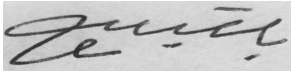




University of
Stavanger

Faculty of Science and Technology

MASTER'S THESIS

Study program/Specialization: Risk management/ Risk assessment and management	Spring semester, 2021 <u>Open</u> / Restricted
Writer: Balkiss Fares	 (Writer's signature)
Faculty supervisor: Roger Flage External supervisor(s): Pengyu Zhu (Safetec)	
Thesis title: An integrated risk analysis framework for safety and cybersecurity of industrial SCADA system.	
Credits (ECTS): 30	
Key Words: ICS SCADA Safety Cybersecurity Risk analysis	Pages:67..... + enclosure: Stavanger, 26/07/2021..... Date/year

In fulfillment of the Master's Degree at Faculty of Science and Technology

An integrated risk analysis framework for safety and
cybersecurity of industrial SCADA system

Balkiss Fares

Stavanger, July 2021

Abstract

The industrial control system (ICS) refers to a collection of various types of control systems commonly found in industrial sectors and critical infrastructures such as energy, oil and gas, transportation, and manufacturing. The supervisory control and data acquisition (SCADA) system is a type of ICS that controls and monitors operations and industrial processes scattered across a large geographic area.

SCADA systems are relying on information and communication technology to improve the efficiency of operations. This integration means that SCADA systems are targeted by the same threats and vulnerabilities that affect ICT assets. This means that the cybersecurity problem in SCADA system is exacerbated by the IT heritage issue. If the control system is compromised due to this connection, serious consequences may follow. This leads to the necessity to have an integrated framework that covers both safety and security risk analysis in this context.

This thesis proposes an integrated risk analysis framework that comprise of four stages, and that build on the advances of risk science and industry standards, to improve understanding of SCADA system complexity, and manage risks considering process safety and cybersecurity in a holistic approach.

The suggested framework is committed to improving safety and security risk analysis by examining the expected consequences through integrated risk identifications and identifying adequate safeguards and countermeasures to defend cyber-attack scenarios. A simplified SCADA system and an undesirable scenario of overpressure in the pipeline are presented in which the relevant stages of the framework are applied.

In loving memory of my father

Ramadan Fares

(March, 2021)

Who has always had faith in my abilities to succeed in my endeavors, you are no longer here, but your faith has enabled me to complete this journey

To my mother Hasna

without her unconditional love, blessings and prayers, this thesis would not have become possible

Acknowledgment

This thesis has been carried out as a fulfillment of the requirements for MSc degree in Risk Management at the University of Stavanger.

First, I would like to express my thanks to my supportive supervisor Roger Flage for their invaluable guidance, suggestions, and willingness to provide me with so much of his time and knowledge throughout the thesis. Your support has been crucial in supporting me to reach my goals and complete this thesis.

Next, I would like to thank Pengyu Zhu for his continuous motivation, guidance, and insight into this field were always available when required.

I also want to acknowledge the support and valuable time received from Idriss El-Thalji on the topic discussed in this thesis.

Further, I would like to express my deepest gratitude to my best friend and lovable husband Ahmed, who encouraged me throughout the study and supported my ambition. Also, thanks to my sweet daughter Razan, who brings happiness to my heart in challenging moments.

I sincerely thank my brother Mohammed for their constant support and interesting discussions.

Last but not least, I would like to thank my family, friends for being there for me and giving me all of your love and support.

Balkiss Fares

Stavanger, July 2021

Table of Contents

1	<i>Introduction</i>	10
1.1	Background.....	10
1.2	Problem statement, research questions and objectives.....	11
1.3	Scope and limitations.....	12
1.4	Thesis structure	12
2	<i>Literature review</i>	13
2.1	Risk.....	13
2.2	Complexity and uncertainty	14
2.3	Risk management	15
2.4	Safety vs security	16
2.5	Safety management system	17
2.6	Threat vs Hazard	19
2.7	New context of risk of SCADA systems in the digital world.....	20
3	<i>Overview of industrial control system (ICS)</i>	21
3.1	Industrial control system definition.....	21
3.2	Comparison between (ICS) and information technology (IT).....	21
3.3	SCADA system architecture	23
3.4	Purdue model of SCADA system.....	24
3.5	Description of standards, regulation, and best practices for ICS safety and security	25
3.5.1	NIST 800-82 guideline.....	25
3.5.2	IEC 62443	26
3.5.3	DNVGL- RP-I08 cyber security in the oil and gas industry based on IEC62443	26
3.5.4	Norwegian Oil and Gas 104	26
3.5.5	IEC 61511	27
4	<i>Lifecycle of functional safety and cybersecurity management systems.</i>	28
4.1	Description of the key elements of functional safety lifecycle	28
4.2	Description of the key elements of cybersecurity management lifecycle	30
4.3	Description of the key element of ICS cybersecurity management system (CSMS).....	32
4.3.1	Risk analysis	32
4.3.2	Addressing risk with the CSMS	33
4.3.3	Monitoring and improving the CSMS	33
4.4	Integrated Functional Safety and Cybersecurity Management Lifecycles	33
5	<i>Overview of the proposed integrated framework</i>	37
5.1	Introduction.....	37
5.2	Stage 1: Identify the context and the functional requirement of SCADA system.	40
5.2.1	Application of stage 1 on simplified SCADA system.	40
5.3	Stage 2: Identify and analyze all assets in the SCADA Purdue model.....	42
5.3.1	Application of stage 2 on simplified SCADA system.	44

5.4	Stage 3: Scan the vulnerability and criticality of the assets.	45
5.4.1	Application of stage 3 on simplified SCADA system.	46
5.5	Stage 4: Integrated risk analysis	46
5.5.1	Application of stage 4 on simplified SCADA system.	50
6	<i>Discussions</i>	56
6.1	Safety vs security in the proposed framework	56
6.2	ICS relevant standards	57
6.3	The integrated risk identification in the proposed framework	58
6.4	Strengths and limitations of the framework	59
6.5	Future work	59
7	<i>Conclusion</i>	60
	<i>List of references</i>	61

List of Figures

Figure 1 Generic safety management system(Li & Guldenmund, 2018)	18
Figure 2 hazard vs threat (Zalewski et al., 2016)	19
Figure 3 SCADA architecture(P. Eden et al., 2015)	23
Figure 4 functions of information security (NOROG 104, 2016).....	26
Figure 5 Functional safety lifecycle (Hildenbrandt & van Beurden, 2019).....	28
Figure 6 Cybersecurity lifecycle (Hildenbrandt & van Beurden, 2019).....	30
Figure 7 key elements of ICS cybersecurity management system (IEC 62443, 2009).....	32
Figure 8 The link between functional safety and cybersecurity Lifecycle (Walkington & Sugavanam, 2019).....	34
Figure 9 The interaction between Safety and security (MDCG 2019)	37
Figure 10 Flow chart of hybrid assets classification and integrated risk analysis	38
Figure 11 Simplified model for SCADA system	41
Figure 12 Purdue model of Scada system (What Is the Purdue Model for ICS Security, n.d.)	42
Figure 13 General Asset Classification	43
Figure 14 PLC general classification	44
Figure 15 The difference between Dependency and Interdependency (Petit et al., 2015).....	45
Figure 16 Emulation of adversary plan	48
Figure 17 Analysis of undesirable event	51
Figure 18 Fault Tree Analysis for Overpressure in the Pressure pipeline	53
Figure 19 Event tree analysis for FDIA attack.....	54

List of tables

Table 1 Risk description.....	14
Table 2 The process of risk management.....	16
Table 3 IT vs ICS (Stouffer et al., 2015).....	22
Table 4 overview of functional safety lifecycle (IEC 61511, 2016).....	29
Table 5 cybersecurity lifecycle	31
Table 6 Functional safety lifecycle vs cybersecurity lifecycle (ISA-TR84.00.09, 2017).....	35
Table 7 Summarize the stages of the framework	39
Table 8 Evaluation of the strength knowledge of a security risk assessment (Askeland et al., 2017).....	49
Table 9 HAZOP analysis with integrated perspective	52
Table 10 Risk level.....	52
Table 11 Risk description.....	55
Table 12 Summarize the domain of relevant standards	57

List of abbreviation

DCS	Distributed control system
HMI	Human Machine Interface
IACS.	Industrial and Automation Control System
ICS	Industrial Control system
ICT	Information and Communication Technology
IT	Information Technology
OT	Operation Technology
PCS	Process Control System
PLC	Programmable Logic controller
RTUs	Remote Terminal Units
SCADA	Supervisory control and data acquisition
SIS	Safety Instrumented System

1 Introduction

1.1 Background

The industrial control system ICS is a collection of numerous types of control system, including Process Control Systems (PCS), Distributed Control Systems (DCS), supervisory control and data acquisition (SCADA) systems, and safety instrumented systems (SIS) (Knapp & Langill, 2015). ICS can be found in industrial sectors and critical infrastructures (Stouffer et al., 2015).

The supervisor control and data acquisition (SCADA) system, which is a type of ICS system that controls and monitors operations and industrial processes and has become increasingly crucial in many application domains, such as energy, oil and gas, transportation, and manufacturing (Gao et al., 2014). SCADA systems spread over broad geographic locations (Cherdantseva et al., 2016; Gao et al., 2014). These locations require a central monitoring and control system for their processes (Nicholson et al., 2012). Each location comprises of field devices such as remote terminal units (RTUs) and programable logic controller (PLC) that are connected directly to sensors and actuators in the process to capture data from the process operation, to send control commands to the field site, and data to the supervisory systems. The supervisory system gathers and analyzes data from all field locations via a communication network and presents graphical results on Human Machine Interface (HMI) (Elhady et al., 2019).

Historically isolated SCADA systems did not prioritize security in general or cybersecurity, particularly in their consideration (Cherdantseva et al., 2016; Patel et al., 2005). Due to the increased use of ICT components and commercial off-the-shelf computers in industrial control systems and especially critical infrastructure industries, more operation technology (OT) devices are relying on the information technology IT networks to improve the efficiency of operations (Elhady et al., 2019). These interconnected between SCADA system and ICT are targeted to the same threats and vulnerabilities to ICT assets. Therefore, the IT heritage problem further increases cybersecurity issues in SCADA systems. Thus, when the control system is compromised because of this interconnection, it may result in severe consequences; in this case, we should consider other threats to the ICS SCADA system (Cherdantseva et al., 2016)

According to the analysis conducted by the Kaspersky ICS CERT team indicates that the percentage of attacked ICS computers globally in the second half of the year 2020 increased by 33.4%, and the sources of the main threats in the ICS environment are the internet, removable media, and Email Clients (Kaspersky ICS CERT, 2021).

The current state of security and safety in ICS SCADA systems is probably best illustrated by the following summary of several incidents that have affected ICS systems:

- The Stuxnet malware in 2010 targeted the Iranian nuclear plant and damaged 1,000 centrifuges in the process, around one-fifth of the nuclear centrifuges in the plant. Stuxnet is a sophisticated malware that specifically targeted industrial software and equipment that it self-replicated and spread throughout multiple systems such as Removable drives, Local area networks (LANs), and HMI database server (Hemsley & E. Fisher, 2018).

- A successful cyberattack on Ukraine power grid in 2015 taking control of the SCADA system, this attack impacted a power outage to nearly a quarter-million Ukrainians for up to six hours (Hemsley & E. Fisher, 2018).
- Hydro was the target of a large-scale cyber-attack on March 19, 2019. The entire worldwide organization was impacted by the attack, with Extruded Solutions facing the most significant operational issues and financial losses. The entire cost is estimated to be between 550 and 650 MNOK. (*Cyber-Attack on Hydro*, 2020).

As illustrated by the incidents mentioned above, SCADA systems are susceptible to a number of vulnerabilities that could compromise both safety and security in a variety of ways. All the above highlights that the primary concern in SCADA systems should be safety and security.

Firesmith (2003) defines safety as “*the degree to which accidental harm is prevented, reduced, and properly reacted to,*” and security is “*the degree to which malicious harm is prevented, reduced, and properly reacted to*” (Johnsen, 2012) .

Therefore, it is essential to strengthening and integrates the safety and security of SCADA systems and develop effective integrated risk management for the safety and security of ICS SCADA systems to minimize the safety impacts due to potential threats.

In this thesis, we suggest an approach to analyze and identify critical assets against these threats, as a cyber-attack in the oil and gas industry may result in a major accident.

1.2 Problem statement, research questions and objectives

There is a lack of an integrated approach to understand and manage risks in the SCADA system with consideration of process safety and cybersecurity from a life-cycle perspective. This thesis aims to propose an integrated risk analysis framework for the SCADA system according to risk science and industry standards.

In order to meet this objective, the following will be done:

- How can safety and security be integrated into a framework for analyzing risk in the SCADA system?
- Technical: What are the relevant international standards, guidelines, and which shall or should be followed?
- Organizational: What are the key elements of cybersecurity and functional safety lifecycle and management system?

1.3 Scope and limitations

The scope of this thesis, as previously stated, is to propose an integrated risk analysis framework for specifically SCADA systems, emphasizing those used in the oil and gas industry. DCS, SIS, and other types of ICS and other sectors will not be covered will be excluded due to time constraints.

1.4 Thesis structure

This thesis is structured as follows. The second chapter presents a scientific literature review and theory. Chapter three is mainly an overview of industrial control systems and relevant standards. The fourth chapter outlines the key elements of the functional safety cybersecurity management system and the link between them. Chapter five propose a safety and security integrated risk analysis framework for the SCADA system. Chapter six includes a discussion, limitations, and future work. Finally, chapter seven is a conclusion.

2 Literature review

Throughout this chapter, we will present the theoretical concepts essential for understanding the subsequent chapters.

2.1 Risk

There are many different risk definitions in risk conceptualization, so we will clarify which perspective is adopted in this thesis.

Risk as a concept can be traced back to the seventeenth-century probability theory (Hacking, 1975; Smith & Brooks, 2013). Various reports and scientific literature have defined risk in a variety of ways; as Dake(1992) the risk defined as “*The probability of an event occurring, combined with an accounting for the losses and gains that the event with would represent if it came to pass.*”

Similarly, according to ISO 31000(2018) “*risk is the effect of uncertainty on objectives*”. Based on these definitions, risk can be viewed negatively (as a threat/hazard) or positively (as an opportunity). In contrast, the risk is defined as a “*combination of the probability of occurrence of harm and the severity of that harm*”; according to the *IEC 61511-1* (2016), the emphasis here is solely on negative risks.

Aven (2015) defines risk as a consequence of activity with associated uncertainties, which is the definition adopted throughout this thesis. Aven (2006) argues that a wide-ranging view of risk is possible in this definition because it allows various assessments of the uncertainties to be made, in addition this approach can describe the right direction for analyzing unique systems; and different kind of threats. The Society for Risk Analysis (SRA) has listed several definitions for the risk, but they are all consistent in their understanding of the concept (SRA, 2018).

As a result of this definition, the consequences C and the uncertainties U are the two primary risk dimensions (Aven, 2015).

According to Aven (2015), a risk description can be written as (C', Q,' K) or as (A,' C,' Q,' K), which means that a specific event A' has the potential to cause inevitable consequences. With associated uncertainties that a particular tool Q can measure, probabilities as a tool for expressing uncertainty,

P and C' are assigned based on the background knowledge K. As suggested by Aven (2015) The Table 1 shows the main elements of risk description.

Table 1 Risk description

Risk Description			
A'	C'	Q	K
<ul style="list-style-type: none"> • Specific event. With potential cause. • Undesirable scenario 	<ul style="list-style-type: none"> • Set of high observable quantities that characterize Consequence 	<ul style="list-style-type: none"> • Measure of uncertainty. • Probabilities as a tool for expressing uncertainty 	<ul style="list-style-type: none"> • The Background knowledge upon which C' and Q are built.

As per Aven(2015), vulnerability is considered an aspect of risk, that can be defined as a combination of consequences and associated uncertainties that are conditional on the occurrence of an initiating event. Generally, can be described as (C', Q, K | A).

2.2 Complexity and uncertainty

The industrial control system, specifically SCADA, is considering in this thesis, which is a complex system that creates uncertainty when performing a risk assessment.

Society of risk analysis (SRA) defined complexity as “Causal chain with many intervening variables and feed-back loops that do not allow the understanding or prediction of the system’s behavior on the basis of each component’s behavior” (SRA, 2018).

The term complexity refer to the entire portfolio of causal relationships that are highly sophisticated and intertwined (Aven & Renn, 2010).

