

RESEARCH REPORT

VTT-R-00499-24



Comparison of cybersecurity and functional safety risk assessments

Authors: Timo Malm, Josepha Berger, Risto Tiusanen, Antti Ranta, Jari Seppälä, Bilhanan Silverajan, and Hanning Zhao

Confidentiality: Public

Version: 16.9.2024



Report's title Comparison of cybersecurity and functional safety risk assessments	
Customer, contact person, address Business Finland	Order reference 627/31/2022
Project name Connected Mobile Machine Lifetime Cyber Security	Project number/Short name 316146 / BF_COMMA
Author(s) Timo Malm, Josepha Berger, Risto Tiusanen, Antti Ranta, Jari Seppälä, Bilhanan Silverajan, and Hanning Zhao	Pages 55/
Keywords cybersecurity, functional safety, risk, risk assessment	Report identification code VTT-R-00499-24
<p>Summary</p> <p>Cybersecurity and functional safety have different objectives and there are differences in risk assessments. Cooperation between the domains is needed, especially, in risk identification and risk treatment phases. It is useful to consider cybersecurity risk treatment actions from many perspectives and levels, like, lifecycle phase, system of systems approach, properties of the target and risk treatment strategy. In addition, defence in depth strategy need to be applied. This kind of holistic approach can make it more probable to avoid the weak links of the cybersecurity.</p> <p>Companies are facing new cybersecurity requirements, and this means that there is a lot of work to fulfil the requirements. On the other hand, the requirements are made, because the number of cyberattacks is increasing and actions are needed to prevent and minimize the impacts of cyberattacks. The requirements are also related to the level of confidence. When machine manufacturers and system providers are fulfilling specific requirements the customers can learn, how confident they can be on cybersecurity measures, and this can be good for business. Also, the user organization and asset owner need to have adequate cybersecurity measures, since they are often the first ones to suffer consequences of the cyberattack. All of this can be considered as a new expense item, but it can be seen also as an opportunity to new business.</p>	
Confidentiality	VTT Public
Tampere 16.9.2024 Written by Timo Malm Senior scientist	Reviewed by Petteri Alahuhta Vice President
VTT's contact address VTT, PL 1300, 33101 Tampere	
Distribution (customer and VTT) VTT Register Office + internet	
<i>The use of the name of "VTT" in advertising or publishing of a part of this report is only permissible with written authorisation from VTT Technical Research Centre of Finland Ltd.</i>	



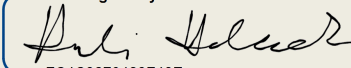
Approval

VTT TECHNICAL RESEARCH CENTRE OF FINLAND LTD

Date:

20 September 2024

Signature:

DocuSigned by:

FC4C3270428F48E...

Name:

Heli Helaakoski

Title:

Vice President, Cognitive production industry



Preface

This research has been conducted as a part of the Connected Mobile Machine Lifetime Cyber Security (COMMA) project, which is mainly funded by Business Finland. The companies and research institutes at the project are: VTT Technical Research Centre of Finland Ltd (VTT), Tampere University (TAU), University of Turku (UTU), Sandvik Mining and Construction Ltd, Cargotec Finland Oy and Ponsse Oyj. The steering group members and active members are: Timo Malm, Eetu Heikkilä (up to May 2023), Risto Tiusanen, Josepha Berger, Jarmo Alanen, Joonas Linnosmaa, Jarno Salonen, Andrea Dalla Costa, Nikolaos Papakonstantinou (up to January 2024), Petteri Alahuhta, Heli Helaakoski, Johannes Hyrynen, Harri Nieminen, Jarno Salonen (VTT), Bilhanan Silverajan, Antti Ranta, Jari Seppälä, Matti Vilkkö, Zhao Hanning (TAU), Marikka Heikkilä, Jonna Järveläinen, Ekaterina Panina (UTU), Jarkko Holappa (Sandvik), Pekka Yli-Paunu, Jani Mäntytörmä (Kalmar), Jyrki Sauramäki (EPEC), and Simo Nieminen (Ponsse).

Tampere 16.9.2024

Authors



Contents

Preface.....	3
Definitions and classifications.....	5
1 Introduction.....	9
2 Materials and methods	10
3 Cybersecurity requirements in EU legislation and international standards	11
4 Comparison of cybersecurity and functional safety risk assessment processes.....	13
4.1 Parameters of functional safety and cyber security risks.....	13
4.1.1 Items related to cybersecurity and functional safety.....	15
4.1.2 Taxonomies of dependability and cybersecurity.....	16
4.1.3 Cyberattack effects on safety.....	19
4.1.4 Comparison of cybersecurity properties in IT and OT systems	20
4.2 Categorizing cybersecurity and functional safety	23
4.2.1 Security levels	23
4.2.2 Safety Performance Levels.....	24
4.3 Comparison of risk assessment processes.....	26
4.3.1 Machinery safety and information security risk assessment.....	26
4.3.2 Information security and industrial automation security risk assessment.....	27
4.3.3 Functional safety and industrial automation security risk assessment.....	28
4.3.4 An example of risk assessment of a single safety function	29
4.4 Risk treatment	31
4.4.1 General risk treatment options.....	31
4.4.2 Risk treatment methods.....	32
4.4.3 Possible conflicts between risk treatment measures.....	33
4.4.4 Defence in depth	34
4.5 Cybersecurity and functional safety differences.....	36
5 Cybersecurity risk assessment	41
5.1 Examples of cybersecurity risk assessment methods	41
5.1.1 STPA-SEC	41
5.1.2 STPA-Sec + STRIDE.....	42
5.1.3 Security Threat Analysis (STA).....	43
5.1.4 Uncontrolled Flows of Information and Energy (UFoI-E).....	44
5.2 Risk assessment of System of Systems	45
5.3 Cybersecurity perspective on risk assessment	45
6 Discussions with companies.....	46
7 Discussion.....	48
8 Conclusions.....	52
References.....	53

Definitions and classifications

- Access control (cybersecurity):** Protection of system resources against unauthorized access; a process by which use of system resources is regulated according to a security policy and is permitted by only authorized entities (users, programs, processes, or other systems) according to that policy. [26]
- Asset:** Physical or logical object having either a perceived or actual value to a control system. [33]
- Attack:** Assault on a system that derives from an intelligent threat. [33]
Unauthorized attempt to compromise the confidentiality, integrity, or availability of an (IACS) industrial automation and control system(s) that derives from an intelligent threat. [31]
- Authentication:** Provision of assurance that a claimed characteristic of an identity is correct. [30]
- Authorization:** Right or permission that is granted to a system entity to access a system resource. [26]
- Availability:** Ability of an item to be in a state to perform a required function under given conditions at a given instant or over a given time interval, assuming that the required external resources are provided. [33]
- Conduit (cybersecurity):** Logical grouping of communication channels, connecting two or more zones, that share common security requirements. [29]
- Confidentiality:** Assurance that information is not disclosed to unauthorized individuals, processes, or devices. [33]
- Countermeasure:** Action, device, procedure, or technique that reduces a threat, a vulnerability, or an attack by eliminating or preventing it, by minimizing the harm it can cause, or by discovering and reporting it so that corrective action can be taken. [33]
- Control (cybersecurity):** Measure that is modifying risk. [29]
NOTE 1 Controls for information security include any process, policy, procedure, guideline, practice or organizational structure, which can be administrative, technical, management, or legal in nature which modify information security risk.
NOTE 2 Controls may not always exert the intended or assumed modifying effect.
NOTE 3 Control is also used as a synonym for safeguard or countermeasure. [43]
- Control:** Purposeful action on or in a process to meet specified objectives. [IEC 60050-351]
- CPS:** Cyber-Physical System. CPSs are integrations of computation with physical processes. A new generation of digital systems, composed of computational and physical capability that engages with humans. [6]
- CRC:** Cyclic Redundancy Check is a way to calculate a checksum, based on a polynomial. CRCs are used to check that no errors occurred transmitting or storing the data. [Wikipedia]
- Cyberattack:** Attempt by digital means to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset. [32]
- Cybersecurity:** <of the machine control system> Set of activities necessary to protect network and information systems of the machine control system, the users of such systems, and other persons from cyber threats, typically regarding the aspects of confidentiality, integrity and availability. [33]
Set of activities and measures the objective of which is to prevent, detect, and react to:
- malicious modifications (integrity) of functions that may compromise the delivery or integrity of the required service by I&C programmable digital systems (incl. loss of control) which could lead to an accident, an unsafe situation or plant performance degradation;
 - malicious withholding or prevention of access to or communication of information, data or resources (incl. loss of view) that could compromise the delivery of the required service by I&C systems (availability) which could lead to an accident, an unsafe situation or plant performance degradation;

– malicious disclosures of information (confidentiality) that could be used to perform malicious acts which could lead to an accident, an unsafe situation or plant performance degradation. [32]

Dangerous failure: Failure of an element and/or subsystem and/or system that plays a part in implementing the safety function that: a) prevents a safety function from operating when required (demand mode) or causes a safety function to fail (continuous mode) such that the machine is put into a hazardous or potentially hazardous state; or
b) decreases the probability that the safety function operates correctly when required. [33]

Data integrity: Property that data has not been changed, destroyed, or lost in an unauthorized or accidental manner. NOTE: This term deals with constancy of and confidence in data values, not with the information that the values represent or the trustworthiness of the source of the values. [26]

Defence in depth: Provision of multiple security protections, especially in layers, with the intent to delay if not prevent an attack. Defence in depth implies layers of security and detection, even on single systems, and provides the following features: attackers are faced with breaking through or bypassing each layer without being detected; flaw in one layer can be mitigated by capabilities in other layers; a system security becomes a set of layers within the overall network security. [26]

Security architecture based on the idea that any one point of protection may, and probably will, be defeated. NOTE: Defence in depth implies layers of security and detection, even on single systems, and provides the following features: attackers are faced with breaking through or bypassing each layer without being detected; a flaw in one layer can be protected by capabilities in other layers; system security becomes a set of layers within the overall network security. [27]

DMZ, Demilitarized zone: DMZ is physical or logical subnetwork that contains and exposes an organization's external-facing services to an untrusted usually larger network such as internet. (Wikipedia)

An interface on a routing firewall that is similar to the interfaces found on the firewall's protected side. Traffic moving between the DMZ and other interfaces on the protected side of the firewall still goes through the firewall and can have firewall protection policies applied. [40]

FMEA, FMECA, FTA: FMEA: failure modes and effects analysis, FMECA: failure modes, effects and criticality analysis, FTA: fault tree analysis. [35]

Failure: Termination of the ability of a device to perform a required function.

