Master's thesis

NTNU
Norwegian University of Science and Technology
Faculty of Information Technology and Electrical Engineering
Department of Engineering Cybernetics

Kristine Sørum Bakken

Application of Combined Safety and Cybersecurity Risk Analysis of Industrial Automation and Control Systems

Master's thesis in Cybernetics and Robotics
Supervisor: Mary Ann Lundteigen
Co-supervisor: Knut Øien & Lars Flå
June 2023

NTNU
Norwegian University of
Science and Technology

Kristine Sørum Bakken

Application of Combined Safety and Cybersecurity Risk Analysis of Industrial Automation and Control Systems

Master's thesis in Cybernetics and Robotics
Supervisor: Mary Ann Lundteigen
Co-supervisor: Knut Øien & Lars Flå
June 2023

Norwegian University of Science and Technology
Faculty of Information Technology and Electrical Engineering
Department of Engineering Cybernetics

NTNU
Norwegian University of
Science and Technology

Preface

This report is a 30 credits master thesis, completed as a part of the study program Cybernetics and Robotics in the Department of Engineering Cybernetics (ITK) at the Norwegian University of Science and Technology (NTNU). The work was carried out during the spring of 2023.

The supervisor is NTNU Professor Mary Ann Lundteigen, from the Department of Engineering Cybernetics. The co-supervisors are Knut Øien and Lars Flå from Sintef. The project is associated with the research project Cybersecurity Barrier Management (CBM).

The work is focused on safety and cybersecurity risk analysis of operational technology. It will regard relevant concepts, frameworks and international standards. Additionally, two relevant OT cyberattack will be presented.

Acknowledgments

I want to thank my supervisor, Mary Ann Lundteigen, for her continuous guidance and support; her positive and caring nature has been an encouragement throughout this process. I am so grateful to Øystein, my rock, and a never-ending source of comfort, laughter, and food, lots of food. A big thank you to Hannah, who has not only endured living with me for five years, but also made our "samboerskap" one of the highlights of my time in Trondheim. I am eternally grateful for your unwavering friendship. A huge thank you to Sif and AJ; having these wonderful girls in my corner got me through some of the hardest parts of my studies. Lastly, I want to thank my amazing family, Mamma, Pappa, Håkon, and Thomesine. I finally also have the ring!

Summary

Safety and cybersecurity risk analysis in Industrial Automation and Control Systems (IACS) involves assessing and managing the potential risks and threats that can impact the safety and security of critical industrial processes. It encompasses identifying, evaluating, and mitigating vulnerabilities, hazards, and potential incidents that could lead to loss of availability, integrity, or confidentiality.

In past years there have been cybersecurity attacks on Operational Technology (OT) that demonstrate the potential safety risk that stems from cyberattacks, like the attack on the Oldsmar water treatment facility and the TRISIS malware. Safety and cybersecurity have traditionally been regarded as separate fields of study. For each, there has been developed international standards and risk analysis methods. The increasing interconnectivity between OT and information technology (IT) systems has created new ways for cyber threats to impact the safety and functionality of industrial processes. This growing integration necessitates a holistic approach to risk analysis that considers both safety and cybersecurity in combination, ensuring comprehensive protection against emerging threats in complex and interconnected environments.

New combined standards and methods address the risk associated with increased interconnectivity. One such standard is the ISA *84.00.09 Cybersecurity Related to the Functional Safety Lifecycle*. ISA TR 84.00.09 emphasizes the importance of integrating cyber risk into the analysis of industrial processes, addressing the historical ignorance of cyber-related attacks. A method for combined safety and cybersecurity analysis is the Uncontrolled Flows of Information And Energy (UFoI-E) causality concept and its use of the Cyber-Physical Harm Analysis for Safety and Security (CyPHASS) scenario builder. UFoI-E views uncontrolled information and/or energy flows as risks in a Cyber-Physical System (CPS). CyPHASS is a scenario builder tool that organizes risks graphically and offers a comprehensive database of potential risk sources and prevention measures. Consequence-driven Cyber-informed Engineering (CCE) is another combined safety and cybersecurity risk analysis method. CCE provides a framework for assessing risks, emphasizing identifying cyberattack paths. It supports the development of engineering measures to mitigate risks and highlights the importance of comprehensive systems knowledge.

Combined safety and cybersecurity risk analysis offer advantages by ensuring system robustness and protection. It enables a comprehensive evaluation of

risks, addressing potential threats and vulnerabilities from both safety and cybersecurity perspectives. This holistic approach enhances system resilience, supports informed decision-making, facilitates knowledge transfer, and promotes cross-disciplinary collaboration for effective risk management.

Combining safety and cybersecurity risk analysis presents challenges, such as needing expertise in both disciplines and potential data compartmentalization existing between different departments in an organization. Sharing necessary data while maintaining necessary confidentiality can be difficult. Cybersecurity-related work often has a high confidentiality level. A combined safety and cybersecurity risk analysis must have the level of confidentiality required by the cybersecurity content, often significantly higher than what the safety elements require. This increased confidentiality restricts access and data sharing. This restriction could impede collaboration, learning, and competence building.

The main takeaway from this work is that while combined safety and cybersecurity risk analysis has many advantages and is increasingly necessary given the growing interconnectivity in IACS, it is a complex process with many challenges, and one must assess the situation to find the optimal solution.

Sammendrag

Sikkerhets- og cybersikkerhetsrisikoanalyse i industrielle automatiserings- og kontrollsystemer (IACS) involverer å vurdere og håndtere potensielle risikoer og trusler som kan påvirke sikkerheten og cybersikkerheten til kritiske industrielle prosesser. Det omfatter å identifisere, evaluere og redusere sårbarheter, farer og mulige hendelser som kan føre til tap av tilgjengelighet, integritet eller konfidensialitet.

De siste årene har det vært cybersikkerhetsangrep på operativ teknologi (OT) som viser den mulige sikkerhetsrisikoen som kommer fra cyberangrep, som TRISIS skadevaren og angrepet på Oldsmar vannbehandlingsanlegg. Sikkerhet og cybersikkerhet har tradisjonelt blitt sett på som egne fagfelt. For begge er det utviklet internasjonale standarder og risikoanalysemetoder. Den økende sammenkoblingen mellom OT og informasjonsteknologi (IT) har skapt nye måter for cybertrusler å påvirke sikkerheten og funksjonaliteten til industrielle prosesser. Denne økende integrasjonen krever en helhetlig tilnærming til risikoanalyse som vurderer både sikkerhet og cybersikkerhet i kombinasjon, og sikrer omfattende beskyttelse mot nye trusler i komplekse og sammenkoblede miljøer.

Nye kombinerte standarder og metoder adresserer risikoen forbundet med økt sammenkobling. En slik standard er ISA 84.00.09 Cybersikkerhet knyttet til den funksjonell sikkerhetslivssyklus. ISA TR 84.00.09 understreker viktigheten av å innlemme cyberrisiko i analysen av industrielle prosesser, og adresserer tidligere mangel på bevissthet rundt cyberrelaterte angrep. En metode for kombinert sikkerhets- og cybersikkerhetsanalyse er årsaks konseptet UFoI-E (Ukontrollerte strømmer av informasjon og energi) og dets bruk av scenariobyggeren Cyber-fysisk skadeanalyse for sikkerhet og cybersikkerhet (CyPHASS). UFoI-E ser på ukontrollert informasjon og/eller energistrømmer som en risiko kilde i et cyber-fysisk system (CPS). CyPHASS er et verktøy for scenario bygging som organiserer risikoer grafisk og tilbyr en omfattende database med mulige risikokilder og forebyggende tiltak. Konsekvensdrevet cyberinformert ingeniørteknikk (CCE) er en annen kombinert risikoanalysemetode for sikkerhet og cybersikkerhet. CCE gir et rammeverk for å vurdere risikoer, og legger vekt på å identifisere mulige veier i systemet for cyberangrep. Den støtter utviklingen av tekniske tiltak for å redusere risiko og fremhever viktigheten av omfattende systemkunnskap.

Kombinert sikkerhets- og cybersikkerhetsrisikoanalyse medfører fordeler da det vil øke systemets robusthet og gi bedre beskyttelse. Dette gjør det mulig å gjennomføre en omfattende evaluering av risikoer, og adresserer potensielle trusler

og sårbarheter fra både sikkerhets- og cybersikkerhetsperspektiver. Denne helhetlige tilnærmingen forbedrer systemets motstandskraft, støtter informert beslutningstaking, forbedrer kunnskapsoverføring og fremmer tverrfaglig samarbeid for effektiv risikostyring.

Å kombinere sikkerhets- og cybersikkerhetsrisikoanalyser byr på utfordringer, for eksempel at det blir et behov for ekspertise innen begge disipliner og potensiell nødvendig kompartmentalisering av data mellom ulike avdelinger i en organisasjon. Cybersikkerhetsrelatert arbeid har ofte et høyt konfidensialitetsnivå. En kombinert sikkerhets- og cybersikkerhetsrisikoanalyse må ha det konfidensialitetsnivået som cybersikkerhets innholdet krever, ofte betydelig høyere enn det sikkerhetselementene krever. Denne økte konfidensialiteten begrenser tilgang og datadeling. Denne begrensningen kan hindre samarbeid, læring og kompetansebygging.

Det største læringsutbytte fra dette arbeidet er at mens kombinert sikkerhets- og cybersikkerhetsrisikoanalyse har mange fordeler og er stadig mer nødvendig gitt den økende sammenkoblingen i IACS, er det en kompleks prosess med mange utfordringer, og man må vurdere hver enkelt situasjon for å finne den optimale løsningen.

Contents

Figures

Tables

Acronyms

ATA Attack Tree Analysis. 32

CBM Cybersecurity Barrier Management. iii

CCE Consequence-driven Cyber-informed Engineering. 45

CDC Center for Disease Control and Prevention. 57

CF Critical Functions. 49

CISA Cybersecurity and Infrastructure Security Agency. 18

CL Cyber Layer. 42

CPL Cyber-Physical Layer. 42

CPS Cyber-Physical System. 40

CyPHASS Cyber-Physical Harm Analysis for Safety and Security. 41

DMZ Demilitarized Zone. 5

EF Enabling Functions. 49

ETA Event Tree Analysis. 27

EUC Equipment Under Control. 8

EWS Engineering Workstations. 5, 20

FTA Fault Tree Analysis. 27

HAZOP Hazard and Operability study. 27

HCE High Consequence Event. 46

HMI Human Machine Interface. 16

IACS Industrial Automation and Control Systems. 8

ICS Industrial Control Systems. 8

IEC International Electrotechnical Commission. 29

INL Idaho National Laboratory. 45

ISA International Society of Automation. 37

ISO International Organization for Standardization. 24

IT Information Technology. 5

NaOH Natrium hydroxide. 16

NTNU Norwegian University of Science and Technology. iii

OS Operator Stations. 5

OT Operational Technology. 5

PL Physical Layer. 42

PPT People, Process, Technology. 49

PV-F Process Variable and Functional deviations. 42

SCAI Safety Controllers, Alarms, and Interlocks. 38

SIF Safety Instrumented Functions. 9

SIS Safety Instrumented System. 8

UFoE Uncontrolled Flow of Energy. 42

UFoI Uncontrolled Flow of Information. 42

UFoI-E Uncontrolled Flow of Information and Energy. 40

Chapter 1

Introduction

1.1 Background and Motivation

The increasing exposure of Industrial Automation and Control Systems (IACS) to cybersecurity threats necessitates a deeper understanding of the potential safety risks associated with successful cyberattacks. IACS systems were often isolated in the past. However, the risk landscape has evolved with the integration of information and communication technology. These evolving risks pose new challenges for risk assessments, emphasizing the need for combined safety and cybersecurity analyses.

The purpose of this master thesis is to explore selected standards and methods to shed light on the importance of combined analyses in addressing these emerging safety and cybersecurity risks and the need to evaluate them together. The motivation behind the choice to look at combined safety and cybersecurity risk in IACS stems from the author's specialization project, which focused on cybersecurity in IACS. This work made it clear that cybersecurity can create new safety risks, but did not delve into the issue.

The motivation behind including the CCE method and the UFoI-E concept and the CyPHASS method stemmed from its relative novelty and limited coverage in existing literature, particularly in Norway.

1.2 Main Objective and Tasks

The main objective of this master thesis is to explore selected standards and methods that regard safety and cybersecurity analysis and to explain why combined analyses are needed.

The tasks for this thesis are:

- Present and discuss illustrative case studies of how cybersecurity attacks can create new safety risks at various types of processing plants
- Describe standards and methods for safety risk analyses and cybersecurity risk analyses for OT systems.

- Carry out a literature study on the prevalence and use of integrated safety and cybersecurity risk analysis,
- Describe a relevant standard for combined safety and cybersecurity risk analysis and present the two methods, CCE and UFoI-E/CyPHASS.
- Illustrate the application of CCE on the selected case studies and discuss some of the challenges and opportunities of applying the method.
- Based on the application of CCE, give some recommendations and clarifications that can be helpful when conducting such analysis.

1.3 Research Approach

The research approach employed in this master thesis primarily involved a qualitative study of relevant literature from reputable publishers, guided by the supervisor and co-supervisors. The sources selected included publications by prominent researchers and experts in the field, such as Marvin Rausand, Nelson Carreras Guzman, Igor Kozine, and Mary Ann Lundteigen, as well as publications from reputable organizations like INL, NIST, ISA, and IEC. Additionally, participation in CBM workshops and meetings facilitated valuable insights from academic and industry experts with relevant experience and knowledge. Regular weekly meetings with the project supervisor proved instrumental throughout the 20-week research period. Certain parts of this work incorporate and rework content from the author's specialization project on OT Cybersecurity [1], particularly in sections 2.1, 2.3.1, and 4.3.1.

1.4 Limitations and Delimitations

When applying the CCE and CyPHASS methods to the case studies, a delimitation was the author's limited system insight and knowledge as an outsider. Consequently, the lack of information and knowledge regarding the systems' inner workings hindered an effective application of the methodologies, resulting in incomplete analyses intended solely to illustrate parts of the methods rather than provide comprehensive and accurate analysis results. The CCE method was prioritized and is covered more extensively than the UFoI-E/CyPHASS method.

Many standards are relevant to safety, cybersecurity, and combined safety and cybersecurity. Multiple standards could have been discussed, but this report limits it to one standard per topic.

1.5 Structure of the Thesis

The report starts with Chapter 2 explaining relevant concepts, terminology, and definitions. Chapter 3 presents two selected cyberattacks as case studies relevant to this report. For the first attack, Oldsmar, the focus will be the potential public

safety consequences, not the attack's technicality. For the second, TRISIS, the focus will be on the technical aspects and the progression of the malware.

This report has divided the topic of safety and cybersecurity risk analysis into two chapters. Chapter 4 covers safety risk analysis and cybersecurity risk analysis separately, not as a combined assessment. The intention behind this is to show how these topics traditionally have been handled before the newer approach of combining them. For both safety and cybersecurity, one relevant standard will be presented, as well as short presentations of common risk analysis methods. Chapter 5 covers the combined safety and cybersecurity risk analysis. It will include some observations of the prevalence of academic publication and present a relevant standard and the UFoI-E/CyPHASS method and the CCE method. The case studies will be used to demonstrate parts of these methods.

Lastly Chapter 6 discusses the advantages and disadvantages of combined safety and cybersecurity risk analysis and some insight regarding the choice of standards. Chapter 7 is the conclusion and further work.

Chapter 2

Key Concepts and Terminology

2.1 OT systems

OT Operational Technology (OT) and IT Information Technology (IT) are two closely related but distinct areas of technology used to support the operation and management of various technical systems. OT systems are typically focused on the control and optimization of physical processes. In contrast, IT systems focus on managing and processing data and information. OT systems often consist of sensors, actuators, and other devices connected to a network and used to monitor and control industrial processes, equipment, and infrastructure. IT systems include computers, servers, networks, storage, and devices that support collaboration, communication, and data management and governance in many organizations. In many cases, OT and IT systems are integrated to enable the exchange of data and information between different systems and optimize the performance of industrial processes.

The Purdue architecture model is used to explain the relationships between different levels of an industrial control system and the enterprise network and how the two interact. In addition, the Perdue architecture model is often used to explain the difference between IT and OT, as seen in figure 2.1. The different levels in the model often include elements like:

- Level 0: Sensors, actuators
- Level 1: Controller network, I/O cards, and if required, Engineering Workstations (EWS)
- Level 2: Operator Stations (OS), historian, and exchange servers. EWS if needed.
- Level 3: Technical and process information network with condition monitoring and servers for aggregated and historical data. It can also include PCs for configuration.
- Level 3.5: Demilitarized Zone (DMZ) is a buffer that controls traffic between higher and lower internal levels.
- Level 4/5: Office Network for the facility. Internet interface, with an “Inter-

net DMZ" firewall that adds an extra layer of protection between the internet and an organization's private network. If multiple facilities are connected to a parent IT system, the latter is called Level 5.

- Level 6: External network and cloud services.

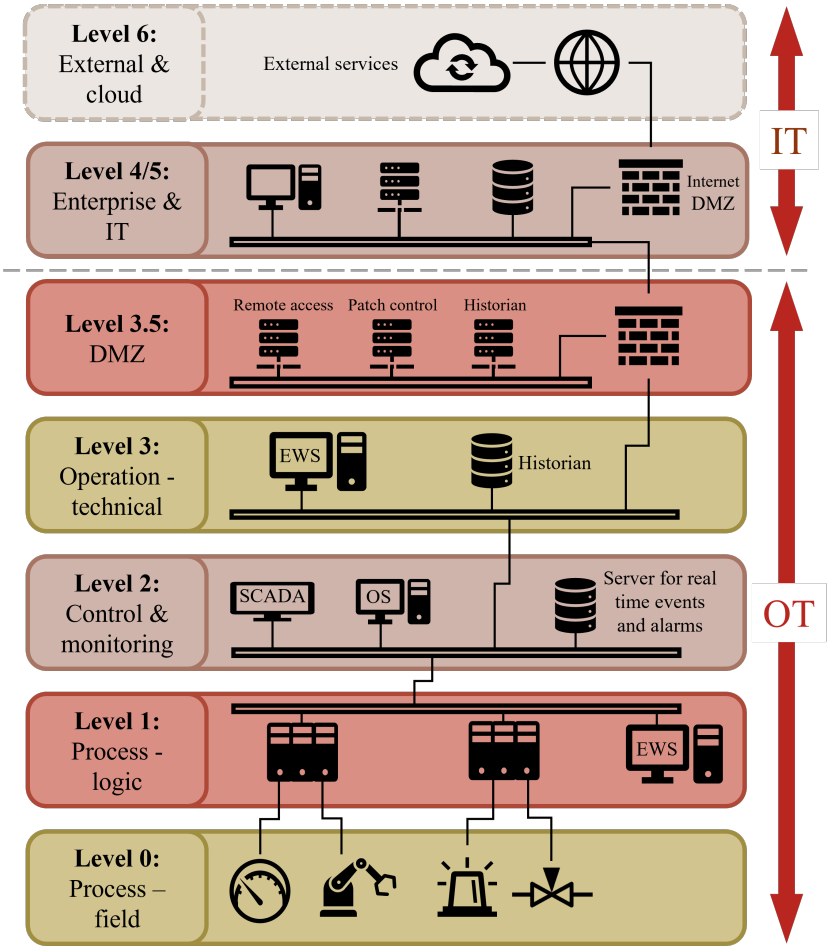


Figure 2.1: An illustration of the Purdue Architecture Model. Reproduced from TTK4175 - Instrumentation Systems [2]

Levels 0-3.5 are the OT systems, and levels 4-6 describe the IT systems. Zone 3.5 is called the Demilitarized Zone. This zone is a network partition and a security measure designed to protect the OT systems from external threats, like cyberattacks. The DMZ functions as a buffer, limiting or restricting network traffic between the higher and lower levels in the Purdue model. In addition, it will prevent external parties from having the ability to access the control level directly. However, IT and OT environments can both have network devices like switches,

servers, gateways, and ethernet, thereby both systems are receptive to vulnerabilities that network devices may possess.

Purdue uses the principle of zones and conduits to separate and secure an OT environment. A simple example of this is shown in figure 2.2. Zones are areas within a system or network that are logically or physically separated from one another based on the level of trust and security required. Zones are used to segment a system or network into different areas with different security requirements, and they can help to prevent unauthorized access or movement of data between different areas of the system or network. Conduits are communication pathways or channels that transfer data or signals between different zones or areas within a system or network. Conduits may include physical cables, wireless communication channels, or other communication links. A level in the Purdue model can consist of multiple zones with different security requirements and conduits between them. The DMZ is a type of zone.

