entity 1	External entity	P
External Entity	External entity 2	External entity	CP

Table 6: Example of system asset identification table, adapted from Khalil et al. (2023)

Asset types for information category has been derived from case-study conducted by Khalil et al. (2023) and are presented here as an example. Information asset types should be categorized according to the characteristics of the target system.

Similarly, to system asset types, the table assesses the cyber-physical dimension of the data flow. In this case, an item is cyber-physical if the dataflow crosses cyber-physical trust boundary. It can be either cyber or physical in nature if such a boundary is not crossed. Multiple dimensions can be attached to a single item if the same data flows through distinct types of interactions.

Asset Type	*Data category*	*DFD Type*	*C/P/CP*
Operational Data	Measurement data	Dataflow	P, CP
	Event data	Dataflow	C
	Alarm data	Dataflow	C
Control Data	Control data	Dataflow	C
External Data	External data source	Dataflow	C
Service and Management Data	Configuration, logs, admin access	Dataflow	C

Table 7: Example of information asset identification table, adapted from Khalil et al. (2023)

Appendix 2. Security Context Template

Security context record is a guiding document for threat assessment and should be updated when new information about the system is revealed during the threat modelling process.

This template utilizes an assumption record described by Shostack (2014, p. 136) as a base. The question areas are partially based on the issues mentioned by Khalil et al (2023). Context area and sub-areas are examples and can be freely expanded or altered. As emphasized in the chapters 3.3.3 and 4.2.4, security context can include wide variety of issues specific to target system. Exhaustive listing of all possible areas is out of the scope for this thesis. Context sections in this template are divided in the general DFD diagram element types, supplemented by environmental and resource considerations.

Security context should not only include negative assumptions (e.g., the database has scarce resources to handle only a set amount of process metrics). Positive assumptions (e.g., database has ample resources to handle the process metric) are important to be identified as well as focusing on only on the assumptions where the need of improvement is already identified can lead to misanalysis of the threat impact and needed enhancements to mitigate the threat.

Each assumption should document the impact on assumption failure when feasible, i.e. what are the risks or effects, if event occurs against the assumption. For example, if the assumption regarding a threat actor using a specific tactic to infiltrate the system than expected, what can be the consequence?

Security controls already in place within the system should be added to attack tree analysis.

Context Area	**Context sub-area**	**Context assumptions** *(directing questions included)*	**Impact on assumptior failure**	**Security controls in place** *(in design or implementation)*	**DFD element(s** *(Use an ID for easier identification)*	**Notes** *(additional information for interpretation included)*
Trusted external entities	Users	*What are legitimate user groups and what level of access each group have? Which components legitimate users have access to?*	-	-	-	-

		What user groups can access the system remotely, how, and which component?				
	Technical accounts	*What technical user accounts /group are present in the system?* *What technical user accounts/groups access the system remotely (API, integration, etc.)? What level of access do they have in system?*	-		-	-
Environment	Physical interaces	*Who can physically access the system components? Where is the system / component located? What kind of physical interfaces does the system have (human-machine interfaces, external ports, etc.)?*	-	-	-	*Physical interfaces are important to be identified to enumerate physical entry points to the system.*
	Location	*Where is the system located (Country, Area, etc.)? Is the system or any of its components physically movable during normal operation, e.g. a vehicle?*	-	-	-	
Untrusted external entities	Threat actors	*Are there an identifiable threat actor who has interest in the target system? Can threat actor capabilities be assessed? Can threat actor's targets of interest be identified?*	-	-	-	List of identified threat actors, enriched with analysis of their potential targets, capability and used tactics, techniques and procedures (TTP) if feasible.
	Other entities	*Are there untrusted external entities other than threat actors that can be identified? What kind of access are they expected to attempt?*	-	-	-	
Processes an dataflows	Data flows	*Does the system accept untrusted data flows as part of functionality? Does the system send data to untrusted destination via untrusted networks?*	-	-	-	
	System processes	*Are the processes of system overridable? By whom?*	-	-	-	
Resilience an resources	System resources	*Are there resource constraints within the system (computing resources, network resources, etc.)?*	-	-	-	

	System resilience	*Are there identifiable single points of failures within the system?*	-	-	-	*I.e., are there any component physical or virtual, that would cause the system to halt key operation or reduce functionality when component is unavailable?*
		Which system components are resilient in virtual or physical configuration?	-	-	-	*E.g., are there hot-spare hardware or logic*
		Are system components responsible for controlling physical processes capable of operation even when disconnected from upstream control services? For how long?	-	-	-	*E.g., does the system controlling the physical process keep maintaining the process according to last known parameters when upstream control service is unavailable?*

Table 8: Template for security context recording adapted from Shostack (2014, p. 136) and Khalil et al. (2023)

The following table presents an example of entries for such record.