Note 1 to entry: After a failure, the device has a fault.

Note 2 to entry: "Failure" is an event, as distinguished from "fault", which is a state.

Note 3 to entry: Failures which only affect the availability of the process under control are outside of the scope of this document. [35]

Functional safety: Considers the failure characteristics of elements/components performing a safety function. For each safety function, this failure characteristic is expressed as the frequency of dangerous failure per hour (PFH). ISO 13849-1:2023

Harm: Physical injury or damage to health. [35]

Hazard: Potential source of harm. [35]

IACS: Industrial automation and control system(s). [30]

IT-security, Information Technology security, cyber security: Protection of an IT-system from the attack or damage to its hardware, software or information, as well as from disruption or misdirection of the services it provides [8]

IT-system: Information Technology Systems are related to communication between computers in office automation. Table 1 describes the differences between IT and OT systems.

NIS2: Network and Information Systems Directive II (EU NIS2 directive, second edition). [14]

NIST: National Institute of Standards and Technology. U.S. department of commerce.
[<https://www.nist.gov/>]

OSI: Open Systems Interconnection. In the OSI reference model, the communications between systems are split into seven different abstraction layers: Physical, Data Link, Network, Transport, Session, Presentation, and Application. [Wikipedia]

OT security: OT security is the process of securing the practices and technologies deployed to monitor, detect, and control changes to operational technology infrastructure, people, and data. Operational



technology (OT) refers to hardware and software systems that execute monitoring and/or control over industrial equipment and processes. (Paloalto. Cyberpedia)

OT-system: Operation Technology Systems are related to communication systems that are related to industrial machines and processes (see Operational technology).

Operational technology: A broad range of programmable systems and devices that interact with the physical environment or manage devices that interact with the physical environment. These systems and devices detect or cause a direct change through the monitoring and/or control of devices, processes, and events. Examples include industrial control systems, building automation systems, transportation systems, physical access control systems, physical environment monitoring systems, and physical environment measurement systems. [14]

PL_r (required performance level): Performance level required in order to achieve the required risk reduction for each safety function. [35]

PL, Performance Level: Discrete level used to specify the ability of safety-related parts of control systems to perform a safety function under foreseeable conditions. [35]

PHA: Preliminary hazard analysis. [39]

RAMSS: Reliability, availability, maintainability, safety, security.

Risk (functional safety): Combination of the probability of occurrence of harm (physical injury or damage to health) and the severity of that harm. [35]

Risk (cybersecurity): Expectation of loss expressed as the likelihood that a particular threat will exploit a particular vulnerability with a particular consequence. [28]

The level of impact on agency operations (including mission, functions, image, or reputation), agency assets, or individuals resulting from the operation of an information system, given the potential impact of a threat and the likelihood of that threat occurring. [14]

Risk estimation: Defining likely severity of harm and probability of its occurrence. [34]

Risk evaluation: Judgment, on the basis of risk analysis, of whether the risk reduction objectives have been achieved. [34]

Safety: Freedom from risk which is not tolerable. [33]

Safety integrity: Probability of a safety-related control system satisfactorily performing the specified safety functions under all the stated conditions within a stated period of time. [33]

SIL, Safety Integrity Level: Discrete level (one out of a possible four) for specifying the safety integrity requirements of safety functions to be allocated to the safety-related systems, where safety integrity level 4 has the highest level of safety integrity and safety integrity level 1 has the lowest. [35]

Security:

- a) Measures taken to protect a system
- b) condition of a system that results from the establishment and maintenance of measures to protect the system
- c) condition of system resources being free from unauthorized access and from unauthorized or accidental change, destruction, or loss
- d) capability of a computer-based system to provide adequate confidence that unauthorized persons and systems can neither modify the software and its data nor gain access to the system functions, and yet to ensure that this is not denied to authorized persons and systems
- e) prevention of illegal or unwanted penetration of, or interference with, the proper and intended operation of a machinery and its control system. [33]

SL, Security Level: Measure of confidence that the IACS is free from vulnerabilities and functions in the intended manner. [29]

SL-T (target): The desired level of security for a particular IACS, zone or conduit. This is usually determined by performing a risk assessment on a system and determining that it needs a particular level of security to ensure its correct operation.

SL-A (achieved) The actual level of security for a particular system. These are measured after a system design is available or when a system is in place. They are used to establish that a security system is meeting the goals that were originally set out in the SL-Ts.



- SL-C (capability)** The SLs that components or systems can provide when properly configured. These levels state that a particular component or system is capable of meeting the SL-Ts natively without additional compensating countermeasures when properly configured and integrated. [28]
- Security risk:** Expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular consequence. [33]
- STA:** Security Threat Analysis. See 5.1.3, [2]
- Stand-alone system (SaS):** Independent, organisationally homogeneous system as opposed to a SoS. [37]
- STRIDE:** Stride is a model for identifying computer security threats. Security threat categories are **Spoofing** (a person or program successfully identifies as another by falsifying data), **Tampering** (many forms of sabotage or intentional modification of products), **Repudiation** (authentication problems), **Information disclosure** (privacy breach or data leak), **Denial of service** (network resource unavailable to its intended users) and **Elevation of privilege** (an application or person can perform unauthorized actions). [Wikipedia]
- STPA:** System-Theoretic Process Analysis. STPA is qualitative safety analysis method, which addresses system-based hazards and reveals design and requirements flaws, dysfunctional interactions between components that themselves act as intended. [4]
- System of Systems (SoS):** Set of systems or system elements that interact to provide a unique capability that none of the constituent systems can accomplish on their own. Note: System elements can be necessary to facilitate the interaction of the constituent systems in the system of systems. [37]
- Threat:** Circumstance or event with the potential to adversely affect operations (including mission, functions, image or reputation), assets, control systems or individuals via unauthorized access, destruction, disclosure, modification of data and/or denial of service. [33]
Any circumstance or event with the potential to adversely impact agency operations (including safety, 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. [14]
- Threat source:** The intent and method targeted at the intentional exploitation of a vulnerability or a situation and method that may accidentally trigger a vulnerability. [14]
- Threat vector:** path or means by which a threat source can gain access to an asset. [28]
- Validation:** confirmation by examination and provision of objective evidence that the particular requirements for a specific intended use are fulfilled. [35]
- Verification:** confirmation, through the provision of objective evidence, that specified requirements have been fulfilled. [35]
- Vulnerability:** <of the machine control system> Weakness of a machine control system or a countermeasure that can be exploited by one or more threats to violate the machine control system's integrity. [33]
Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source. [14]
- Zone (cybersecurity):** Grouping of logical or physical assets that share common security requirements. [29]
- UFOI-E:** Uncontrolled Flows of Information and Energy. An integrated method for analyzing safety and security. Shows relationships between the energy and information flows. See 5.1.4. [7]

1 Introduction

As number of cyberattacks increases, safety systems in machines can also be endangered. Risk assessment is one way to identify and assess the threats and vulnerabilities of safety related systems. Safety risk assessments have already a long tradition in machinery sector, but cybersecurity assessments have a shorter history, and good practices need to be developed.

Safety analysis has a long history. E.g., FMEA was developed in 1940's in military applications (Wikipedia). Functional safety related standard family was first published in 1998, but there were discussions and related standards already in 1980's. Safety logics are mentioned at Machinery Directive (2006/42/EC) [36]. One of the first IT-security standards was ISO/IEC 17799:2000 and its successor ISO/IEC 27000 series. OT-security standards started as ANSI/ISA 62443 family (International Society of Automation) 2010 and later it became IEC standard family (Wikipedia). One could estimate that in machinery domain national safety requirements are almost thirty years older than functional safety requirements and OT-security is more than decade behind functional safety. All cybersecurity requirements are evolving continuously with increasing speed, but the maturity of different domains is different. Maturity is often related to the speed of requirement changes and cybersecurity requirements can be assumed to change rapidly.

The aim of the study was first to introduce both functional safety and cyber security domains by describing and comparing their risk parameters, main attributes and taxonomies and secondly compare and then find out similarities and differences between risk assessment processes of cybersecurity, machinery safety and functional safety.

The objectives of the study were to find phases of the process, where there is connection between cybersecurity and functional safety and when information sharing is needed and most useful, and to create ideas how risk assessment of the OT security domain can be improved by learning from processes and risks in other domains. One objective was also to point out cases, where there may be a conflict between cybersecurity counter measures and functional safety protective measures. This means that in such cases discussions between these two domains would be important. A cyberattack can have effects on functional safety and countermeasures against attack may cause conflicts between safety and security objectives. On the other hand, typical safety function is stopping the machine, and this reduces availability, which is an issue from cybersecurity perspective. It is possible that in a cyberattack a safety function is triggered, and machine stops. This is not an immediate safety issue, but it can be an availability problem. It is difficult to identify safety issues, which can cause a cybersecurity risk (cyberattack).



2 Materials and methods

The research question in this study was:

Is it useful to merge cybersecurity and safety risk assessments. Can merging bring advantage, like finding more risks, or is it just laborious. If merging is not practical for complete process, are there phases, where cooperation is useful?

Risk assessment process is here related to cybersecurity, machinery safety and functional safety. Can risk assessment be common for cybersecurity and safety or do they need to be separate processes? If they are separate, are there specific contact points in the analysis when information exchange is necessary? Hypothesis in this study was that safety and security objectives and properties have so many differences that complete merging of risk assessment processes is not usually practical. However, cooperation between analyses is essential.

Material for the study was gathered from literature, standards, discussions with companies, company presentations at seminars and workshops.

The research method in this study included an analysis of standards for risk assessment processes, literature review for cybersecurity risk assessment methods, a compilation of findings from recent research projects, discussions with companies about whether the processes and methods are feasible and applicable in their domain. The results were then merged and are documented in this report.

Some discussion topics with companies were selected to describe the current situation and for example the current relevance of methods or requirements to the companies. One part in the discussions with companies was an iterative process, in which the results of each discussion were added to the next discussion template and finally each company was able to comment the merged results. The idea of the iterative process was first to give generic examples and then find more practical cases and practical experiences to help to understand better the differences between cybersecurity and safety risk assessment objectives.