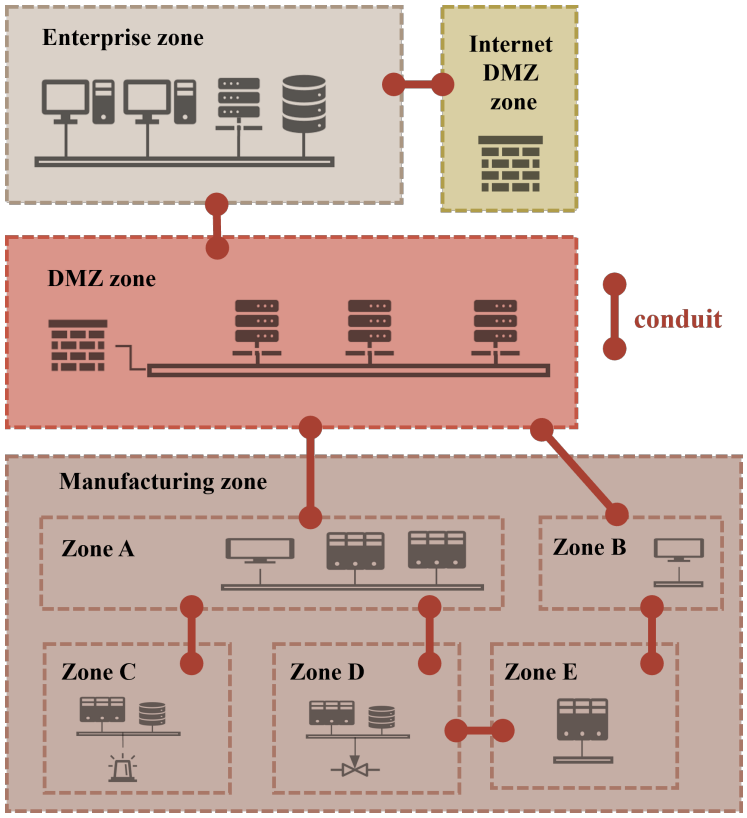


Figure 2.2: A simplified example of zones and conduits in a network architecture

It is important to note that while there is a separation, the OT systems are not isolated from IT systems. Communication between OT and IT is becoming increasingly necessary and prevalent for ongoing operations and can no longer be avoided. Even if communication is limited and sent through a DMZ, this connectivity opens up vulnerabilities adversaries can exploit. Concepts like Industry 4.0

and Internet of Things are erasing the separation between OT and IT. In addition, there is now extensive data transmitted between the systems. This connectivity raises new concerns and requirements regarding the security of OT systems as they become increasingly less isolated. So, where cybersecurity was traditionally seen as an IT problem, the industry has realized the vulnerabilities OT systems have and the importance of protecting them.

2.1.1 Terminology: OT, ICS, and IACS

Other terms are used about OT systems or environments, namely Industrial Control Systems (ICS) and Industrial Automation and Control Systems (IACS). ICS and OT both pertain to the same types of systems, both refer to levels 0-3.5 in the Purdue model in figure 2.1. IACS is more comprehensive than OT/ICS. IACS is a term coined by IEC 62443 [3] to include OT/ICS, but it also encompasses people, processes, and the related interface with IT necessary for the operation of OT/ICS.

In this report, OT and IACS will mainly be used. However, this report will respect the chosen term used in the frameworks that will be discussed. For instance, the term ICS will be used for the ICS cyber Kill Chain [4] discussed in section 3.2.2.

2.2 Safety-Instrumented Systems

Safety Instrumented System (SIS) is a special type of barrier system in industrial processes designed to ensure the safe operation of equipment and processes. These systems are responsible for preventing, detecting, and mitigating dangerous conditions that may arise during the operation of industrial systems. The primary purpose of safety controllers is to allow a process to fail safely. Figure 2.3 shows the common protection layers that surround an industrial process. Many different versions of this figure exist with different names and layers. Figure 2.3 follows the Guidelines for Safe and Reliable Instrumented Protective Systems by the Center for Chemical Process Safety [5]. In this case, the process is the Equipment Under Control (EUC). Rausand [6] defines EUC as a specified hazardous system such as machinery, vehicle, or an industrial process.

In figure 2.3, both layers 4 and 6 are SIS. It should be noted that in Norway, it is standard practice that the ESD is defined as SIS, as established in the Norwegian Oil and Gas Guideline 070 [7]. However, this is not commonly done in other places. The SIS found in layer 4 is a Process Shutdown. Its goal is to safely shut down the process if it is no longer in a safe state, thereby preventing the situation from escalating into a dangerous situation. The SIS found in layer 5 is an Emergency Shutdown. This barrier shuts down the entire area and deploys the fire and gas system.

A SIS is designed to operate independently of the main control system and is activated only when a hazardous condition is detected. According to Rausand [6],

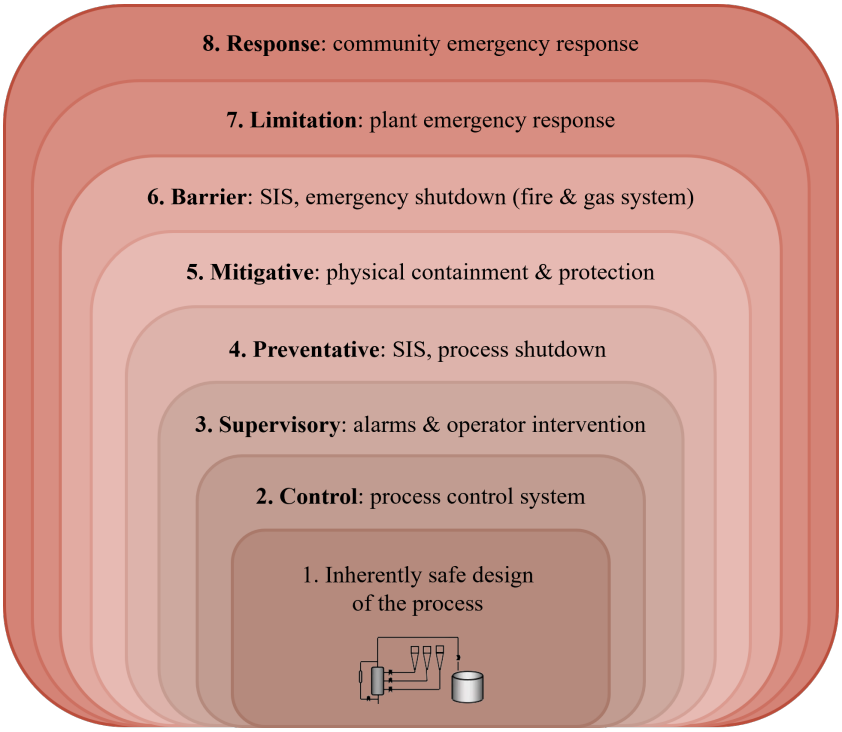


Figure 2.3: Common protection layers surrounding an industrial process. Adapted from [5]

the main elements of a SIS are one or more input elements (sensors, etc.), one or more logic solvers, and one or more actuating elements (valves, motors, etc.). A SIS can consist of multiple Safety Instrumented Functions (SIF). Rausand defines a SIF as " a barrier function that is implemented by a SIS and that is intended to achieve or maintain a safe state for the EUC with respect to a specific process demand". Figure 2.4 shows A SIS consisting of two SIFs connected to the EUC with a separate main process control system.

A SIS can be implemented as either a proactive or a reactive barrier. For instance, if a car is the EUC, the ABS brakes are a proactive SIS, and the airbag is a reactive SIS. Another example is shown in figure 2.5. Suppose a tank with pressurized gas has dangerously high pressure. In that case, the reactive barriers will try to reduce the pressure by closing the input valve and/or opening a release valve. If they are unable and a gas leak or fire should occur, the proactive SIS, the fire and gas suppression system, will activate to try and mitigate the situation.

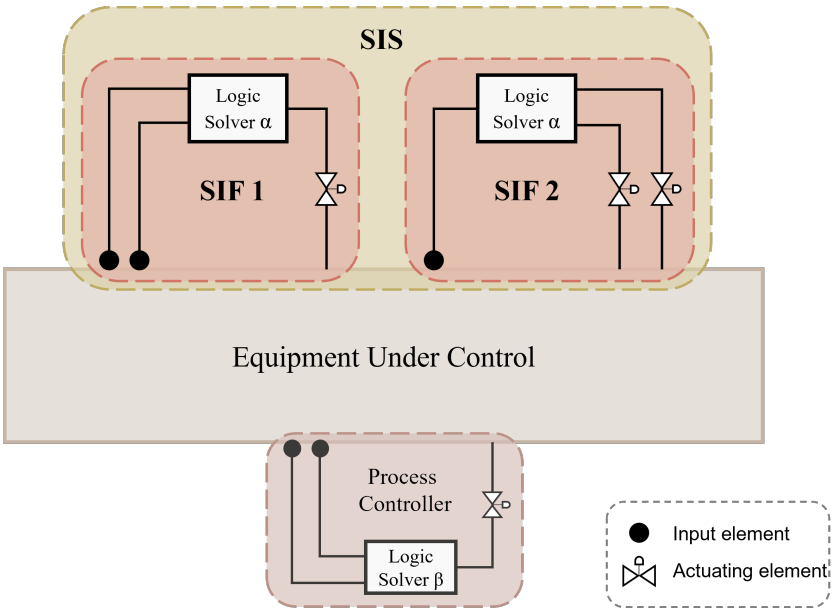


Figure 2.4: A safety instrumented system (SIS) consisting of two safety instrumented functions (SIF) connected to the equipment under control (EUC), along with its separate main process control system.

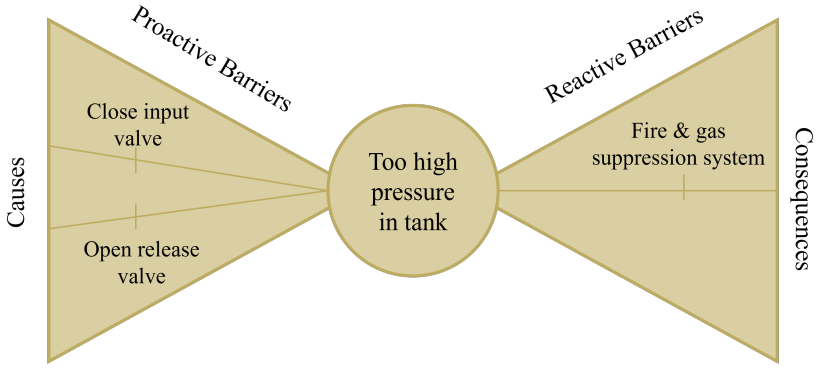


Figure 2.5: Different proactive and reactive safety barriers connected to a gas tank.

The importance of a SIS lies in its ability to prevent accidents, mitigate their effects, and protect both personnel and the environment. They provide an additional layer of protection to the primary control system, which may be insufficient to handle all potential hazards. For instance, if the primary control system fails to prevent a runaway reaction, SIS can intervene and safely shut down the process before an explosion occurs. Depending on the risk associated with the process, different levels of reliability and effectiveness of the SIS can be required.

2.3 Security, Information Security, and Cybersecurity

Numerous definitions of security, information security, and cybersecurity exist, each with its own angle. However, many definitions are cumbersome and overly detailed. Furthermore, they do not showcase the relationship between security, information security, and cybersecurity. Some of these definitions given by NIST and IEC 62443 can be seen in table 2.1. Figure 2.6 gives a short and simple definition of the terms.

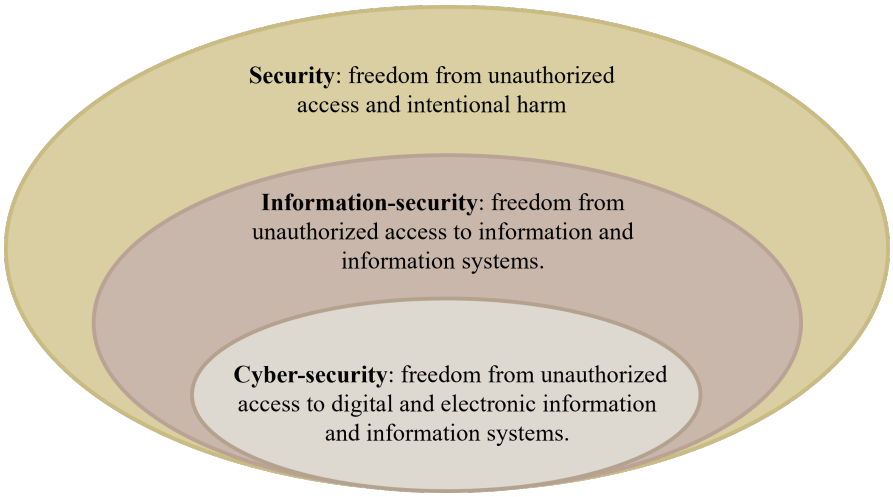


Figure 2.6: Definitions of security, information security, and cybersecurity, and their relationship.

They are as follows:

- Security is freedom from unauthorized access and intentional harm.
- Information-security is freedom from unauthorized access to information and information systems.
- Cyber-security is freedom from unauthorized access to digital and electronic information and information systems.

Moreover, these more concise definitions show the terms' connection more readily; cybersecurity is a subgroup of information security which again is a subgroup of security. "Freedom from" is used here as an all-encompassing term based on adhering to the NIST security framework [8], as seen in figure 2.7. To achieve freedom from unauthorized access, an organization must be able to identify threats, protect systems, detect intrusion, respond to incidents, and recover from them. The choice of using the term "freedom from" stems from the IEC 62443-1-1 [9] definition of safety: safety is freedom from unacceptable risk.

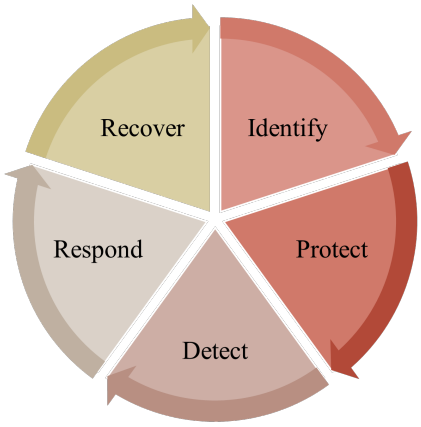


Figure 2.7: The NIST security framework [8]

2.3.1 Cybersecurity in OT and IT

In general, cybersecurity is the actions taken to protect a system's confidentiality, integrity, and availability. In a security context, confidentiality means no unauthorized read-access to a system to avoid a data breach and leak of proprietary or sensitive information. A system's integrity hinges on having no unauthorized write-access, i.e., altering data. Finally, availability means guaranteeing system access when required, i.e., denial of service is a typical loss of availability.

Cybersecurity is different when it comes to IT and OT systems. The priorities in IT cybersecurity are in descending order: confidentiality, integrity, and availability. However, for OT systems, the order is flipped, with availability being the most important, followed by integrity and then confidentiality. Availability is commonly considered the highest priority because it refers to the ability of a system to be accessed and used when needed. OT systems often run around the clock, and if a system loses availability, it cannot be used to perform its intended function, which can have severe consequences in industrial environments since OT systems control and monitor critical processes. Furthermore, if an OT system is unavailable and thereby uncontrollable, it can enter an unsafe state or safety functions can be disengaged. Both can lead to dangerous situations.

Table 2.1: Definitions of security, information security, and cybersecurity given by NIST [10][11][12] and IEC 62443-1-1 [9]

	NIST	**IEC 62443-1-1**
Security	A condition that results from the establishment and maintenance of protective measures that enable an organization to perform its mission or critical functions despite risks posed by threats to its use of systems. Protective measures may involve a combination of deterrence, avoidance, prevention, detection, recovery, and correction that should form part of the organization's risk management approach	The prevention of illegal or unwanted penetration, intentional or unintentional interference with the proper and intended operation, or inappropriate access to confidential information in IACS
Information-Security	The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.	
Cyber-Security	The prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.	The actions required to preclude unauthorized use of, denial of service to, modifications to, disclosure of, loss of revenue from, or destruction of critical systems or informational assets

Chapter 3

Selected Cyberattacks

3.1 Oldsmar Water Facility

3.1.1 Description of the Attack

On February 5th 2021 unknown hackers accessed to the Oldsmar Water Treatment facility. According to a press conference by the Pinellas County Sheriff's Office [13] and the Oldsmar city manager, the attackers used compromised credentials and the remote access software TeamViewer to log in to a plant operator console. A timeline of the attack can be seen in figure 3.1. Initial access was at 08.00 when the attackers logged on, immediately logged off, and disconnected the session. The console was manned by an operator at this time who mentally noted the abnormal behavior but took no action.

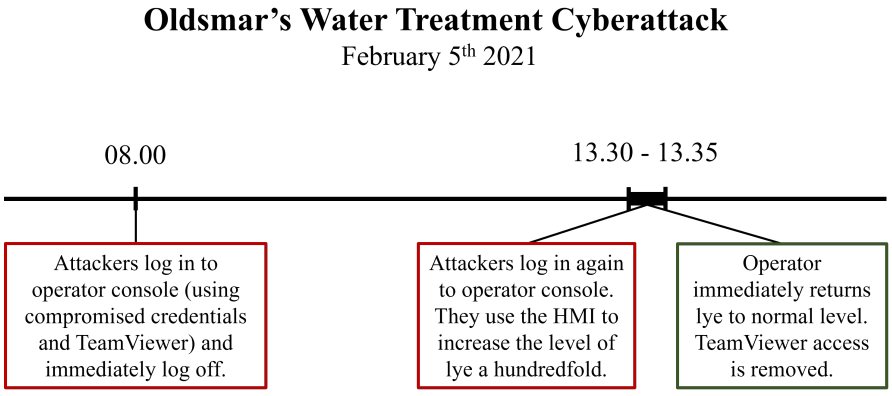


Figure 3.1: A timeline of observed events during the attack on the Oldsmar water treatment facility, as stated by Cervini et al. [14] and the local Sheriff's Office [13]

Researchers at The Johns Hopkins University in Baltimore, Cervini et al. [14] speculate that the log on and off was likely the attackers confirming system connection and credential validity. In addition, Cervini et al. [14] propose that the attackers may have taken screenshots of the console to support their planning of

further action.

The second and final move of the attackers came later that day. The Pinellas County Sheriff's Office [13] reported that at 13.30, the attackers logged back on to the operator console and used the plant's Human Machine Interface (HMI) to increase the level of Natrium hydroxide (NaOH) being added to the water. A simplified illustration of the attackers' movements in the system is seen in figure 3.2. NaOH, also known as lye, is added to the drinking water as a part of the purification process. The normal dose is 100 parts per million (ppm), which is harmless for humans. The attackers, however, increased the amount a hundredfold to 11 100 ppm. According to Cervini et al. [14], exposure to lye in such concentrations can cause painful burns to the exposed area and permanent damage if ingested. A real-life case of this happened on May 29th. in Kvinesdal, Norway. NRK [15] reported that high concentrations of lye had been in the local drinking water. Two people were sent to the hospital, one of them had first-degree burns on his body after having showered in the contaminated water. As of May 31st. There have been no reports on what caused the high levels of lye or how high the levels were. In addition, Kvinesdal has a warning system that should have detected the elevated pH but, for unknown reasons, did not. The contaminated water in Kvinesdal supplied water to about 160 people, whereas Oldsmar supplies water to approximately 15,000 people.

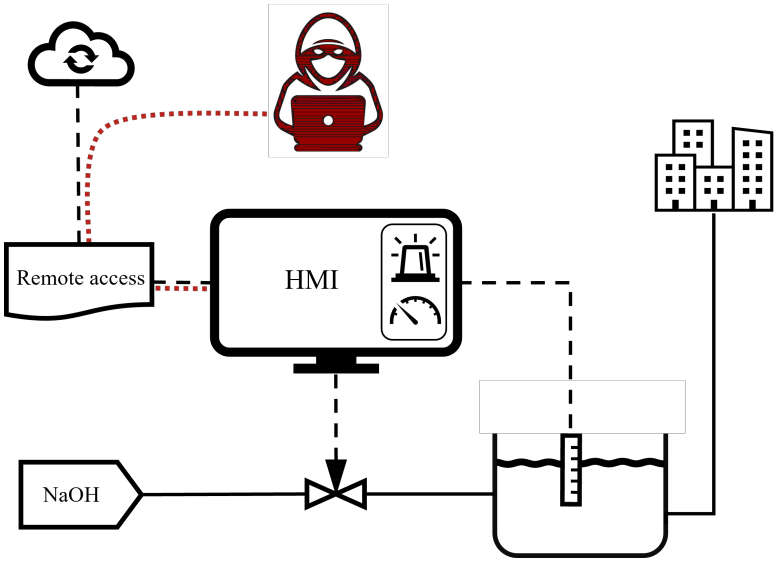


Figure 3.2: A simplified illustration of the attackers movement within the Oldsmar system.