In theory, we can acquire accurate forecasts of the quantities of interest if we know all the causal factors contributing to this occurrence of an undesirable event, understand the mechanisms by which these elements work, and have enough evidence about relationships. This means similar scenarios can be created for technological malfunctions or even terrorist activities if we know their preferences and methods ahead of time. The inability to reestablish causal relationships with a high degree of confidence in the prediction and reliability is referred to as uncertainty. This means uncertainty is the difficulty of predicting events' occurrence and their consequences. Uncertainty depends on the following factors (Aven & Renn, 2010):

- Inadequate database.
- Incomplete reduction of complexity.

A fundamental and vital component of risk analysis is uncertainty, and it is classified into two forms in the context of risk analysis (Aven & Zio, 2011):

- The first type is uncertainty caused by randomness, which happens owing to the intrinsic variability of systems.
- The second form of uncertainty arises from a lack of knowledge and understanding of the phenomena or observable quantities

Complexity and uncertainty are essential while characterize and identify safety and security risk and to enhance the ability to manage surprises a resilience strategy can be used. (Johnsen, 2012).

Due to the integration of both systems, SCADA/ICT systems with process equipment. The systems may be destroyed by accident and making it challenging to examine data (Johnsen, 2012).

The two features that can distinguish between different classifications of risk problems are complexity and uncertainty degree. In this thesis, complexity refers to the highly mutual causal connection obvious to sophisticated causal relationships and specific effects. That often leads to disagreement in expert judgment about the characterization of risk. Therefore, scientific risk assessment can manage this complexity (Aven & Renn, 2010).

2.3 Risk management

Various sources of risk can arise in a SCADA system, and to effectively manage these risks, a systemic approach is needed to managing cybersecurity and safety risks in SCADA systems.

Risk management encompasses all measures and activities undertaken to manage risk. It is concerned with all activities, situations, events, and other factors that may affect an organization's capacity to reach its objective (Aven,2015). The risk communication and management strategies might be inadequate if risk definitions lack a solid scientific base (Aven, 2011). Furthermore, if the organization's management is not extensively involved in the process.

The ISO 31000:2018 Risk management standards are developed by the International Standards Organization (ISO). ISO 31000 (2018) is a general normative standard that applies to any organization, regardless of its industry, and provides a framework to manage risk to achieve its objectives and inform that risk management should integrated into all the activities of the organization. Various fields, including safety, the environment, and security, can benefit from its application. The table 2 shows the risk management process (*ISO 31000*, 2018):

Table 2 The process of risk management

Establishing context	It comprises the scope of the risk management, objectives of the process, risk acceptance criteria. and influencing external and internal factors.
Risk identification	Includes positive and negative effect of outcome on objectives
Risk analysis	Causes and consequences analysis to provide a risk picture
Risk evaluation	Evaluating if the residual risk is acceptable by comparing risk analysis results to risk acceptance criteria
Risk treatment	Planning and implementing risk treatment; evaluating the efficiency of that treatment and determining if the residual risk is acceptable.
Communication and consultation	The goal of communication is to increase stakeholders' awareness of the risk and cope with it while assessing it, whereas consultation aims to obtain feedback, information, and diverse points of view.
Monitoring, review	This stage is to ensure and enhance process design, execution, and results in terms of quality and effectiveness.

2.4 Safety vs security

As stated earlier, the thesis is concerned with integrated risk analysis of SCADA system focusing on security risks with a safety consequence. This subchapter will offer definitions and extra explanations so that you can better comprehend them and distinguish between safety and security risks.

Firesmith (2003) defines the safety is as *“the degree to which accidental harm is prevented, reduced and properly reacted to”*, that is primarily concerned with preventing damage to valuable assets (particularly humans) due to accidents (Johnsen, 2012). According to IEC61511 (2016) safety is defined as freedom from unacceptable risk.

As per Firesmith(2003) security is defined as *“the degree to which malicious harm is prevented, reduced and properly reacted to”*, this is primarily concerned with preventing assaults on valuable assets and particularly sensitive data (Johnsen, 2012).

On the other hand, IEC 62443 (2009) defines security as "prevention of illegal or unwanted penetration, intentional or unintentional interference with the proper and intended operation or inappropriate access to confidential information in IACS".

Generally, the three-factor view, which covers (assets, threats, and vulnerabilities) captures the widespread concept of risk in the security field. According to traditional definitions, safety analysis is limited to accidents and unintentional risks, whereas security analysis is concerned with intentional sources of risk (Amundrud et al., 2017).

Amundrud et al. (2017) criticized the (value, threat, and vulnerability) security risk perspective for failing to recognize uncertainty as a significant component of the risk perspective, and this perspective is entirely contradictory to current safety risk thinking.

As stated by the SRA Glossary (2018) is defined (safe or secure) as being without unacceptable risk, and (safety or security) is interpreted in the same way (e.g., when saying that (safety or security) is achieved. The term “safety or security” is sometimes used as an antonym for “risk” (the (safety or security) level is linked to the risk level, a high (safety or security) level means low risk level and vice versa. Risk is a key concept in these definitions, as it is utilized to define safe and secure, which means the concepts of risk are considered applicable to both safety and security (Amundrud et al., 2017).

2.5 Safety management system

A safety management system (SMS) defined as a system used to manage and control safety or as a management system specifically designed to ensure the safety of people and property. An SMS is the intersection of three perspectives: safety, management, and system. The unique advancement of each of these three factors effects how an SMS evolves over time. SMS is commonly defined as the management procedures, elements, and activities designed to improve the organization's overall safety performance in different industries (Li & Guldenmund, 2018).

This systematic procedure can enhance overall safety and manage risk by identify, assess, and control hazards to process and personnel in all operations. Figure 1 presents a generic safety management system based on Hale's (2005) model that can be used in a variety of industries and organizations (Li & Guldenmund, 2018).

The risk control system and the learning system are the two essential elements of a generic SMS, and each element divided into multiple sub-elements or management processes. The following are the sub-elements of the risk control system (Li & Guldenmund, 2018):

1. The primary and subsidiary business processes describe the safety management system covering all life cycle phases (LCP). It is also responsible for the organization's design, construction, technology, and output(s).

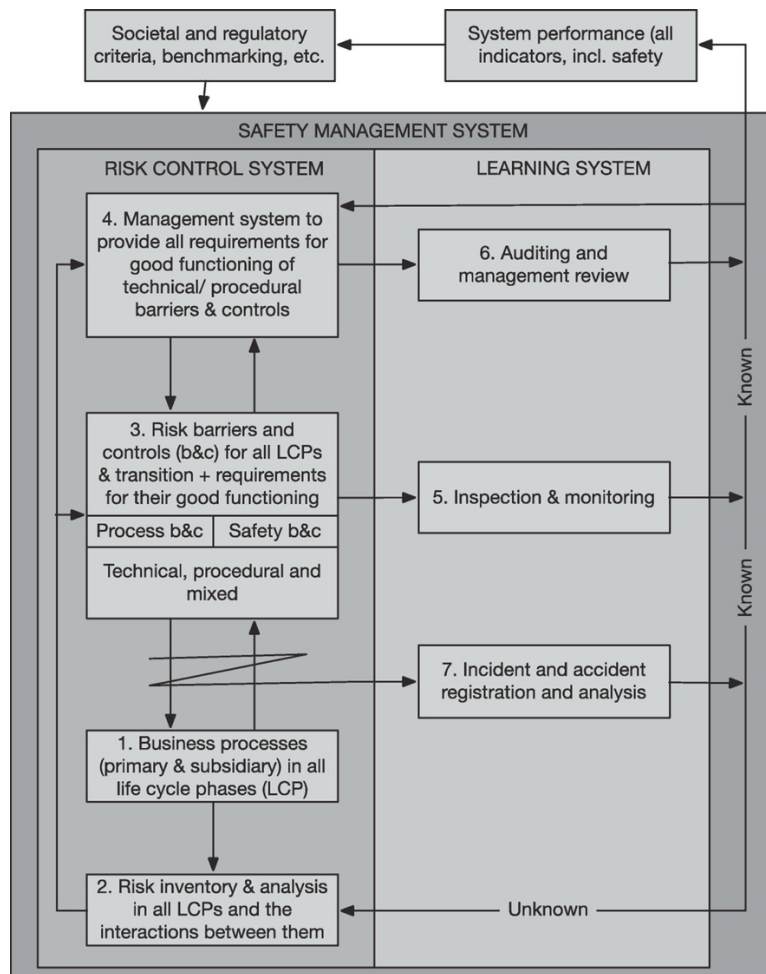


Figure1 Generic safety management system(Li & Guldenmund, 2018)

2. The risk inventory and analysis in all LCPs are involved with identifying and assessing the organization's hazards and understanding how these can become visible and controllable.
3. The risk barriers and controls for all LCPs and transitions, plus requirements for their excellent functioning, concern implementing risk barriers and controls. It describes the management system within its context and its proper functioning.
4. The management system to provide all functional requirements for technical and procedural barriers and controls contains the so-called delivery systems, which deliver the safety barriers and controls to function as designated.

The learning system includes the following sub-elements or management processes:

5. Inspection and monitoring are the process that collects real-time information from the actual risk controls.
6. The auditing and management review is concerned with assessing safety management and their performance to make continuous improvement possible.

- The incident and accident registration and analysis are the end and start box in an SMS. This process aims to identify hazards and provide critical information for the management of safety in the organization.

2.6 Threat vs Hazard

The threat is defined as “any indication and circumstances, with potential to cause the loss of or damage to the assets”. It also necessitates a thorough understanding of the adversaries' intentions and motives and their ability to jeopardize the assets concerned. (Roper, 1999; Smith & Brooks, 2013). While NIST SP 800-53 defined threat as “Any circumstance or event with the potential to adversely impact agency operations (including mission, functions, image, or reputation), agency assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service”. Whereas hazard is defined according to *IEC 61511-1(2016)* as the event that cause harm. Similarly Rausand (2013) defined hazard as “a source of danger that may cause harm to an asset”. Both hazard and threats can cause the same impact on the assets and compromise the safety as shown in the Figure 2.

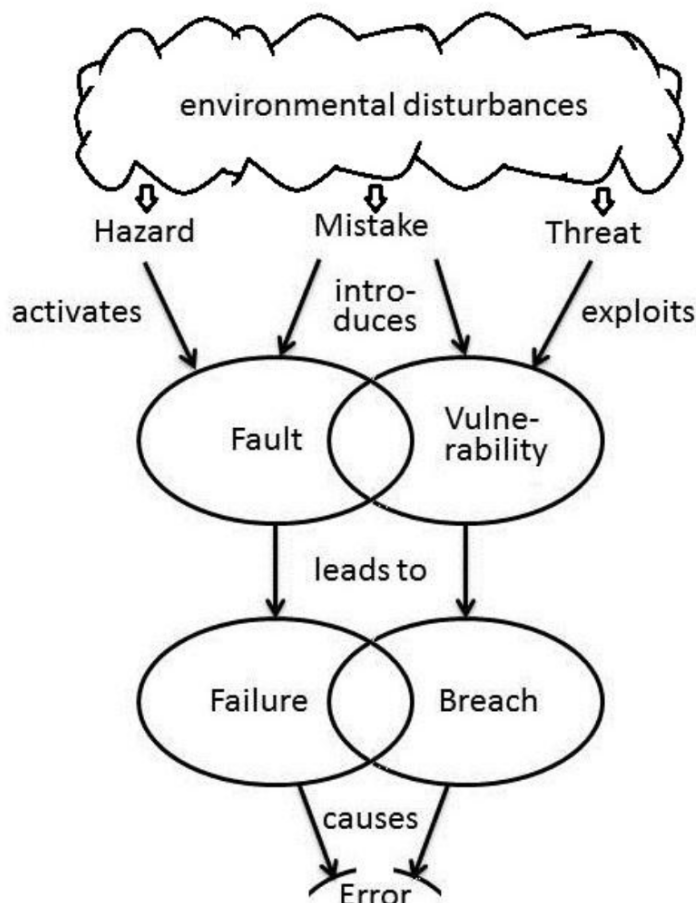


Figure 2 hazard vs threat (Zalewski et al., 2016)

2.7 New context of risk of SCADA systems in the digital world

Historically, before the improvement of data acquisition and control systems, components of SCADA systems were air gapped and operated on isolation (Gao et al., 2014), and this isolation made them less exposed to cyber threats. It can be considered a secure and complex system at the same time because it was challenging to collect data and control remote operations. However, integrating SCADA systems with the ICT opens the possibility of cybersecurity and safety risks. Security and safety considerations for SCADA systems are getting more attention as security incidents increased on critical infrastructures (Pliatsios et al., 2020).

Several older legacy ICS systems are not compliant with modern security technologies such as enhanced encryption and intrusion detection devices, which is a significant difficulty with ICS security (Warren & Leitch, 2015).

SCADA systems are available in critical infrastructures, therefore used in production plants and distribution systems such as oil and gas industry. Which made SCADA systems are attracted for threat actors (Obodoeze et al., 2018).

SCADA systems are prone to different sorts of cyber threats, including insider attacks by a human or malicious software that takes control of the system to cause risk to the system, and people safety (Gao et al., 2014). For example, the human-machine interfaces (HMI) of a SCADA system are a common gateway for malware, Since the intention of threat actors is usually the to get access to the control system and cause a significant damage.

ICS systems have traditionally been closed, stand-alone systems; however, they are now interconnected in corporate networks and connected to the internet to enable remote access and monitoring. However, these new technological advancements bring with them unknown security risks (Warren & Leitch, 2015).

3 Overview of industrial control system (ICS)

3.1 Industrial control system definition

The Stouffer et al. (2015) defines ICS as “*a general term that encompasses several types of control systems, including supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other control system configurations such as Programmable Logic Controllers (PLC) often found in the industrial sectors and critical infrastructures.*”

ICS is a collection of numerous control system, including Process Control Systems (PCS), Distribution Control Systems (DCS), supervisory control and data acquisition (SCADA) systems, and safety instrumented systems (SIS)(Knapp & Langill, 2015). These systems control and monitor local and remote processes with fully or partially automated control in manufacturing and industrial facilities.

Industrial Control Systems (ICS) are used for various social infrastructure facilities and play an essential role in performing their control functions and ensuring their safety. ICS currently uses an open architecture and is often connected to external systems, such as office systems(Kondo et al., 2018).

3.2 Comparison between (ICS) and information technology (IT)

Confidentiality, integrity, and availability, also known as the CIA triad, is a model for security policy formulation in the information security area and each feature reflects a primary data security goal in order to achieve the following (Bonandir et al., 2021; Dardick, 2010):

- Integrity: it is necessary to provide protection against illegal information tampering or loss, which necessitates a declaration of non-repudiation, accuracy, and authenticity.
- Confidentiality: to preserve data privacy and classified information, maintain authorized access and limit transparency.
- Availability: to make sure that information is accessible and used in a timely and accurate manner.

The availability and integrity of the ICS security triad are more critical than confidentiality in terms of overall effectiveness(Tariq et al., 2019). The goal of the ICS system is to maximize availability so that systems can continue to operate and perform without being interrupted.

Data integrity is critical in control systems; if the operator's screen in the control room does not accurately reflect the current situation, there could be a significant problem. This is will significantly impact security and operations. Since the data in an ICS context, such as temperature, vibration, and speed, is only transient (Bonandir et al., 2021).

ICS systems are concerned with the continued availability of the connected industry process, such as power generation or water treatment, a security distinction between ICS systems and information technology systems. IT systems, on the other hand, are concerned with preventing information from being hacked or damaged (Warren & Leitch, 2015).

Stouffer et al.(2015) outlines in Table 3 some of the most common differences between information technology systems and industrial control systems.