3 Cybersecurity requirements in EU legislation and international standards

The importance of cybersecurity is increasing and according to “IEC TS 63074:2023. Safety of machinery – Security aspects related to functional safety of safety-related control systems” there are some specific reasons. Industrial automation systems can be exposed to security threats exploiting vulnerabilities due to the fact that [33]:

- ‘access to the control system is possible, for example re-programming of machine function (including safety);
- "convergence" between standard IT and industrial systems is increasing;
- operating systems have become present in embedded systems, for example IP-based protocols are replacing proprietary network protocols and data is exchanged directly from the SCADA network into the office world;
- software is developed by reusing existing third-party software components;
- remote access from suppliers has become the standard way of operations / maintenance, with an increased cyber security risk regarding for example unauthorized access, availability, and integrity.’

Cybersecurity is mentioned more often in legislation and new standards are introduced continuously. For machinery cybersecurity there are currently IEC TS 63074:2023 [33] and CEN ISO/TR 22100-4:2020 [8]. These give some specific guidelines for understanding the cybersecurity issues in machinery and functional safety. However, there are no harmonized standards related to cybersecurity of machinery. Situation is changing, since preparation of new B type standard has started 2023 and the intention is to address the requirements of (Machine regulation (EU) 2023/1230 – Annex III, 1.1.9. and Annex III, 1.2.1. a) and f)). The current name of the standard proposal is “prEN 50742 Safety of machinery - Protection against corruption” [Genorma]. IEC 62443 standard family gives automation related (OT-Security) requirements and process for cybersecurity and risk assessment. ISO/IEC 27005:2022 gives guidelines and requirements related to IT-Security [43].

New **Machinery Regulation** (EU) [2023/1230](#) of June 2023 [13] determines some requirements related to cybersecurity, which were not in old Machinery Directive (2006/42/EC) [36]. Hardware and software shall be adequately protected against accidental or intentional corruption. This means that if the cybersecurity requirements are violated and the occasion is related to safety or healthy the manufacturer can be liable according to the Machinery Regulation. The transition period for the Machinery Regulation is up to 20.1.2027.

There are also other EU legal acts, which are related to cybersecurity:

- **Network and Information Systems Directive II (NIS2 directive)**, (EU) [2022/2555](#) [14]. This directive is a revision of the current NIS1 directive from 2016. NIS2 extends the scope and obligations of NIS1. NIS2 categorizes organizations into two groups: essential and important entities. The cybersecurity related obligations depend on which group and organizations falls into. The criteria for the grouping are based on the size of the organization (economic size and staff size), the criticality of the sector it operates on, and on the assessment of each member state. Because NIS2 is a directive, each member state has some room to determine which entities it deems critical. In Finland NIS2 is interpreted in its minimal form (for example Finnish universities are not seen as organizations that fall under NIS2). Additional criteria that can deem an organization as an essential entity can come from Critical Entities Resilience Directive ([EU](#) [2022/2557](#) [15]) (which is an accompanying legal act to NIS2). In the end, an organization which falls under NIS2 should have an Information Security Management System or a Cybersecurity Management System. And it should ready its policies and procedures to co-operate with EU and national cybersecurity authorities. It is very likely that an organization that deals with machinery which use digital components and are connected to external networks are also in the scope of NIS2 – either directly or indirectly via supply chain.

- **Cybersecurity Act**, (EU) [2019/881](#) [19] defines ENISA the European Union Agency for Cybersecurity, its structure and roles. Additionally, the Cybersecurity Act describes frameworks for cybersecurity certification schemes. These certifications may be used by other EU legal acts to satisfy cybersecurity requirements. In other words, they can be seen as means to get a product on the internal market of EU. In this manner, they have the same role as harmonized standards or common specifications defined by the European Commission. NIS2, Artificial Intelligence Act, Cyber Resilience Act and Machinery Regulation all mention these cybersecurity certification schemes as possible means to satisfy some of the cybersecurity requirements of those acts.
- **Cyber Resilience Act proposal** [11]. CRA covers products with connected digital elements. In practice, this means software and hardware products. The CRA includes, among others, requirements related to vulnerability of products and their risk assessment. Products are categorized into different classes based on risk. High risk products require third-party conformity assessment. Low risk products may be self-assessed. CRA intends to be a horizontal legislation. For example, the CRA refers (in article 12) to the Artificial Intelligence Act as a way to satisfy its cybersecurity requirements. There is a draft for a standardization request by the European Commission in the works for the CRA.
- **Radio Equipment Directive** ([2014/53/EU](#)), and its cybersecurity related delegated act ([EU](#) [2022/30](#) [9]). The original Radio Equipment Directive did not account for cybersecurity which is why a separate delegated act was published in 2022. It aims to lay out cybersecurity requirements for radio equipment. A standardization request by the European Commission for harmonized standards exists for the delegated act.
- **Artificial Intelligence Act** [2024/1689](#) [18]. A completely new legal act that aims to regulate products that use artificial intelligence. It categorizes products into risk classes. Products in the highest risk category related to, e.g. social scoring and biometric categorisation, are outright banned from the internal market of EU. Cybersecurity requirements are laid out for many high-risk AI systems and in some cases also general-purpose and other AI systems. The cybersecurity requirements may be satisfied by the Cybersecurity Resilience Act (see article 12 of CRA) or by specific cybersecurity schemes described in the Cybersecurity Act. Also, a standardization request by the European Commission for **non**-harmonized standards has been published.
- **Data Act** ([EU](#) [2023/2854](#) [20]). The Data Act aims to regulate what happens to the data that is generated by the use of a product. This covers both personal and non-personal data. For example, by using a machine the operator generates information on how the machine functions. The Data Act lays out provisions on what to do with that data and who owns it.
- **New Product Liability Directive proposal** [18]. This is a general legal act that deals with liability of defective products. Whereas the other previously mentioned product legislation focuses mainly on requirements on getting the product on the market with some emphasis on market surveillance, the Product Liability Directive concerns what happens after a defect has occurred. The proposal also explicitly mentions cybersecurity in the recitals and in article 6. There are also other legal acts which concern liability of specific product categories. For example, there is [a proposal](#) for Liability Directive specifically for Artificial Intelligence [17].

NIST Special Publication NIST SP 800-82r3: “Guide to Operational Technology (OT) Security.” gives guidelines to OT security and how to secure operational security with an American style. The new revision is published 2023 and it gives wide perspective to OT security. Some terminology has been adopted, in addition, from this NIST publication to widen understanding of the slightly different ISO/IEC terminology. [14]

4 Comparison of cybersecurity and functional safety risk assessment processes

The purpose of risk assessment in this context is to improve workplace or system safety and security. The focus is here on cybersecurity and functional safety. This means identifying hazards (safety), threats and vulnerabilities (security) and furthermore estimating and evaluating risks. After the assessment risks are minimized by using risk reduction (safety) or risk treatment (security) methods.

Risk assessment can be related to design, operation, modification, or decommissioning phase of a system. Risk assessment can be started, when there is at least a concept of a system, and it can be updated in later phases. Risk assessment method often changes in the next design phase, when there is more information about the analysed object. One purpose of risk assessment can be to verify that the risks of a system or workplace are at acceptable level.

Here both cybersecurity and functional safety are considered according to risk-based approaches, which are used to identify, prioritize, mitigate, and manage functional safety and cybersecurity risks of machinery systems. There is no single method for assessing or securing risks, but often many methods need to be applied and they need to be chosen according to the application. One aspect is that every organization has a different tolerance for risks.

Section 4 describes aspects related to cybersecurity and functional safety:

- Section 4.1: Cybersecurity and functional safety can be divided into parameters, which can help to make more detailed risk analysis.
- Section 4.2: Systems, functions and protective measures can be categorized in order to prioritize and select parts or measures associated to specified risks.
- Section 4.3: Each risk assessment method has a specified process, and the overall principles of the main processes are described.
- Section 4.4: When risk analysis and risk evaluation is done, the risk needs to be reduced and examples of the risk reduction methods are introduced.
- Section 4.4.4: Defence in depth is an important approach to manage risks, especially, in cybersecurity domain. Some related viewpoints are described.
- Section 4.5: The differences between cybersecurity and functional safety are described. By knowing the differences, it is easier to estimate the pros and cons of combining (cybersecurity and functional safety) risk assessments.

4.1 Parameters of functional safety and cyber security risks

The risk is defined in functional safety domain as combination of the probability of occurrence of harm (physical injury or damage to health) and the severity of that harm [35]. A wider definition could be applied, when safety is not the main concern and in addition damages to properties and environment are considered and, in some cases, (e.g., from business view) positive uncertainty and risk can be considered. According to “ISO 31000:2018 Risk management – Guidelines”: Risk is effect of uncertainty on objectives [44]. This definition is not applied in this report, since here the risk is always negative. There are also many other definitions for risk depending on the domain.

According to “IEC 62443-3-2:2020. Security for industrial automation and control systems – Part 3-2: Security risk assessment for system design” [27] risk is expectation of loss expressed as the likelihood that a particular threat will exploit a particular vulnerability with a particular consequence.

Figure 1 compares risk definitions related to safety and cybersecurity. In both cases there is probability or likelihood and severity or negative impact, which together form the risk concept [8]. Figure 1 shows also how probability and likelihood can be divided into attributes. In functional safety, severity is associated to harm (damages against a person) and in cybersecurity, the negative impact has much wider scope, including among others, losses of confidential information and property.

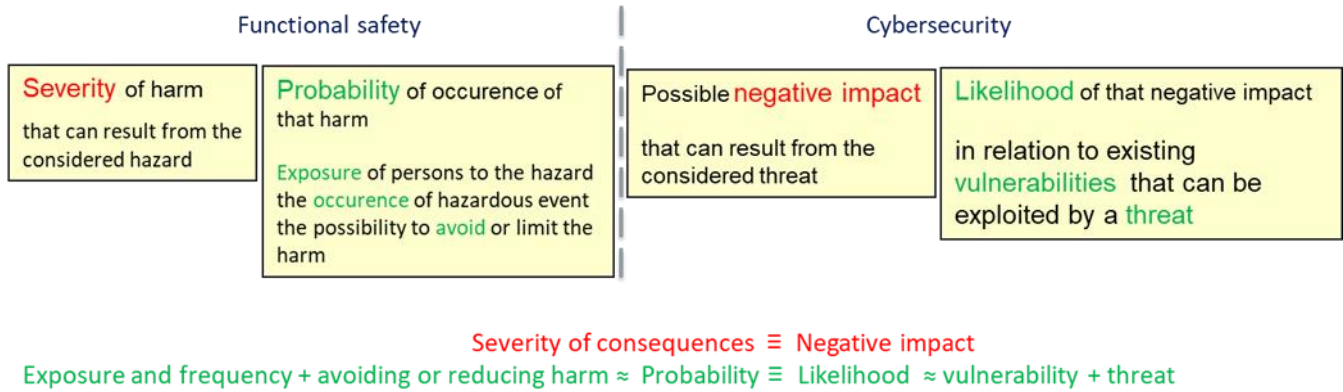


Figure 1. Risk parameters in safety and security. [8]

Figure 2 shows the main parameters that are related to the safety and security risk management process from risk identification to manifesting residual risk. The colours in the figure show a specific viewpoint how parameters in different domains resemble (to some extent) each other. More detailed processes are described at Figure 10. The process in Figure 2 begins from the left by identifying safety hazards and security threats and vulnerabilities. The meaning of hazard and threat plus vulnerability are not the same, but they resemble each other, since vulnerability and threat together cause possibility of cybersecurity incident, which resemble hazard (possible harm) in safety domain. Severity is related to harm, which is related to persons in machinery domain, whereas negative impact has a wider meaning, including in addition damages to assets, confidentiality, and reputation [8]. Probability and likelihood represent here quantitative analysis. System limits (e.g. speed, who is authorized to use system, safe distances), properties, assets and controls are parameters describing the system and they can include parameters, which reduce residual risk. Protective measures and countermeasures both reduce residual risk. The result of this process is residual risk, which can have qualitative or quantitative value.