The operator manning the operator console saw the change and immediately returned the levels to normal values. The plant supervisor was notified, and the TeamViewer access was removed. According to County officials [13] it would have taken 24 to 36 hours of the increased lye setpoint for tainted water to reach a point of distribution where where customers could have consumed it. Further-

more, county officials [13] stated that the plant uses sensors that monitor the pH level of the water. Had an abnormal pH been achieved because of the increased amounts of lye, an alarm would have sounded, and the operators would have been notified of the imbalance. The county officials, therefore, stated that even if the change had not been immediately noticed, the situation would have been detected and remedied long before an unsafe situation for consumers could have occurred. However, that is what should have happened in Kvinesdal and did not.

3.1.2 Update

When section 3.1.1 was initially written at the start of February 2023, there was no doubt that what occurred at Oldsmar was a cyberattack. However, at the start April 2023, articles started surfacing that claimed that the incident was in fact, not a cyberattack but rather an error made by the employee who discovered the supposed attack. The Tampa Bay Times [16] times published an article stating that the former Oldsmar city manager made a claim at an industry conference that what happened at Oldsmar was a "nonevent" likely caused by the operator "banging on his keyboard". Oldsmar's current city manager denied commenting when contacted by the Tampa Bay Times[16]. The Tampa Bay Times' article [16] goes on to say that the FBI Tampa office made the statement "Through the course of the investigation the FBI was not able to confirm that this incident was initiated by a targeted cyber intrusion of Oldsmar". This is the first statement from the FBI, even though the investigation was concluded some months after the incident. In addition, no major authority on cybersecurity as of May 2nd. 2023 published any findings or statements supporting the claims that Oldsmar was not a cyberattack. MITRE att&ck framework [17], a renowned knowledge base and model for cyber adversary behavior, still classifies what happened at Oldsmar as a "cyber incident" involving "unidentified threat actors".

With these latest developments, what actually happened at the Oldsmar facility on February 5th, 2021, has become unclear. The incident at Oldsmar, regardless of what caused it, raised awareness about the threat to critical infrastructure. The event can still be an example of why protecting industrial control systems is essential and what could happen if a threat actor compromises a critical system.

3.2 TRISIS

This chapter discusses the TRISIS malware and is based on two primary sources. Firstly, a malware analysis report from the Cybersecurity and Infrastructure Security Agency (CISA) written in collaboration with the producers of the targeted systems. Secondly, a report from Dragos, the industrial cybersecurity company that first identified the TRISIS malware.

3.2.1 Background and Context

The TRISIS malware was discovered in 2017 and is, according to Dragos [18], the fifth of seven publicly known ICS-tailored malware, see the timeline in figure 3.3. More pointedly, TRISIS was the first publicly known ICS-tailored malware to target safety instrumented systems. According to CISA [19] "the malware surpasses [its] forerunners with the ability to directly interact with, remotely control, and compromise a safety [instrumented] system —a nearly unprecedented feat". The main purpose of safety controllers, as discussed in chapter 2.2 is to allow a process to fail safely. The capability to disable, inhibit or modify SIS could, worst-case scenario, result in serious physical consequences.

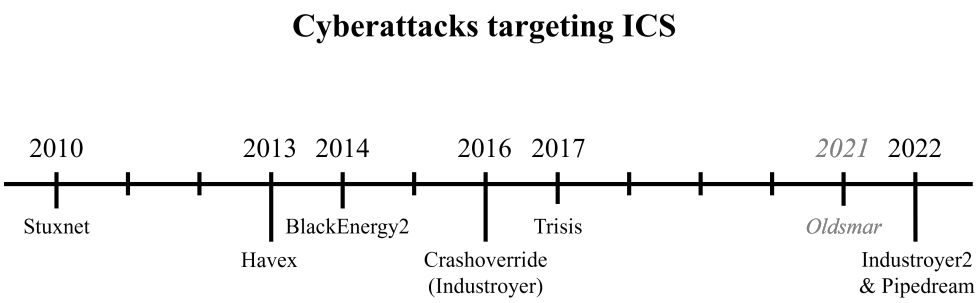


Figure 3.3: A timeline of the seven ICS cyberattacks as identified by Dragos [18], as well as the Oldsmar attack, for reference's sake.

According to Dragos [20], in August of 2017, a petrochemical plant in Saudi Arabia experienced an unexpected shutdown of its safety instrumented systems. A team of security experts from Dragos was brought in to determine the cause of the shutdown. During their analysis, they discovered a previously unknown piece of malware specifically designed to target the plant's SIS. The malware targeted Schneider Electric's Triconex Tricon safety controllers. Dragos gave the malware the name TRISIS as it targeted the Tricon SIS. It has also become known as TRITON and HatMan. In this report, the name TRISIS will be used.

3.2.2 The Progression of the Attack

TRISIS is a Stage 2 ICS attack, as defined by the SANS Institute ICS Cyber Kill Chain [4]. The ICS Cyber Kill Chain, as seen in figure 3.4, describes an attack

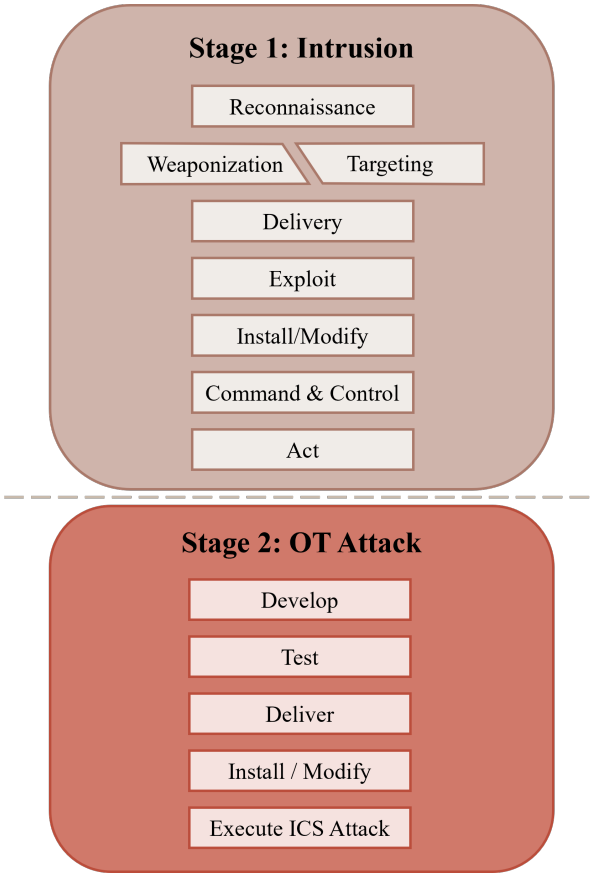


Figure 3.4: The two stages of the ICS Cyber Kill Chain, reproduced from SANS [4]

against an ICS system as unfolding in two separate stages. The first stage is often aimed at IT systems and consists of cyber intrusion, preparation, and execution. The second stage is developing and executing the ICS system-specific attack. The first stage is similar to traditional IT cyberattacks, whereas stage two is unique to ICS systems. As TRISIS is a Stage 2 attack, it requires that Stage 1 has been successfully completed and that the IT system is compromised. In addition, the threat actor must have gained access to the ICS network. This work focuses on the three last steps of the ICS Cyber Kill Chain in figure 3.4; Deliver, Install/Modify, and Execute ICS Attack, as these are the observable steps of TRISIS.

The threat actor, having compromised a computer within the safety network, was able to upload and run their own script on it. According to CISA [19], this compromised computer is a PC-based component that communicates with the safety controller. Furthermore, it is described as capable of running engineering and maintenance software toolset protocols. The TRISIS python script disguises itself as such a protocol. Given the description in the CISA [19] report, it is assumed that this PC-based component is a part of or connected to an engineering

workstation. Engineering Workstations (EWS) ia a PC with software and network connections that allows someone to configure equipment within the OT system, such as controllers and servers.

The TRISIS malware's progression from having access to an engineering station to having malicious capability on the SIS controller is shown in simplified form in figure 3.5, as described by CISA [19]. According to CISA [19], the threat actor starts by executing the main TRISIS Python Script on the compromised engineering workstation. The main script leverages the attacker's own specialized implementation of an internal TriStation protocol. The Python script establishes a connection to the Tricon controller and gathers information on the system states. The script downloads the injector and the implant onto the controller disguised as new program for the system to run. The injector is a piece of malicious code designed to be executed on the target system to deliver or install the malware payload, referred to as the implant. Adding a program to a running controller, known as appending, is very complicated and will not be explored further. For more information, see the full CISA [19] report.

The injector that has been appended to the controller begins executing automatically. Meanwhile, the main script periodically checks the systems states of the controller to see if the injector has finished executing. The injector begins by testing and verifying that the controller can be compromised. Afterward, the injector uses a system vulnerability to escalate its own privileges. With the escalated privileges, the injector is capable of writing the implant into the in-memory firmware of the controller, thereby enabling the implant. In-memory firmware is stored in a volatile memory component, such as RAM, rather than a non-volatile memory component, such as a ROM or flash memory. This type of firmware is loaded into memory at boot time or during system operation and executed directly from memory.

Finally, the injector reverts its privileges and reports that it has completed. The Python script registers that the injector has finished its execution. To cover its tracks, the script overwrites the program slot used with a "dummy" program before exiting. The Tricon controller is now fully compromised. The end result is that the implant will be available to the attackers via the compromised network using the TriStation protocols, providing the functionality of a rudimentary Remote Administration Tool (RAT).

Using similar methods as before ,the threat actor can now use the Python script to establish a connection to the compromised safety controller and trigger the implant. Due to the modifications made, when the command from the script is received, the implant will be executed on the controller instead of the normal processing. The implant allows the threat actor to read and write memory, including within in-memory firmware, and execute arbitrary code regardless of the key switch position, including if it is in "RUN". Due to its capabilities, the malware can make changes to running firmware while the safety controller is in full operation, not just while it is being programmed. However, any changes will be lost when the deception is fully reset, as they persist only in the memory.

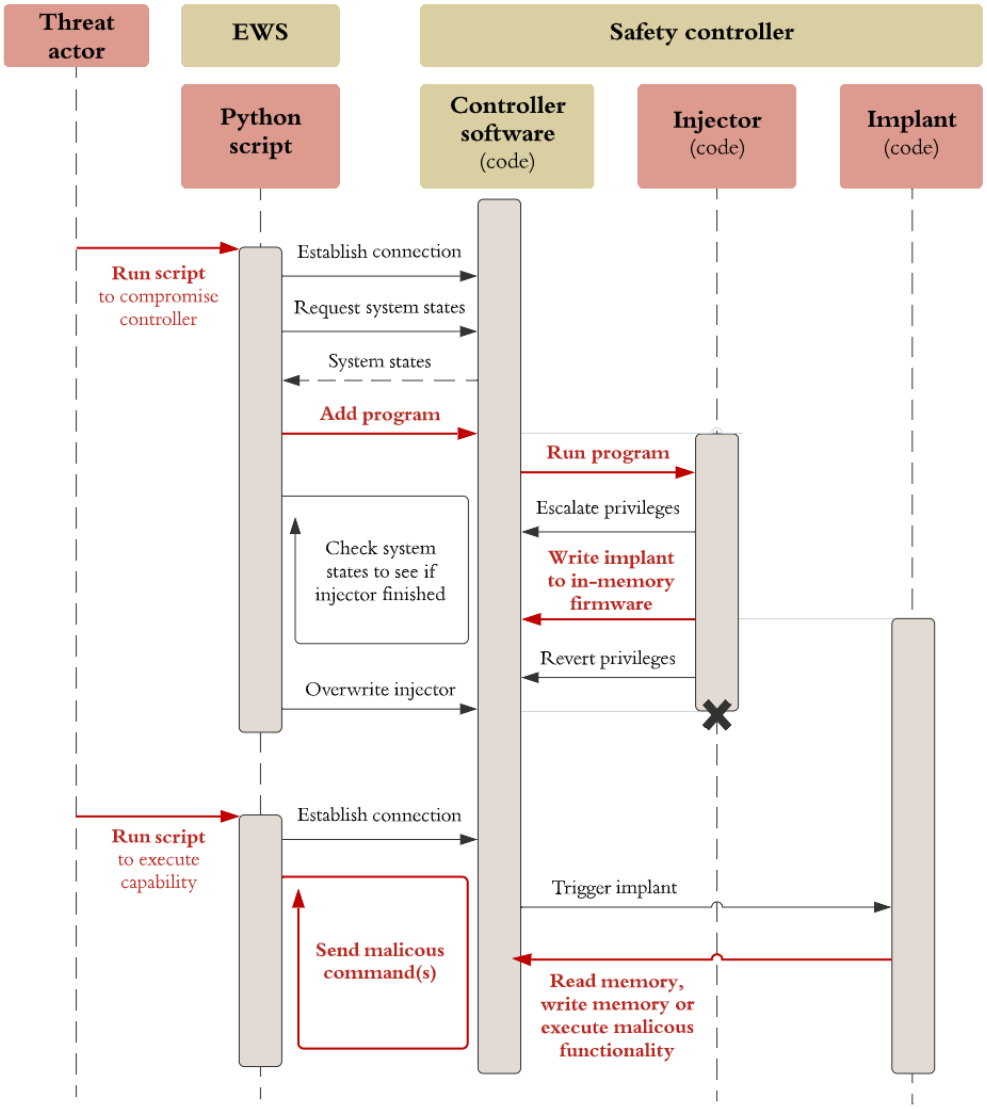


Figure 3.5: The progression of the TRISIS malware. Adapted from CISA [19]

3.2.3 Implications

According to CISA [19], TRISIS is a valuable tool for an attacker as it can be used for OT reconnaissance. However, it was likely designed to be a part of a multi-pronged attack that collectively would compromise industrial facilities or worse. If just the SIS is compromised, it is unlikely that any harm will come from it as long as the plant operates normally and the safety systems are not activated. However, the results could be disastrous should something happen, and a safe shutdown by the SIS is required but unavailable. If a combined attack was to degrade an industrial process simultaneously as the safety systems are compromised and unable to function correctly, the consequences could be severe for people, property, and the

environment.

According to Dragos [20], TRISIS is the first SIS-targeted malware and represents a game-changer for OT security. While previously identified in theoretical attack scenarios, targeting SIS equipment specifically, represents a dangerous evolution within OT computer network attacks. Adversaries are becoming bolder, according to Dragos [20], and an attack on a SIS is a considerable step forward in causing harm to people and the environment, not just monetary loss. Furthermore, according to [19], components from TRISIS could allow another party to build a similar attack or use it as a basis for attacks on other safety controllers or systems.

Chapter 4

Safety and Cybersecurity Risk Analysis

This chapter examines safety risk analysis and cybersecurity risk analysis as distinct assessments rather than a combined approach. The aim is to examine the traditional practices associated with each domain before the emergence of the integrated perspective.

4.1 Terminology

The term risk analysis, as used in this work, follows the definition given by Marvin Rausand [6], professor emeritus at NTNU. According to Rausand [6], a risk analysis is a systematic use of available information to identify hazards and estimate the likelihood, consequences, and causes. Risk analysis consists of identifying hazards and threats, identifying hazardous events, determining the frequency of occurrence and the consequence, and establishing a risk picture.

As seen in figure 4.1, risk analysis is part of risk assessment, which also includes risk evaluation. According to Rausand[6], risk evaluation is the process of comparing the risk determined by the risk analysis with risk acceptance criteria, and judgments are made on the tolerability of the risk.

Risk control is, as defined by Rausand [6], using the acquired insight from the risk assessment to identify and introduce risk control measures to eliminate or reduce potentials harms to people, the environment, or other assets. Risk analysis, evaluation, and control comprise the continuous risk management process, as illustrated in figure 4.1.

This thesis focuses on two types of risk analysis: safety risk analysis and cybersecurity risk analysis. Although the focus is on cybersecurity, some sources refer to general security.

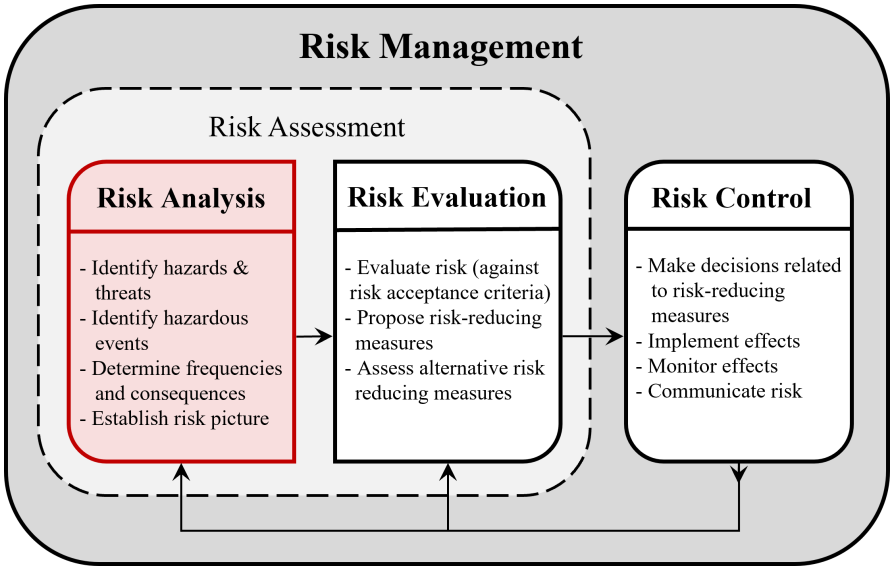


Figure 4.1: Risk analysis, evaluation, assessment, and management and their connection. Reproduced from Rausand [6]

4.2 Safety Standard and Methods

Performing risk analysis as a part of risk assessment has become a standard best-practice for most organizations. The apparent benefit of incorporating risk analysis in business practices is to reduce risk and harm. This reduction protects an organization's assets, both personal and material, as well as an organization's reputation. In many cases, risk reduction is not just best-practice but can be mandatory to comply with local rules and regulations and be contractually required or necessary for insurance coverage.

International standards and guidelines have been developed to provide principles, frameworks, and processes for risk assessment, including risk analysis. This thesis will give two examples: one geared toward safety risk analysis and the other toward cybersecurity risk analysis. The two standards are ISO 31000 *Risk Management* [21] and IEC 62443 *Security for industrial automation and control systems Part 3-2: Security risk assessment for system design* [22].

4.2.1 Standard: ISO 31000

ISO 31000 *Risk Management* [21] provides guidelines for organizations on managing potential risks. It is published by the International Organization for Standardization (ISO). ISO is an independent non-governmental organization with a membership of 165 national standards bodies. In addition, ISO has advisory status in the UN [23].

ISO 31000 [21] is intended to be used by organizations of all types and sizes and across all sectors. It is designed to help organizations establish a systematic

and effective risk management process that can be integrated into their overall management system. The standard emphasizes the importance of incorporating risk management into an organization's structure, processes, objectives, and activities. ISO 31000 [21] does not provide specific requirements or procedures for risk management. Instead, it provides a framework for organizations to develop their risk management process tailored to their specific needs and objectives. The standard is intended to allow for flexibility and adaptability so that organizations can appropriately incorporate it to their specific circumstances. The ISO 31010 [24] standard supports the ISO 31000 standard. It supplies information on the selection and application of risk assessment techniques. The techniques are used for identifying, analyzing, and evaluating risk as described in ISO 31000 and whenever there is a need to understand uncertainty and its effects.

Although ISO 31000 [21] states it can be used for all types of risk, it focuses on quantitative goals for risk acceptance, which works well for safety risks but is less suited for cybersecurity risks. Therefore, the focus here is ISO 3100 used in the context of safety risk analysis.

ISO 31000 [21] states that risk assessment should be conducted systematically, iteratively, and collaboratively. It should draw on the collective knowledge and views of stakeholders. Furthermore, it should use the best available information and, if necessary, supplement it with additional inquiries. ISO 31000 [21] divides risk assessment into three parts: risk identification, risk analysis, and risk evaluation, as seen in figure 4.2. This definition differs from Rausand's [6] definition as explained in section 4.1, where risk identification is the first part of risk analysis. As previously mentioned, this thesis follows Rausand's [6] definition. It will regard both ISO 31000's [21] risk identification and risk analysis as part of safety risk analysis.

According to ISO 31000 [21], an organization should, as a part of risk identification, find, recognize, and describe risks that might prevent them from achieving their objectives. To do this ISO 31000 [21] lists several factors that should be considered, as well as any relationship between them. The factors are as follows:

- tangible and intangible sources of risk
- causes and events
- threats and opportunities
- vulnerabilities and capabilities
- changes in the external and internal context
- indicators of emerging risks
- the nature and value of assets and resources
- consequences and their impact on objectives
- limitations of knowledge and reliability of the information
- time-related factors
- biases, assumptions, and beliefs of those involved.