Table 3 IT vs ICS (Stouffer et al., 2015)

Category	IT	ICS
Performance Requirements	<p>Non-real time Response must be consistent High throughput is demanded High delay may be acceptable Less critical emergency interaction Tightly restricted access control can be implemented to the degree necessary for security.</p>	<p>Real-time Response is time-critical Modest throughput is acceptable High delay and/or jitter is not acceptable Response to human and another emergency interaction is critical Access to ICS should be strictly controlled but should not hamper or interfere with human-machine interaction.</p>
Availability (Reliability) Requirements	<p>Acceptable responses such as rebooting.</p> <p>Availability deficiencies can often be tolerated, depending on the system's operational requirements</p>	<p>Responses such as rebooting may not be acceptable because of process availability requirements.</p> <p>Availability requirements may necessitate redundant systems Outages must be planned and scheduled days/weeks in advance High availability requires exhaustive pre- deployment testing</p>
Risk Management Requirements	<p>Manage data Data confidentiality and integrity is paramount Fault tolerance is less important – momentary downtime is not a major risk Major risk impact is delay of business operations</p>	<p>Control physical world Human safety is paramount, followed by protection of the process Fault tolerance is essential, even momentary downtime may not be acceptable Major risk impacts are regulatory non- compliance, environmental impacts, loss of life, equipment, or production</p>
Communications	<p>Standard communications protocols Primarily wired networks with some localized wireless capabilities Typical IT networking practices</p>	<p>Many proprietary and standard communication protocols Several types of communications media used to include dedicated wire and wireless (radio and satellite) Networks are complex and sometimes require the expertise of control engineers</p>
Component Lifetime	3 to 5 years	10 to 15 years
Components Location	Components are usually local and easy to access	Components can be isolated, remote, and require extensive physical effort to gain access to them

3.3 SCADA system architecture

SCADA architecture has evolved gradually over the course of four generations of SCADA systems, from monolithic to distributed, interconnected, and internet of things technology. The first generation: monolithic SCADA systems with remote terminal units work in isolation environments, with no relation to other systems. The second generation was introduced, in which RTUs were connected to communication servers via a wide area network (WAN). Due to the entry of new equipment vendors into the market, industrial expansion, and an increase in the number of automated processes, it became necessary to implement the next generation of SCADA systems, also known as networked SCADA systems or third generation SCADA systems. The Internet of Things (IoT) and the cloud are fundamental in the fourth generation. With the Internet of Things (IoT), different devices or sensors can collect data from remote locations and communicate with their respective SCADA masters via wireless LANs; the data collected is then sent to the cloud for further processing. In addition to being simple to maintain and integrate, these systems also offer faster data availability, scalability, efficiency, and cost reduction (Tariq et al., 2019).

The components of a SCADA system can be divided into two main categories: field sites and control centers. More than one field site spread across a large geographical area, remote terminal units (RTUs) are examples of field-side components that are connected to physical processes such as motors, valves, thermostats, and other instruments. The control center collects information about the status of field devices and the physical processes occurring in its area of responsibility. The Control Center, which consists of the HMI (Human Machine Interface), the Historian, and the MTU (Master Terminal Unit), receives real-time data regarding the status of PLCs and RTUs through the use of a data acquisition system (Eden et al., 2015).

Generally, a SCADA system architecture as shown in Figure 3 includes the following components (Eden et al., 2015; Gao et al., 2014):

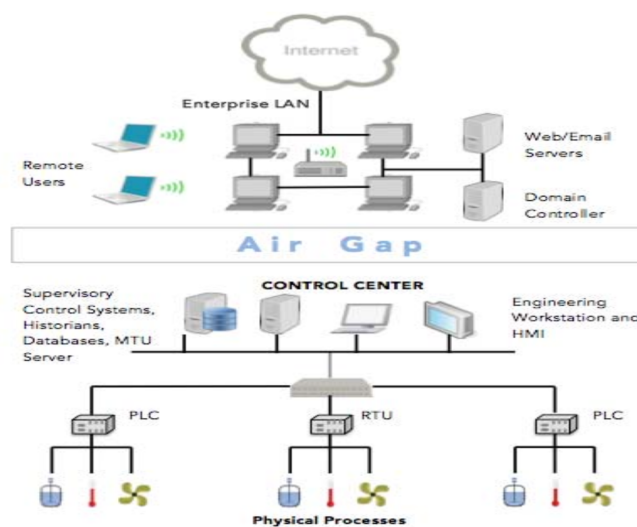


Figure 3 SCADA architecture(Eden et al., 2015)

- Master terminal unit (MTU)

Serves as the primary monitoring station, it is in charge of controlling and commanding the remote terminal unit (RTU). It also responds to messages from the RTU/ processes and stores them to facilitate future communication with the device (Yadav & Paul, 2021).

- Human machine Interface (HMI)

The human-machine interface (HMI) serves as a communication link between SCADA hardware and software components. SCADA operational information, such as controlling, monitoring, and communication between several RTUs and MTUs in the form of text, statistics, or other comprehensible content, is in charge of this component of the SCADA system (Yadav & Paul, 2021).

- Remote terminal units (RTUs)

The RTU is a microprocessor controlled electronic device that are used to interface the signals of physical objects (sensors) in the system to digital data. In addition, these units are used to transmit real-time data toward the supervisory system and, receive the commands from the master terminal unit for controlling the connected objects. Although, it is very similar to a PLC and performs almost the same function However, RTUs have faster CPUs and much more extensive communication support. They also tend to be more reliable in harsh environments(Eden et al., 2015).

- Programmable Logic Controllers (PLCs)

Computerized devices used to control process such as sensory devices Supervisory systems (Eden et al., 2015).

- IED (Intelligent Electronic Device):

The IED enables monitoring and controlling the operational process and power protection and is entirely independent of other devices to perform high-level communication (Eden et al., 2015).

- Communications infrastructure

It is responsible for facilitating communication between various components of the SCADA network framework. Wireless or wired connections can be made depending on the situation. Wireless media is widely used today because it allows people in geologically dispersed areas to communicate with people in less accessible regions without wires(Yadav & Paul, 2021).

3.4 Purdue model of SCADA system

The Purdue model shows typical architecture of ICS SCADA system the interconnections and interdependencies of all the main components of the system (*What Is the Purdue Model for ICS Security*, n.d.):

- Level 0-Physical process: Represents the actual physical processes.

- Level 1 -Intelligent devices: Process sensors, analyzers, actuators, and other associated instruments are used to detect and manipulate physical processes.
- Level 2-Control systems: SCADA software is used to manage, monitor, and control physical processes. The distributed control system (DCS) and programmable logic controllers (PLCs) are generally implemented within the facility. However, SCADA can manage systems over great distances from the actual location of the facilities. The human-machine interface provides basic controls, and monitoring (HMI) coupled to DCS and PLCs, whereas SCADA systems aggregate data and transfer it upstream for historian recording at level 3.
- Level 3 - operations systems: This is where the manufacturing floor's production workflow is managed. Batch management, data recording, operations, and plant performance are handled by customized systems based on operating systems like Windows. This layer also includes databases or historians for storing data from operations. Any disturbances at this level can affect the entire manufacturing facility and can result in hours or days of downtime, including a massive potential for revenue loss.
- Level 3.5 - Demilitarized zone (DMZ): This level contains security systems like firewalls and proxies used to divide or air gap the IT and OT systems. At this point, the IT "converge" with OT systems, increasing the security risks for OT systems. The rising demand for bidirectional data flows between OT and IT systems have resulted from automation, which has resulted in improved efficiencies. For businesses accelerating their digital transformation.
- Level 4/5 – Enterprise: This is often where the core business functions occur on the IT network as we know it today. It supervises business operations and gives business direction. Plant production plans, material usage, shipping, and inventory levels are controlled by enterprise resource planning (ERP) systems. Every disturbance at this level might cause days or even weeks of downtime, resulting in severe revenue loss due to delayed or stopped downstream processes.

3.5 Description of standards, regulation, and best practices for ICS safety and security

Here is a brief overview of commonly used ICS SCADA safety and security related technical standards, best practices that are relevant for this work and categorized in the following areas:

3.5.1 NIST 800-82 guideline

In May 2015, the "Computer Security Division" published a guideline relevant to this thesis. The "Special Publication 800-82 (Final Public Draft), Guide to Industrial Control Systems (ICS) Security". It provides an overview of cybersecurity strategy for ICS and SCADA systems. The NIST SP 800-82 describes common ICS architectures, and listed the system's critical threats and vulnerabilities. A security countermeasure to reduce the risk associated with ICS vulnerabilities and threats are suggested(Stouffer et al., 2015).

3.5.2 IEC 62443

The Industrial Automation and Control System (IACS) Security Committee of the ISA developed ISA standards and technical reports. The IEC 62443 family of standards establishes the overall framework for securing IACS and addressing the essential cybersecurity management aspects throughout the lifecycle. The main objective of these standards is to establish the objectives and maturity level of cybersecurity toward its automation system. And can be used by an asset owner, system operators, integrators(IEC 62443, 2009).

3.5.3 DNVGL- RP-108 cyber security in the oil and gas industry based on IEC62443

Recommended practices report by DNV GL, Cybersecurity in the oil and gas industry based on IEC 62443, covers how to implement the standard and the control systems that are frequently used by organizations that operate in critical infrastructures, such as petroleum production and distribution facilities. This recommended practice clarifies the roles and duties of the respective parties (asset owner, system integrator, product supplier, service provider, compliance authority), as well as who performs the tasks, who should be involved, and what is anticipated in terms of inputs and outputs from each party (DNVGL-RP-G108, n.d.).

3.5.4 Norwegian Oil and Gas 104

The Norwegian Oil and Gas Association NOROG 104 (2016) developed a recommended guidelines on information security baseline requirements for process control, safety, and support of ICT systems. Furthermore, to improve the safety and consistency of Norwegian Continental Shelf (NCS) operations and increase the focus on information security in the offshore industry. The guideline contains several obligatory Information Security Baseline Requirements (ISBRs). For each ISBR, a control and an objective are defined, and then implementation guidance is structured following the phases of the NIST Cybersecurity Framework, as shown in Figure 4.

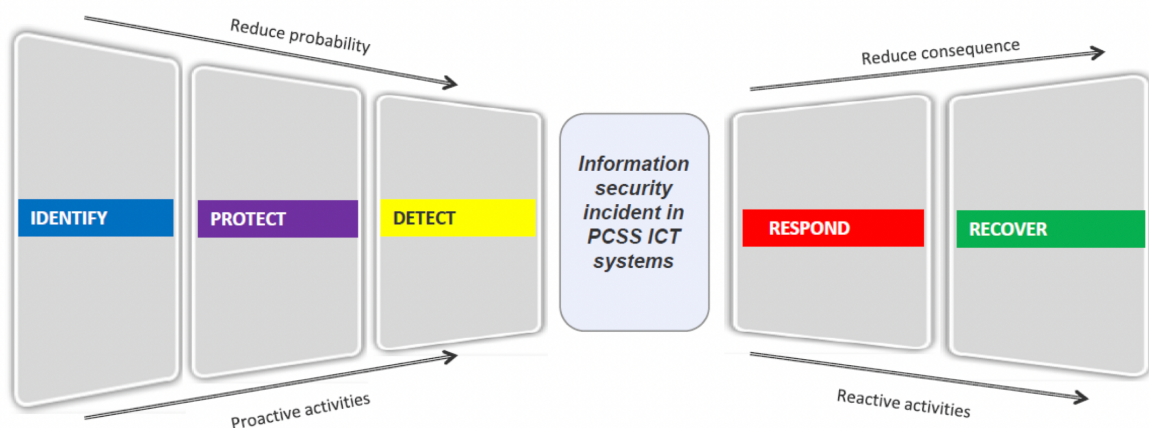


Figure 4 functions of information security (NOROG 104, 2016)

3.5.5 IEC 61511

The IEC 61511(2016) standard specifies the application of safety instrumented systems (SISs) in the process industries, and it covers the requirement for specification, design, installation, operation, and maintenance of safety instrumented systems in the process industry entire lifecycle, to reach or maintain a safe process. It suggests a risk-based approach for evaluating the safety instrumented functions (SIFs) performance levels by assigning a safety integrity level (SIL).

This standard focus on the lifecycle requirements for system architecture hardware configuration, application programming, and system integration to achieve functional safety, Specifications for attaining functional safety are provided; however, there is no indication of who is accountable for putting the requirements into action (e.g., designers, suppliers, owner/operating business, contractor). Safety planning, project planning and management, and national legislation will all play a role in allocating this duty to the appropriate parties.

In the 2016 version, IEC 61511 included two clauses to address SIS security:

- 8.2.4: A security risk assessment shall be carried out to identify the security vulnerabilities of the SIS.
- 11.2.12: The design of the SIS shall be such that it provides the necessary resilience against the identified security risks.

4 Lifecycle of functional safety and cybersecurity management systems.

4.1 Description of the key elements of functional safety lifecycle

Safety lifecycle is defined by IEC 61508 as the ‘Necessary activities involved in the implementation of safety-related systems, occurring during a period of time that starts at the concept phase of a project and finishes when all of the E/E/PE safety-related systems, other technology safety- related systems and external risk reduction facilities are no longer available for use.’ Management of functional safety encompasses all activities needed to guarantee safety integrity level requirements are identified, designed, and maintained throughout the whole lifecycle of the systems (IEC 61511-1:2016, n.d.; NOG 070, n.d.). The key elements of IEC 61511 functional safety lifecycle are divided in three phases as shown in Figure 5 are(Hildenbrandt & van Beurden, 2019):

- Assessment phase.
- Develop & implement phase.
- Operate & maintain phase.

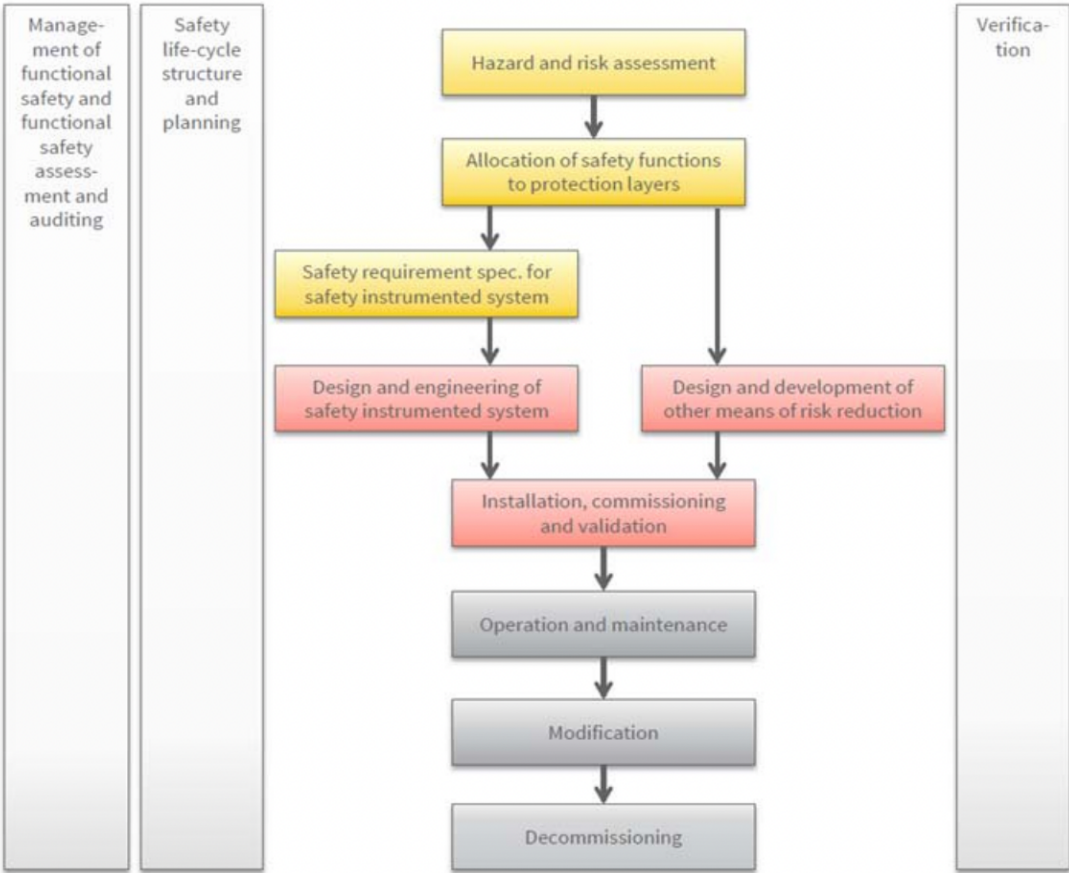


Figure 5 Functional safety lifecycle (Hildenbrandt & van Beurden, 2019)

The Overall functional safety lifecycle comprises all the activities needed to reach the requirements and the relating objectives of the different lifecycle phases according to IEC 61511(2016) are presented in the Table 4 :

Table 4 overview of functional safety lifecycle (IEC 61511, 2016)

Safety Lifecycle	Objectives
1. Hazard and risk analysis	Define hazards and potential hazardous events, their consequences. Perform a risk analysis to determine the event sequences leading to each event, the requirements for risk reduction, and the safety functions needed to meet the required risk reduction.
2. Allocation of safety function	The allocation of safety functions to protective layers and the determination of the related safety integrity level for each safety integrity function.
3. Safety requirements specification	The Safety Requirements Specification (SRS) for each safety-instrumented system must be defined. The SRS is created by allocating SIFs and identifying requirements throughout the safety planning process to obtain the required functional safety(<i>NOG 070</i> , n.d.).
4. SIS design and engineering	To design the SIS to satisfy the requirements for SIF and the safety integrity that goes along with them.
5. Installation commissioning, validation	It is necessary to integrate and test the SIS to ensure that the SIS satisfies all safety criteria, including the needed SIF and related safety integrity.
6. Operation and maintenance	Assuring that the functional safety of the SIS is maintained throughout its operation and maintenance
7. Modification	Ensure that the requisite SIL is acquired and maintained; adjustments and improvements must be made to the SIS.
8. Decommissioning	To guarantee a good review, sector structure, and SIF's continued applicability.