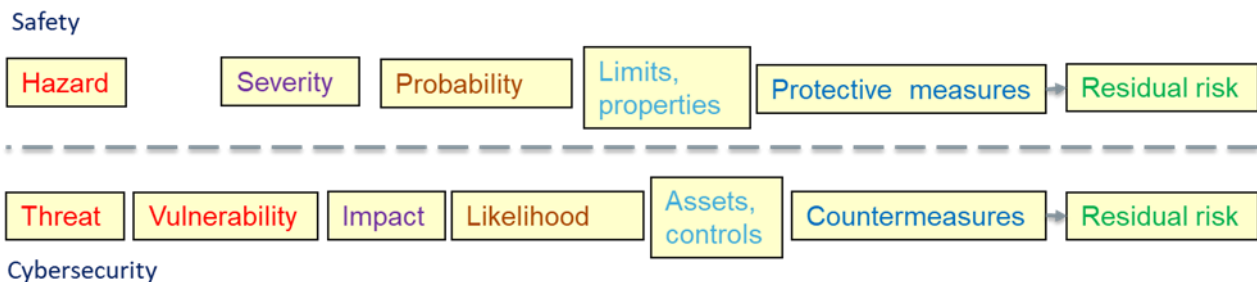


Figure 2. Parameters at the safety and security processes, which are targeting to minimized residual risks.

4.1.1 Items related to cybersecurity and functional safety

The items related to cybersecurity and functional safety refer here to many kinds of failures, initial events, and attributes. The items are considered in safety or cybersecurity analysis of a control system.

Figure 3 shows mind map covering cybersecurity and functional safety risks and such related items like, failures, attributes, assets, vulnerabilities, threats, and misuse. All items are somehow connected to both cybersecurity risks and functional safety risks. Some attributes are closer to functional safety (e.g. random failure) and some to cybersecurity (e.g. vulnerability).

Failures are related to functional safety and cybersecurity. Random hardware failures are usually more related to functional safety and probability of dangerous failures per hour can be calculated (PFH). Systematic failures are considered both in functional safety and cybersecurity. In safety domain, systematic failures are related mainly to design failures, which cause hazardous errors in functions and cybersecurity is related more to failures, which allow malicious access into the system. Furthermore, the failures affect system attributes like integrity, and availability. The attributes affect assets and safety functions.

The objective of the analysis is different. In functional safety, mitigating design failures (hardware and software) is related to lifecycle model according to IEC 61508 or other functional safety standard, and there are specific alternative and obligatory methods to be applied in the design process. The methods depend on the case, PL and SIL. Also in cybersecurity domain, the methods depend on the case. Systematic failures may be mutual, but it is difficult to combine universally the cybersecurity and safety risk assessment processes or the design processes.

One interesting aspect mentioned in Machinery Directive is “reasonably foreseeable misuse”, which is related to “Misuse prevention” in Figure 3. “Reasonably foreseeable misuse” means the use of a machinery or related product in a way not intended in the instructions for use, but which may result from readily predictable human behaviour. This does not include intentional violation of a machine. Every kind of intentional violation (sabotage/spying) of a machine is de facto a criminal act which is outside the scope of current safety legislation and standards [8]. According to new EU Machinery regulation: HW & SW is adequately protected against accidental or intentional corruption [13]. This means that currently intentional misuse is not considered in safety regulations, but criminal regulations. In the future (after 20.1.2027) intentional corruption may not be totally neglected by safety regulations.

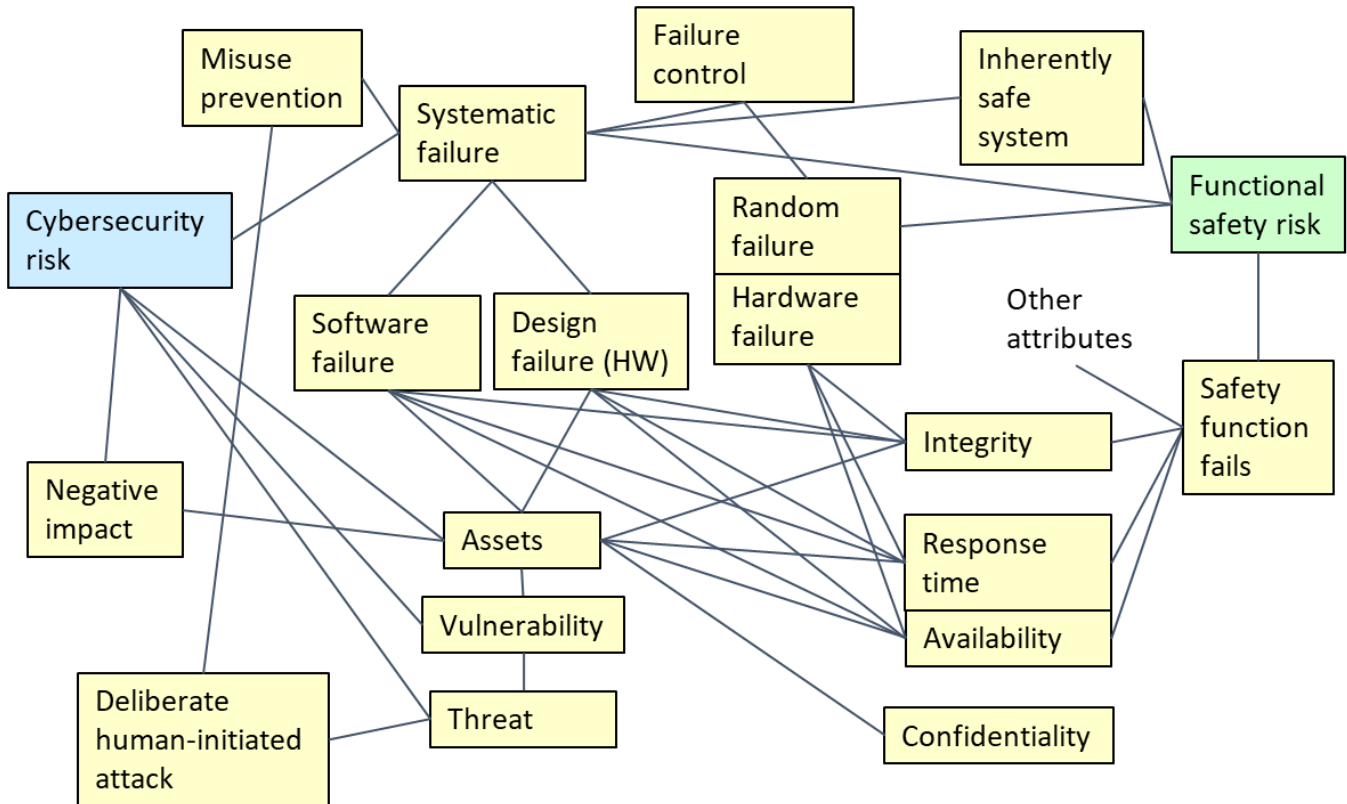


Figure 3. Mind map of cybersecurity and functional safety.

4.1.2 Taxonomies of dependability and cybersecurity

Taxonomy refers here to classification of systems related to dependability and cybersecurity. Classification is important in order to understand the relations between dependability, safety, and cybersecurity with respect to risks, defences, and attributes.

Figure 4 shows taxonomy related to software, risk concept, defences and attributes of dependability and cybersecurity [3]. On the left side is a risk, which is realised as a failure. This includes both dependability and cybersecurity associated failures, although the risk is formulated differently. Some cybersecurity risks are not manifested as failures, for example information leakage and service denial. Failure effects can be minimized by using defences, which appear in the attributes. If the defence is inadequate, then the risk manifests as reducing the value of an attribute. Changes in the attributes manifest in change of dependability and/or cybersecurity.

Reliability (readiness for correct service), safety (absence of catastrophic consequences on the user(s) and the environment), maintainability (ability to undergo modifications, and repairs), integrity (absence of improper system alterations), and availability (readiness for correct service) are attributes of dependability [3]. The attributes are often related to each other, for example integrity and availability are related to safety and reliability can be a parameter in other dependability attributes.

Integrity, availability, confidentiality (the absence of unauthorized disclosure of information) are associated to cybersecurity. Confidentiality is usually not related to dependability. Reputation can be related straight to cybersecurity, or it may be considered as part of confidentiality. Reputation can be lost also after impaired safety, i.e., due to an accident, but it is minor factor compared to the accident itself. RAMSS (reliability, availability, maintainability, safety, security) includes about the same attributes as

dependability and cybersecurity, although the integrity is missing. Here integrity can be considered to be included in both safety and cybersecurity.