Once risks have been identified, they should, according to ISO 31000 [21], be analyzed to comprehend the nature of the risk and its characteristics. Risk analysis

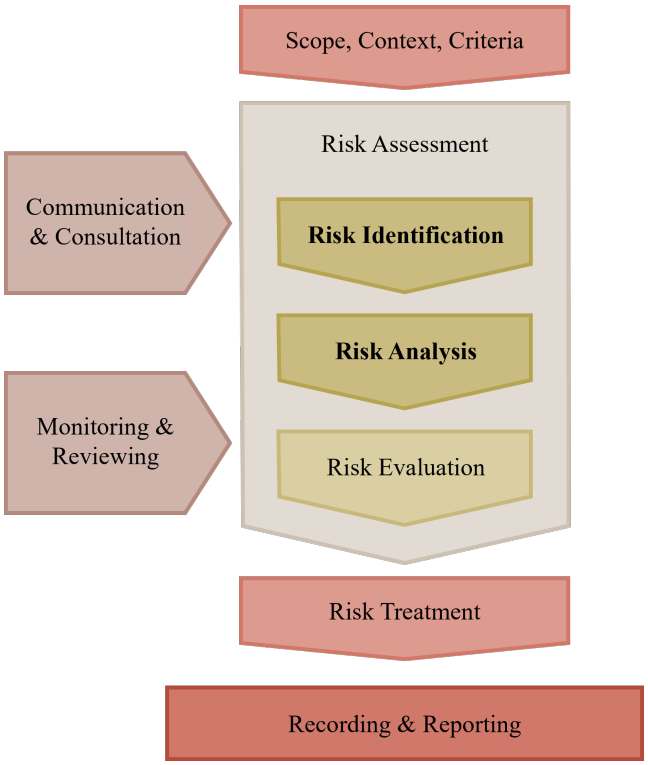


Figure 4.2: How ISO 31000 defines risk assessment. Reproduced from ISO 31000 [21]

can be carried out with varying degrees of detail and complexity. It mainly depends on the purpose of the analysis, the availability and reliability of the information, and the resources available. According to ISO 31000, risk analysis should consider factors like:

- the likelihood of events
- the nature and magnitude of the consequences
- connectivity, complexity, and volatility of risks
- time-related factors
- the effectiveness of existing controls
- sensitivity and confidence levels

ISO 31000 [21] points out that risk analysis can be affected by differences in opinions, biases, perceptions of risk, and judgment of those performing the analysis. Additionally, the quality of information, assumptions, exclusions, and limitations of techniques can also impact the process and results. Therefore, according to ISO 31000 [21], these factors should be considered, documented, and communicated to those who use the results of the analysis.

4.2.2 Methods: Safety Risk Analysis

Several methods for safety risk analysis have been developed. They include

A **Hazard and Operability study (HAZOP)** is, according to Rausand [6], a systematic hazard identification process that is carried out by a team of experts to identify and assess potential risks to people and equipment. The team explores how the system or plant deviates from the design intent and how that creates hazards and operability problems. The aim is to uncover any hidden design or engineering issues. HAZOP is a qualitative technique.

Event Tree Analysis (ETA) is, according to Rausand [6], the most common method for the development of accident scenarios. ETA is a top-down risk assessment technique used to analyze potential sequences of events following an initial event or accident. It involves constructing a graphical representation of events that may unfold, branching out from the initial event, as seen in figure 4.3. Each branch represents a possible outcome or consequence if different safeguards are successful or fail. ETA aims to provide a visual approach to understanding the potential consequences of an event and how different safeguards approve outcomes. The event tree structure is suitable for quantitative analysis.

Fault Tree Analysis (FTA) is, according to Rausand [6], the most common method for causal analysis of hazardous events. FTA is a type of top-down failure analysis examining an undesired system state. It involves constructing a graphical representation of the logical relationships between various contributing factors or failures that lead to the undesired event, as seen in figure 4.4. The top event represents the final failure, while the lower-level events are the contributing factors. By analyzing the fault tree, probabilities of individual events and combinations of events can be assessed, helping identify critical factors and potential areas for improvement or mitigation. FTA is suitable for qualitative and quantitative analysis

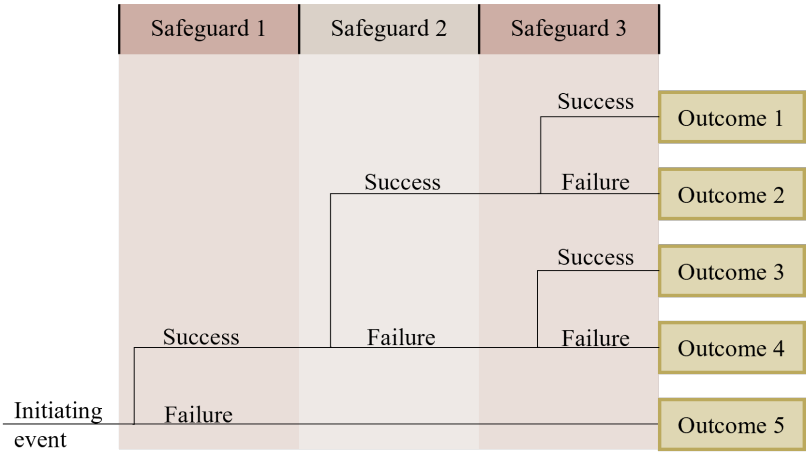


Figure 4.3: A generic example of an Event Tree

of complex systems but is not well suited to handle dynamic systems. Furthermore, the method is also sometimes too rigid in its requirements regarding binary states and Boolean logic.

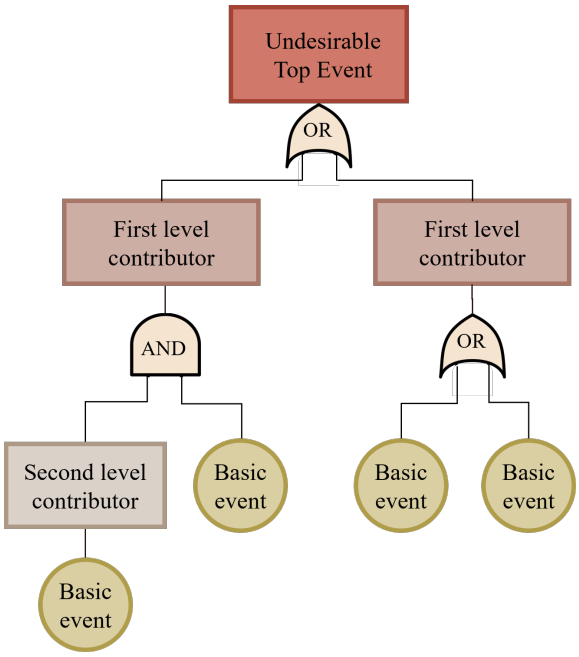


Figure 4.4: A generic example of a Fault Tree

A **Bowtie diagram** [6], as seen in figure 4.5, depicts the relationship between an identified hazardous event, its causes and consequences, and the barriers implemented to reduce the likelihood of the event and mitigate its consequences. The barriers on the left side are proactive barriers to reduce the probability of the

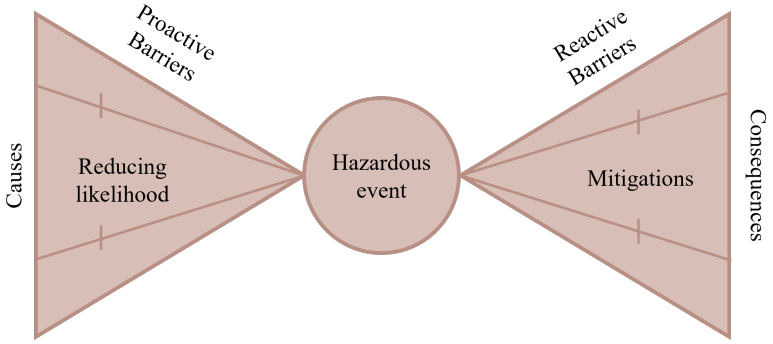


Figure 4.5: A generic example of a bow tie diagram

event, and the barriers on the right are the reactive barriers to mitigate potential damages. The bowtie can be viewed as a combination of ETA and FTA but more comprehensive.

4.3 Cybersecurity Standard and Methods

4.3.1 Standard: IEC 62443-3-2

IEC 62443 *Industrial Communication Networks - Network and System Security* [3] is an international series of standards, technical specifications, and technical reports released by the International Electrotechnical Commission (IEC). IEC is an international standards organization that prepares and publishes electrotechnology and related technology standards. 62 countries are members of the IEC through their national standards committee. IEC 62443 [3] comprises international standards, technical specifications, and technical reports. IEC 62443 is structured in four main parts, each consisting of several publications, as seen in figure 4.6. The parts are General, Policies and Procedure, System, and Component. Part 3 provides guidance on designing and implementing a secure IACS at the system level, including security policies and risk assessment. Part 3-2 deals with security risk assessment for system design.

IEC 62443-3-2 [22] is based on the concept of partitioning the SUC into zones and conduits, as explained in section 2.1. IEC 62443-3-2 [22] establishes requirements for partitioning the SUC into zones and conduits, assessing risk for each zone and conduit, establishing the target security level for each zone and conduit, and documenting the security requirements. The use of zones and conduits limits the potential for lateral movement of attacks and reduces the overall attack surface.

The standard assists in establishing target security levels for each security zone and conduit within the IACS. This concept involves defining the desired level of protection and specifying the necessary security controls. By setting these targets,

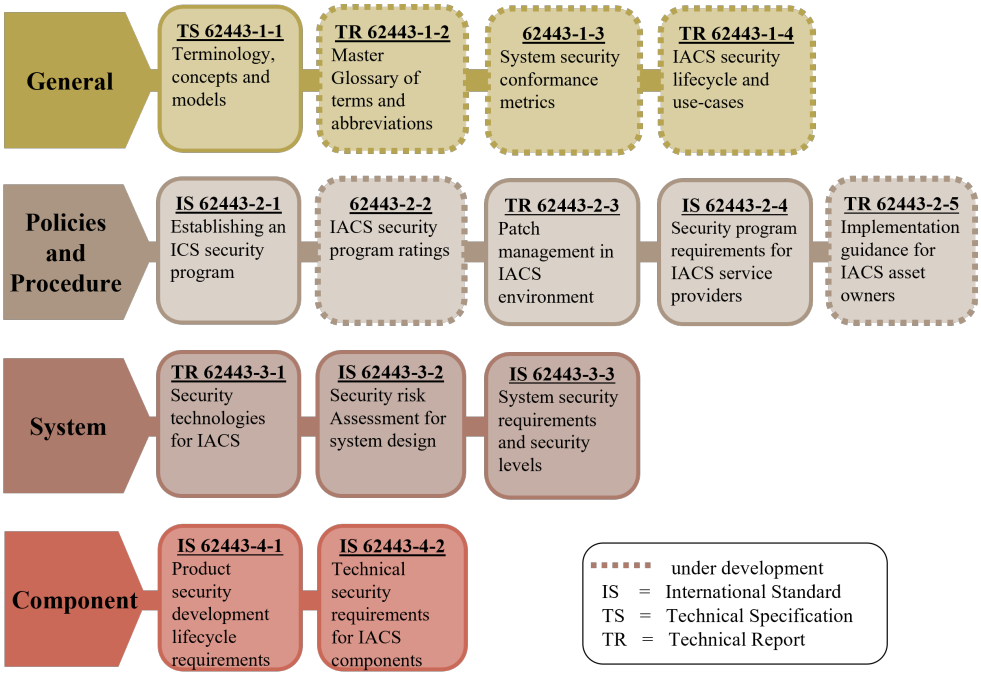


Figure 4.6: The different parts of the IEC 62443 series of standards.

organizations can work towards achieving a consistent and adequate security posture throughout their IACS.

According to IEC 62443-3-2 [22], to perform a detailed cybersecurity risk assessment an organization must

1. Identify threats.
2. Identify vulnerabilities .
3. Determine the consequence and impact.
4. Determine the unmitigated likelihood.
5. Determine the unmitigated cybersecurity risk.
6. Determine the targets for the security levels (SL-T).
7. Compare unmitigated risk with tolerable risk.
8. Identify and evaluate existing countermeasures.
9. Reevaluate the likelihood and impact.
10. Determine residual risk.
11. Compare residual risk with tolerable risk.
12. Identify additional cybersecurity countermeasures.
13. Document and communicate the results.

This recommended workflow is illustrated in figure 4.7.

The final step is documenting and communicating the results of the risk assessment. IEC 62443-3-2 emphasizes the importance of documenting security requirements, policies, and procedures. This documentation ensures clarity and consistency in implementing security measures throughout a facility. It also aids in au-

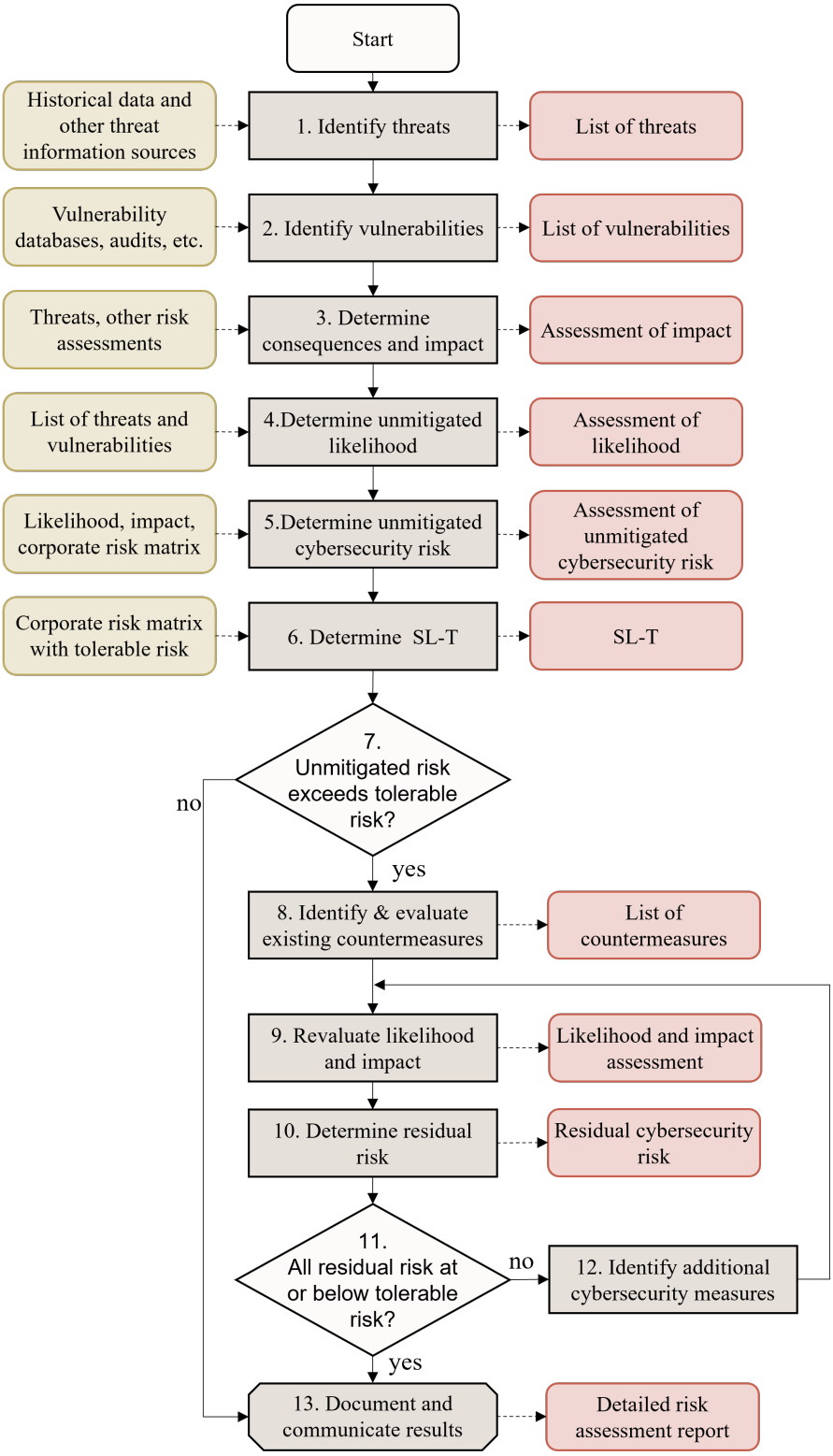


Figure 4.7: How IEC 62443-3-2 detail cybersecurity risk assessment workflow. Reproduced from IEC 62443-3-2 [22]

diting and verifying compliance with established security practices. Lastly, these results must be effectively communicated to stakeholders to improve awareness and facilitate informed decision-making.

4.3.2 Methods: Cybersecurity Risk Analysis

Several methods have been developed for cybersecurity risk analysis. For instance, **Threat Modeling** which is a systematic approach used in cybersecurity to identify and understand potential threats and vulnerabilities in a system or application. It involves analyzing the system from an attacker's perspective to identify potential entry points, weaknesses, and attack vectors. The main objective of threat modeling is to proactively identify and prioritize potential threats, allowing organizations to develop adequate security controls and countermeasures. However, most Threat Modeling methodologies are developed for IT systems and may not be ideal or unsuitable for OT systems.

Attack Tree Analysis (ATA) [25] is a quantitative analysis method that can work with OT systems. ATA [25] is used to evaluate potential attack scenarios systematically. It involves breaking down the main objective of an attacker, known as the "root" of the tree, into smaller attack goals or sub-objectives, seen in figure 4.8. Each sub-objective represents a specific attack vector or vulnerability. These sub-objectives are further expanded into sub-nodes, forming a hierarchical structure and using logical ports to represent the attack's steps or stages. The child nodes often represent certain conditions that must be satisfied for a method to succeed. By analyzing the attack tree, organizations can identify potential attack paths and assess the associated risks. The analysis helps to understand the dependencies and relationships between different attack vectors. Attack tree analysis allows prioritizing critical risks based on quantified likelihood and impact assessments. The analysis results inform decision-making regarding security risk mitigation strategies.

ATA has some similarities with FTA from section 4.2.2 as they both used to assess risks and analyze potential events or scenarios. Both methods use a hierarchical tree-like structure and logic gates to visually represent the events or scenarios being analyzed, as seen in figures 4.8 and 4.4. FTA focuses on reliability analysis and the identification of potential failure modes. ATA focuses on security analysis and identifying vulnerabilities and weaknesses from an attacker's perspective. While FTA considers the system from a reliability and failure perspective, ATA adopts an attacker's viewpoint. FTA is concerned with identifying the causes and events that lead to system failures or undesired events. It assesses failure probabilities and critical failure modes. Contrarily, ATA identifies potential attack paths and analyzes the steps an attacker may take to achieve their objectives.

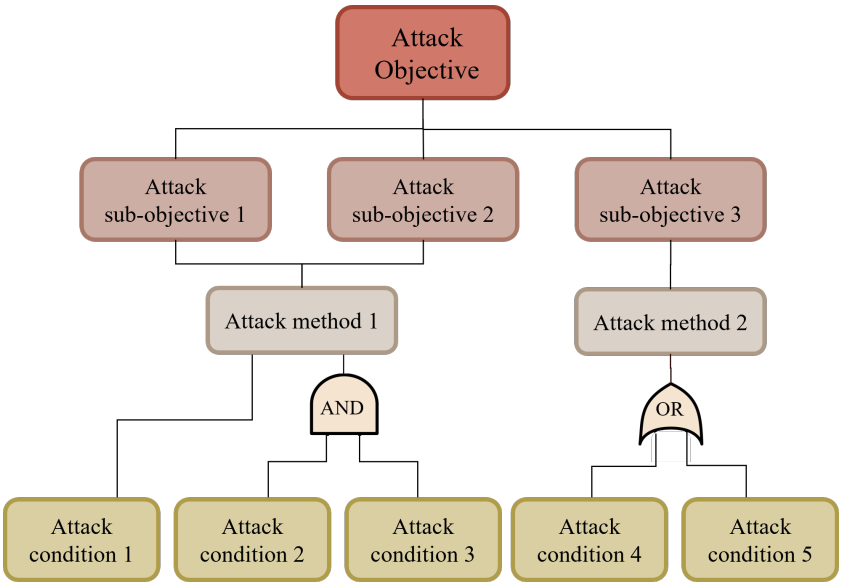


Figure 4.8: A generic example of an Attack Tree Analysis

Chapter 5

Combined Safety and Security Risk Analysis

In this chapter, the focus is on examining the combined analysis of safety and cybersecurity risks. It is becoming increasingly necessary for the industry to implement a combined safety and cybersecurity risk analysis. Firstly, the growing interconnectivity of industrial systems and the increased industrial use of information technology exposes them to cyber threats that can compromise safety. Traditional safety analysis methods alone are insufficient to address these evolving risks. Secondly, the convergence of OT and IT systems has blurred the boundaries between safety and cybersecurity, requiring a holistic approach to risk management. Thirdly, cyberattacks on critical infrastructure have demonstrated the potential for severe physical consequences, emphasizing the need to integrate safety and cybersecurity measures. Additionally, regulatory bodies are recognizing the importance of addressing safety and cybersecurity in risk assessments and are developing their standards accordingly. By implementing combined analyses, the goal is that organizations can proactively identify and mitigate vulnerabilities, protect against emerging threats, and ensure the overall resilience and security of their systems.