4.2 Description of the key elements of cybersecurity management lifecycle

IEC 62443 (2009) defines Cybersecurity as "actions required to preclude unauthorized use of, denial of service to, modification to, disclosure of, loss of revenue form, or destruction of critical systems or information assets". Figure 6 shows the key elements of cyber Security lifecycle defined by IEC 62443 (2009) and there are divided in three phases (Hildenbrandt & van Beurden, 2019):

- Assessment Phase**
 This phase including the scope of the system, a high level of cybersecurity risk assessment to define the initial security target level, and a detailed cybersecurity risk assessment to determine the security level for each zone and conduit.
- Implement Phase**
 In this phase, cybersecurity countermeasures are applied, and a validation of security level is conducted to demonstrate that countermeasures are in place and that risk acceptance requirements are met.
- Maintain Phase**
 This phase ensures that the security considerations are maintained and that the procedures to maintain that level are accomplished and that no modifications will impact the system during the modification process.

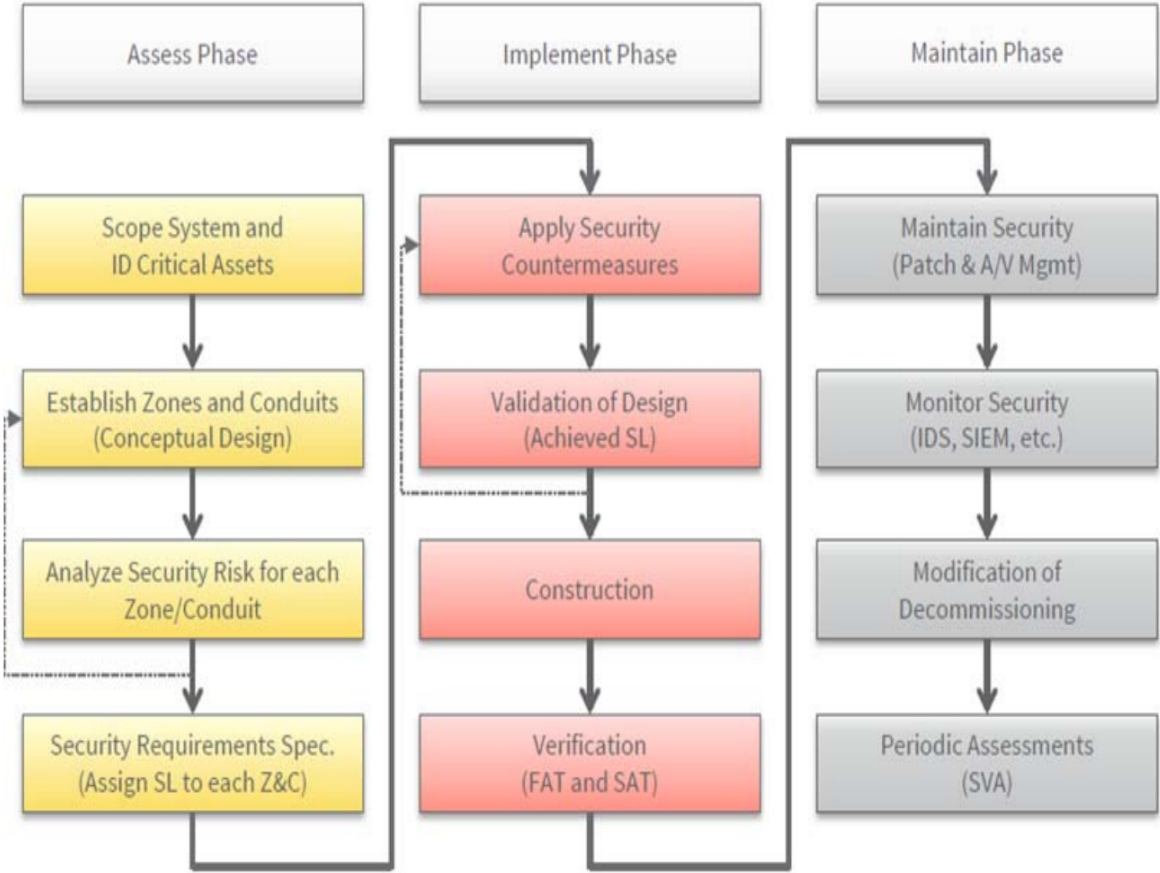


Figure 6 Cybersecurity lifecycle (Hildenbrandt & van Beurden, 2019)

The overall cybersecurity lifecycle, which includes all steps required to meet the criteria and corresponding objectives of the several lifecycle phases, as defined by IEC 62433(2009) are presented in the Table 5:

Table 5 cybersecurity lifecycle

Cyber security lifecycle	Objectives
1. Specification	The System under consideration (SUC) is identified, an initial high level of cybersecurity risk assessment is performed, and the system is divided into security zones and conduits, among other activities. Ultimately, the Target Security Levels for each Zone and Conduit in the System Under Consideration are determined through this procedure.
2. Design	This phase of the lifecycle involves a detailed cybersecurity risk assessment for each zone and conduit and a comprehensive design of the (SUC), including technical security measures based on the Security Level security for each zone and conduit.
3. Implementation	The organizational security measures needed for the operations and maintenance phases are created in this phase to be used during the verification and validation phase and develop organizational security measures for the maintenance phase and operations phase.
4. Verification & Validation	Ensure that the technological and organizational security measures fulfill the security criteria defined in the cybersecurity requirements specification.
5. Operation	Regularly evaluate and update the ICS risk assessment, organizational and technological security measures and perform operational security measures, such as incident response and recovery.
6. Maintenance	Implement management of change processes, including evaluating risk assessments and update organizational and technical security measures. Perform organizational security measures for maintenance and monitor threats and security vulnerabilities.
7. Decommissioning	The decommissioning process must be carried out in a manner that does not jeopardize the asset owner's ongoing activities. The deletion or purging of sensitive data is a critical action at this phase of the process.

4.3 Description of the key element of ICS cybersecurity management system (CSMS)

When it comes to protecting ICS from cyber-attacks, these elements reflect what must be included in the CSMS. Generally, the key elements as shown in the Figure 7 are divided into the following three categories (*IEC 62443, 2009*):

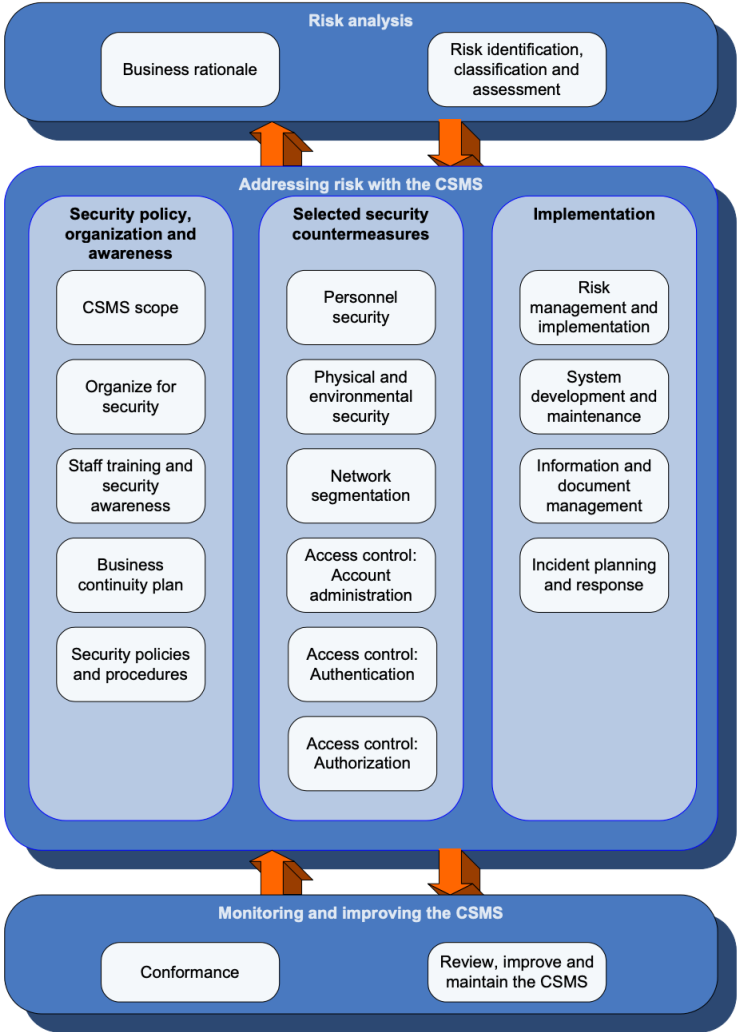


Figure 7 key elements of ICS cybersecurity management system (*IEC 62443, 2009*)

4.3.1 Risk analysis

The CSMS's first key element is risk analysis, and it is split into two parts that fall within this category:

- Business rationale.

ICS cyber incidents can have severe financial, health, safety, environmental, and other consequences. A business rationale is based on the type and scale of these potential consequences. The primary goal is to identify and record each organization's specific requirements to mitigate cyber risk for ICS. Along with ensuring that senior management continues to support an appropriate level of investment in the ICS cybersecurity program.

- Risk identification, classification, and assessment.

Organizations protect their operation capabilities by systematically identifying, prioritizing, and assessing possible security risks using acceptance criteria. The main goal is to identify the set of ICS cyber risks that the business confronts and estimate the likelihood and severity of these risks.

4.3.2 Addressing risk with the CSMS

The CSMS's second key element is addressing risk with the CSMS, and it represents the objectives and information in the CSMS. It is split into three parts:

- Security policy, organization, and awareness.
- Selected security countermeasures.
- Implementation.

4.3.3 Monitoring and improving the CSMS

Monitoring and improving the CSMS is the third key element of the CSMS. It comprises both verifying that the CSMS is being used and assessing the efficacy of the CSMS itself. It is split into two parts:

- Conformance.
- Review, improve and maintain the CSMS.

4.4 Integrated Functional Safety and Cybersecurity Management Lifecycles

Only being aware of process risks is no longer sufficient for plant operators, engineers, design, and support employees. Risks from cyber-attacks not only have a financial impact on a company's operations, but they can also result in process safety events being initiated (Hildenbrandt & van Beurden, 2019). For that reason, in this subchapter, we review the link between the functional safety and cybersecurity lifecycles and how they are related.

The functional safety and cybersecurity lifecycle have a comparable structure as shown in the Figure 8, consisting of risk assessment or analysis of the system, followed by the design and implementation, finally operation and maintenance safeguards or countermeasures to protect or secure the system (Hildenbrandt & van Beurden, 2019).

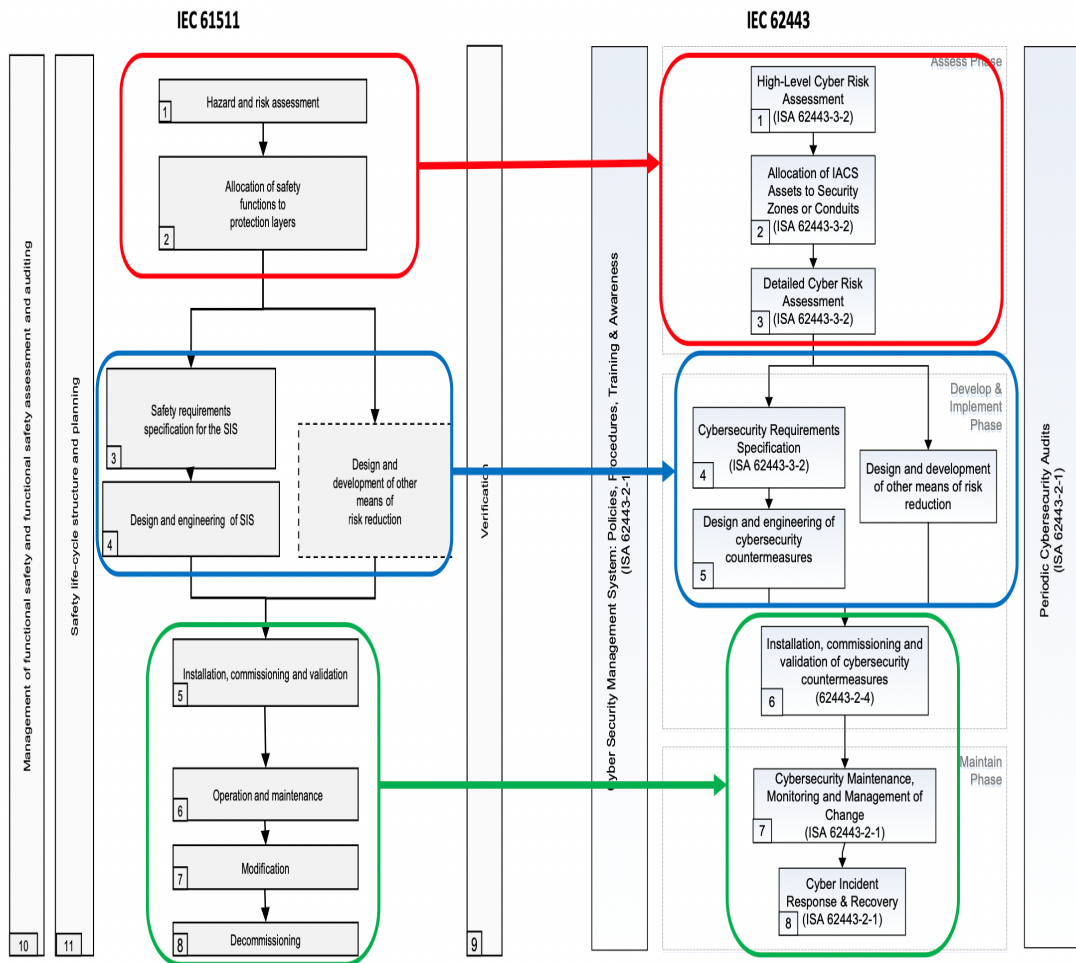


Figure 8 The link between functional safety and cybersecurity Lifecycle (Walkington & Sugavanam, 2019)

The table 6 illustrates the distinction between cybersecurity and functional safety in terms of lifecycle for a better understanding of both domains (ISA-TR84.00.09, 2017).

Table 6 Functional safety lifecycle vs cybersecurity lifecycle (ISA-TR84.00.09, 2017)

Lifecycle phase		Functional safety	IACS cybersecurity
Risk analysis	Target of evaluation	- Equipment under control (EUC)	- System under Consideration (SuC)
	Failure likelihood	- Random failures due to operational and environmental stresses - Systematic failures due to errors during safety lifecycle	- Threats: internal, external or combination - Vulnerabilities due to <ul style="list-style-type: none"> • component or system design flaws • making non-validated changes • not following cybersecurity practices and procedures • Threats exploiting vulnerabilities leads to failure
	Consequence severity	- Impact on environment, health and safety of personnel and the general public	- Loss of availability and/or data integrity has direct impact, and loss of confidentiality has indirect impact on functional safety
	Risk categorization	- Based on likelihood and severity; risk may be quantified	- Based on likelihood and severity; risk is currently qualitative - Risk categorization for every cybersecurity requirement - Multi-dimensional problem - Assigned to zone with target SL for each zone/conduit
	Risk mitigation measures	- Relies on independent protection layers concept - Safeguards reduce likelihood of consequence evaluated - Identifies integrity requirements for safeguards; for SIF assigns target SIL	- Relies on cybersecurity countermeasures within zones, conduits interconnecting zones, and defense in depth concept - Countermeasures reduce likelihood - Identifies requirements for countermeasures to meet the zone target SL for each threat vector
Implementation of measures		- Safety manual for components - Quantitative SIL verification for SIF	- Cybersecurity manual for components - Verification through different levels of testing for target SL
Operation and maintenance		- Restrict access to IACS components to competent personnel with necessary access privileges - Periodic testing of measures - Demand rate and component failures to be monitored - Awareness and training	- Restrict access to IACS components to competent personnel with necessary access privileges - Periodic testing of measures - Frequent reviews to identify new vulnerabilities and take appropriate action, if necessary - Awareness and training - Cyber risk reassessment after each software or hardware change
Management system		- Defines requirements for competency, training, verification, testing, audit, MOC, and documentation	- Defines requirements for competency, training, verification, testing, audit, MOC, and documentation

As per (Walkington & Sugavanam, 2019) the similarities between functional safety and the cybersecurity lifecycle are:

- Performance based standards.
- The same need to achieve a safety culture.
- Supporting systematic capability and processes.
- Competency management is required.
- Require adequate maintenance, regular auditing, and assessment.
- They can cause a potentially dangerous event.