The safety defence approaches in Figure 4 are focusing on SW/HW single failures, and security defences have a little bit wider perspective. In the Figure 4 the defences related to safety are:

- Fault prevention, which intends to prevent the occurrence or introduction of faults.
- Fault tolerance, which intends to avoid service failures in the presence of faults.
- Fault removal, which intends to reduce the number and severity of faults.
- Fault forecasting, which intends to estimate the present number, the future incidence, and the likely consequences of faults. [3]

The defences related to security in Figure 4 are:

- Risk modification, which intends to manage risks by introducing, removing, or altering controls so that the residual risk can be reassessed as being acceptable.
- Risk retention, which intends to retain the risk by providing it clearly satisfy the organization’s policy and criteria for risk acceptance.
- Risk avoidance, which intends to avoid risks by not allowing actions that would cause the risks to occur.
- Risk sharing, which intends to share the risk with another party that can most effectively manage the particular risk depending on risk evaluation. [43]

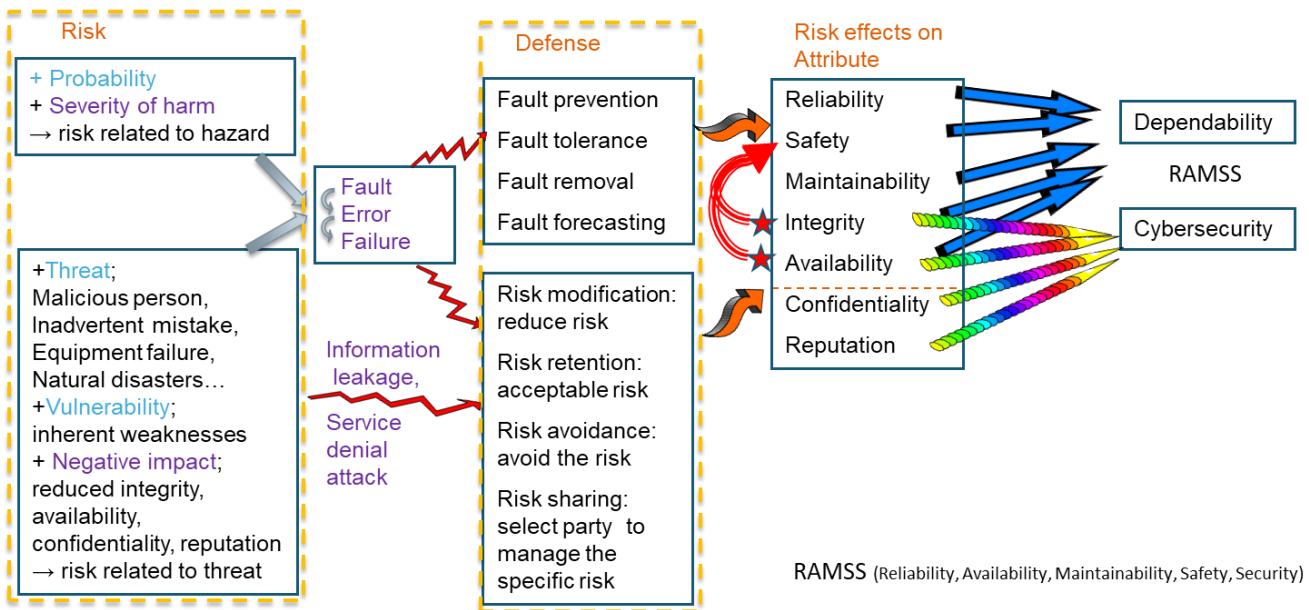


Figure 4. Dependability and security taxonomy in programmable control systems.

Note that risk responses can be stated also according to IEC 62443-1-1 as follows: design risk out, reduce the risk, accept the risk, transfer, or share the risk and eliminate, or redesign redundant or ineffective controls. [26]

There are some similarities between defence approaches of both domains. These common defence approaches can be said as follows:

- probability of the risk/fault needs to be reduced (fault prevention, fault tolerance, fault removal; risk modification, risk avoidance)
- severity needs to be minimized (fault removal; risk modification) and
- trust to the system increased (fault forecasting; risk retention, risk sharing).

4.1.3 Cyberattack effects on safety

Figure 6 shows cyberattack effects on functional safety and emphasizes the importance of integrity. In functional safety domain integrity is the most important attribute and impaired integrity can cause a hazardous situation. Impaired integrity includes situations, where safety function is not operating at all or is operating only partly. Also weakened availability can cause a hazardous situation. However, typically delayed communication triggers a safety function and removes hazardous situation, usually by stopping the machine. This can be an availability issue, but usually not a safety issue. Availability is a safety issue, when safety function is not triggered, or the system requires continuous control to maintain safety. Such systems can be related for example to stability control, ventilation, or firefighting. In these cases, stopping the machine also causes loss of safety function.

Figure 6 bottom shows how confidentiality is not straight a safety issue, but if threat vectors, passwords or safety configuration is leaked out, the threat and vulnerability situation change and impaired integrity or weakened availability situation can be more probable.

One possibility is that the cyberattack itself does not affect availability, but as a countermeasure availability is limited to stop the cyberattack. For example, a remote emergency stop function is denied (not allowed). Risk assessment should reveal such a failure in design, but the safety function can be more complex. However, usually machines have limited capability to detect cyberattacks and additional countermeasures are fairly simple, for example, several password trials may cause limitation to access. The safety implications of such measure need to be considered.

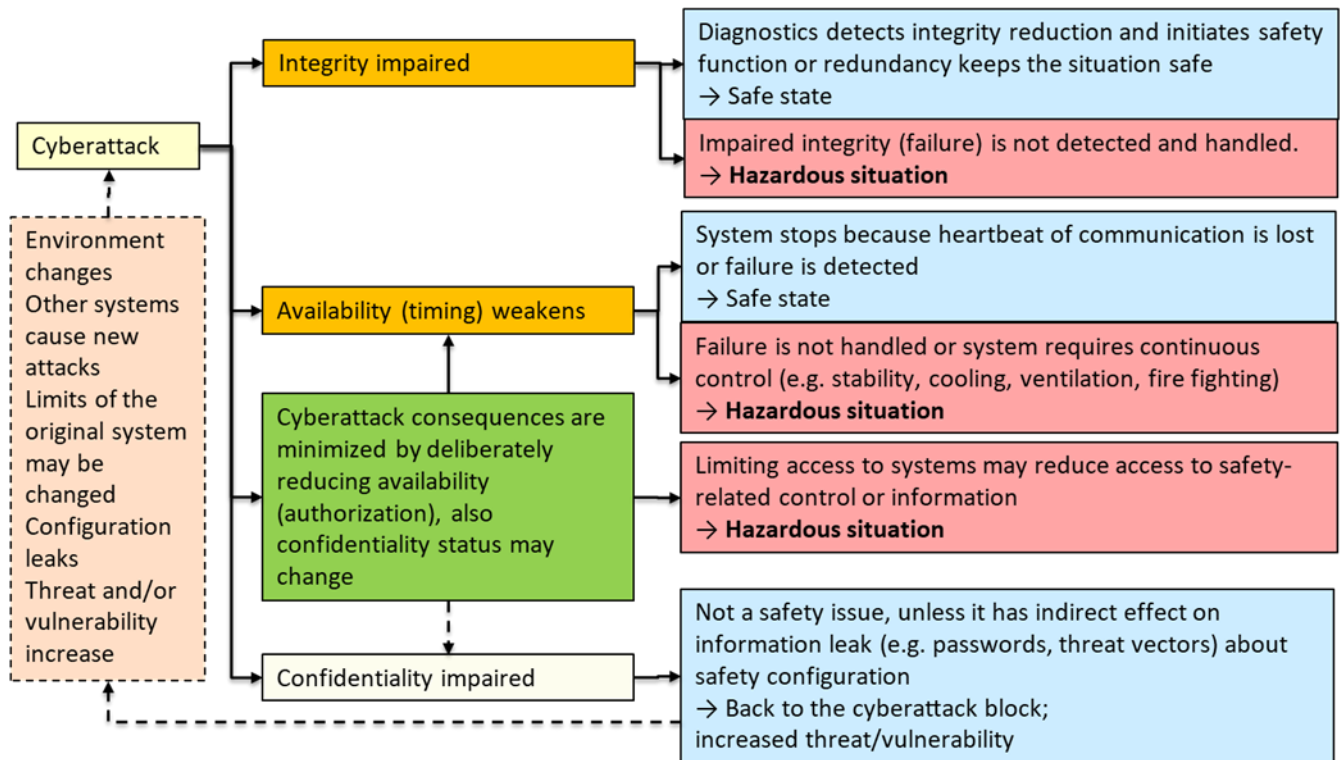


Figure 6. Effects on safety attributes during cyberattack.

Figure 6. shows how cyberattack can affect integrity and availability. Another viewpoint is to see how cyberattack affects risk reduction measures implemented by designer. According to ISO 12100 [34] risk reduction measures are in order: inherently safe design measures, safeguarding, and information for use. According to ISO/TR 22100-4 [8] the target for cyberattack is safeguarding and perhaps in some (rare) cases inherently safe design. Safeguarding cases include here safety function failures.



4.1.4 Comparison of cybersecurity properties in IT and OT systems

Information technology (IT) systems are focusing on achieving three objectives: confidentiality, integrity, and availability. Their primary focus is on confidentiality and the necessary access controls needed to achieve it. Integrity might fall to the second priority, with availability as the lowest. [26]

Industrial operational technology (OT) systems' primarily concern is on maintaining the availability of all system components. Integrity is often second in importance. Usually confidentiality is of lesser importance, because often the data is raw in form and need to be analysed within the context to get any value [26]. From safety viewpoint integrity is often the most important objective.

Table 1. shows typical differences between IT and OT systems according to NIST Guide to Operational Technology (OT) Security [40]. The table shows that IT systems have more standardized products and practices, but in many cases OT systems have more strict requirements for properties and practices. IT systems are usually not related to safety, since basically IT systems manage data. The safety implications related to IT systems are often indirect. OT systems manage the world beside machines and there are safety implications and safety requirements, but not always.

It can be noted that in OT systems protection of the process can be an important factor from, among others, economical, and security viewpoint, but in machinery domain impaired process does not necessarily have safety implications. On the other hand, safety messages in OT systems are time-critical and to ensure safety the messages are often redundant and fault tolerant.

Table 1 considers ideal systems where IT systems are close to office and OT systems close to machine devices. In the real world, systems are not purely either OT or IT systems, but they can have features from both systems.

Table 1. Typical differences between IT and OT systems [40].

Category	Information Technology	Operational Technology
Performance Requirements	Non-real time Response must be consistent. High throughput is demanded. High delay and jitter may be acceptable. Emergency interaction is less critical. Tightly restricted access control can be implemented to the degree necessary for security.	Real-time Response is time-critical. Modest throughput is acceptable. High delay and/or jitter is unacceptable. Response to human and other emergency interaction is critical. Access to OT should be strictly controlled but should not interfere with human-machine interaction.
Availability (Reliability) Requirements	Responses such as rebooting are acceptable. Availability deficiencies can often be tolerated, depending on the system's operational requirements.	Responses such as rebooting may not be acceptable because of process availability requirements. Availability requirements may necessitate redundant systems. Outages must be planned and scheduled in advance. High availability requires exhaustive pre-deployment testing.
Risk Management Requirements	Manage data. Data confidentiality and integrity is paramount. Fault tolerance is less important.	Control physical world Human safety is paramount, followed by protection of the process. Fault tolerance is essential.