5.1 Frequency of Academic Publication

The frequency of academic publication on the topics was examined to gain insight into how prevalent the topic of safety and cybersecurity risk analyses is in the professional community. This examination was done using Engineering Village [26], a search and discovery platform focused on engineering topics. The search compared three categories: safety risk analysis, cybersecurity risk analysis, and safety and cybersecurity risk analysis. The Boolean search expressions that were used are found in table 5.1. Both the terms "cybersecurity" and "cyber security" were included as both spellings are commonly used.

First, the total number of hits generated for each search expression was ex-

Table 5.1: The Boolean search expressions used for the literature review using Engineering Village.

	The Boolean search expression used
Safety Risk Analysis	safety "risk analysis" NOT security NOT cybersecurity
Cybersecurity Risk Analysis	(cybersecurity OR "cyber security") AND "risk analysis" NOT safety
Safety & Cybersecurity Risk Analysis	Safety AND (cybersecurity OR "cyber security") AND "risk analysis"

amined, this included conference article, journal articles, standards, and so forth. The results are seen in figure 5.1. The disparity in publications is evident, with a significantly larger body of work focused on safety compared to cybersecurity and notably fewer publications combined safety and cybersecurity analysis.

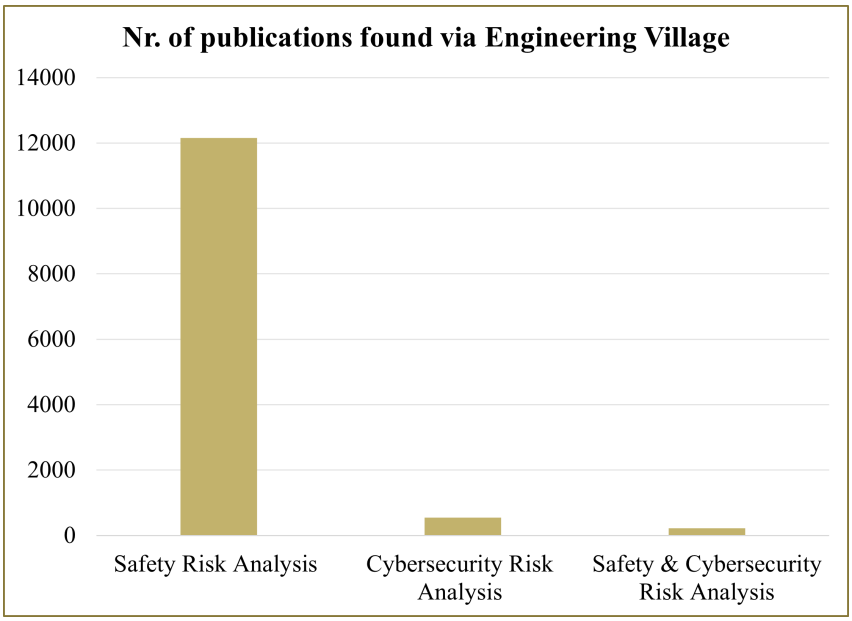


Figure 5.1: The total number of hits Engineering Village supplied when searching for the different types of risk analysis.

Second, the development within the three categories over the last ten years was examined. The graphs in figure 5.2 show the number of documents published per year for the last ten years for each search term. For safety risk analysis, the number is pretty stable and averages around 650, with one unusual spike in 2014. The number has steadily risen over the last decade for cybersecurity risk analysis and combined safety and cybersecurity risk analysis. This increase can point to safety risk analyses being an established field of study, whereas cybersecurity and combined risk analyses are a growing area of research.

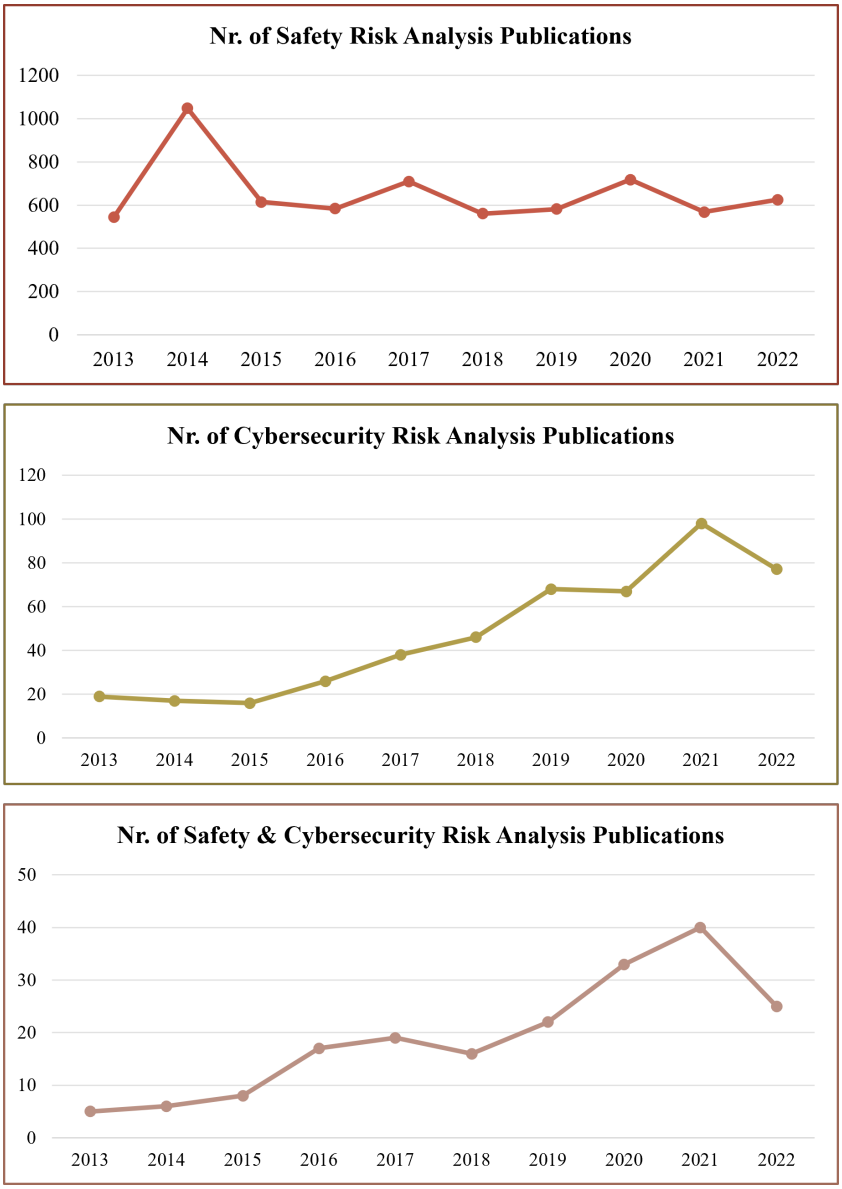


Figure 5.2: The number of hits per year Engineering Village supplied when searching for the different types of risk analysis.

5.2 Safety and Cybersecurity Standard: ISA TR 84.00.09

ISA 84 is a series of standards and technical reports that deal with various aspects of achieving functional safety in the process industries published by the International Society of Automation (ISA). ISA is a non-profit organization that develops and promotes standards, education, and networking opportunities for industrial automation. ISA TR 84.00.09 *Cybersecurity Related to the Functional Safety Lifecycle* [27] is one of the technical reports in the ISA 84 series. ISA TR 84.00.09 was

published in 2017, with a new update in the works and planned for publication in 2023. The 2017 version will be regarded first, and then some comments will be made regarding the update.

ISA TR 84.00.09 [27] was developed on the premise that it is necessary to include cyber risk in risk and hazard analysis of industrial processes in today's world. The technical report[27] states that the traditional analyses have generally excluded cyber-related attacks that could potentially cause process safety incidents. The technical report targets process control, process safety, and operations personnel to better understand the impact cybersecurity has on process safety and the necessary relationship with IT.

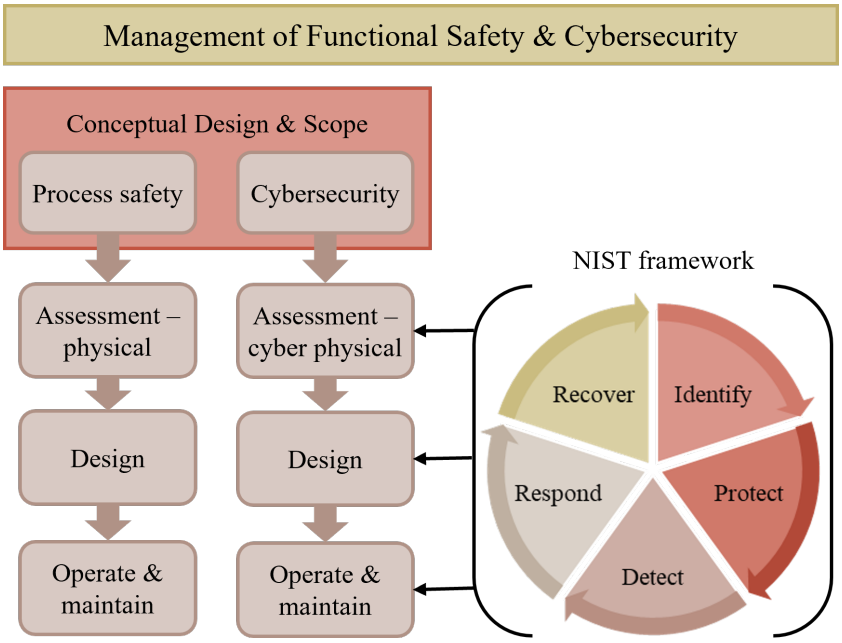


Figure 5.3: Cybersecurity lifecycle integrated with process safety management. Adapted from ISA TR 84.00.09 [27].

ISA TR 84.00.09 [27] states that the underlying premise of the report is to aid the users in understanding how to integrate cybersecurity into the safety lifecycle. The technical report provides guidance on how to implement, operate, and maintain Safety Controllers, Alarms, and Interlocks (SCAI) securely. ISA TR 84.00.09 [27] emphasizes that although achieving higher security levels may result in less convenience to the end user, it is a necessary part of the integration. A key element of ISA TR 84.00.09 is the integrated lifecycle. The technical report [27] states that the work done to ensure the security of an IACS should account for the entire safety lifecycle and that security should be addressed at all phases of the safety lifecycle. Figure 5.3 is how ISA TR 84.00.09 proposes that functional safety and cybersecurity could integrate within the overall safety lifecycle. The lifecycle starts with a new process plant, the initial scope stage, and continues throughout all the phases. According to ISA TR 84.00.09 [27], it is impossible to adequately

understand the relative independence and integrity of various layers involving instrumented systems, including SIS, without addressing cybersecurity throughout the entire safety lifecycle.

The scope of ISA TR 84.00.09 [27] is to address and provide guidance on integrating the cybersecurity lifecycle with the safety lifecycle as they relate to SCAI, including SIS. This scope includes work processes and countermeasures implemented to reduce the risk that cybersecurity threats pose to IACS networks. Cyberattacks can act like a common mode failure that can cause hazardous events and prevent instrumented protection functions, including SIS, from performing their intended purpose. Therefore, the technical report provides recommendations to ensure that SCAI are adequately secured. ISA TR 84.00.09 addresses both external and internal cybersecurity threats.

ISA TR 84.00.09 [27] proposes that successful cybersecurity programs must consider the difference between traditional IT roles and IACS to develop a cohesive safety and cybersecurity program. Table 5.2 shows the contrasts between cybersecurity and functional safety risk analysis, as stated in ISA TR 84.00.09 [27].

Table 5.2: Comparison of risk analysis of functional safety and cybersecurity in IACS, as stated in ISA TR 84.00.09 [27]

	Functional Safety	**IACS Cybersecurity**
Target of evaluation	Equipment under control (EUC)	System under consideration (SUC)
Failure likelihood	Random failures due to operational and environmental stresses. Systemic failures due to errors during safety lifecycle.	Threats, both internal, external or combination. Vulnerabilities due to component or system design flaws, non-validated changes and not following cybersecurity practices and procedures.
Consequence severity	Impact on environment, health and safety of personnel and general public	Loss of availability, data integrity, and/or confidentiality has direct impact on functional safety.
Risk categorization	Based on likelihood and severity. Risk may be quantified	Based on likelihood and severity. Risk is currently qualitative. Assigned to zone with security level for each zone and conduit.

5.2.1 2023 update

A draft of ISA TR 84.00.09-2023 has been released for review and comment. It is set to be published in 2023 but has yet to be as of April 2023. It is more comprehensive, almost three times as long, and will supersede the 2017 version when published. According to security consultant John Powell [28], the new version will make notable changes to the functional safety lifecycle via cybersecurity additions. The 2023 version will also include more detailed information explaining how to use the IEC-62443 standards and the functional safety from the IEC-61511 standards. According to Powell [28], some of the significant addition will include:

- Network topology and the Purdue reference model.
- Zero Trust architecture concept.
- Vulnerability identification.
- Access management.
- Incident management.
- Security Protection Ratings, similar to maturity level.
- Project scope development.
- Greater detail on how to perform a cyber risk assessment.
- Secure configuration practices.
- Identifying the roles and responsibilities of stakeholders.
- Defining cybersecurity alarm and alert responsibilities.

5.3 UFoI-E/CyPHASS

The Uncontrolled Flow of Information and Energy (UFoI-E) framework is designed to identify safety and security risk scenarios in Cyber-Physical System (CPS). The premise is that a cyber threat can be related to a loss of control of information flows in a system. This uncontrolled flow of information can in turn lead to uncontrolled flow of energy in a physical process, for example malicious commands from malware to system actuators.

This section is based on publications the researchers behind UFoI-E and CyPHASS, by Guzman et al. [29] [30], and researcher at the Technical Research Centre of Finland, Alanen et al. [31].

The framework consists of three components, the first is conceptual, and the last two are more practical:

- **UFoI-E causality concept**, the theoretical foundation of the UFoI-E method. Guzman et al. [29] defines a causation model to “abstract the causal chains in physical harm scenarios”.
- **CPS master diagram**,a generic framework for representing CPSs to have a common model for safety and security analysis, seen in figure 5.4. According to Guzman et al. [29], the diagram’s purpose is to supply a shared conceptualization of a system that can be used by multidisciplinary teams when developing diagrammatic representations of their systems for analysis.

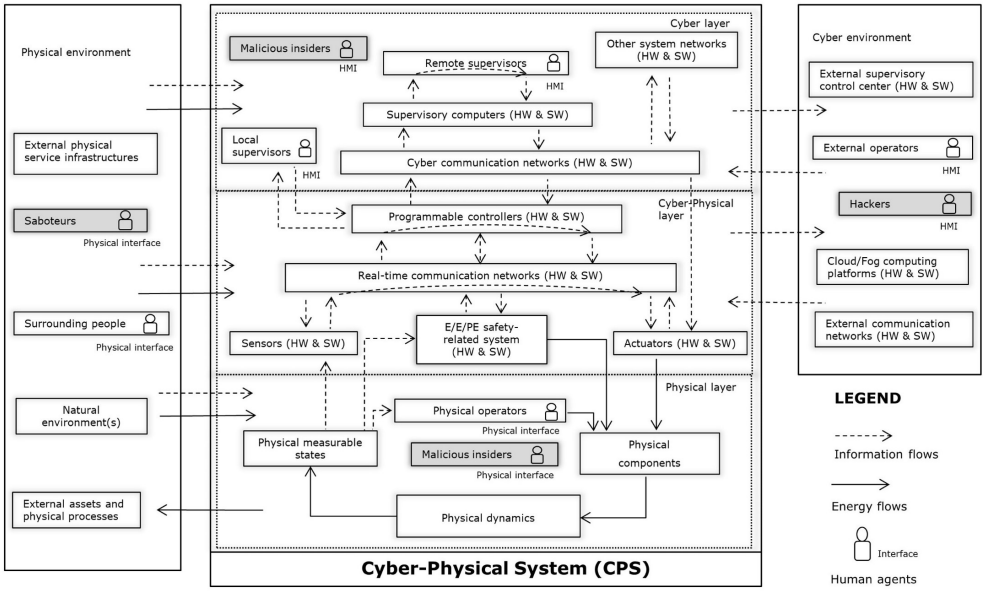


Figure 5.4: Cyber-Physical System master diagram. From Guzman et al. [29]

- **Cyber-Physical Harm Analysis for Safety and Security (CyPHASS)**, a harm scenario builder designed as a practical risk identification tool, as seen in figure 5.5 and a larger version in found in appendix A. CyPHASS combines the ontology of scenarios in an extended bowtie model, as discussed in section 4.2.2, with an extensive database of risk sources and barriers to identify harm scenarios.

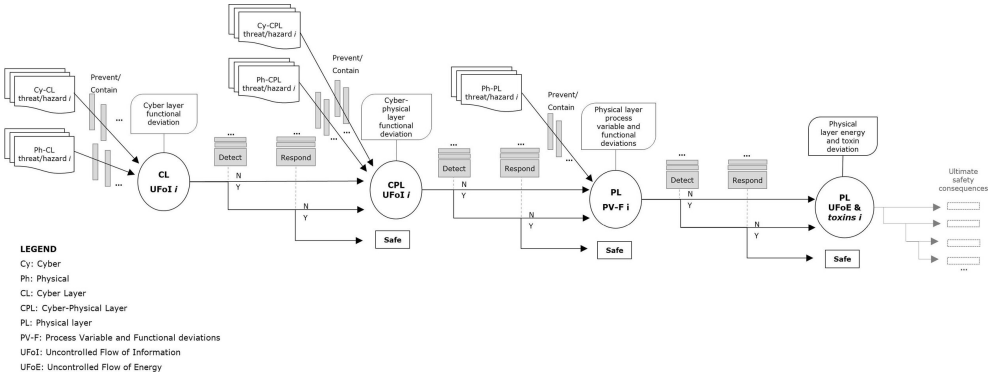


Figure 5.5: The CyPHASS scenarios builder. A larger version is found in appendix A. From Guzman et al. [29]

The three components of UFoI-E and their relation are illustrated in figure 5.5.

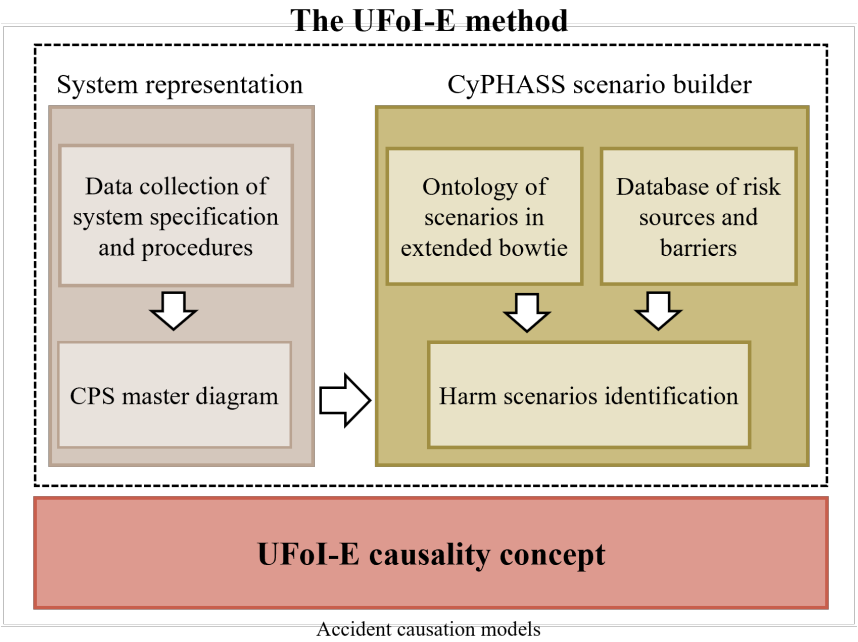


Figure 5.6: The CyPHASS scenario builder and the CPS diagram as a part of the UFoI-E method. Reproduced from Guzman et.al. [29]

The CPS master diagram represents the CPS being analyzed as a three-layer system, consisting of:

- **Cyber Layer (CL)**, the operations layer.
- **Cyber-Physical Layer (CPL)**, the control layer.
- **Physical Layer (PL)**, physical manifestation layer, such as energy flows.