Context Area	**Context sub-area**	**Context assumptions**	**Impact on assumption failure**	**Security controls in place**	**Notes**
Untrusted external entitites	Threat actors	APT28 has targeted similar systems previously with identifiable tactics, techniques and procedures (TTP).	APT attack uses a different TTP than ATP28.	N/A	Threat model should include ATP28 favored attack types.
Resilience and resources	System resilience	Control network has the capability to withstand spikes in network traffic.	Unavailability of the relay control network if the traffic volume exceeds the network bandwidth.	Automatic traffic shaper, prioritizing critical component communication. Network requires device authentication.	Physical process components can operate independently with last known configuration.

Table 9: Example of security context records.

Appendix 3. Threat Analysis Matrix

The following table template can be used to enumerate the identified threats for analysis and mitigation planning. The matrix has been adapted from Shostack's threat enumeration table (2014, p. 134-135), expanded with fields to assist design and implementation follow-up of mitigative measure, and cyber-physical impact assessment to support the focus of the proposed methodology Heartfield et al. (2018).

The ID column can be selected freely as suitable for the organization and target system in question.

The asset column should include the name of the asset or if asset identification matrix like the one presented in Appendix 2 is use, ID of the information and system asset to identify the row for specific dataflow diagram element.

The threat type should be selected from the selected attack taxonomy. Proposed methodology uses MITRE ATT&CK for ICS, where the type is selected from attack tactic column. The used framework also provides an ID for the tactics, allowing easier mapping in later analysis or mitigation planning, for example TA0106 for Impair Process Control (MITRE, n.d.b). When other frameworks than MITRE is used, suitable type should be selected according to the frameworks approach.

The threat column should indicate what is the actual threat. For example, "unsensitized input can be used to cause unintended outcomes for asset A data transform process". MITRE framework can provide input for this column in form of technique name (e.g., T0836 for Modify Parameter), supplemented with system specific details.

Impact can be assessed in the separate column, and column for impact CP analysis can be used to assess whether the consequence of the realized threat is in the cyber or physical domain. Concretely, this means whether the attack causes physical effects e.g., by altering a physical process.

Finally, the mitigation follow-up ID is used for later tracking of the mitigative measure implementation, for example in through change management system or system design process. Template for the threat analysis is presented in Table 10.

ID	Asset	Threat Type	Threat	Assessed impact	Impact CP analysis	Security context notes	*Mitigation*	Mitigation follow-up ID
Threat ID (freely selected)	*Asset name or ID from DFD*	*Type according to attack taxonomy.*	*Threat in detail, enriched with information e.g., from attack taxonomy, other external sources, and system specific details.*	*What happens when the threat is realized?*	*C = Cyber, P = Physical*	*Additional information derived from security context.*	*Bried description of mitigation strategy.*	*Mitigation implementation follow-up issue ID (freely selected)*

Table 10: Template for threat analysis matrix, adapted from approach by Shostack (2014, p. 134-135) and Heartfield et al. (2018).

Table 11 contains an example of threat analysis entries based on the Attack Tree presented in Figure 15.

ID	Asset(s)	Threat Type	Threat	Assessed impact	Impact CP analysis	Security context notes	*Mitigation*	Mitigation follow-up ID
T0812	*A01, A04*	*Lateral movement*	*Default credentials used to access device.*	*Attacker can access the system component, gaining foothold or expand laterally.*	*C*	*-*	*Ensure default credentials are changed in HMI/PLC.*	*MIT-01*
T0819	*A05*	*Initial access*	*Public facing application exploited.*	*Attacker can access the system component, gaining foothold or expand laterally.*	*C*	*PLC comms. module is in restricted network.*	*Ensure all security updates are applied, audit the network implementation and edge gateway where PLC is connected.*	*MIT-02*
T0821	*A04*	*Execution*	*Modify PLC tasking configuration.*	*Task schedule is manipulated, or malicious tasks added.*	*CP*	*-*	*PLC integrity should be checked periodically, preferably in an*	*MIT-03*