Category	Information Technology	Operational Technology
	The major risk impact is a delay of business operations.	The major risk impacts are regulatory non-compliance, environmental impacts, and the loss of life, equipment, or production.
System Operation	Systems are designed for use with typical operation systems (OS), such as Windows and Linux. Upgrades are straightforward with the availability of automated deployment tools.	Systems often use different and possibly tailored systems, sometimes without security capabilities built in. Software changes must be carefully made, usually by software vendors, because of the potentially modified hardware and software involved.
Resource Constraints	Systems are specified with enough resources (e.g. memory, computing capacity) to support the addition of third-party applications, such as security solutions.	Systems are designed to support the intended industrial process and may not have enough memory and computing resources to support the addition of security capabilities.
Communications	Standard IT communications protocols are used (e.g. Ethernet). Primarily wired networks with some localized wireless capabilities (e.g. WLAN). Typical IT networking practices are employed.	Many kinds of standard communication protocols are used (e.g. Profinet and EtherCAT). Several types of communications media are used, including dedicated wired and wireless (e.g., radio and satellite). Complex networks exist that sometimes require the expertise of control engineers.
Change Management	Software changes are applied in a timely fashion in the presence of good security policies and procedures, and the procedures are often automated.	Software changes must be thoroughly tested and deployed incrementally throughout a system to ensure that the integrity of the OT system is maintained. OT outages must often be planned and scheduled in advance. OT may use OSs that are no longer supported. OT systems often have custom applications.
Managed Support	Allow for diversified support styles	Service support is usually provided through a single vendor.
Component Lifetime	Lifetime on the order of three to five years	Lifetime on the order of 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.

NIST’s view lists correctly the different features of Office and OT. However, the view is over simplified since it compares only the closest to the physical process layers of OT systems and office systems. This comparison is like comparing apples and oranges. Automation security standard IEC 62443 has introduced security zone concept which is based on ANSI/ISA95 domain levels which again are based on old Purdue Enterprise Reference Architecture or just the Purdue model concept. The Figure 7 depicts Security Zones according to IEC 62443. From this illustration we can see couple of important security and safety related aspects.



First and probably from security perspective the most important is that the main design feature of control borders between zones are different where IT is the dominating functionality. This is depicted as Security Border which means providing traditional CIA (Confidentiality, Integrity, Availability) of IT systems is the main requirement for the border.

From this we can make conclusion that all the way to I(A)CS DMZ zone (Industrial Automation Control System Demilitarized zone) typical IT security measures are applicable directly. This means malware control, centralized Office identities as well as regular monthly updates. Of course, all updates like in office environments needs to be tested before applying but mostly they work without problems. The OT software behave in this zone like any other specialized software in IT environments.

Second and the most important from safety perspective is that dominating design feature changes when we cross the Dependability Border. Here the reliability, availability, real-time and other requirements listed in NIST's table come into effect. The upper Dependability Border should be designed more like Security Border however there may be compulsory OT requirements which affect the applicable control decisions. For example, if there must be continuous environmental reporting of the production this might require 100% availability between actual production from the lower levels to the database which may reside in the I(A)CS DMZ zone.

The requirements of Dependability Border design are to enable RAMS, not CIA. RAMS means Reliability, Availability, Maintainability, and Safety. As the wording already hints, this is where NIST table OT features come fully into play. Here the typical IT security controls are dangerous if implemented like in normal Office environments.

OT systems must always be controllable and observable. If these requirements are not met, then usually the Safety functions will force the process or system to a safe state. Typical IT security solution, that is proposing or enforcing encrypting control and measurement traffic may cause loss of visibility and therefore break the observability requirements. The correct way is to use cryptographic solutions to provide integrity without encryption to control and measurement traffic to be able to trust the values and in addition use network traffic limitation controls to prevent false control signal sources. Using integrity protection can also be implemented with respecting real-time requirements since it does not require indeterministic retransmissions. Why control and measurement traffic need deterministic communication is topic for another publication but simply said the mathematics of deterministic control is hugely easier than asynchronous control.

OT systems are networked software products which make automatic control decisions based on received data. If data cannot be trusted, then the control decisions cannot be trusted. Integrity protections is also less computing intensive which is welcome in OT environments where the long lifecycles and cost optimization result in scarce resources in OT devices.

Encryption, however, can be and should be enforced to configuration traffic. Configuration traffic is usually not needed to provide operators the needed real-time state of the system. Configuration traffic itself has not real-time requirements, nor communication based on handshakes cannot be deterministic due to various retransmission probabilities. All traffic encryptions may be possible in couple of decades but probably even then there are still too old equipment running and the security landscape has changed to prevent the full encryption possibility.

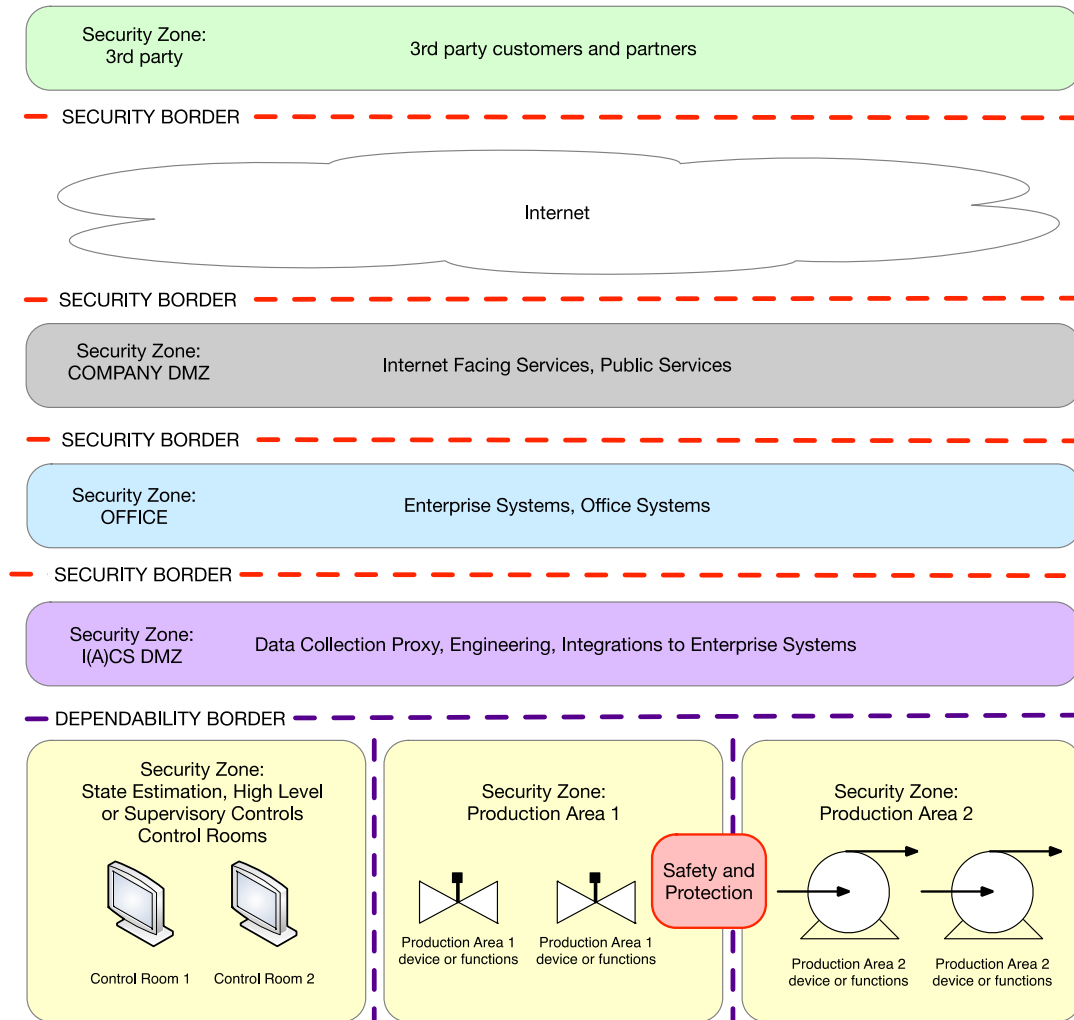


Figure 7. Security zones according to IEC 62443.

4.2 Categorizing cybersecurity and functional safety

In both safety and security domains it is useful to categorize risks and associated requirements and system capabilities. In security domain the unit is **Security Level (SL)**, and it is associated to requirements, countermeasures, and system capability[28]. In functional safety domain the most common units associated to machinery are **Safety Integrity Level (SIL)** [23] and **Performance Level (PL)** [35], which can be associated to requirements and system capabilities. The categorization enables comparison of different categories/levels and requirements can be specified to each category.

4.2.1 Security levels

According to IEC 62443-3-2:2020 [28] SL-T means the desired level of security for a particular industrial automation and control system(s), zone, or conduit. SL-T for a zone and conduit is determined during risk assessment. SL-C (capability) is associated to countermeasures and inherently secure properties, and they can contribute to SL-A (achieved). When the system is complete, the actual SL is measured as the SL-A. The achieved SL-A can be compared to the SL-T requirements. [28] The different levels indicate the resistance against different classes of attackers. The security levels are associated to zones

and conduits, which furthermore are related to individual devices and systems. Security levels provide a qualitative frame of reference for making decisions on the use of countermeasures and devices with differing inherent security capabilities. [26]

Table 2. Security Levels. [28]

Security Level	Explanation
SL 0	Implicitly defined as no security requirements or security protection necessary.
SL 1	Protection against casual or coincidental violation.
SL 2	Protection against intentional violation using simple means with low resources, generic skills, and low motivation.
SL 3	Protection against intentional violation using sophisticated means with moderate resources, industrial automation, and control systems (IACS) specific skills and moderate motivation.
SL 4	Protection against intentional violation using sophisticated means with extended resources, IACS specific skills and high motivation.