Alanen et al. [31] state that CyPHASS is a top-down method that begins by identifying the hazard that is the ultimate safety consequence. UFoI-E is separated into Uncontrolled Flow of Information (UFoI) and Uncontrolled Flow of Energy (UFoE) and regarded individually. The process starts at the right side of the CyPHASS scenario builder seen in figure 5.5 and works backward. The organized stepwise process of the identification of risk scenarios is summarized by Guzman et al. [29] in the following steps:

1. Identify the cases of UFoE that could lead to ultimate safety consequences.
2. For each UFoE, identify the causes as PL Process Variable and Functional deviations (PV-F)
    a. For each PL PV-F deviation. identify and recommend detection and response barriers in all three layers
3. For each PL PV-F deviation, identify causes as physical hazards and threats
    a. For each physical hazard and threat, identify and recommend preven-

tion barriers in the physical layer

4. For each PL PV-F deviation, identify causes as cyber-physical UFoI
    a. For each cyber-physical UFoI, identify and recommend detection and response barriers in all layers
5. For each cyber-physical UFoI, identify causes as cyber and physical hazards and threats
    a. for each cyber and physical hazard and threat, identify and recommend prevention barriers in the cyber-physical layer
6. For each cyber-physical UFoI, identify causes as cyber UFoI
    a. For each cyber UFoI identify and recommend detection and response barriers in all layers
7. For each cyber UFoI, identify causes as cyber and physical hazards and threats
    a. For each cyber and physical hazard and threat, identify and recommend prevention barriers in the cyber layer

Guzman et al. [29] state that compared to conventional safety analysis methods for risk identification, the extended bowtie model utilized in CyPHASS exhibits a clear correlation with fault tree analysis (FTA) and event tree analysis (ETA). CyPHASS incorporates an expanded bowtie ontology comprising four consecutive top events, effectively enhancing the qualitative identification of safety and security scenarios through its comprehensive framework. By leveraging the CPS master diagram and a database of checklists and guidewords, CyPHASS enables a stepwise analysis that facilitates tracing propagation effects across different layers of the CPS. This approach offers improved capabilities for qualitatively identifying safety and security scenarios.

5.3.1 TRISIS analysis

The CyPHASS scenario builder was used to examine the UFoIs present in the TRISIS attack. The results are split into figures 5.7 and 5.8. Figure 5.7 shows the three cyber-physical UFoIs that were identified: violation of data integrity, logic integrity, and logic availability. The associated threat and hazard is the TRISIS malware manipulating or disabling the SIS.

Figure 5.8 shows the two cyber UFoIs that were identified: violation of data integrity and logic integrity. The associated threat and hazard is the TRISIS malware.

As the TRISIS attack did not actually result in physical consequences, there are no UFoEs. Had the-two part attack, as discussed in 3.2.3, been carried out, there would likely have been UFoEs that could have resulted in an explosion or fire.

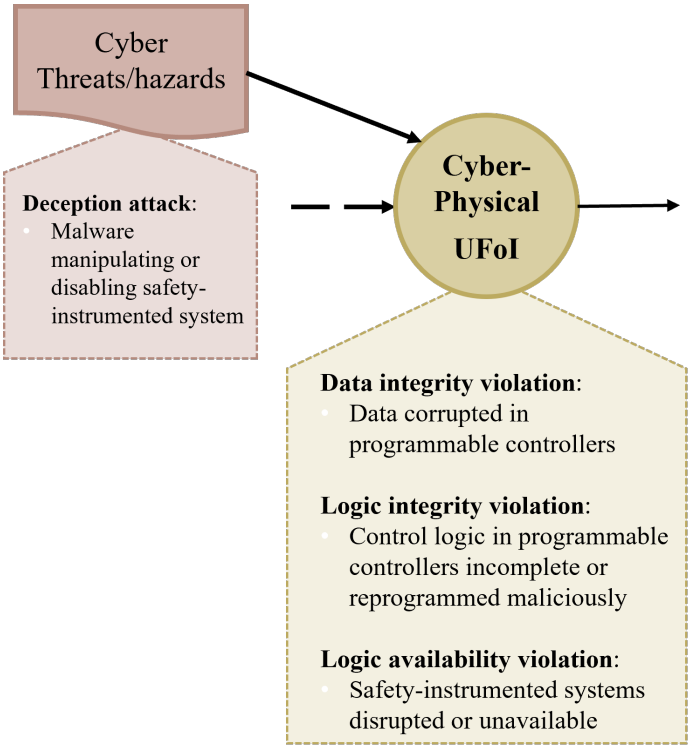


Figure 5.7: The cyber-physical UFoIs identified in the TRISIS attack.

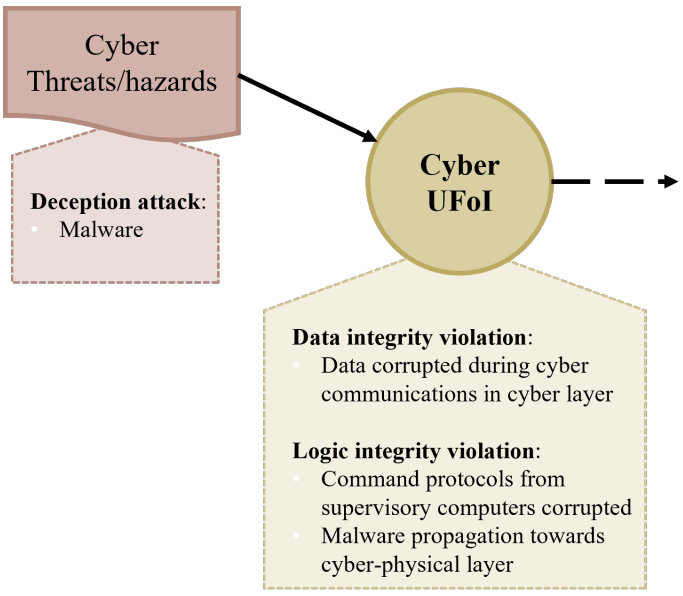


Figure 5.8: The cyber UFoIs identified in the TRISIS attack.

5.4 CCE

Consequence-driven Cyber-informed Engineering (CCE) is a methodology to identify worst-case functional impacts and determine High Consequence Events (HCE). CCE was developed by Idaho National Laboratory (INL), one of the United States Department of Energy's national laboratories. CCE is based on the INL's [32] assumption that if a skilled and determined threat actor targets critical infrastructure, the targeted infrastructure can and will be penetrated. Therefore, organizations must have a way to evaluate their complex systems, determine what must be safeguarded and then apply engineering solutions to isolate and protect their must critical assets.

According to the INL [33] CCE offers a framework for both private and public organizations to assess their own environments for HCEs and risks. It involves identifying the implementation of critical devices and components that facilitate those risks. Furthermore, CCE aims to illuminate specific and plausible cyberattack paths that threat actors could use to exploit these devices with a think-like-an-adversary approach. Lastly, CCE aims to assist in developing tangible mitigations, protections, and tripwires to effectively address and mitigate the risks associated with the identified HCEs.

The CCE methodology is designed to be performed iteratively by an organization's collaborative team and takes advantage of an organizations detailed knowledge of their own operation. CCE leverages an organizations unique and in-depth understanding of their own functions and operation from a technical and operational perspective. This makes it more challenging to apply CCE as an outsider. Completing a full CCE process is an extensive and considerable undertaking.

CCE consists of four phases, each includes several steps. The four phases are Consequence Prioritization, System-of-Systems Analysis, Consequence-based Targeting, and Mitigations and Protections, as seen in figure 5.9.

The following section is based mainly on the CCE Four-Phase Reference Document [34], the CCE Fact Sheet [32], and a CCE case study called "Stinky Cheese Company" [35], all published by the INL. As CCE is meant to be performed by a knowledgeable group, this entity will be referred to as team in the following sections.

5.4.1 Phase 1: Consequence Prioritization

The INL [34] states that the primary goal of the Consequence Prioritization phase is to identify potential disruptive cyber events that would significantly disrupt an organization's ability to provide their critical services and operations. INL [34] defines cyber events as physical events that are achievable through cyber means. Rather than focusing on the likelihood of a cyberattack, Consequence Prioritization is primarily concerned with the impact of potential adverse events.

The first step of Phase 1 is to identify the Objective. By combining both an adversarial viewpoint, and an internal viewpoint the team will choose what a threat

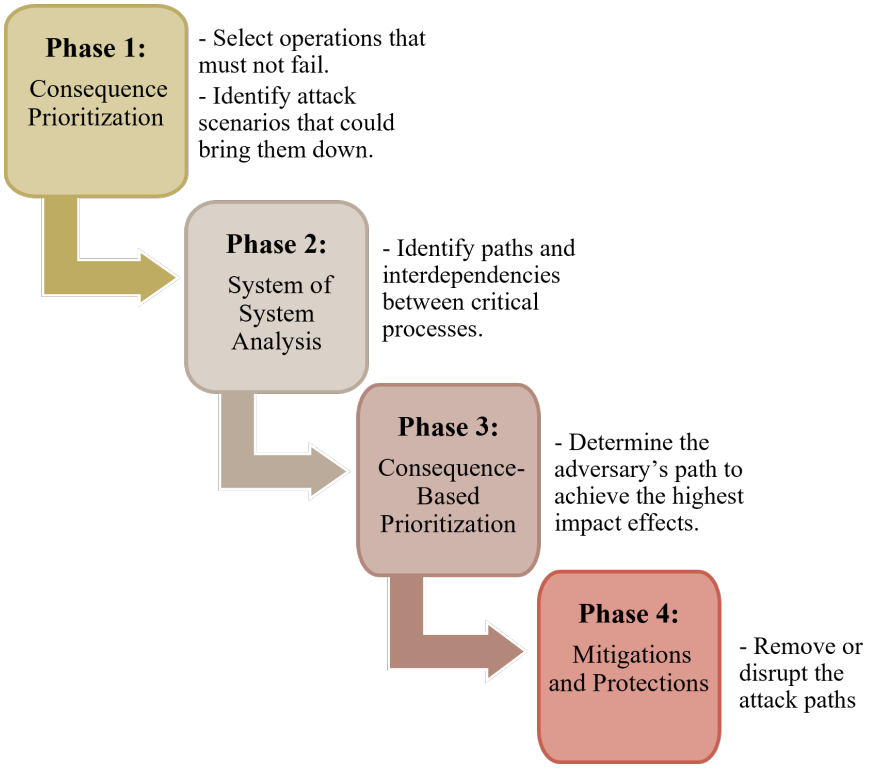


Figure 5.9: The four phases of Consequence-driven Cyber-informed Engineering (CCE).

actor's likely Objective is. For example, to cause a public health/safety incident. Next, the team specifies the Scope, i.e. focusing on what part of the organization's production would be targeted to meet the Objective. Based on the Objective and the Scope, the team will set the Boundary Condition, for example, to cause a public health/safety incident by creating a quality issue in a specified process that will compromise the supply integrity for a given time frame. Next, the team generate possible disruptive Events that could achieve the Boundary Conditions. Based on the generated events, the team develops the cyber-events by describing how cyber-means could achieve the events.

The next step is to evaluate the severity of an event and finally identify what the INL call High Consequence Event (HCE). This event that would be most catastrophic to the organization based on the chosen criteria.

The list of Criteria could include elements such as

- Impact to public health or safety
- Financial loss
- Disruption of production
- Loss of reputation

Each criteria is given a criteria weight of low, medium, and high, based on the teams evaluation.

Criteria Weighting can be

- Impact to public safety: HIGH (3)
- Financial loss: HIGH (3)
- Disruption of production: MEDIUM (2)
- Loss reputation: LOW (1)

By combine the list of criteria with their assigned weighting values the team can develop a cyber-event matrix as seen in table 5.3. A cyber-event matrix is developed for every identified cyber-event.

Table 5.3: A general cyber-event scoring matrix for evaluating each cyber-event.

		HCE severity scoring			
		None (0)	Low(1)	Medium (3)	High (5)
Criteria weighting	Criteria A $\alpha =$				
	Criteria B $\beta =$				
	Criteria C $\gamma =$				

Lastly, all the severity scores for the different cyber-events are gathered in a comparative table such as table 5.4. The comparative severity score for each cyber event is the sum of the severity ranking multiplied by the corresponding criteria weight. The Severity % is calculated by finding what percentage of the maximum impact points the scored impact points are.

Table 5.4: Comparative severity score for the identified cyber-events.

Event	α * **event scoring**	β * **event scoring**	γ * **event scoring**	**Severity score**	**Severity %**
Cyber-event 1					
Cyber-event 2					
Cyber-event 3					

After scoring is complete, the CCE Team will have identified the HCEs that have the greatest impact to the organization. The INL [34] recommends that the team should then present these findings to the organization's decision-makers. This sharing of information is done to validate that they agree with the group's findings and are willing to commit time and resources to the remaining CCE

phases. This approval from the top is essential for the team to avoid internal barriers or delays while accessing the information, people, equipment, and processes necessary to complete the rest of the CCE phases. The choice can be made to move forward with one or more HCEs.

5.4.2 Phase 2: System-of-Systems Analysis

The INL [32] states that the primary goal of the System-of-Systems Analysis is to gather information and identify the systematic interdependencies between critical processes, defense systems, and enabling or dependent components. This gathering of information is, according to the INL [34], mostly done by identifying, collecting, and organizing documentation relevant to an HCE. The team should also map out the systems and processes related to the HCE and investigate the dependencies and "unverified trust" which would enable them.

The team should, according to the INL [35], begin by creating a simple HCE block diagram, as seen in figure 5.10, that depicts the HCE from a functional perspective. The HCE block diagram should be designed starting with the system and component that must be affected to cause the HCE and then grown outward. Using this block diagram as a starting point, the team can then identify which production or business functions an adversary would have to disrupt to cause the HCE.

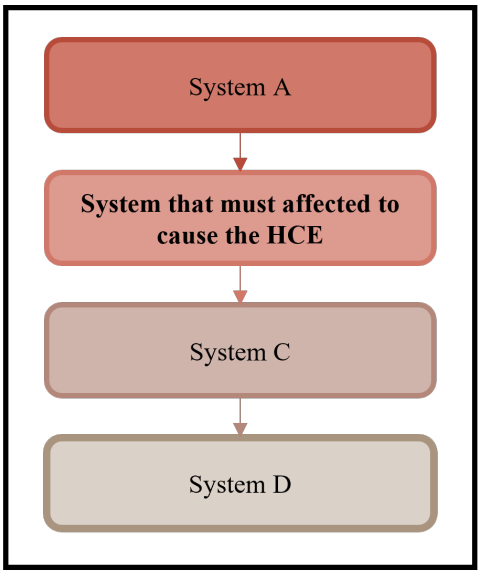


Figure 5.10: An example of a simple HCE block diagram, it should depict the HCE from a functional perspective.

The next step is to look deeper at the production function identified in the HCE diagram. The team must, according to the INL [35], consider

- What systems and components are involved in the HCE?

- What documentation is needed to describe interconnected systems and dependencies?
- What relationships with other entities are involved?

The team must develop “perfect knowledge” of the systems, operations, and support to succeed with this step. The objective is to identify the technical and operational details and where the information is documented and stored. Furthermore, they must determine if critical information is stored only on internal servers or is it also available on public-facing assets.

The INL [35] states that establishing "perfect knowledge" is most accurately and efficiently achieved through the development and use of a functional taxonomy. A functional taxonomy is a relational framework used for describing an organization’s critical functions, the People, Process, Technology (PPT) that enable those critical functions, and the so-called artifacts that document an organization’s unique implementation for function delivery. Most importantly, the taxonomy maps the organization’s Critical Functions (CF) and the Enabling Functions (EF) that support them. CFs describe the actions that make up the entity’s primary purpose. Should any of them be disrupted, it would have a severe negative impact on the entity. The EFs describe the infrastructure, people, processes, and systems that the entity uses to both physically and logically deliver the CFs. A simple taxonomy that only includes high-level CFs and EFs is seen in figure 5.11

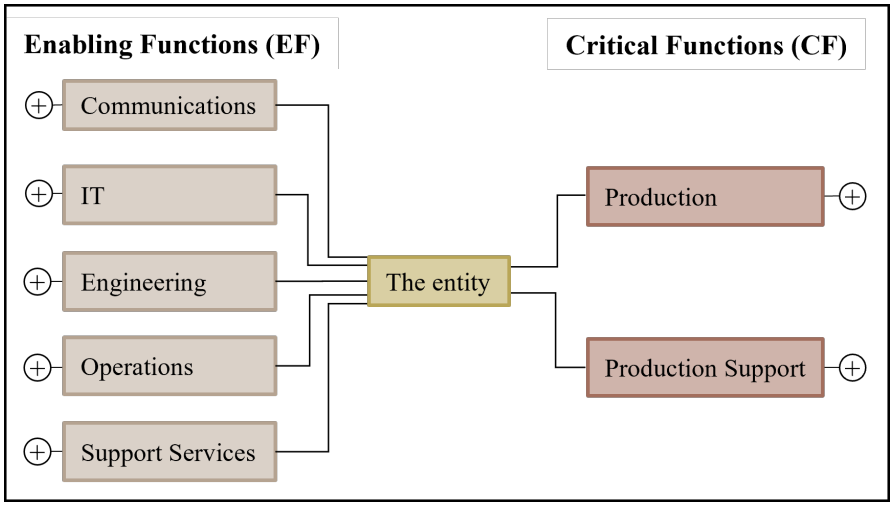


Figure 5.11: A simple taxonomy with high-level Critical Functions and Enabling Functions. Adapted from the Stinky Cheese CCE case study [35]

Each CF and EF in the taxonomy should be developed and branched out to include all elements they are a part of. The artifacts and their relative location within the taxonomy framework describe the “what”, “where”, “when”, “how,” and “who” of the HCE. A very detailed example of a functional taxonomy can be found in the Stinky Cheese case study [35].

The final step of Phase 2 is to create a System Description, which the INL [35]

defines as a summary of all the information gathered in Phase 2. This description should summarize the functional taxonomy mapping and provide traceability to where all the information is stored ad who has access to it.

Based on the Stinky Cheese case study [35], a general system description could involve elements such as:

- **Facility**. A description of the facility and the different process are involved.
- **Process**. A description of the selected process.
- **Process control**. A description of the controllers that regulate the process.
- **Control Platform**. A description of what systems, for example HMI, are used.
- **Operations**. A description of the operating procedures, for example what the plant operator does during a normal shift.
- **Vendor Support**. A description of which vendors are involved, what they provide and any network connectivity to the system they have.

5.4.3 Phase 3: Consequence-based Targeting

The INL [32] states that the primary goal of the Consequence-based Targeting phase is to determine an adversary's path to achieve the HCE, what parts of the system they must gain access to conduct the attack, and what information is required to achieve their goals.

During this phase, the team refines and develops the targeting requirements an adversary would need to fully understand to carry out an attack. Based on the system's description from Phase 1, the system is examined from an adversarial perspective. The goal is to determine what elements of the systems the adversary needs to manipulate to achieve the HCE. The primary goal is to identify what the INL [34] call "choke holds", any points the adversary must access or traverse to achieve a particular outcome. Choke holds are ideal locations to implement potential mitigations and protections to cut off a potential adversary's progress.

The INL [35] divides the adversary's activities into two stages: payload development and payload deployment. Payload development includes all the information, equipment, and software needed to develop a payload. Payload deployment includes the pieces of critical information the adversary needs to deliver the payload to the intended location.

Using the system description, the team should identify an adversary's:

- **Systems targeting description**: a combination of the System Description and the system analysis for targeting.
- **Technical approach**: what the adversary must do to cause HCE.
- **Targeting detail**: detailed description of the system's component(s) the adversary must manipulate to cause the HCE.

When phase 3 is completed, the team should have fully developed attack scenarios that can accomplish the HCE and a fully documented and referenced systems targeting description. According to the INL [34], each identified attack sce-

nario should include:

- **Technical Approach**: the requirements for each target, including the access to the target, the actions needed to be taken, and the timing and triggering of the payload.
- **Target Details**: a description of the technical details of each target that will be exploited or manipulated in order to implement the requirements from the Technical Approach.
- **Critical Needs**: what an adversary requires (information, access, components, software, etc.) for both payload development and deployment, including the most likely or easiest place to obtain them.

5.4.4 Phase 4: Mitigations and Protections

The INL [32] states that the primary goal of the Mitigations and Protections phase is to remove or disrupt the digital attack paths and take the possibility of the physical effect through cyber means out of the equation using engineering or process changes. Second, if this is not possible, using the detailed targeting requirements from phase 3 to detect adversary activity and implement other types of mitigation.