				Actuators work unintentionally.			*automated manner.*	
T0831	*A02*	*Impact*	*Actuator control traffic is manipulated*	*Attacker achieves goal of manipulating actuator control traffic, altering the process in an unintentional manner. Process is disrupted, possible physical damage.*	*P*	*Process safety ensured by SIS.*	*Safety instructions and safety measures around actuator-controlled process physical space will be reviewed and trained to all personnel accessing the space. Threat modelling of SIS in the scope of the actuator must be conducted. Further controls to prevent and mitigate threat shall be investigated.*	*MIT-04*
T0836	*A04*	*Impair process control*	*Parameter(s) controlling safe process thresholds might be altered, invalid parameters may be introduced, or existing parameters changed.*	*Attacker gains capability to execute arbitrary control commands to actuators, potentially circumventing security controls of PLC otherwise in place.* *See T0831* *Additionally, changing safety thresholds may increase impact of physical damage.*	*CP*	*Process safety ensured by SIS.*	*PLC capability to validate program inputs must be verified for additional information. Integrity of PLC firmware and configuration must be regularly checked. Threat modelling of SIS in the scope of the actuator must be conducted.*	*MIT-05*
T0847	*A04*	*Initial access*	*Removable data device with malicious content.*	*Malware or tailored malicious software may cause unavailability of PLC hindering process control or cause changes in process control if expanded on*	*C*	*Requires physical access to PLC equipment room.*	*Disabling autorun features on PLC and other components should be investigated. USB and other data capable interfaces must be disabled physically or on OS level, or access must be restricted to*	*MIT-06*

				by the attacker.			*allowed personnel only.*	
T0848	*A04*	*Initial access*	*Control data accepted from rogue control server. Legitimate looking traffic is sent from spoofed control server.*	*Attacker can gain capability to issue control commands without establishing a foothold to any system components.* *Can lead to T0831*	*C*		*PLC must accept connections from only allowed hosts. Network filtering must restrict traffic to allowed hosts only. Network monitoring rules must be created to identify unknown connections and abnormal traffic to PLC.* *Threat modelling of edge gateway devices must be expanded.*	*MIT-07*
T0855	*A01, A04*	*Impair process control*	*Unauthorized, legitimate command message is sent from affected device to alter process controller by actuators.*	*See T0831*	*CP*	*Requires local or network access (A01, A04)*	*Communication to assets connected to actuators must be authenticated e.g. by MAC address. Network filtering must deny all unknown traffic, PLC control network must implement strict segmentation, Actuators should validate input before implementing if feasible.*	*MIT-08*
T0864	*A01, A05*	*Initial access*	*Transient cyber asset in network allows attacker to gain access to system components via unconventional access points (i.e., outside of control rooms and defined operator access stations).*	*Attacker can access the system component, gaining foothold or expand laterally.*	*C*	*Requires physical access to site or site's proximity (wireless networks).*	*All transient assets, e.g. maintenance laptops and other similar authorized devices must be documented and connecting them to the network must be done according to approved schedule, notifying the security monitoring team. All unauthorized device connections in*	*MIT-09*

							network(s) must be monitored. When feasible, all network traffic must be encrypted to protect data integrity and confidentiality.	
T0866	A01, A05	Initial access	Public facing service vulnerability is exploited.	Attacker can access the system component, gaining foothold or expand laterally.	C	PLC comms. module and HMI are not in fact “public facing”; PLC offers remote services which over networks implemented on public network (VPN or mobile broadband, via edge gateway). HMI is connected to site’s management network. I.e., requires access to local network.	Unnecessary network services shall be disabled on affected devices, Network filtering and segmentation must be audited. All software on system components offering remote services must be kept up to date with security patches regularly.	MIT-10
TC01	A04	Execution	Field device type specific attack tailored against site A system design is	Attacker gains capability to execute arbitrary control commands to actuators, potentially circumventing security controls of PLC otherwise in place.	CP	Can lead to T0831. Can also cause hard to detect changes over long period of time.	Requires modified firmware or tasking of PLC.	MIT-11

Table 11: Example of threat analysis matrix (*based on Figure 15*). Threat IDs, threat types, assessed impacts and mitigations are partially enriched with MITRE ATT&CK of ICS (MITRE, n.d.b).