Seven foundational requirements (FR) are applied to define control system capability to security levels [33] [26]. Foundational requirements and relations to safety-related control system are described at Table 3 in section 4.4 “Risk treatment”. Furthermore, there are more specific component requirements (CR) and requirements enhancements to more detailed specification in “IEC62443-4-2 Technical security requirements for IACS components”. [31]

4.2.2 Safety Performance Levels

According to ISO 13849-1:2023 functional safety process begins by identifying hazards, estimating risks and defining which risks can be minimized by applying safety functions (Figure 8, point 1) [35]. This phase may require many kinds of risk assessments before the decision to apply functional safety means is decided (Figure 8, point 2). The risks are categorized as PL_r (Performance Level required) or SIL (Safety Integrity Level), which furthermore defines the requirements for the safety function (Figure 8, point 3). PL and SIL have corresponding PFH_D (Probability of Dangerous Failure per Hour) value according to Figure 9. The quantitative value PFH_D is associated to stochastic (random) failures, and requirements for software and design are qualitative according to selected SIL or PL. The right side of the Figure 8 (point 5) shows factors, which need to be designed and validated. These factors are architecture (category), Mean Time to Dangerous Failure (MTTF_d) for components and channels, Diagnostic Coverage (DC), common cause failures, systematic failures, software failures and environmental conditions.

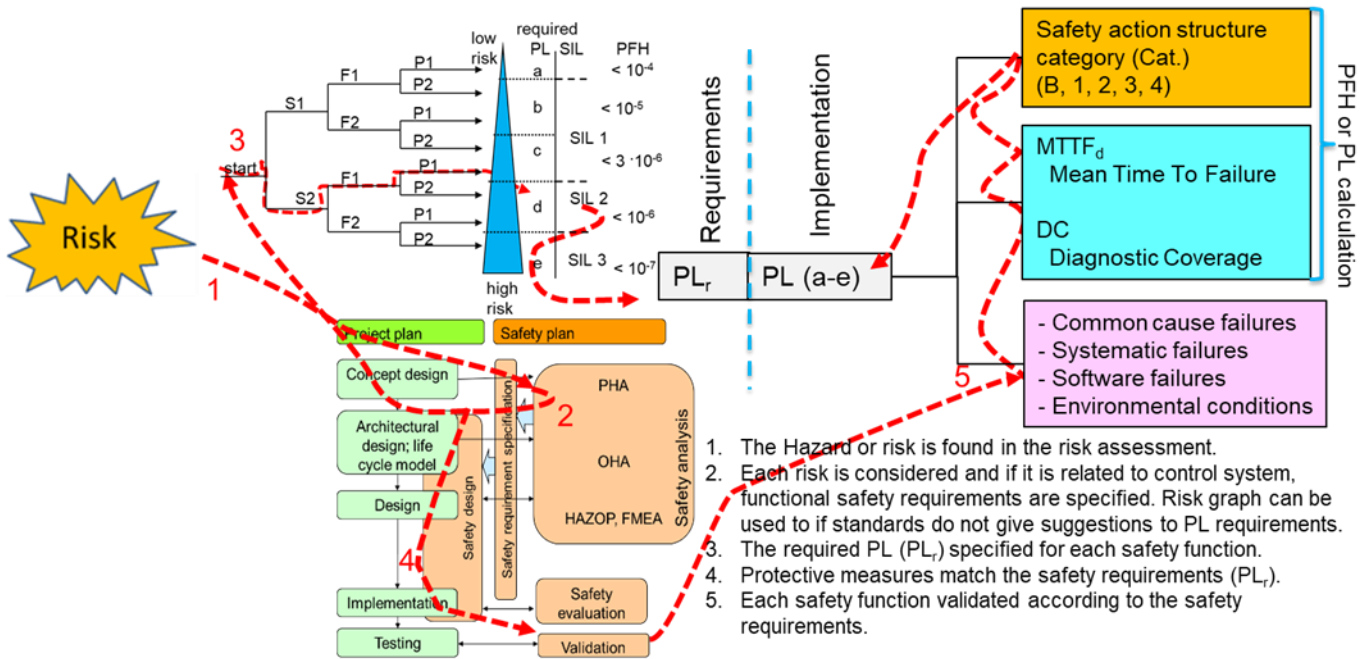


Figure 8. Risk assessment and functional safety phases. [39]

Figure 9 shows how PL is assigned by first checking severity, frequency, and possibility to avoid hazard [35]. The figure also shows the correlation between PL_r, SIL and PFH_D (or PFH). The PFH_D is related to performance of the safety function (in the control system) and the value is associated to quantitative risk reduction. For example, PL d means that the safety function has less than 10⁻⁶ dangerous hardware failures per hour. Figure shows also how functional safety is associated to probabilities, whereas in cybersecurity the SL is described qualitatively. When the PL or SIL is assigned then the safety function is designed according to the selected PL/SIL requirements. In addition to the PFH_D requirements, there are qualitative requirements and requirements related to the design process.

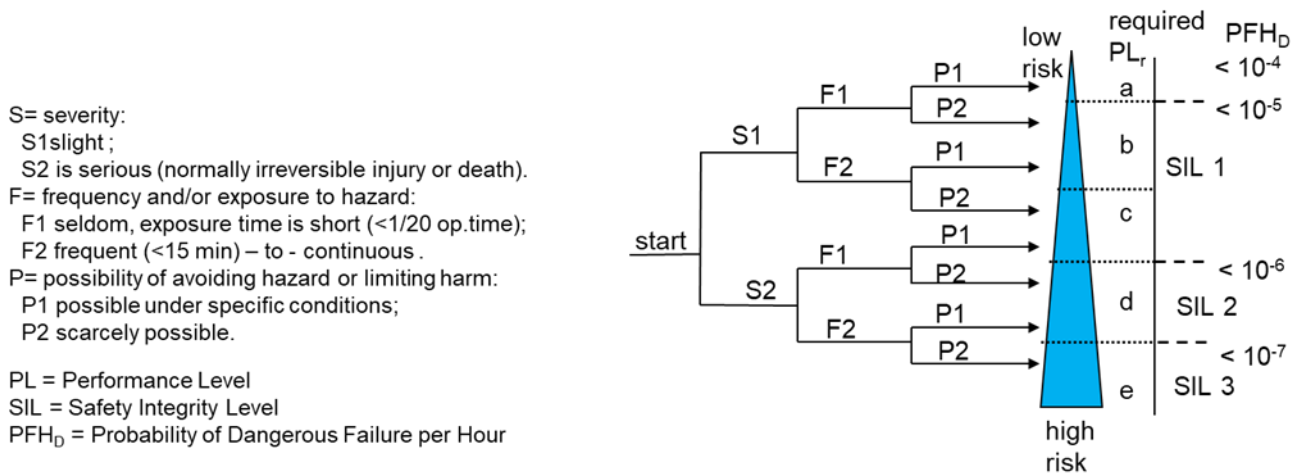


Figure 9. PL assignment process. [35]

One should note that PFH_D is related to random or stochastic failures, and it is not associated to Security Levels (SL), since they are associated more to intentional events and risk is more dependent on attacker resources, knowledge, motivation, and system vulnerability. These factors are not random, but they either exist to a certain extent or not. Likelihood is used to express the uncertainty of a cyberattack. Likelihood is small if system is not vulnerable, possible attackers have no known resources, knowledge, or motivation to attack. [33]

4.3 Comparison of risk assessment processes

Many kinds of risk assessment methods are needed in machinery safety, functional safety, IT security and OT security and there are specific processes associated to different domains. Although there are different processes in different domains there are similarities such as, identification, risk estimation, evaluation, and risk reduction. It is possible to apply risk assessment process related to different domains, but usually, requirements can be best found and met when the process related to the specific domain is followed.

One aspect in this section is that when analysing a system and applying different analysing processes, the discussion points between machinery safety, functional safety and cyber security analyses can be found by comparing the processes. Figure 11, Figure 12 and Figure 13 show risk assessment processes and compare similar phases, where discussions between these domains may be needed.

4.3.1 Machinery safety and information security risk assessment

Comparison between machinery safety and information security risk assessment processes was done by studying machinery safety risk assessment according to ISO 12100 [34] and information security risk assessment according to IEC 27005 [43]. The comparison illustrated in Figure 10 shows the phases, which have similarities. The thicker lines indicate the importance of cooperation in the phases (risk identification and risk treatment). The machinery risk assessment identifies basic risks, and it can be considered often as an input for other risk assessments. Information security risk assessment shows the basic elements related to information security, and some risks may be mutual to safety domain.

The most important phase of risk assessment is risk/hazard/vulnerability/threat identification [40]. Unidentified risk is not under control or it increases uncertainty of the risk. Identified risks should be known as potential input in other analyses to minimize the possibility of not identifying hazards. Since risk identification is so important phase, cooperation between domains is important to maximize risk identification probability.

Risk estimation or defining the level of risk is done separately in safety and security domains, since there is no straight correlation between safety and security risk levels. IEC TS 63074 mentions that there is no correlation between SIL and SL [33].

During risk evaluation phase cooperation is important to see are the system safety and cybersecurity properties acceptable. If the properties are not acceptable, some changes need to be done.

Risk treatment or reduction phase shows safety measures and countermeasures to minimize risks. Cooperation between safety and cybersecurity experts is important to avoid conflicts between measures.