According to Hildenbrandt & van Beurden (2019) these similarities give opportunity to combine both lifecycles to build a single integrated lifecycle that covers functional safety, cybersecurity that can enhance the awareness of all potential hazards, mitigation measures, and response plans due to communication and cooperation among engineering, operation technology, and information technology teams.

5 Overview of the proposed integrated framework

5.1 Introduction

The integrated framework can be seen as a variant of process hazard analysis with a consideration of cybersecurity assessment that is based on scientific grounds and standards compliance. Its purpose is to examine the SCADA systems security risk with safety impacts, as shown in Figure 9, to provide a comprehensive analysis and holistic approach to ensure all assets within the scope of the study. This can allow decision-makers to view the risk from several perspectives. Moreover, the framework is a straightforward process, although it is challenging to implement due to the system's complexity precisely, understanding the interdependencies between various assets, and the necessity for diverse experts to participate in the assessment.

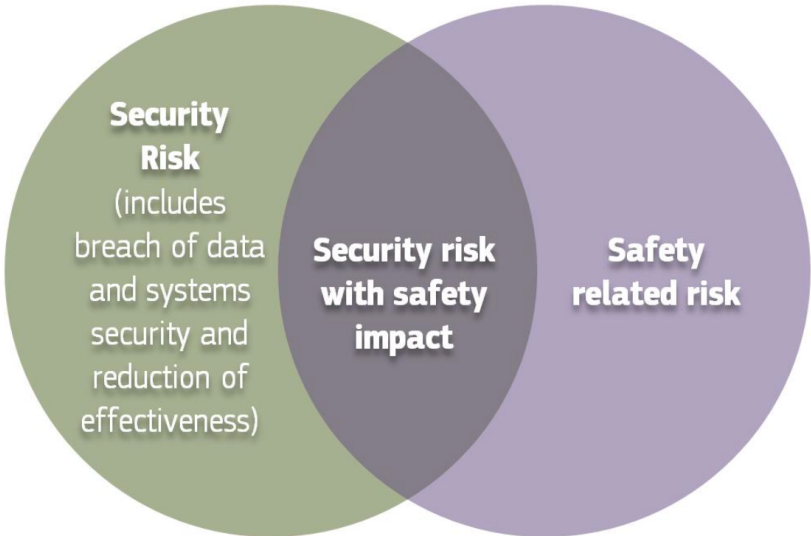


Figure 9 The interaction between Safety and security (MDCG 2019)

This framework is built mainly on the structure of ISO 31000 (2018) standards, Risk management, and the scientific article "A unified framework for risk and vulnerability analysis covering both safety and security" (Aven, 2006). It is the process that includes understanding and analyzing the system, finding, and describing the risk. The flowchart shown in Figure 10 illustrates the proposed integrated framework (Hybrid assets classification and integrated risk analysis).

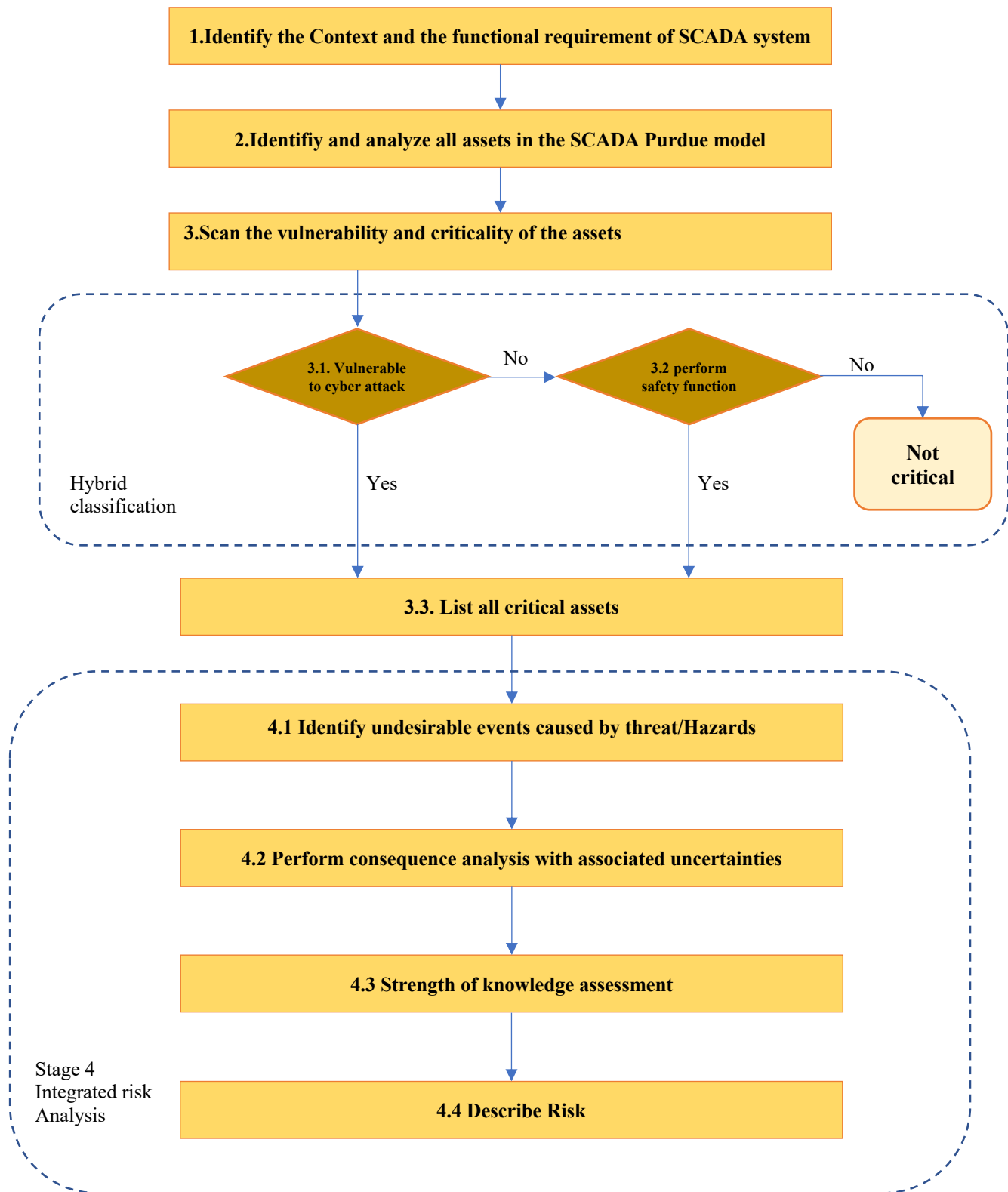


Figure 10 Flow chart of hybrid assets classification and integrated risk analysis

The first stage of the integrated framework, "Identify the context and the functional requirement of the SCADA system," is the outcome of combining two steps, Establish the context 31000 (2018) and identify the relevant functions and subfunctions to be analyzed and relevant performance measures (observable quantities) into a single step.

Whereas the second stage, Identify and analyze all assets in the SCADA Purdue model, is similar to the concept of "asset management" from ISO 27001 (2017), and "assets" (IEC 62443, 2009).

The third stage scan the vulnerability and check the criticality of asset features in each level in the SCADA Purdue models is requirement from NIST800-82(2015) to understand the complexity and interdependency of the system.

The steps of the fourth stage are adopted from several standards and frameworks; The following steps are the same as in Aven (2006), identify relevant sources of risk (threats, hazards) and perform an uncertainty analysis of these sources Perform a consequence analysis, with associated uncertainties and describe risks, which is similar to risk identification and risk analysis steps in (ISO 31000, 2018). Adversary analysis tactics and techniques based on real-world observations developed by (MITRE ATT&CK®, n.d.). The strength of knowledge assessment is the same as the framework proposed by Flage & Aven (2009) for assessing the strength of background knowledge in risk assessments. We provide Table 7 summarize what is the stages of integrated framework and related reference.

Table 7 Summarize the stages of the framework

Stages of the framework	References
1. Identify the context and the functional requirement of the SCADA system.	(ISO 31000, 2018) (Aven, 2006) (IEC 62443, 2009) (Cherdantseva et al., 2016)
2. Identify and analyze all assets in the SCADA Purdue model	(ISO 27001, 2017) (IEC 62443, 2009)
3. Check the criticality of asset features in each level in the SCADA Purdue	(NIST800-82,2015)
4. Integrated risk analysis	(Aven, 2006) (ISO 31000, 2018) (MITRE ATT&CK®, n.d.). (Flage & Aven, 2009) (Askeland et al., 2017)

5.2 Stage 1: Identify the context and the functional requirement of SCADA system.

In ISO31000 (2018) establishing the context is one of the main stages of a risk management process, and in NORSOK Standard Z-013(2010), it is a part of the risk assessment process. This stage aims to identify and facilitate the scope and objective of the whole process, especially for a support decision (Cherdantseva et al., 2016). Moreover, to assess the risk to (people, environment, assets) from a cyber-attack perspective on process Safety systems.

This stage should include the following:

- The objective and the scope of the assessment (*ISO 31000*, 2018)
- Deep knowledge and good understanding of SCADA system architecture its interdependencies with other systems, such as interactions between the safety requirement and information security, the goal of stakeholders, roles, and responsibilities, in addition to the interactions between human and machine. Understands the degree of integration between SCADA system and safety system), and all related information to identify the related risk to a system and perform a risk assessment (Cherdantseva et al., 2016; *IEC 62443*, 2009).
- Studying several aspects such as the structure of the organization, the culture state of safety and cybersecurity, specific goals, and strategies and investigates possible internal and external influences (*ISO 31000*, 2018).
- Risk acceptance criteria should be documented, especially regarding potential cyber-attacks and process safety, in addition to responsibilities, available resources, time, tools, methods, and associated constraints (*ISO 31000*, 2018).

Without establishing the context, it may not properly identify the risks related to the system, which are the basis for well-informed risk management (Cherdantseva et al., 2016).

5.2.1 Application of stage 1 on simplified SCADA system.

- The objective and the scope of the assessment
The Objective and the scope of the assessment is to assess risk to personnel (Safety impact) from cyber-attack. This stage covers the strategies and methods needed for the assessment and decision-making process. HAZOP for hazard and threat identification. In causes analysis, the fault tree can be used, and in the analysis of the consequences, the event tree can be used.
- Deep knowledge and good understanding of SCADA system architecture
In chapter 3 we illustrated in detail the SCADA system architecture and main components.
- The structure of the organization, the culture state of safety and cybersecurity
The proposed simplified model SCADA system, as shown in Figure 11, is one of ICS in the oil and gas industry that can perform several functions; for example, The operator or the engineer can monitor and control the pipeline system, perform maintenance, and shut down a valve. All these actions can be done remotely at the control room via human-machine interface HMI or by web access via mobile device.

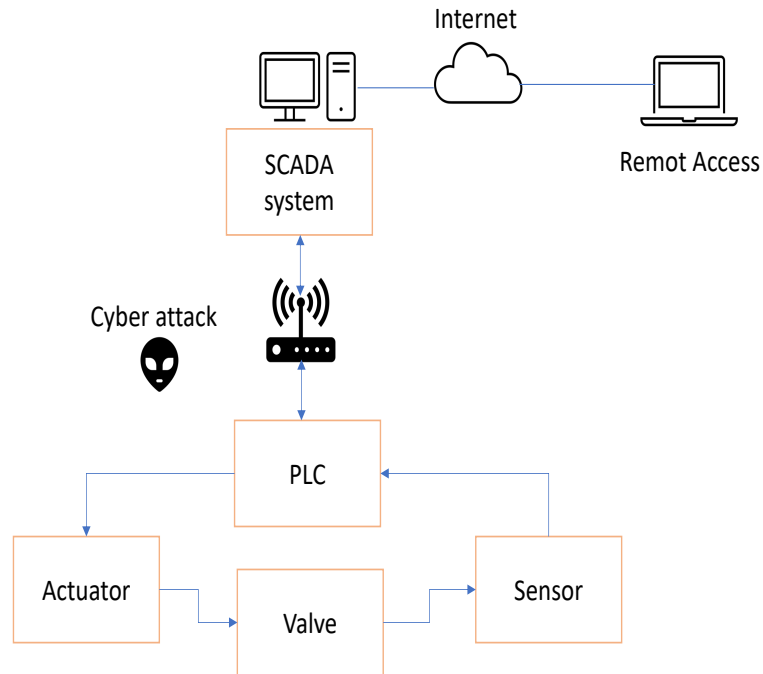


Figure 11 Simplified model for SCADA system

- Risk acceptance criteria

The relevant risk acceptance criteria should be in line with risk acceptance criteria established with the organization.

Throughout the analysis, we assume the following assumptions:

- PLC and SCADA system monitors and controls pressure and flow rate measurements in pipeline.
- Through the SCADA communication protocols, adversaries can infiltrate the system and plan attacks on sensors and actuators.

5.3 Stage 2: Identify and analyze all assets in the SCADA Purdue model

The classification analysis outlined in this stage provides a comprehensive basis for collecting information about the assets of the SCADA Purdue model as shown in the Figure 12. During this stage, the technical equipment of the SCADA system is not the only assets that is addressed (Cherdantseva et al.,2015).

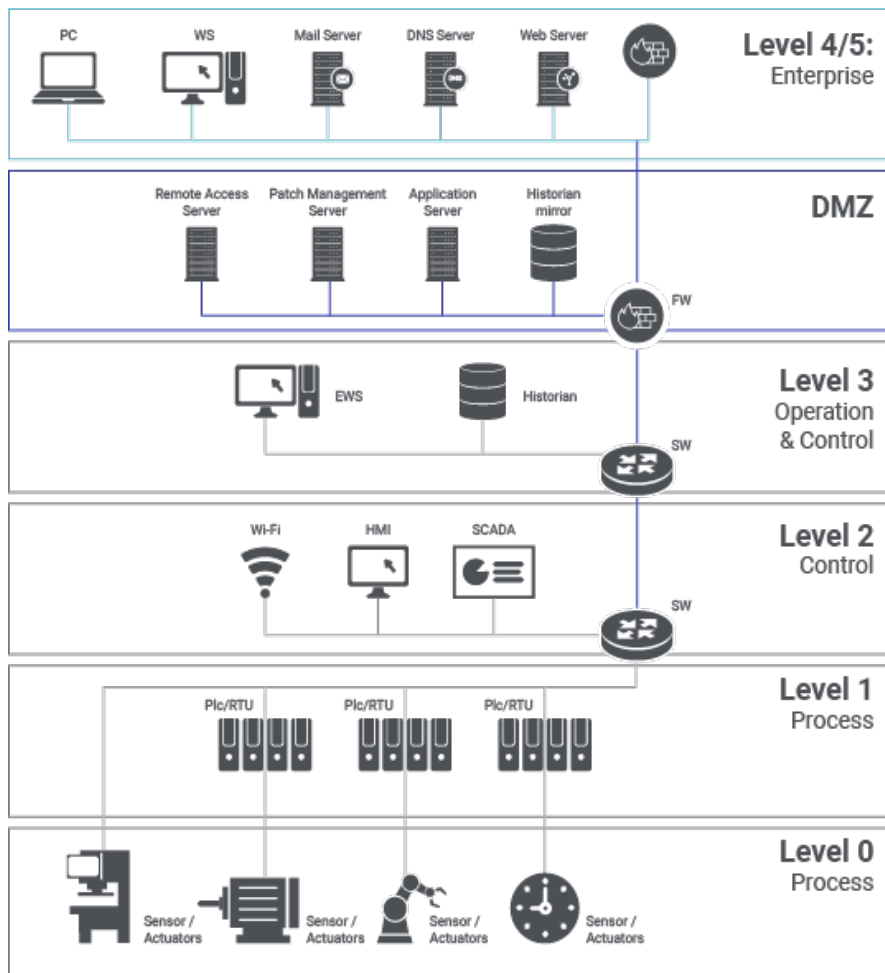


Figure 12 Purdue model of Scada system (What Is the Purdue Model for ICS Security, n.d.)

A security program's primary focus is to keep assets protected; it is necessary to compile an inventory of the assets that must be safeguarded to gain a comprehensive understanding of the risk to an ICS environment; Assets can be divided into three categories (IEC 62443, 2009):

- **Physical Assets:** Any physical component or combination of components that belong to an organization is considered a physical asset, such as Control systems, physical network components, and transmission media. The most valuable physical assets comprised the equipment controlled by the automation system.