This primary goal is what is unique about CCE. Other methods, such as the CyPHASS database focus on what barriers to put in place. CCE on the other hand aims to make the attack unachievable, not only with a strong defense but with an inherently secure process design. This philosophy is not always possible to adhere to, especially with older systems, and there is still a need for traditional barriers.

CCE [35] recommends adhering to the NIST cybersecurity framework as seen in figure 2.7 but focuses on the last four: protect, detect, respond, and recover, as seen in figure 5.12.

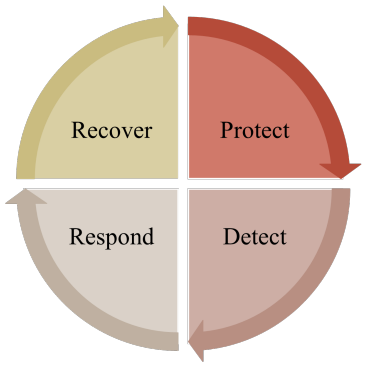


Figure 5.12: The parts of the NIST cybersecurity framework that CCE focuses on. Adapted from NIST [8]

The INL [34] has made its own definitions for the four functions to better address CCE's goal of protecting critical infrastructure:

- **Protect**: The ability to remove the objective of cyber-enabled sabotage (take

it “off the table” for an adversary)
- **Detect**: Enables timely discovery of adversary activities
- **Respond**: The ability to contain or disrupt adversary activities
- **Recover**: Timely restoration of critical functions and services

The INL [34] emphasizes the importance of the Protect function as such actions will, if implemented properly, effectively make it impossible for the adversary to cause a given HCE via cyber means. The majority of activity related to Protect is often day-to-day normal operation and "housekeeping". This applies to a significant part of Detect as well. Respond and Recover, however, apply exclusively when a cyber-event occurs. An organization needs incorporated routines for Protect and Detect that are a part of everyday life and protocols for executing Respond and Recover when needed.

5.4.5 Oldsmar analysis

The Oldsmar water treatment facility and the attack that occurred from section 3.1 there will be used as an example for the CCE process. The steps of Phases 1 and 2 will be done more completely, as the other phases require system insight into Oldsmar that is not publicly available.

It was wrongly assumed that adding the chemical lye to drinking water to increase the water’s pH played a part in disinfecting the water and removing harmful bacteria. However, it later became clear that the purpose of adding lye in the purification process is only to increase the water’s pH to improve taste and does not clean the water. Nevertheless, it is not an unlikely assumption that if an attacker can change the dosage of one added chemical, like lye, they can alter another, like chlorine, which is used to remove harmful bacteria. For the sake of simplicity, in the following example, too low a dosage of lye can lead to potentially unclean water.

Phase 1

The first steps are to identify the Objective, the Scope, and the Boundary Condition as explained in section 5.4.1. For Oldsmar they could be

1. **Objective**: cause a public health/safety incident that will compromise Oldsmar’s water supply for at least three days.
2. **Scope**: Oldsmar’s water purification process.
3. **Boundary Condition**: cause a health/safety incident by creating a water quality issue in the purification process that will compromise the water supply capability for at least three days.

The next step is to generate possible disruptive Events related to the Boundary Conditions. For Oldsmar, the events could be:

1. **No purification**: No lye is added to the water, potentially allowing unclean water to enter the water supply.

2. **Insufficient purification**: Too little lye is added to the water, potentially allowing unclean water to enter the water supply.
3. **Excessive purification**. Too much lye is added, potentially allowing toxic water to enter the water supply.

Developing the events into cyber-events gives

1. **No purification**: The threat actor gains access to the water purification system and targets the purification process. Malicious modification focuses on the purification control. The controller logic is changed so no lye is added to the water. The final water contains no lye.
2. **Insufficient purification**: Threat actor gains access to the water purification system and targets the purification process. Malicious modification focuses on the purification control. The controller logic is changed such that too little lye is added to the water. The final water contains significantly less than 100 ppm lye.
3. **Excessive purification**. Threat actor gains access to the water purification system and targets the purification process. Malicious modification focuses on the purification control. The controller logic is changed such that too much lye is added to the water. The final water contains significantly more than 100 ppm lye.

The list of Criteria that each cyber-event will be considered for Oldsmar are:

- Impact to public health or safety.
- Disruption of production (water supply).
- Loss of public trust.

Criteria Weighting can be

- Impact to public safety: HIGH (3)
- Disruption of production (water supply): HIGH (3)
- Loss of public trust: LOW (1)

The cyber-event scoring matrix for Oldsmar can be seen in table 5.5, the scorings are adapted from the Stink Cheese case study [35]. Several assumptions are made. In general, the matrix is made on limited knowledge about water treatment and the Oldsmar facility. More specifically, the severity scoring given to disruption of water supply is based on recommendations from the Norwegian Directorate for Civil Protection [36]. They recommend that every household have enough water to sustain themselves for three days. Consequently, disruption lasting longer than three days is given the highest severity. There is a lot of uncertainty involved. Different assumptions and information bases could lead to the events being assessed differently.

Table 5.5: Oldsmar's Cyber-event scoring matrix for evaluating each cyber-event.

	HCE severity scoring			
	None (0)	Low (1)	Medium (3)	High (5)
Impact to public safety $\alpha = 3$	There is no risk to public safety	There is a low but definite risk to public safety - a few illnesses but no permanent injuries occur	Danger to public safety due to significant number of illnesses, and one or more permanent injuries	Danger to public safety is widespread including significant number of illnesses, injuries, and on or more deaths
Disruption of water supply $\beta = 2$	Water supply will not be disrupted	Water supply is disrupted for 1 day	Water supply is disrupted for 3 days	Water supply is disrupted for 4 days or more.
Loss of public trust $\gamma = 1$	There is no risk of loss of public trust	Public trust is slightly damaged but not widely considered untrustworthy. Poor public opinion is minimal and temporary	Public trust is significantly damaged. Is considered untrustworthy but trust can be restored with significant sustained effort.	Irreparable damage to public trust, may be considered untrustworthy by wide public consensus

The cyber-event scoring matrix for each identified cyber event can be seen in tables 5.6, 5.7, and 5.8.

The identified cyber-events all focus on the lye purification process, and it is assumed that the other steps of water treatment such as filtration will remain intact. Therefore, the water that is insufficiently purified and not purified is still partially treated and doesn't carry as high a risk for disease and such as if all treatment steps were affected.

It is assumed that it will take three days for the water to return to normal levels of purification. This is based on information from the Sheriff's Office [13] that it could take up to 36 hours for changes made at the facility to reach the consumers. Combined with the potential time to Detect, Respond, and Recover, the conservative estimate of three days was made.

The calculated severity score for the three cyber-events can be seen in table 5.9. The max severity score for Oldsmar would be a score of 30, the severity % is calculated based on this number.

Using the established criteria for the Oldsmar example the Excessive Purifi-

Table 5.6: Oldsmar's Cyber-event scoring matrix for evaluating the No Purification cyber-event.

	HCE severity scoring			
	None (0)	Low (1)	Medium (3)	High (5)
Impact to public safety $\alpha = 3$			Danger to public safety due to significant number of illnesses, but no permanent injuries	
Disruption of water supply $\beta = 2$			Water supply is disrupted for up till 3 days	
Loss of public trust $\gamma = 1$			Public trust is significantly damaged. Is considered untrustworthy but trust can be restored with significant sustained effort.	

cation event scored the highest, as seen in table 5.9 and is the natural choice if choosing only one HCE to proceed with.

Table 5.7: Oldsmar's Cyber-event scoring matrix for evaluating the Insufficient Purification cyber-event.

	HCE severity scoring			
	None (0)	Low (1)	Medium (3)	High (5)
Impact to public safety $\alpha = 3$		There is a low but definite risk to public safety - a few illnesses but no permanent injuries occur		
Disruption of water supply $\beta = 2$			Water supply is disrupted for up till 3 days	
Loss of public trust $\gamma = 1$		Public trust is slightly damaged but not widely considered untrustworthy. Poor public opinion is minimal and temporary		

.

Table 5.8: Oldsmar's Cyber-event scoring matrix for evaluating the Excessive Purification cyber-event.

	HCE severity scoring			
	None (0)	Low (1)	Medium (3)	High (5)
Impact to public safety $\alpha = 3$				Danger to public safety is widespread including significant number of illnesses, injuries, and one or more deaths
Disruption of water supply $\beta = 2$			Water supply is disrupted for up till 3 days	
Loss of public trust $\gamma = 1$			Is considered untrustworthy, but trust can be restored with significant sustained effort.	

Table 5.9: The severity score for Oldsmar's cyber-events

Event	α * **event scoring**	β * **event scoring**	γ * **event scoring**	**Severity score**	**Severity %**
No purification	3 * 3	2 * 3	1 * 3	18	60 %
Insufficient purification	3 * 1	2 * 3	1 * 1	10	33 %
Excessive purification	3 * 5	2 * 3	1 * 3	24	80 %

Phase 2

A lack of publicly available information that describes the steps and processes of the Oldsmar water treatment facility makes making an HCE block diagram difficult. Therefore, a block diagram was made based on what the Center for Disease Control and Prevention (CDC) [37] says are common steps used for public water systems. For Oldsmar, the system that must be affected to cause the HCE is the systems and components that control the dosage of lye, as seen in the simplified figure 5.13.

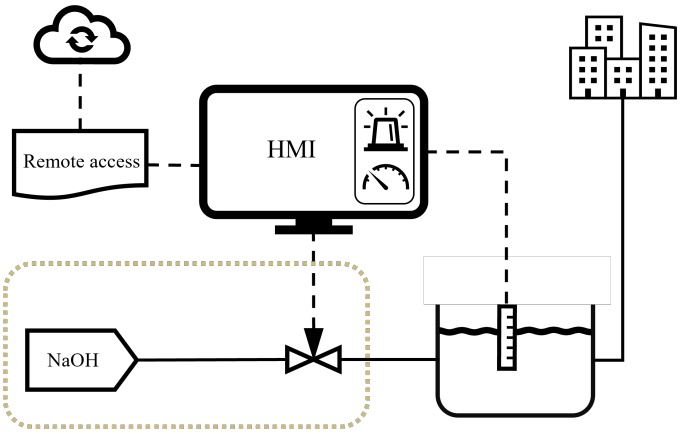


Figure 5.13: The part of the Oldsmar system (simplified) that must be affected to cause the Excessive Purification cyber-event.

Correlating that to the information provided by the CDC [37], that is the Disinfection step. The hypothetical HCE block diagram for Oldsmar is seen in figure 5.14.

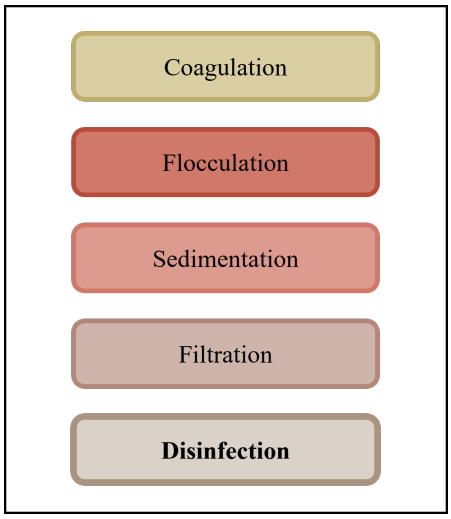


Figure 5.14: A hypothetical HCE block diagram for Oldsmar.

The basic structure of what the functional taxonomy of Oldsmar could look like including only high-level CFs and EFs is seen in figure 5.15. Each CF and EF in the taxonomy should be developed and branched out to include all elements they are a part of.

Based on the Stinky Cheese case study [35] the System Description for Oldsmar would include:

- **Water treatment**. A description of the water treatment facility and the dif-

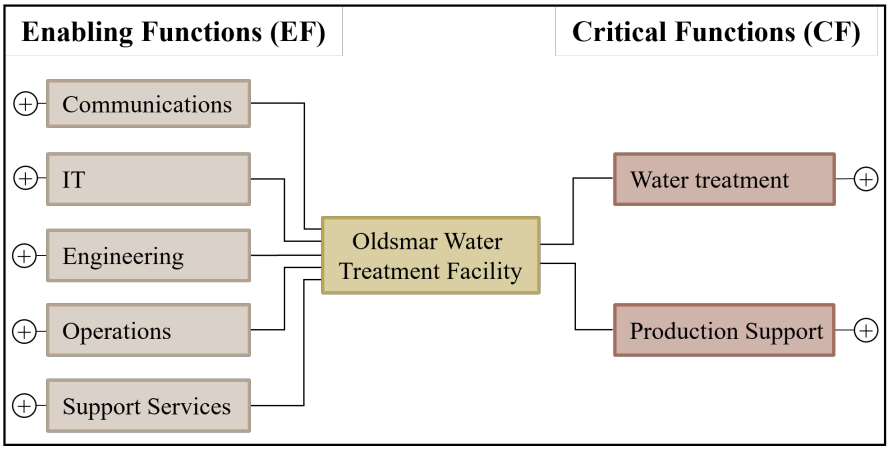


Figure 5.15: The high-level enabling functions and critical functions potentially related to the Oldsmar water treatment facility. Adapted from the Stinky Cheese CCE case study [35]

ferent processes that are involved.

- **Water purification**. A description of the water purification process, including the details of the lye dosage process.
- **Process control**. A description of the controllers that regulate the level of lye added to the water.
- **Control Platform**. A description of what systems, for example, Human Machine Interface, are used.
- **Operations**. A description of the operating procedures, for example, what the plant operator does during a normal shift.
- **Vendor Support**. A description of which vendors are involved, what they provide, and any network connectivity to the system they have. For example, if Oldsmar uses any vendors that have access via TeamViewer.

Phase 3

When considering both payload development and payload deployment, the System description from phase 2 should be used to identify the System Targeting Description, Technical Approach, and Target details.

Based on the Stinky Cheese case study [35] one should consider that an adversary's Payload Development will lead them to discover the following information about the Oldsmar facility.

- **Facility**. The physical location, process subsystems, and distribution breadth.
- **Process**. Critical subsystems and major control elements
- **Process control**. Sequencing, major control elements, and critical parameters for control.
- **Control Platform**. Controller and HMI identification, process screenshot.
- **Operations**. Process parameter monitoring and process visibility source.

- **Vendor Support**. Vendor technical support and remote access capabilities.
- **Safety**. Process/safety requirements.

Note, under Control Platform it states "process screenshot". This is what Cervani et al. [14] speculated that the attackers accomplished the first time they logged into the Oldsmar system.

Phase 4

The INL [34] emphasizes the importance of the Protect function as such actions will, if implemented properly, effectively make it impossible for the adversary to cause a given HCE via cyber means. A simple example of this using Oldsmar could be to change the valve used in the lye dosage to something with a lower capability such that delivering an extremely high level of lye is physically impossible for the actuator. A cyber-barrier on could be to incorporate some sort of a two-factor authentication requirement when making significant to the process changes, such as large setpoint changes.

Having identified the attack paths, the team could use another tool like the CyPHASS database to help identify the specific risk sources. IEC 62443-3-2 could be used to assess the system design. It may be beneficial to implement or improve the use of zones and conduits. Since the attackers accessed Oldsmar's OT systems remotely, they could benefit from adding or improving a DMZ.

ISA 84.00.09 could be used by the team to define cybersecurity alarm and alert responsibilities, improve access management, and aid with establishing secure configuration practices.

Chapter 6

Discussion

6.1 Advantages and Disadvantages of Combined Analysis

Combining safety and cybersecurity risk analysis offers several significant advantages. Firstly, some integration is crucial because intentional incidents like cyberattacks can have severe safety consequences. Cyberattacks have evolved beyond traditional objectives like data theft and ransomware, posing physical risks like explosions or fires. By conducting a combined analysis with a holistic evaluation of threats, vulnerabilities, and potential consequences, one is better equipped against potential incidents.

Furthermore, a combined analysis enhances the overall resilience of a system. It enables the identification of vulnerabilities and potential cascading effects that may arise from the interaction between safety and cybersecurity incidents [38]. This identification supports the development of robust protective measures to mitigate risks effectively. From a decision-making perspective, combined risk analysis provides a comprehensive view of the potential impacts and trade-offs associated with safety and cybersecurity measures. It empowers decision-makers to make informed choices by considering the broader context and consequences of different risk management strategies.

In the past, cybersecurity was sometimes regarded as an isolated and nonessential budget item, receiving limited attention and financial resources. However, by connecting or integrating cybersecurity with safety, there is an opportunity to tap into a larger funding source typically allocated for safety-related initiatives [28]. Emphasizing the link between cybersecurity and safety can help secure more financial support for cybersecurity measures. Additionally, combining safety and cybersecurity risk analysis allows for harmonization between the two fields. Cybersecurity, being relatively younger, can learn from the more established safety field. As seen in section 5.1 safety is a more mature discipline. The transfer of knowledge and best practices from safety to cybersecurity contributes to the overall effectiveness of risk analysis and management.

In conclusion, the advantages of combined safety and cybersecurity risk analysis lie in its ability to provide a comprehensive evaluation of risks, enhance system

resilience, support informed decision-making, access greater funding opportunities, and foster knowledge transfer between the fields. This integrated approach is vital in addressing evolving challenges and ensuring the overall safety and security of systems and processes.

Several disadvantages and challenges are associated with the combination of safety and cybersecurity risk analysis. One of the primary challenges is the requirement for expertise in both the safety and cybersecurity disciplines. Finding individuals or teams with the necessary knowledge and skills to analyze and mitigate risks in both areas effectively can be difficult. Collaboration between safety and cybersecurity experts is essential but may involve significant coordination and communication efforts.

Another challenge is the potential compartmentalization of safety and cybersecurity data and information within different organizational departments or domains. Sharing relevant data and information between these domains can be challenging due to confidentiality concerns, organizational barriers, and differences in terminology and understanding.

Confidentiality is a significant concern in both individual cybersecurity risk analyses and combined analyses. While cybersecurity risk analysis is inherently more confidential, merging it with safety risk analysis requires treating the combined analysis with the same level of confidentiality as cybersecurity risk analysis. This increased level of confidentiality means limiting access to safety risk analyses and can hinder learning and competence building. Confidentiality also becomes a consideration when using performance standards. Having separate standards for cybersecurity allows for stricter confidentiality measures if needed. However, if safety and cybersecurity are combined, all elements involving cyber challenges must adhere to the same rigorous confidentiality requirements.

Performing a risk analysis is not enough; it becomes meaningless unless the results are actively used and integrated into the system. Risk analysis should be continuously consulted and applied throughout every stage, from design and implementation to operational phases, rather than being treated as a mere band-aid solution at the end. By incorporating risk analysis into every step, organizations can proactively address potential hazards and ensure that safety and security considerations are deeply embedded in their systems, fostering a culture of resilience and proactive risk management.

6.2 Choice of standards

ISO 31000 and IEC 62443-3-2 are at very different levels. ISO 31000 is general and applies to all types of risk, both positive and negative. It provides principles and guidelines, not requirements. IEC 62443-3-2 applies specifically to cybersecurity in OT systems. It sets requirements and refers to IEC 62443-3-3, where further requirements exist. It also has a specific focus on zones and conduits. The majority of risk standards refer to and conform to ISO 31000. IEC 62443-3-2 also references ISO 31000 and complies with it but does not refer to it in the text.

Conversely, ISO 31000 cares little about specific standards such as IEC 62443-3-2. Having learned this, it could have been beneficial to regard another safety standard, like IEC 61511 Functional Safety. This different choice could have facilitated considering the safety standard and the cybersecurity standard in relation to each other, as was the original aim. Furthermore, ISA 84.00.09 references both the IEC 62443 series and IEC 61511, so it makes more sense that IEC 61511 could have been chosen. However, this realization was made too late in the process to allow for the necessary pivot and having to read and understand new standard.

6.3 Efficient use of CCE

There are several things that should be done for the best results when conducting a CCE analysis. First off, the analysis scope needs to be clearly defined. It is necessary to gather comprehensive system information, including architecture, components, and dependencies. A cross-disciplinary team should conduct the analysis to ensure all aspects are considered to achieve an optimal outcome. The team should develop realistic attack scenarios to identify any vulnerabilities. Cybersecurity should be integrated throughout the engineering process when mitigating vulnerabilities, from design to operation. Furthermore, the team must document and communicate analysis findings to facilitate necessary organizational changes. The organization must continuously reassess and improve risks and mitigations, staying updated with emerging practices. These recommendations should lead to enhanced system resilience.

6.4 Limitations of the Frequency Literature Review

While the examination of academic publications in section 5.1 indicates how widespread safety-, cybersecurity, and combined analyses are, it is a superficial and not a thorough review. An attempt was made to be as accurate and concise as possible with the specific search phrases. However, it is very likely that the searches yielded both false hits and did not catch every publication that covers the topics. Furthermore, only one database was used. In addition, most of the publications found with Engineering Village are academic publications; therefore, the statistics do not include the prevalence in the industry. Nonetheless, the review was not intended to be very thorough, only to give an indication of the frequency of the current publication when it comes to safety analysis, cybersecurity analysis, and combined analysis.