- **Logical Assets:** Informational assets such as intellectual property, algorithms, proprietary practices, process-specific knowledge, public reputation, and other elements that reflect an organization's ability to operate or innovate can be included. Process assets include the automation logic that is used to carry out the industrial process. It may be compromised through physical (e.g., media destruction) or nonphysical (e.g., unauthorized modification) ways, resulting in a loss of process integrity or availability.
- **Human Assets:** People, the knowledge, and skills they hold linked to their production activities, certificates, expertise are considered human assets. Processing facilities are rarely fully automated. Thus, any disruption to the operations staff could significantly impact production, even if the physical and logical systems are unaffected. Every accident or attack that results in a person's injury would be considered an impact on human assets.

The classification analysis outlined in this stage presents a general basis for collecting information about the assets of the SCADA system, as shown in the Figure 13:

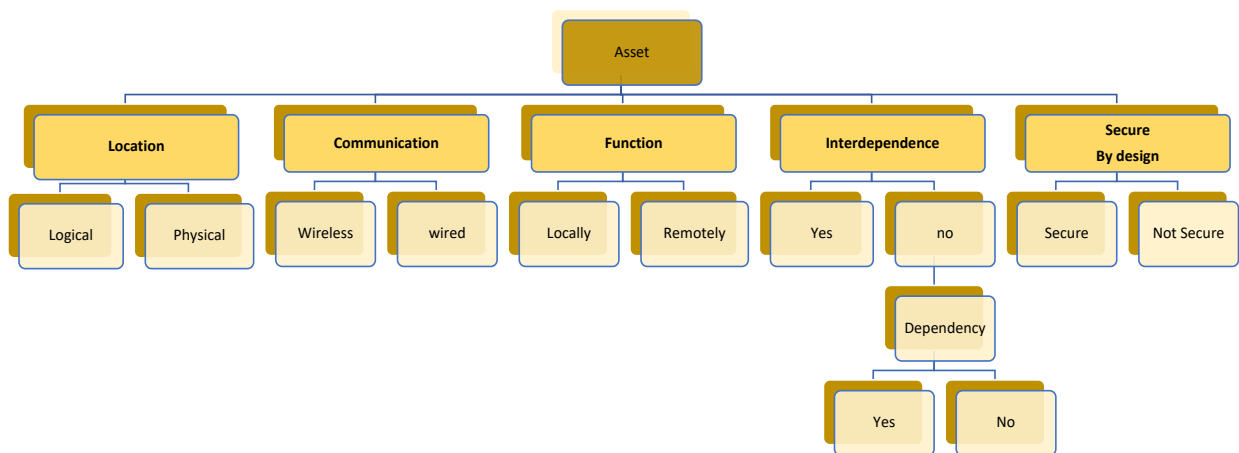


Figure 13 General Asset Classification

5.3.1 Application of stage 2 on simplified SCADA system.

In this system, the asset (PLC) can be analyzed accordance to several classification for example as shown in the Figure 14:

- Location of PLC in the Purdue model is in the basic control level/ level 1, the physical asset is in the control room.
- The way of communication with other assets, which depend on the attributes and location (physical, logical) of other assets that communicated with.
- The PLC's function is to remotely monitor a system's pressure state and execute the appropriate actions connected to the controlled process.

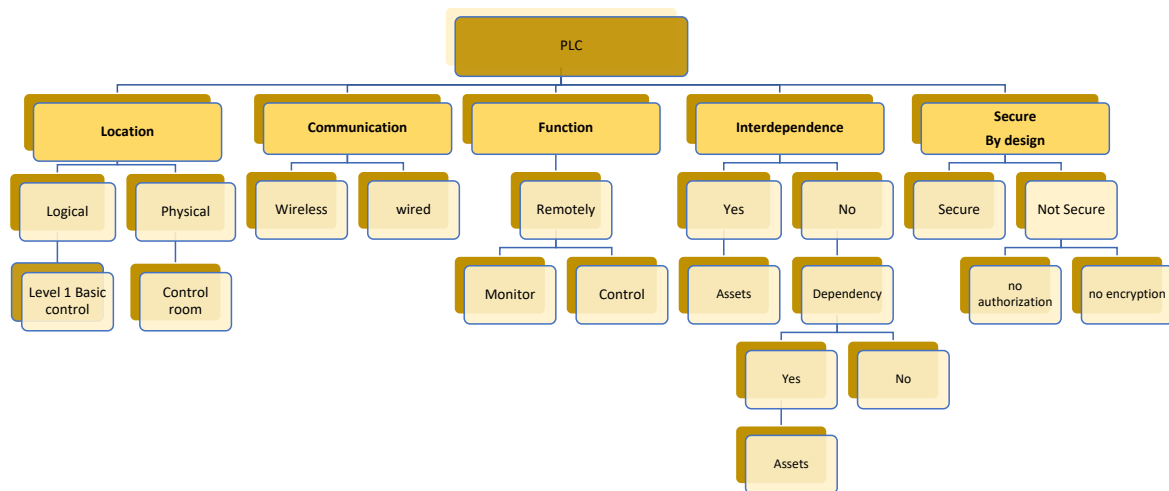


Figure 14 PLC general classification

- Interdependency means when two assets are interdependent; there is a bidirectional relationship between them in which the operations of asset A have an influence the functioning of Asset B and the processes of Asset B have an influence the functioning of Asset A. Whereas the dependency is a one-way relationship that exists between two assets as illustrated in the Figure 15 (Petit et al., 2015).

PLC ↔ SCADA system (Level 2) interdependent
 PLC ← Sensor (Level 0) are dependent.
 PLC → Actuator (Level 0) are dependent

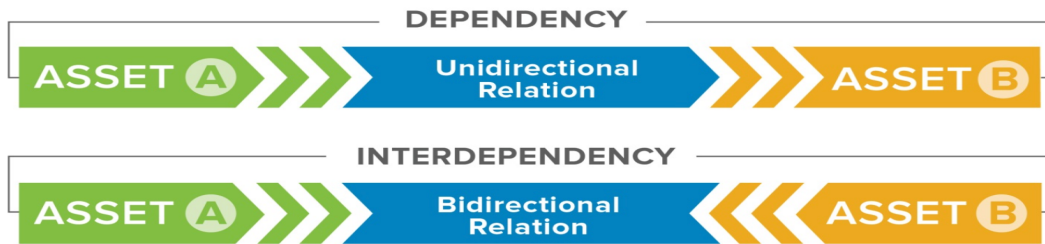


Figure 15 The difference between Dependency and Interdependency (Petit et al., 2015)

- Secure by design, we determine whether the asset was designed with security features and capabilities such as encryption solutions or authentication. In this system, if the adversary has logical access to the PLC, they can write commands and change the process without authenticating themselves.

5.4 Stage 3: Scan the vulnerability and criticality of the assets.

This stage illustrates the interdependencies and complexity between different asset types by examining the relationship between assets that might be vulnerable to cyber-attack and the assets that perform a safety function to assist organizations in prioritizing their most assets in the safety system domain. Moreover, it can help to identify threats as soon as they are identified.

Critical assets are defined in this framework as the asset that can directly or indirectly affect the availability of operation and process safety function.

- This asset can perform a safety or process function and connect to vulnerable asset.
- This asset would be a risk entry point or placing future potential resources at risk. This means a compromised or failure of connected assets can cause a catastrophic event. These assets would be considered critical.

This stage gives an overview of the assets features in the control and process safety system to enhance and visualize the way we identify the source of hazards and threats as soon as the assets are identified.

The Critically classification process is the analysis that evaluate the assets based on two criteria:

- Vulnerability scan to cyber-attack
This process is to classify the security weaknesses in all assets to check if hold a feature that is obviously vulnerable to cyber-attack. This scan performed to the following:
 - Assets in each level in SCADA system.
 - Physical, logical, human assets.

A security engineer can check this asset based on his/her knowledge about the system. In addition, to the available tools, references, and databases for obtaining information about

assets vulnerabilities, but in this step, we consider the asset is critical if there is a dependency to a vulnerable asset.

The Scada system is vulnerable due to a variety of factors and causes, including but not limited to complex and insecure design There are issues with humans, elements/automation, and configuration (Weed, 2017).

- Check the asset function (process or safety)

In this stage we check the function of the assets and the interdependency with vulnerable assets. And the evaluation of assets covers the following attributes:

- Perform process and safety functions.
 - Influences or dependence on the asset in step 1 including direct and indirect dependencies.
- List all critical assets.

5.4.1 Application of stage 3 on simplified SCADA system.

In this simplified system, PLC is the main asset that can be considered vulnerable to cyber-attack bases on the results of stage 2:

1. PLC performs the functions remotely via wireless connection and no authentication and encryption in communication protocols.
2. No authentication and encryption in its design.
3. PLC can be access via HMI.

We repeat this scan to the connected assets to PLC, which are actuator, because of the scan the actuator as device is not vulnerable to cyber but it is connected to a vulnerable asset. In this case we check the function of the actuator, The actuator influences the connected asset, the valve that perform a safety process and we conclude and list the relation between the vulnerable assets and the assets that influence or perform safety function.

As a result of this analysis, we consider PLC as critical asset, due to the vulnerability to cyber-attack and indirectly connected to a safety valve that perform a safety function.

5.5 Stage 4: Integrated risk analysis

Integrated risk analysis is a systematic analysis that aims to assess undesirable risk scenarios from a safety and security perspective that could result in catastrophic events.

- Identify relevant sources of risk (threats, hazards) and perform an uncertainty analysis of these sources.

In process hazards, the cause of hazard is more predictable because individual control of loops is considered. The overall common mode of failure of the entire controller fails equally at all outputs. On the other hand, cyber hazards consider the entire control process, which consists of multiple loops simultaneously (*ISA-TR84.00.09*, 2017).Cyber and physical processes CPS such as SCADA in CPSs are intertwined and interact through feedback control loops (for example, embedded cyber controllers monitor and control the system's physical variables,

while physical processes affect the monitoring system and computation units via wired or wireless networks (Zio, 2018).

Several methods and approaches can be used to identify sources of threat and hazards, such as former knowledge with similar system architecture and analysis, statistics, historical data, brainstorming exercises, and particular techniques such as failure mode and effect analysis, hazards and operability studies HAZOP(Aven, 2015).

Many different types of threats can be posed to an ICS and classified into four categories: adversarial, accidental, structural, and environmental(Stouffer et al., 2015).

- Identify the undesirable events and causal roots and attack path

The purpose of this step is to figure out how the initiating event might take place and what conditions must be met in order to occur. In addition to the coordination of the attack with regards to the logical location of the asset in the SCADA Purdue model.

It is possible to perform this step using event trees to identify the potential consequences of the initiating events(Aven, 2006).

According to Aven (2006) mentioned the following tasks to perform an analysis to the risk sources for their level of uncertainty:

1. obtaining information.
2. identifying scenarios.
3. assessing uncertainty.
4. assigning probabilities.

Threats must be characterized in sufficient depth to assist in the assessment of vulnerability and risk. The following are essential features to consider Type, motivation, triggers, capability methods, and trends(Motteff, 2005).

There are a variety of possible attack scenarios and major risks related to integrated operations according to the Sintef report Jaatun et al.(2007), these are the common suggested risk scenario for ICS SCADA system:

- Scenario 1: Virus infection influencing ICT and SCADA systems.

One of the most common causes of virus infections offshore is when the supplier's computer is connected to the production network, and the virus is distributed from a supplier to an operator. This incident can happen for several reasons, such as the supplier and the operator have different patching systems and security measures, lack of effective updating systems, or no barriers and safeguards. An infected computer connected to the process control component was discovered after a week of being in the booting process. This virus can lead to different consequences, including possible disruption of safety instrumented systems resulting in safety incidents or accidents and reduced production and profit.

- Scenario 2: Denial of service incident influencing the SCADA systems

The Denial of Service (DoS) attacks are a significant threat to the ICS. It is the goal of attack to prevent a system from accessing authorized resources or from using those resources in the manner intended(Ylmaz et al., 2018) . A denial-of-service (DoS) attack targets a component

of information technology at an offshore production facility. This attack flooding the target with traffic that increases the traffic load of the system that leads to production shutdown, loss of communication, and the possible impact on SIS.; the reason for DOS attack can be a malfunction or a malicious attack on a component that continually sends out error packets.

- Scenario 3: Insider threat

An insider threat comes from a dissatisfied employee who builds a backdoor in the production environment, creating a critical situation or allowing a shutdown during production. A disgruntled employee causes that because he got fired due to the reductions in the workforce. As a result of this decision, he wants to get revenge on his company by accessing the offshore production network and implementing a backdoor that may never be discovered except if the attacks launched and cause visible consequences. The consequences of an insider can destroy, manipulate, or edit data that are resulting in reduced or stopped production, business disruption, difficulties with safety instrumented systems, loss of communication between on- and offshore control rooms.

- Scenario 4: Missing situational awareness.

The service provider representative was shutting down a valve in production on an offshore oil and gas facility. The service provider deemed he shut down a valve in the test environment. Fortunately, the central control room operator discovered what occurred and managed to open the valve, thus detecting, and avoiding a critical situation. This condition has happened as a result of a lack of situational awareness among actors.

To analyze uncertainty due a cyber-attack scenario, a threat analysis is performed based on the asset identification and classification steps results on the assets that could be used as an adversary entry point into the system to investigate potential attack paths and attack scenarios result from interdependencies.

An adversary's behavior can be emulated using adversary emulation plans (AEPs) as shown in the figure, which are defined by a specific set of tactical tactics and procedures (TTPs) in MITRE ATT&CK.

To illustrate how advanced persistent threat compromises a system and exfiltrates sensitive information. AEPs are used by security teams to develop attack simulations based on specific adversaries to test their defense as shown in Figure 16 (MITRE ATT&CK®, n.d.).



Figure 16 Emulation of adversary plan (MITRE ATT&CK®, n.d.)

- Perform a consequence analysis, with associated uncertainties.

In the integrated risk assessment of SCADA systems, various undesirable scenarios and their potential consequences are analyzed and associated uncertainties. With particular attention to interactions among the two sectors, safety, and security. Event tree is one of the methods that relevant for performing consequences analysis(Aven, 2006).

Another method to analyze the possible consequences is a vulnerability analysis with particular attention paid to the system's weakness) of potential threats and hazards(Aven & Renn, 2010).

According to Stouffer et al. (2015), deep analysis and understanding of the source of vulnerabilities can reveal specific underlying causes and observations and help identify optimum mitigation strategies, and suggested the following groups of vulnerabilities:

1. Policy and Procedure.
2. Architecture and Design.
3. Configuration and Maintenance.
4. Physical.
5. Software Development.
6. Communication and Network.

- Strength of knowledge assessment

In this stage we should always present the strength of knowledge judgments alongside hybrid classification and uncertainties analysis in a security and safety environments.

Askeland et al.(2017) suggested a set of qualitative criteria for evaluating the strength knowledge of a security risk assessment in the Table 8:

Table 8 Evaluation of the strength knowledge of a security risk assessment (Askeland et al., 2017)

SoK label	Criteria for SoK label
Strong	<ol style="list-style-type: none"> 1. The phenomena involved are considered well understood: <ol style="list-style-type: none"> a. All risk sources (actors) are known. b. Both the capacity and the intention of the risk sources are considered well understood. c. Both models used to reflect and predict risk source (actor) knowledge and behavior (including knowledge of and response to measures) and models used to predict consequences, are known to give predictions with the required accuracy. 2. Much reliable data is available: <ol style="list-style-type: none"> a. High-frequency events: Both common-cause variation and special-cause variation are well characterized b. Rare events: Knowledge component data not relevant 3. There is broad agreement among experts 4. All assumptions have been identified, documented, and are seen as very reasonable: <ol style="list-style-type: none"> a. All explicit assumptions are documented b. A process for identifying tacit assumptions has been carried out c. All explicit assumptions are seen as highly reasonable, and the effect of potential further tacit assumptions is considered negligible 5. The knowledge K has been thoroughly scrutinised
Moderate	Conditions between strong and weak

Weak	<ol style="list-style-type: none"> 1. The phenomena involved are not considered well-understood: <ol style="list-style-type: none"> a. No risk sources (actors) are known b. Both the capacity and the intention of the risk sources are considered poorly understood c. Both models used to reflect and predict risk source (actor) knowledge and behaviour (including knowledge of and response to measures), and models used to predict consequences, are non-existent or known to give poor predictions 2. Data are not available, or are unreliable: <ol style="list-style-type: none"> a. High-frequency events: Both common-cause variation and special-cause variation are poorly characterized b. Rare events: Knowledge component data not relevant 3. There is considerable disagreement among experts 4. Assumptions have not been identified and documented, or represent strong simplifications: <ol style="list-style-type: none"> a. Explicit assumptions have not been documented b. A process for identifying tacit assumptions has not been carried out c. Most explicit assumptions (if any) are seen as representing strong simplifications, and the effect of tacit assumptions is considered non-negligible 5. The knowledge K has not been scrutinised
-------------	--

- Risk description

The multidisciplinary experts can identify, and list of hazards/cyber threats and undesirable events related SCADA system. With consideration to the expected consequences that have a safety impact, these consequences can be categorized into minor, moderate and major. Probabilities as a measure of uncertainties are divided by categories as follows: low, medium, and high. Background knowledge is supported by expert judgements, and relevant prior threat and risk assessments.

Risk can describe using the following elements:

- Identify the hazards/ cyber threats and undesirable events A'
- Expected consequences C'

According to Stouffer et al (2015) there are certain factors that must be considered: consequences for dependent systems and processes/ Physical environment/ safety, and the effect on the physical systems and processes.

- Measure of uncertainty P
- Background knowledge K
- Risk level according to the above information

5.5.1 Application of stage 4 on simplified SCADA system.

Programmable Logic Controllers (PLCs) are assets in the SCADA system that supports process control in the oil and gas industry. This asset executes user programs that control

actuators to the pressure valve based on input from digital sensors. This affects physical processes; if the

pressure inside the pipeline rises above a set point level, the excess pressure may cause an undesirable event. Figure 17 shows the analysis of the undesirable event.

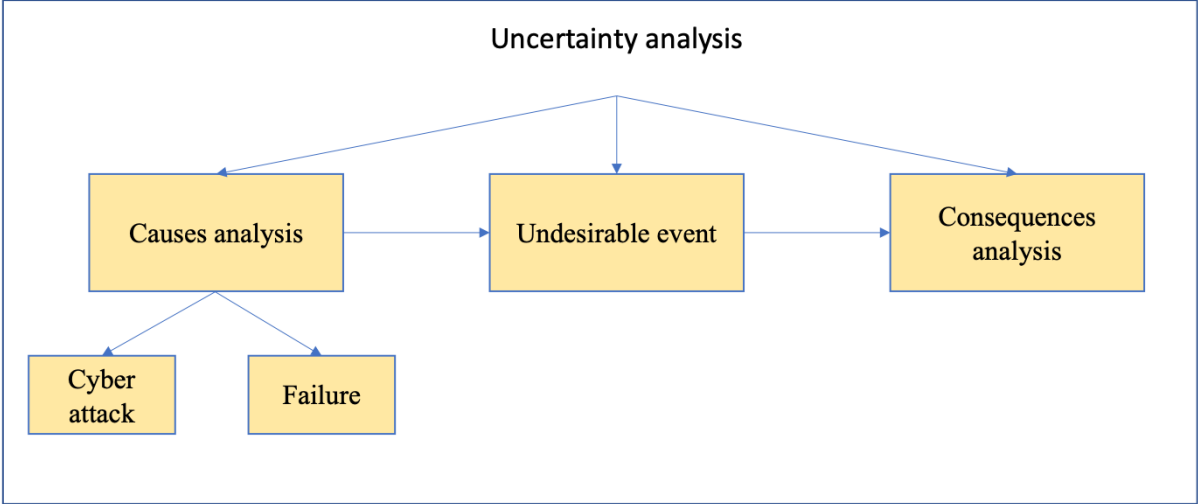


Figure 17 Analysis of undesirable event

- Identify relevant sources of risk (threats, hazards) and perform an uncertainty analysis of these sources.

A HAZOP study is a systematic examination of how deviations from a system's design requirements can occur, as well as an examination of the risks that these deviations may pose. Scenarios that could result in a hazard or an operational problem are recognized using a set of guidewords (Aven, 2015).

The relevant parameter for this process is Pressure and guideword used is more (increase pressure) Table 10 and Table 11 proposed HAZOP analysis with different security and safety perspective.

Table 9 HAZOP analysis with integrated perspective

Deviation	Causes	Cause Category	Consequence	Safeguards	Cybersecurity countermeasure
Increase pressure level	<ul style="list-style-type: none"> Valve Failure 	Malfunction	<ul style="list-style-type: none"> Fire/ explosion Overpressure and damage to pipeline 	<ul style="list-style-type: none"> Pressure relief valve 	<ul style="list-style-type: none"> No
	<ul style="list-style-type: none"> Manipulating the sensor data that is used to inform control system (FDI attack) Stopping the user program executing on the PLC (DOS attack) 	Cyber threat	<ul style="list-style-type: none"> Fire/ explosion Sabotage operation 	<ul style="list-style-type: none"> Pressure relief valve 	<ul style="list-style-type: none"> Secure the connection protocols using encryption that require the clients to authenticate with a password. Intrusion detection system

Table 10 Risk level

Expected consequences	Risk level without mitigation		Risk level with mitigation		
	Probability	Risk level	Expected consequences	Probability	Risk level
Major	Likely	High	Moderate	Likely	High

Some safeguards and countermeasures can affect the likelihood of occurring of an event, and others can affect the consequences of that event.

- Identify the undesirable events and causal roots and attack path.

In this simplified model, the identified scenarios are as follows:

- Valve failure
- False data injection cyber-attack on PLC in SCADA system

The question we may ask in this step is what conditions must be met in order for overpressure to occur? Event tree analysis can be used to answer this question. As shown in the Figure 17, the top event is overpressure in the pressure pipeline, this event could happen due to a valve failure or PLC (control system) failure.

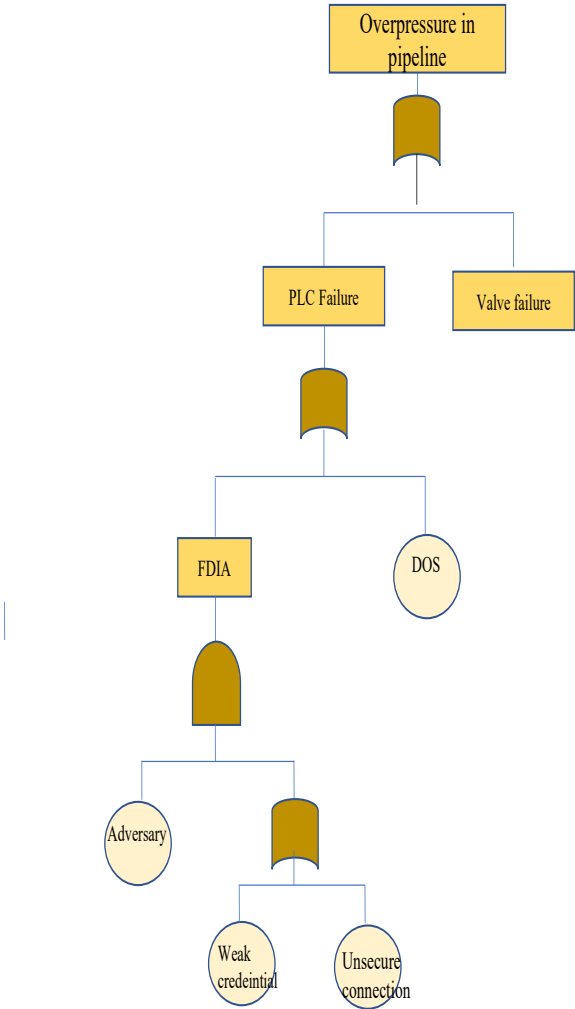


Figure 18 Fault Tree Analysis for Overpressure in the Pressure pipeline

- Perform a consequence analysis, with associated uncertainties.

In the integrated risk assessment of SCADA systems, critical assets are analyzed in consideration of the consequences and associated uncertainties. Paying particular attention to interactions among the two sectors. It is necessary to conduct a consequence analysis for the initiating events of a cyber-attack to understand the consequences of the overpressure as shown in the Figure 19. This analysis can provide a new countermeasure that can reduce the probability of a PLC failure.

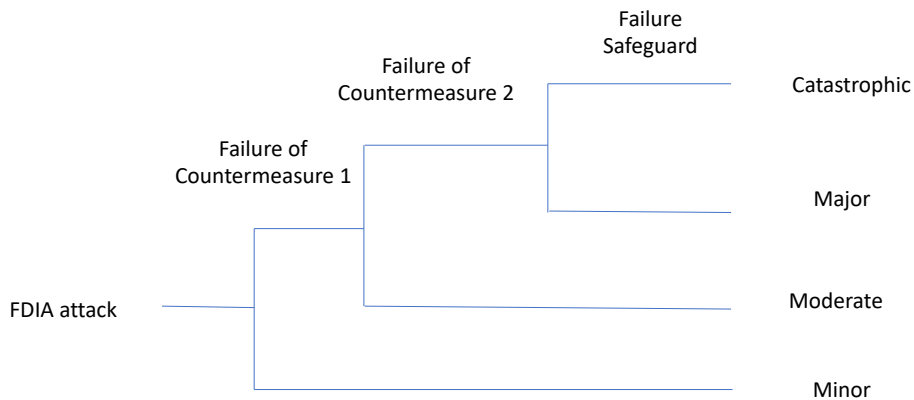


Figure 19 Event tree analysis for FDIA attack

The vulnerabilities of ICS and the architecture of the infrastructure are affecting the whole system. A variety of attack methods are available to exploit these vulnerabilities, with the false data injection attack being one of the most damaging. This is due to the fact that attacks allow for the controlled modification of data as well as the modification of firmware codes (Gönen et al., 2020).

- Strength of knowledge assessment

Understanding relevant phenomena: Are the risk sources /cyber threats outlined in the discussion typical of what we might encounter?

Understanding the assumptions: To what extent do the SCADA architecture and other assets characterize the design and operations of the system.

Reliable data availability: What is the quality level of the data and other documents? Are there any other attacks with similar consequences that we may investigate and compare the system to? Is the data quality sufficient to allocate specific security and safety requirements?

Consensus level between experts: Is there a consensus among the multidisciplinary (safety and security) team after all the discussions? Are we convinced that the risk has been adequately understood and controlled based on our conversations thus far?

Understanding the assumptions: To what extent does the SCADA architecture, and other assets characterize the design and operations of the system.

- Risk Description.

Table 11 presents the risk discription according to R (A`, C`, Q, K)

Table 11 Risk description

Hazard/ threat	Consequences	Probabilities	SoK	Risk level
FDIA Attack	C= Moderate	High	Moderate-weak	High
Scenario 1	C= Major	High	Moderate-weak	High
Scenario 2	C= Minor	Low	Weak	Low

6 Discussions

In this chapter, we will look at some of the issues that came up as a result of the scientific literature review and industry standards, including determining the similarities and differences in terms of safety and security. A summarize of relevant standards were discussed.

The proposed framework's strengths and limitations and the suggested future work are also highlighted.

6.1 Safety vs security in the proposed framework

One of the main questions that need to be addressed is the distinctions between safety and security in terms of concepts, risk viewpoints, and lifecycle? To understand how to integrate safety and security risk analysis into one framework, we must first know the similarities and differences between the two domains and where they intersect.

The terms safety and security are frequently interchanged. Although these are two distinct concepts, they are linked; as we mentioned earlier in chapter 2, safety is generally defined as preventing accidents. On the other hand, security has defined a defense against malicious intentions. In both definitions, they limited the safety to unintentional events and the security to intentional. Security events can occur accidentally, such as an insider that accidentally releases sensitive information without any intention; according to the IEC62443 intentional and unintentional events might be classified as cybersecurity events. In this case, both safety and security undesirable events can occur accidentally.

We have reviewed the safety and security concept in terms of risk in chapter 2 and agreed both safety and security can be viewed as being without unacceptable risk which is sharing the same purpose to keep people safe from harm. Refereeing to the simplified SCADA system in chapter 5, there are two scenarios related to an overpressure pipeline that should be protected in the simplified SCADA model. In the first scenario, the pipeline is protected due to a valve failure, which is most likely an accident related to the safety to protect the pipeline by implementing safety measures. In the second scenario, the pipeline is protected due to a cyber-attack or, most likely, a malicious intention related to the security to protect the pipeline by implementing safety or security measures. The goal in both scenarios is to avoid overpressure and keep the pipeline safe to keep people safe.

6.2 ICS relevant standards

There are limitations with IT standards when applying them in the ICS system due to the significant differences and security requirements, as presented in Table 3 IT vs. ICS. The major risk impact in the IT system is a delay in business operations; on the other hand, loss of life is the major risk impact in the ICS system.

Data confidentiality and integrity are the top priority of IT security, whereas availability is the top priority of ICS security, as previously stated.

Nevertheless, the safety aspect must be considered a priority inside the ICS security as controlling the physical world, and ensuring human safety comes first, followed by safeguarding the process, leading that IT security tried is inadequate for the ICs system.

ISO 31000(2018) is a general risk management standard that does not specifically address safety and security. IEC 61511(2016) is a performance-based standard that focuses on safety-critical systems in the process sector based on the safety lifecycle and clearly states the necessity to carry out the security risk assessment.

The NIST SP 800-82 (2015) and IEC 62433(2009) are the most comprehensive recommendations for security owners and vendors on protecting industrial control systems; moreover, they are examples of the current security standards for the industrial control system. Although a range of safety and security related standards were presented in chapter 3, neither standard, guidelines, and best practices encompass all aspects of safety and cybersecurity for ICS systems as listed in Table 12. The lack of a systematic approach is mainly what motivated us to propose an integrated framework.

Typically, the framework chosen will be determined by the industry and regulatory drivers that may necessitate a particular standard.

Table 12 Summarize the domain of relevant standards

Name	Domain	System
ISO 31000	General	General
IEC61511	Safety/ Partly security	SIS
NIST SP 800-82	Security	ICS
IEC 62433	Security	ICS
DNVGL- RP-108	Security	ICS
NOROG 104	Security/ Partly safety	ICT

6.3 The integrated risk identification in the proposed framework

In relation to the simplified SCADA system described in Chapter 5, PLC features and attributes are presented based on the findings of the asset analysis and hybrid classifications, which provides a proper understanding of the system's shortcomings before moving forward with the suggested design. The results from this stage show the relationship between PLC, sensors, and other assets.

This analysis can be particularly beneficial when doing an integrated risk analysis because it gives insight into discovering hidden hazards and cyber threats beneath the assets features with possible consequences.

Integrated risk identification could assist in determining what safeguards and countermeasures would be required to reduce the risks of a cyberattack. To enable the process safety analysis to visualize the possible threats and hazards and prioritize assets that need to implement the required countermeasures. In case of significant cyber threats, we may be protected by using safeguards that are not vulnerable to cyber-attacks.

In the HAZOP analysis, we consider an overpressure in a pipeline, as illustrated in section 5.5.1. Regularly a process hazard analysis was performed to identify the undesired scenarios that may occur and prevent this from occurring by adding safety measures; in order to guarantee that security requirements in the functional safety life cycle criteria are satisfied, we need to consider in this analysis if a cyberattack produces undesirable scenarios events.

Moreover, based on the HAZOP analysis findings, what the attacker can do if managed to get access to the control center or PLC, the adversary can manipulate the sensors readings and cause catastrophic events. A successful attack in the control center will impact the safety and protection systems to an unacceptable level.

The suggested integrated framework views at risk from the consequences side and associated uncertainties; from that side, we can reduce the risk effectively, first by identifying the undesirable scenarios despite the causes and identifying either a cyber or physical threat causing those. What are the safety measures or countermeasures to prevent cyber events from causing these catastrophic events?

In the HAZOP analysis, we suggest separating process safety safeguards and cybersecurity countermeasures to show that they may compensate each other and present the possible gaps. For example, in the second scenario we had there, cyber threats may cause pressure increases, but the eventual consequence may be mitigated with process safety safeguards, i.e., pressure relief valve in this case. A pressure relief valve is highly effective at preventing a high consequences event from occurring, regardless of what is happening in cyberspace.

6.4 Strengths and limitations of the framework

An integrated risk analysis founded on a robust framework, incorporated with experts' experiences from the safety and security domain, is highly beneficial to organizations that adequately raise their maturity level, efficiency, and cost effectiveness. This framework is built on the finding of the scientific literature and the risk theory. One of the main strengths of this framework is built on risk management standard ISO 31000 (2018), which are applicable in different types of risk (safety or security), and the scientific article "a unified framework for risk and vulnerability analysis covering both safety and security" Aven (2006) that highlighted the uncertainties associated with risk.