Chapter 7

Conclusion and Further Work

7.1 Conclusion

The TRISIS malware targeted the SIS in an IACS, introducing new safety risks and compromising normal safety functions and barriers. This attack highlighted the direct impact of cyber threats and attacks on industrial process safety and the convergence of cybersecurity and safety risks. The Oldsmar attack exposed the vulnerability of critical infrastructure, with potential consequences for public safety due to chemical level manipulation. These incidents underscored the need for integrated approaches addressing both safety and cybersecurity to protect critical infrastructure. Thereby highlighting the connection between cybersecurity incidents and physical harm and emphasizing the importance of holistic risk management.

Through examination of scientific and technical publications, it was clear that the topic of safety risk analysis has more coverage than cybersecurity risk analysis and combined risk analysis. It was also evident that the number of publications regarding cybersecurity risk analysis and combined risk analysis is growing.

ISO 31000 is a standard that regards all types of general risk. However, it is less than ideal for safety risk analysis as it is too general. IEC 62443-3-2 is a very relevant standard for IACS cybersecurity, especially through its coverage of zones and conduits. ISA TR 84.00.09 emphasizes the importance of integrating cyber risk into the analysis of industrial processes, addressing the historical exclusion of cyber-related attacks. It highlights the need for collaboration between process control, process safety, and IT personnel to ensure the safety and security of operations.

UFoI-E causality concept regards uncontrolled flows of information and uncontrolled flows of energy as sources of risks in a CPS. The CyPHASS scenario builder is a practical risk identification tool that represents the ontology of scenarios in an extended bowtie with an extensive database of risk sources and barriers. Using the CyPHASS scenario builder, several flows of uncontrolled information were identified in TRISIS.

CCE provides a framework for assessing HCEs and risks in organizations, iden-

tifying critical devices and potential cyberattack paths. It encourages organizations to out-engineering vulnerabilities and develop tangible mitigations and protections to address the identified risks. CCE encourages integrating cybersecurity considerations into the engineering process, from design to operation, to enhance system resilience and reduce vulnerabilities. The phases of CCE were applied to Oldsmar and allowed for a better understanding of the vulnerabilities and potential consequences involved. Based on the application, it was clear that facilities like Oldsmar would benefit from a more inherently safe and secure system engineering.

Both CCE and UFoI-E/CyPHASS emphasize the crucial importance of in-depth systems knowledge. CCE especially addresses this, and it points out how necessary it is for an organization to know its inventory of systems and components in order for it to be able to protect its operation. Furthermore, it is crucial to have a knowledgeable team performing the analysis. It is essential to recognize that the quality of any assessment is directly influenced by the expertise and capabilities of the individuals involved in conducting it. Therefore, having a proficient and skilled team is paramount to ensuring accurate and reliable results in these methodologies. Organizations can proactively protect their assets and enhance security by leveraging their deep systems knowledge.

Combined safety and cybersecurity risk analysis methods are needed due to the increasing interconnectivity of systems. Traditional approaches that address safety and cybersecurity separately may fail to capture the potential propagating effects and interactions between these domains. By combining the analysis of safety and cybersecurity risks, organizations can gain a more comprehensive understanding of the overall potential risk. This integrated approach allows for a holistic evaluation of threats, vulnerabilities, and potential consequences, leading to more effective risk mitigation. Moreover, as cyberattacks increasingly pose safety risks, combining the analysis of these domains enables proactive identification and mitigation of potential vulnerabilities and their impact on system safety.

7.2 Further Work

There are many ways of combining safety and cybersecurity risk analyses, further work could be done on the difference between security-informed safety risk analysis, safety-informed security risk analysis, and combined safety and security risk analysis. The release of the 2023 update of the ISA TR 84.00.09 standard may also have interesting implications that are worth looking into.

Bibliography

[1] K. S. Bakken, "OT Cybersecurity: An Overview of OT Frameworks and the Stuxnet attack," 2022.

[2] M. A. Lundteigen, "Lecture note #6 - cybersecurity," 2022.

[3] IEC 62443, "Industrial communication networks - Network and system security," International Electrotechnical Commission, 2020.

[4] M. Assante and R. Lee, "The Industrial Control System Cyber Kill Chain," SANS Institute, 2021.

[5] Center for Chemical Process Safety, "Guidelines for Safe and Reliable Instrumented Protective Systems," Wiley, 2007.

[6] M. Rausand, "Risk Assesment: Theory, Methods, and Application," Wiley, 2011.

[7] 070 – Norwegian Oil and Gas, "Application of IEC 61508 and IEC 61511 in the Norwegian Petroleum Industry (Recommended SIL requirements)," International Organization for Standardization, 2001.

[8] NIST, "Framework for Improving Critical Infrastructure Cybersecurity," National Institute of Standards and Technology, 2018.

[9] IEC 62443, "Industrial communication networks - Network and system security - Part 1-1: Terminology, concepts and models," International Electrotechnical Commission, 2009.

[10] National Institute of Standards and Technology. "Glossary: Security." (), [Online]. Available: `https://csrc.nist.gov/glossary/term/security` (visited on 02/25/2023).

[11] National Institute of Standards and Technology. "Glossary: Information security." (), [Online]. Available: `https://csrc.nist.gov/glossary/term/information_security` (visited on 02/25/2023).

[12] National Institute of Standards and Technology. "Glossary: Cybersecurity." (), [Online]. Available: `https://csrc.nist.gov/glossary/term/cybersecurity` (visited on 02/25/2023).

[13] Pinellas County Sheriff's Office. "21-015 Detectives Investigate Computer Software Intrusion at Oldsmar's Water Treatment Plant." (5/02/2021), [Online]. Available: https://pcsoweb.com/21-015-detectives-investigate-computer-software-intrusion-at-%20oldsmar%5C%E2%5C%80%5C%99s-water-treatment-plant (visited on 02/09/2023).

[14] J. Cervini, A. Rubin, and L. Watkins, "Don't Drink the Cyber: Extrapolating the Possibilities of Oldsmar's Water Treatment Cyberattack," The 17th International Conference on Information Warfare and Security, 2022.

[15] H. Weiby, A. Tørressen, and L. Eie. "To personar skadd av lut i drikkevatn." (30/05/2023), [Online]. Available: https://www.nrk.no/sorlandet/lut-i-drikkevatnet-_-minst-ein-skadd-1.16426113 (visited on 05/31/2023).

[16] J. Evans. "Cyberattack on Oldsmar's water supply never happened, official says." (11/04/2023), [Online]. Available: https://www.tampabay.com/news/pinellas/2023/04/11/oldsmar-cyberattack-water-supply-poisoning-fbi-update/ (visited on 05/02/2023).

[17] MITRE att&ck. "Oldsmar treatment plant intrusion." (), [Online]. Available: https://attack.mitre.org/campaigns/C0009/ (visited on 05/02/2023).

[18] Dragos, "ICS/OT Cybersecurity year in review 2022," Dragos, 2022.

[19] CISA, "MAR-17-352-01 HatMan—Safety System Targeted Malware (Update B)," Cybersecurity & Infrastructure Security Agency, 2019.

[20] Dragos, "TRISIS Malware - Analysis of Safety System Targeted Malware," Dragos, 2017.

[21] ISO 31000, "Risk management - guidelines," International Organization for Standardization, 2018.

[22] IEC 62443, "Security for industrial automation and control systems - Part 3-2: Security risk assessment for system design," International Electrotechnical Commission, 2020.

[23] T. Holtebekk, "Iso," Store Norske Leksikon, 2021.

[24] ISO/IEC 31010, "Risk management - risk assessment techniques," International Organization for Standardization and International Electrotechnical Commission, 2019.

[25] S. Mauw and M. Oostdijk, "Foundations of attack trees," in *Information Security and Cryptology - ICISC 2005*, Springer Berlin Heidelberg, 2006.

[26] "Engineeringvillage.com." (), [Online]. Available: https://www.engineeringvillage.com/search/quick.url.

[27] ISA TR 84.00.09, "Cybersecurity Related to the Functional Safety Lifecycle," International Society of Automation, 2017.

[28] J. Powell, "ISA-TR84 and How it Relates to OT Security," OPTIV, 10/03/2023. [Online]. Available: https://www.optiv.com/insights/discover/blog/isa-tr84-and-how-it-relates-ot-security (visited on 04/27/2023).

[29] N. C. Guzman, I. Kozine, and M. A. Lundteigen, "An integrated safety and security analysis for cyber-physical harm scenarios," *Safety Science*, vol. 144, 2021.

[30] N. H. Carreras Guzman, D. Kufoalor, I. Kozine, and M. Lundteigen, "Combined Safety and Security Risk Analysis using the UfoI-E Method: A Case Study of an Autonomous Surface Vessel," European Safety and Reliability Association, Sep. 2019.

[31] J. Alanen, J. Linnosmaa, J. Pärssinen, A. Kotelba, and E. Heikkilä, "Review of cybersecurity risk analysis methods and tools for safety critical industrial control systems," VTT Technical Research Centre of Finland, 2022.

[32] Cybercore Integration Center, "CCE Fact Sheet," Idaho National Laboratory, 2020.

[33] Mission Support Center, "Consequence-driven Cyber-informed Engineering (CCE) Mission Support Center Concept Paper," Idaho National Laboratory, 2016.

[34] S. G. Freeman, N. H. Johnson, and C. P. S. Michel, "Consequence-driven Cyber-informed Engineering," Idaho National Laboratory, 2020. [Online]. Available: https://inl.gov/wp-content/uploads/2021/01/CCE-Phase-1-4-Reference-Document.pdf.

[35] Cybercore Integration Center, "CCE Case Study: Stinky Cheese Company," Idaho National Laboratory, 2020. [Online]. Available: https://inl.gov/wp-content/uploads/2021/01/Stinky-Cheese-Case-Study-INL-EXT-20-58574-Rev-002-published.pdf.

[36] D. for samfunnssikkerhet og beredskap. "Du er en del av norges beredskap." (), [Online]. Available: https://www.dsb.no/globalassets/dokumenter/egenberedskap/dsb_beredskap_brosjyre_original.pdf.

[37] Center for Disease Control and Prevention. "Water treatment." (), [Online]. Available: https://www.cdc.gov/healthywater/drinking/public/water_treatment.html#print.

[38] G. Kavallieratos, S. Katsikas, and V. Gkioulos, "Cybersecurity and Safety Co-Engineering of Cyberphysical Systems—A Comprehensive Survey," *Future Internet*, vol. 12, 2020.

Appendix A

CyPHASS Scenario Builder

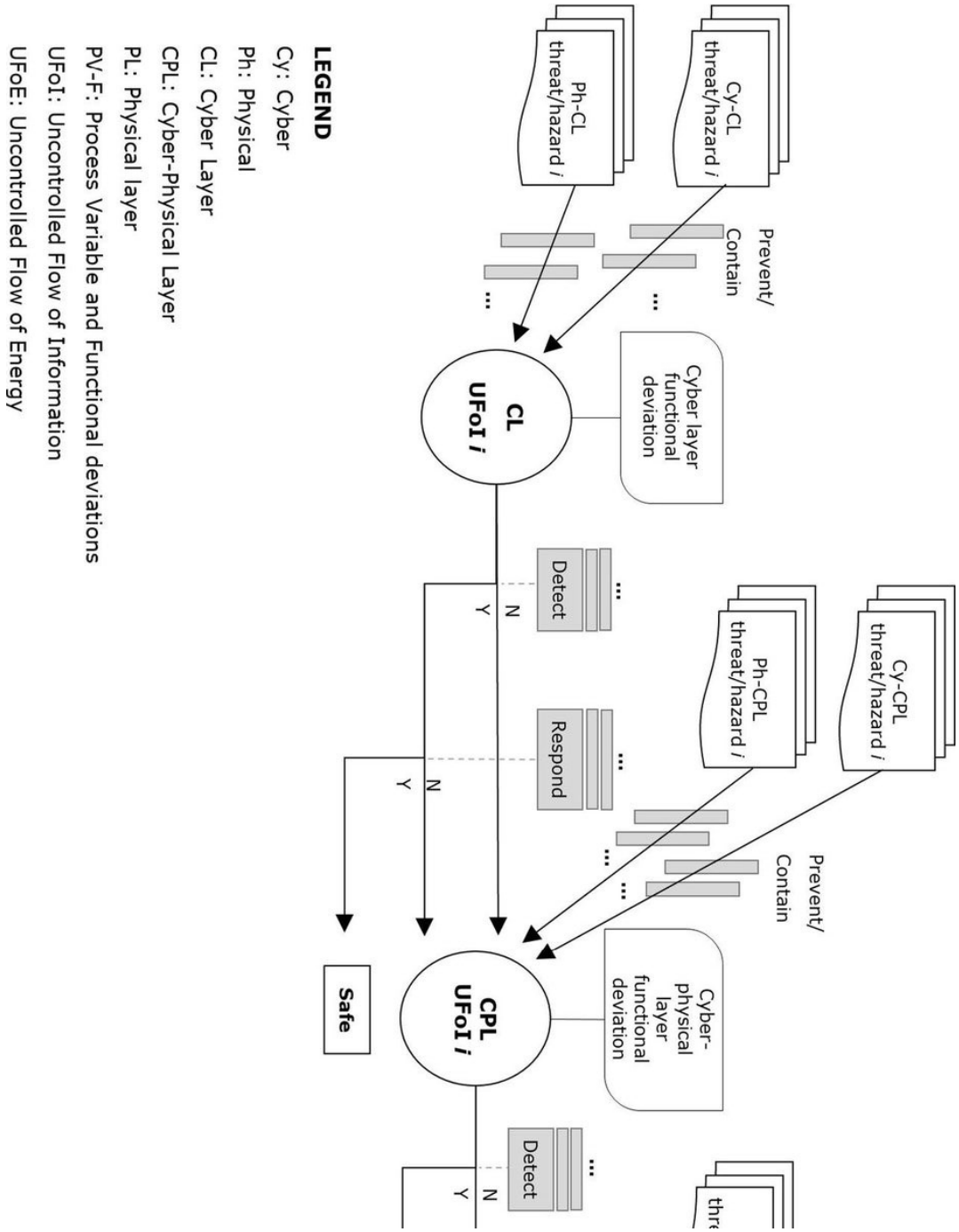


Figure A.1: First half of the CyPHASS Scenario Builder, continues in figure A.2. From Guzman et al. [29]

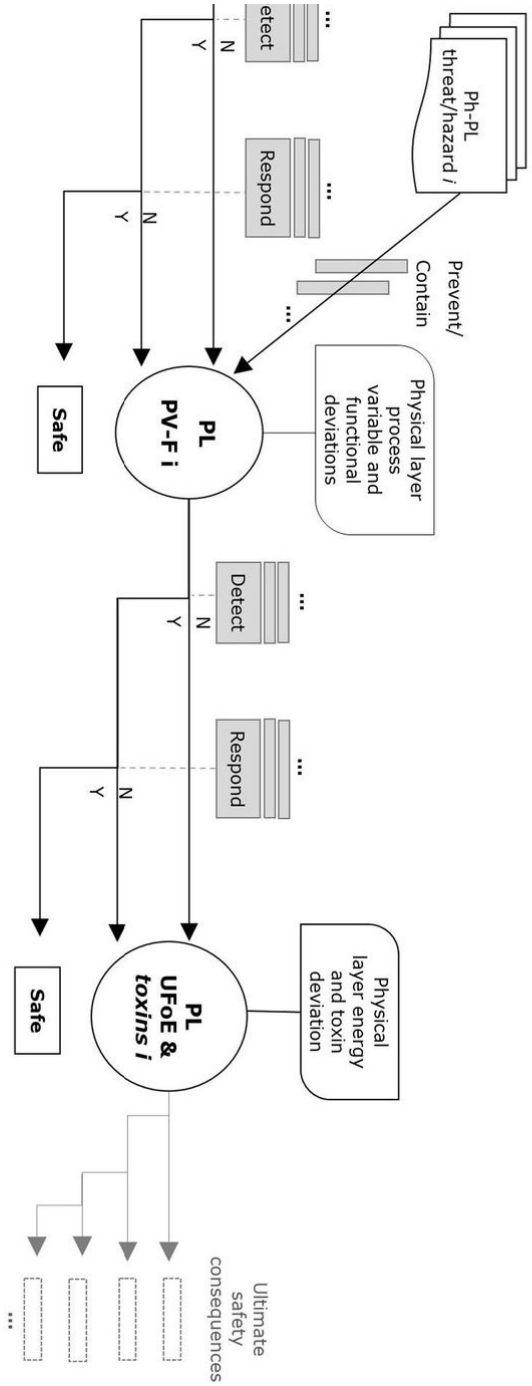
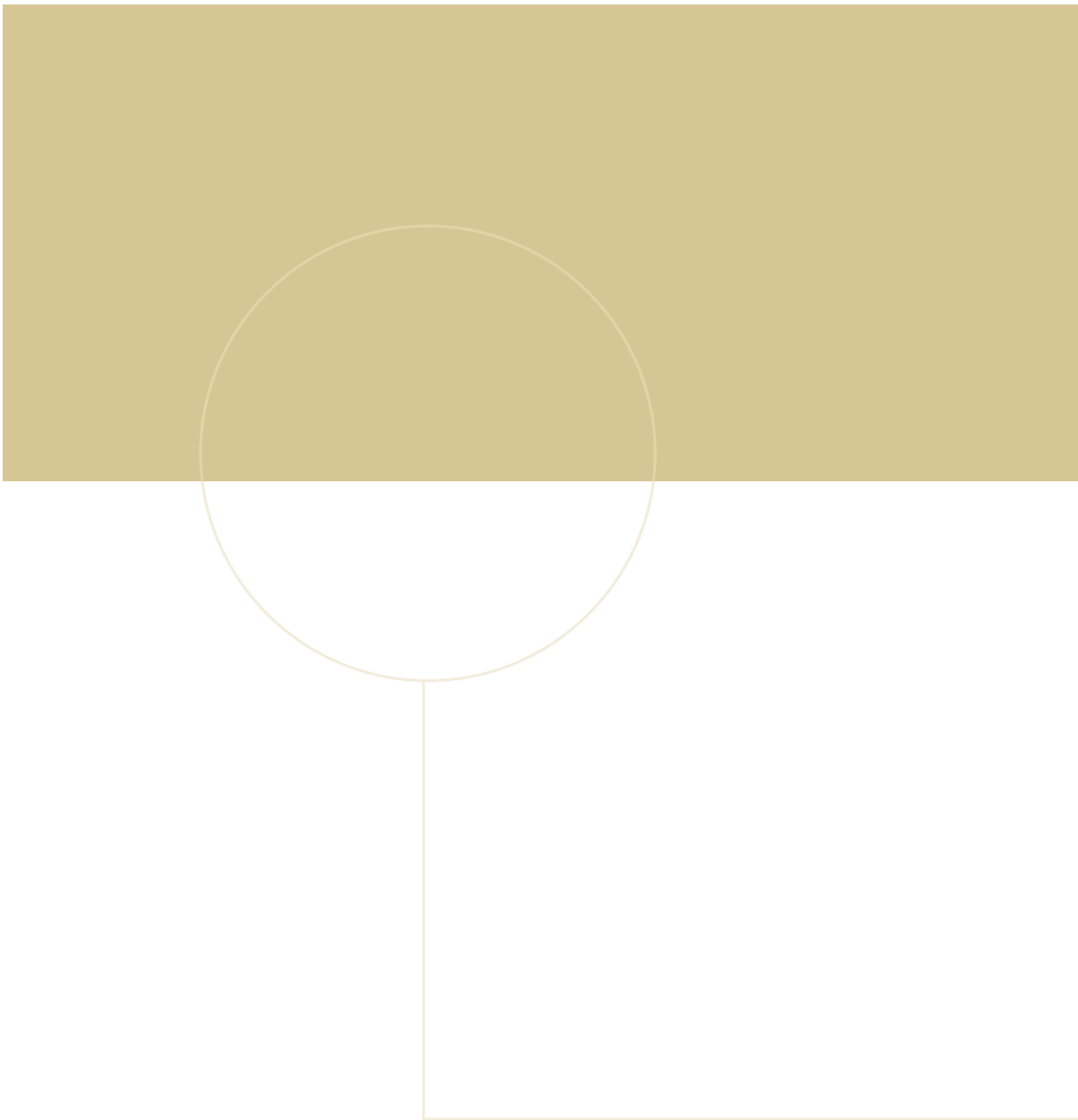


Figure A.2: Second half of the CyPHASS Scenario Builder. From Guzman et al. [29]



NTNU

Norwegian University of
Science and Technology