Moreover, justify why we can use safety and security from one risk perspective; strength of knowledge assessment is applied in this framework which can present the knowledge level about the phoneme to introduce it in the risk picture.

Assets analysis and hybrid classifications are other vital stages in the framework; this stage can present the relationship between assets, which can be an input to integrated risk analysis, discover hidden influencing factors, and visualize the complexity and interdependencies of the SCADA system. The proposed framework can help organizations make better decisions about appropriate safeguards and control measures.

Aside from the advantages that this framework offers, it also has certain limitations:

- This framework has not been tested and validated in full implementation of real SCADA system.
- The stage of analyzing assets is restricted to apparent features and attributes, which may be enhanced by examining these assets using a comprehensive analysis of various features.
- The hybrid classification has limits on understanding the interaction between cyber-attack-vulnerable assets and assets that perform a safety function.
- The vulnerability scan is mainly dependent on the analyst's experience, which may lead to inaccurate results.
- The thesis only investigated limited cybersecurity and safety risk standards and did not include any relevant regulations.

6.5 Future work

Further research is needed to validate and evaluate the scalability of the proposed integrated framework in a real SCADA system, plus examine the framework to other existing ICS systems.

Future studies might consider other standards and regulations. It is crucial to assess all current standard, frameworks, and regulations to detect and address any flaws. Asset analysis is provided and included in stage 2; this classification may be broadened to include other features that can be researched.

7 Conclusion

The main objective of this thesis was to develop an integrated risk analysis for the SCADA system with safety and security perspectives; due to the lack of systematic standards and framework that cover security risk with safety consequences in the ICS system.

Safety and security can be integrated by understanding the distinction between them in terms of concept, risk perspective, and lifecycle since both domains sharing the same goal of keeping people safe. This was done by reviewing scientific risk theories, theoretical concepts, and industry standards to present where safety and security overlapped and differed.

Various safety and security-related standards and recommendations are discussed, but none of them cover all aspects of safety and cybersecurity for ICS system. To determine which standards or framework to choose will be based on industry requirements and regulatory drivers that may necessitate a particular standard. Despite the fact that IEC 61511(2016) standard is mainly concerned with safety, and IEC 62433(2009) standard is primarily concerned with security, Integration between both of them are the most relevant standards when considering the subject of safety and cybersecurity. One of the challenges is that the IEC 62433 is comprehensive, making it difficult to execute. Another challenge is the integration of experts from different disciplines, since each team has its own way and method of analyzing risk and handling the system, which might be difficult to achieve one common language.

Assess, implement, and maintain phase are the key elements of the functional safety and cybersecurity lifecycle, and because of these similarities, engineers, operations technology, and information technology teams can combine the two lifecycles to create a single integrated lifecycle that can improve awareness of all potential hazards, threats, mitigation measures, and response plans.

This thesis proposed an integrated risk analysis framework that is mainly based on risk management standards ISO 31000 (2018), and a scientific article “a unified framework for risk and vulnerability analysis covering both safety and security” Aven(2006), to provide a holistic framework from the safety and security perspective. This framework focuses on a comprehensive understanding of the scope of the SCADA system, assets analysis, and hybrid classification to analyze the complexity and dependency of different types of assets in a SCADA system. A process hazard analysis regarding cybersecurity was undertaken and identified separate adequate safeguards and countermeasures to defend cyber-attack scenarios.

List of references

Amundrud, Ø., Aven, T., & Flage, R. (2017). How the definition of security risk can be made compatible with safety definitions. *Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability*, 231(3), 286–294.

<https://doi.org/10.1177/1748006X17699145>

Askeland, T., Flage, R., & Aven, T. (2017). Moving beyond probabilities – Strength of knowledge characterisations applied to security. *Reliability Engineering & System Safety*, 159, 196–205. <https://doi.org/10.1016/j.ress.2016.10.035>

Aven, T. (2006). A unified framework for risk and vulnerability analysis covering both safety and security. *Reliability Engineering & System Safety*, 92(6), 745–754.

<https://doi.org/10.1016/j.ress.2006.03.008>

Aven, T. (2015). *Risk Analysis*. John Wiley & Sons.

Aven, T., & Renn, O. (2010). *Risk management and governance: Concepts, guidelines and applications*. Springer.

Aven, T., & Zio, E. (2011). Some considerations on the treatment of uncertainties in risk assessment for practical decision making. *Reliability Engineering & System Safety*, 96(1), 64–74. <https://doi.org/10.1016/j.ress.2010.06.001>

Bonandir, N. A., Jamil, N., Nawawi, M. N. A., Jidin, R., Rusli, M. E., Yan, L. K., & Maudau, L. L. A. D. (2021). A Review of Cyber Security Assessment (CSA) for Industrial Control Systems (ICS) and Their Impact on The Availability of the ICS Operation. *Journal of Physics: Conference Series*, 1860(1), 012015. <https://doi.org/10.1088/1742-6596/1860/1/012015>

Cherdantseva, Y., Burnap, P., Blyth, A., Eden, P., Jones, K., Soulsby, H., & Stoddart, K. (2016). A review of cyber security risk assessment methods for SCADA systems. *Computers & Security*, 56, 1–27. <https://doi.org/10.1016/j.cose.2015.09.009>

Cyber-attack on Hydro. (2020). <https://www.hydro.com/en-NO/media/on-the-agenda/cyber-attack/>

Dake, K. (1992). Myths of nature: Culture and the social construction of risk. *Journal of Social Issues*, 48(4), 21–37. <https://doi.org/10.1111/j.1540-4560.1992.tb01943.x>

Dardick, G. S. (2010). *Cyber Forensics Assurance*. 9.

DNVGL-RP-G108. (n.d.). Retrieved June 21, 2021, from <https://rules.dnv.com/docs/pdf/DNV/RP/2017-09/DNVGL-RP-G108.pdf>

Eden, P., Blyth, A., Burnap, P., Cherdantseva, Y., Jones, K., & Soulsby, H. (2015, September 1). *A Forensic Taxonomy of SCADA Systems and Approach to Incident Response*. 3rd International Symposium for ICS & SCADA Cyber Security Research 2015 (ICS-CSR 2015). <https://doi.org/10.14236/ewic/ICS2015.5>

Elhady, A. M., El-bakry, H. M., & Abou Elfetouh, A. (2019). Comprehensive Risk Identification Model for SCADA Systems. *Security and Communication Networks*, 2019, 1–24. <https://doi.org/10.1155/2019/3914283>

Firesmith, D. G. (2003). *Common Concepts Underlying Safety Security and Survivability Engineering*: Defense Technical Information Center. <https://doi.org/10.21236/ADA421683>

Flage, R., & Aven, T. (2009). Expressing and communicating uncertainty in relation to quantitative risk analysis (QRA). *Reliability & Risk Analysis: Theory & Application*, 132.

Gao, J., Liu, J., Rajan, B., Nori, R., Fu, B., Xiao, Y., Liang, W., & Philip Chen, C. L. (2014). SCADA communication and security issues: SCADA communication and security issues. *Security and Communication Networks*, 7(1), 175–194. <https://doi.org/10.1002/sec.698>

Gönen, S., Sayan, H. H., Yılmaz, E. N., Üstünsoy, F., & Karacayılmaz, G. (2020). False data injection attacks and the insider threat in smart systems. *Computers & Security*, 97, 101955.

<https://doi.org/10.1016/j.cose.2020.101955>

Hacking, I. (1975). *The Emergence of Probability: A Philosophical Study of Early Ideas About Probability, Induction and Statistical Inference*. Cambridge University Press.

Hemsley, K. E., & E. Fisher, D. R. (ORCID:0000000277821830). (2018). *History of Industrial Control System Cyber Incidents (INL/CON-18-44411-Rev002)*. Idaho National Lab. (INL), Idaho Falls, ID (United States). <https://doi.org/10.2172/1505628>

Hildenbrandt, K., & van Beurden, I. (2019). Integration of Automation Lifecycles: Leveraging Functional Safety, Cybersecurity, and Alarm Management Work Processes. *Chemical Engineering Transactions*, 77, 625–630. <https://doi.org/10.3303/CET1977105>
IEC 61511. (2016).

<https://www.standard.no/no/Nettbutikk/produktkatalogen/Produktpresentasjon/?ProductID=811348>

IEC 61511-1:2016. (n.d.). Retrieved July 12, 2021, from

<https://www.standard.no/no/Nettbutikk/produktkatalogen/Produktpresentasjon/?ProductID=811348>

IEC 62443. (2009). <https://webstore.iec.ch/publication/7029>

ISA-TR84.00.09. (2017). [ISA-TR84.00.09-2017, Cybersecurity Related to the Functional Safety Lifecycle]. Isa.Org. <https://www.isa.org/products/isa-tr84-00-09-2017-cybersecurity-related-to-the-f>

ISO 27001. (2017).

<https://www.standard.no/no/Nettbutikk/produktkatalogen/Produktpresentasjon/?ProductID=925900>

ISO 31000. (2018). ISO 31000.

<https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/06/56/65694.html>

Jaatun, M. G., Johnsen, S. O., Bartnes, M., Longva, O. H., Tøndel, I. A., Albrechtsen, E., &

Wærø, I. (2007). Incident Response Management in the oil and gas industry. In *83 sider*.

<https://sintef.brage.unit.no/sintef-xmlui/handle/11250/2375186>

Johnsen, S. (2012). Safety and Security in SCADA Systems Must be Improved through

Resilience Based Risk Management. *Securing Critical Infrastructures and Critical Control*

Systems: Approaches for Threat Protection, 3, 286–300. [https://doi.org/10.4018/978-1-4666-](https://doi.org/10.4018/978-1-4666-2659-1.ch012)

[2659-1.ch012](https://doi.org/10.4018/978-1-4666-2659-1.ch012)

Kaspersky ICS CERT. (2021). *Threat landscape for industrial automation systems. Statistics*

for H2 2020. [https://ics-cert.kaspersky.com/reports/2021/03/25/threat-landscape-for-](https://ics-cert.kaspersky.com/reports/2021/03/25/threat-landscape-for-industrial-automation-systems-statistics-for-h2-2020/)

[industrial-automation-systems-statistics-for-h2-2020/](https://ics-cert.kaspersky.com/reports/2021/03/25/threat-landscape-for-industrial-automation-systems-statistics-for-h2-2020/)

Knapp, E. D., & Langill, J. (2015). *Industrial network security: Securing critical*

infrastructure networks for smart grid, scada, and other industrial control systems (2nd

edition). Elsevier.

Kondo, S., Sakashita, H., Sato, S., Hamaguchi, T., & Hashimoto, Y. (2018). An application of

STAMP to safety and cyber security for ICS. In M. R. Eden, M. G. Ierapetritou, & G. P.

Towler (Eds.), *Computer Aided Chemical Engineering* (Vol. 44, pp. 2335–2340). Elsevier.

<https://doi.org/10.1016/B978-0-444-64241-7.50384-0>

Li, Y., & Guldenmund, F. W. (2018). Safety management systems: A broad overview of the

literature. *Safety Science*, 103, 94–123. <https://doi.org/10.1016/j.ssci.2017.11.016>

MITRE ATT&CK®. (n.d.). Retrieved July 3, 2021, from <https://attack.mitre.org/>

Moteff, J. (2005). *Risk Management and Critical Infrastructure Protection: Assessing,*

Integrating, and Managing Threats, Vulnerabilities and Consequences. LIBRARY OF

CONGRESS WASHINGTON DC CONGRESSIONAL RESEARCH SERVICE.

<https://apps.dtic.mil/sti/citations/ADA454038>

Nicholson, A., Webber, S., Dyer, S., Patel, T., & Janicke, H. (2012). SCADA security in the light of Cyber-Warfare. *Computers & Security, 31*(4), 418–436.

<https://doi.org/10.1016/j.cose.2012.02.009>

NORG 070. (n.d.). Retrieved June 17, 2021, from

<https://norskoljeoggass.no/contentassets/adc7e1512f90400cb7fe9f314600bed6/070-guidelines-for-the-application-of-iec-61508-and-iec-61511-incl-attachments.pdf>

NOROG 104. (2016).

[https://norskoljeoggass.No/Contentassets/15263fd7f781409286f319bbeb427d93/104-Recommended-Guidelines-on-Security-Baseline-Requirements.Pdf](https://norskoljeoggass.no/contentassets/15263fd7f781409286f319bbeb427d93/104-Recommended-Guidelines-on-Security-Baseline-Requirements.Pdf).

(NORSOK Standard Z-013. (2010). <https://www.standard.no/en/sectors/energi-og-klima/petroleum/norsok-standard-categories/z-risk-analyses/z-0132/>

Obodoeze, F. C., Obiokafor, I. N., Asogwa, T. C., & Department of Computer Engineering Technology, Akanu Ibiam Federal Polytechnic, Unwana, Ebonyi State, Nigeria. (2018).

SCADA for National Critical Infrastructures: Review of the Security Threats, Vulnerabilities and Countermeasures. *International Journal of Trend in Scientific Research and Development, Volume-2*(Issue-2), 974–982. <https://doi.org/10.31142/ijtsrd9556>

Patel, S., Tantalean, R., Ralston, P., & Graham, J. (2005). *Supervisory control and data acquisition remote terminal unit testbed*.

https://scholar.google.com/citations?view_op=view_citation&hl=en&user=kmtwKR0AAAAJ&citation_for_view=kmtwKR0AAAAJ:hF0r9nPyWt4C

Petit, F., Verner, D., Brannegan, D., Buehring, W., Dickinson, D., Guziel, K., Haffenden, R., Phillips, J., & Peerenboom, J. (2015). *Analysis of Critical Infrastructure Dependencies and*

Interdependencies (ANL/GSS--15/4, 1184636; p. ANL/GSS--15/4, 1184636).

<https://doi.org/10.2172/1184636>

Pliatsios, D., Sarigiannidis, P., Lagkas, T., & Sarigiannidis, A. G. (2020). A Survey on SCADA Systems: Secure Protocols, Incidents, Threats and Tactics. *IEEE Communications Surveys & Tutorials*, 22(3), 1942–1976. <https://doi.org/10.1109/COMST.2020.2987688>

Rausand, M. (2013). *Risk Assessment: Theory, Methods, and Applications*. Wiley.

<http://rbdigital.oneclickdigital.com>

Roper, C. (1999). *Risk Management for Security Professionals*. Elsevier Science.

Smith, C. L., & Brooks, D. J. (2013). *Security science: The theory and practice of security*.

Elsevier, BH.SRA. (2018).

Stouffer, K., Pillitteri, V., Lightman, S., Abrams, M., & Hahn, A. (2015). *Guide to Industrial Control Systems (ICS) Security* (NIST SP 800-82r2; p. NIST SP 800-82r2). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.SP.800-82r2>

Tariq, N., Asim, M., & Khan, F. (2019). Securing SCADA-based Critical Infrastructures: Challenges and Open Issues. *Procedia Computer Science*, 155, 612–617.

<https://doi.org/10.1016/j.procs.2019.08.086>

Walkington, J., & Sugavanam, S. (2019). *Functional Safety & Cyber Security Lifecycle Management*. 19.

Warren, M. J., & Leitch, S. (2015). Cyber Security and Protection of ICS Systems: An Australian Example. In M. Lehto & P. Neittaanmäki (Eds.), *Cyber Security: Analytics, Technology and Automation* (Vol. 78, pp. 215–228). Springer International Publishing.

https://doi.org/10.1007/978-3-319-18302-2_14

What is the Purdue Model for ICS Security. (n.d.). Zscaler. Retrieved July 5, 2021, from

<https://www.zscaler.com/resources/security-terms-glossary/what-is-purdue-model-ics-security>

Yadav, G., & Paul, K. (2021). Architecture and security of SCADA systems: A review.

International Journal of Critical Infrastructure Protection, 34, 100433.

<https://doi.org/10.1016/j.ijcip.2021.100433>

Ylmaz, E. N., Ciylan, B., Gonen, S., Sindiren, E., & Karacayilmaz, G. (2018). Cyber security in industrial control systems: Analysis of DoS attacks against PLCs and the insider effect.

2018 6th International Istanbul Smart Grids and Cities Congress and Fair (ICSG), 81–85.

<https://doi.org/10.1109/SGCF.2018.8408947>

Zalewski, J., Buckley, I. A., Czejdo, B., Drager, S., Kornecki, A. J., & Subramanian, N.

(2016). A Framework for Measuring Security as a System Property in Cyberphysical

Systems. *Information*, 7(2), 33. <https://doi.org/10.3390/info7020033>

Zio, E. (2018). The future of risk assessment. *Reliability Engineering & System Safety*, 177,

176–190. <https://doi.org/10.1016/j.ress.2018.04.020>