Machinery safety risk assessment

Information security risk assessment

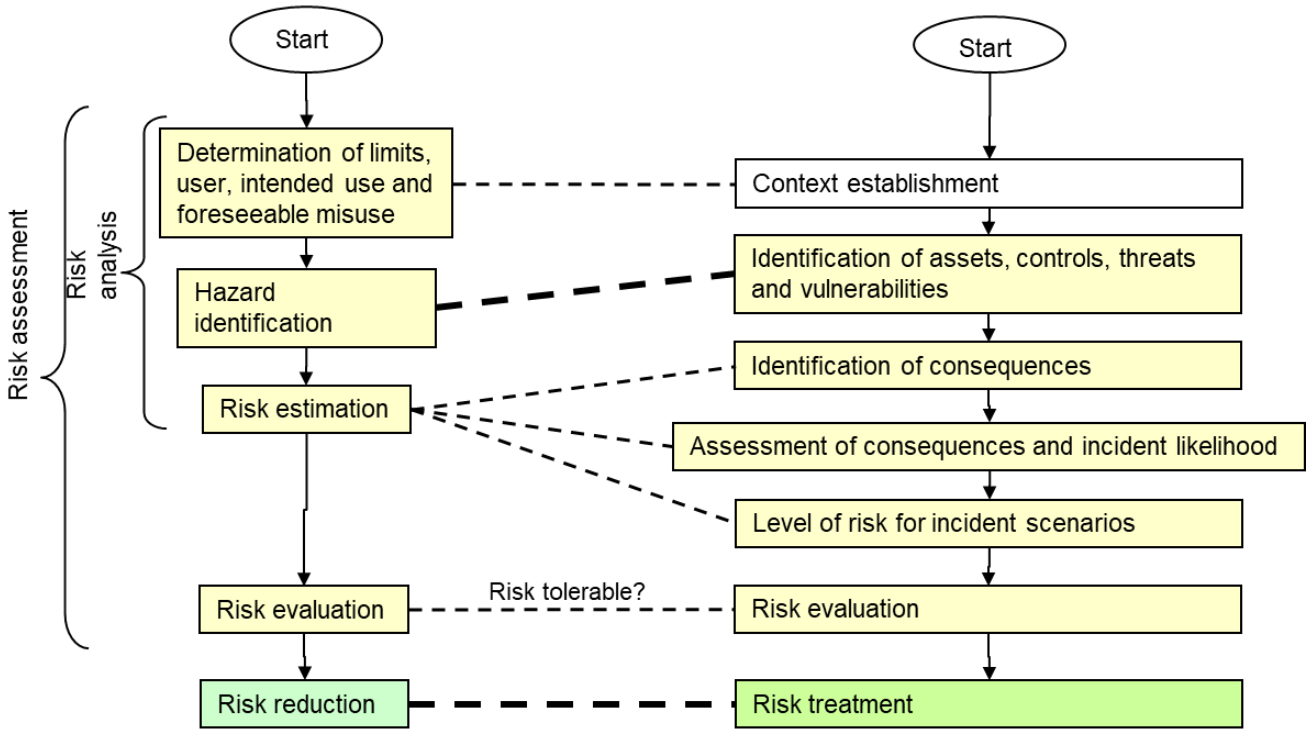


Figure 10. Comparison of machinery safety and information security risk assessment processes. [34], [43]

4.3.2 Information security and industrial automation security risk assessment

Comparison between information security and industrial automation security risk assessment processes was done by studying information security risk assessment according to IEC 27005 [43] and industrial automation security risk assessment according to IEC 62443-3-2 [28]. The comparison illustrated in Figure 11 shows the process phases, which have similarities. The industrial automation security risk assessment process shows many detailed phases and, especially, phases 2 to 4, 6, and 7 have some general requirements for the analysis. For example, safety-related assets, wireless networks, external connections, and temporary devices need to be analysed separately (utilising more detailed analysis). The phase 5 is the actual analysis, but according to the standard phase 5 can be replaced with a specific risk assessment method or process [28].

Figure 11 shows also that information security and automation security risk assessments resemble each other, and they have often similar objectives. Similar factors, like, vulnerability, threats, and assets are studied, but automation risk assessment includes some more detailed phases, like determining security levels and partitioning the system to zones and conduits.

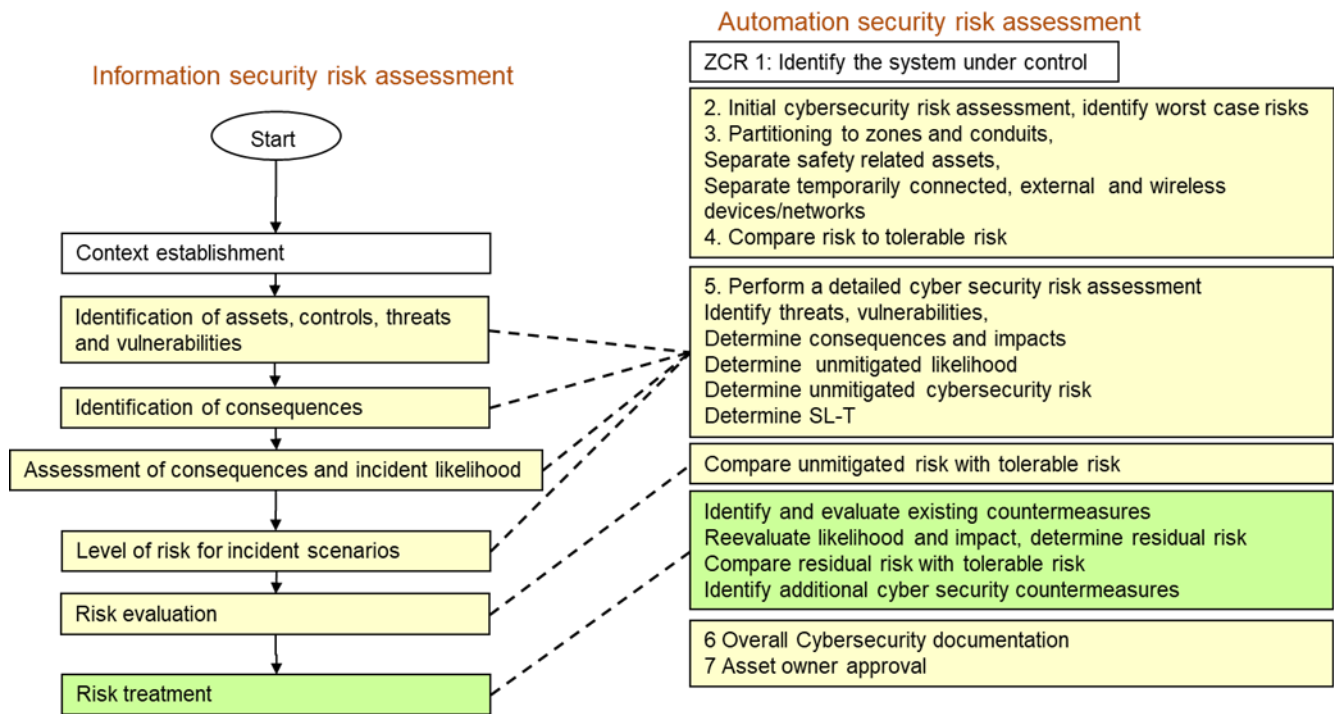


Figure 11. Comparison of information security and Automation security risk assessment processes. [43], [28]

4.3.3 Functional safety and industrial automation security risk assessment

Comparison between functional safety and industrial automation security risk assessment processes was done by studying industrial automation security risk assessment according to IEC 62443-3-2 [28] and functional safety design according to ISO 13849-1 [35]. The comparison illustrated in Figure 12 shows the process phases, which have similarities. Before the actual functional safety design process risk assessment according to ISO 12100 is made and the parts that are related to functional safety are identified and risks are estimated according to performance levels (see Figure 9).

It can be assumed that functional safety design process from ISO 13849-1 [35] points out safety critical parts of the control system and safety functions, which can be potential targets for cyberattacks. IEC 62443-3-2 [28] points out that safety related assets need separate security analysis. This indicates that safety assets are important parts, and they need to be analysed carefully. One aspect is that due to different objectives of safety and security, most of the input to security risk analyses comes from other sources than safety risk assessment.

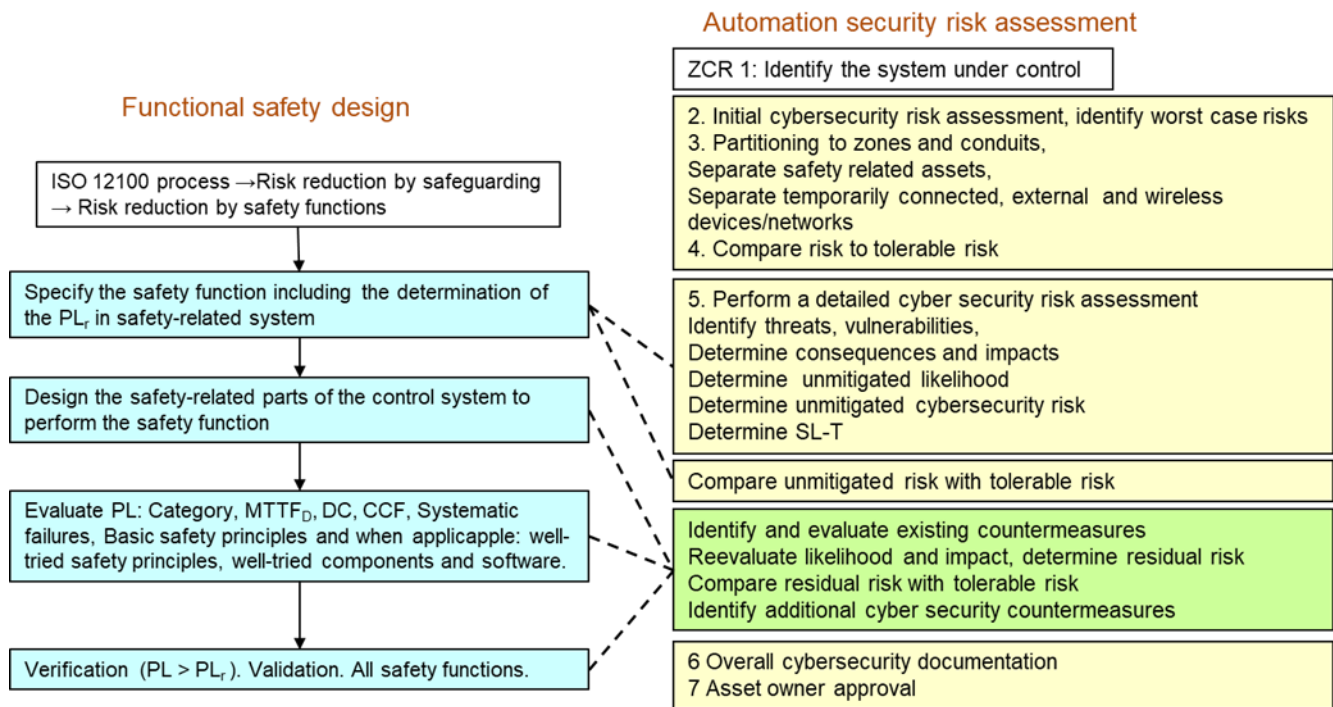


Figure 12. Comparison of functional safety and automation security risk assessment processes. [35], [28]

4.3.4 An example of risk assessment of a single safety function

An example of a single safety function and how security assets like conduits and zones are related to it is shown in Figure 13. One system can have several safety functions and each safety function has always **input unit** (initiating devices like sensors and switches), **output unit** (power control elements) and **safety logic** as described in the Figure 13.

All safety functions need to be analysed and the analyses can include parts, which have results of e.g., FMECA of logic unit, since the same logic unit is involved with several safety functions. PL or SIL including both qualitative and quantitative (PFH=Probability of Dangerous Failure per Hour) requirements is evaluated for each safety function. PL is related to the ability of safety-related parts of control system to perform a safety function under foreseeable conditions. Usually, communication is realised by applying certified commercial (COTS) system and the published safety values are applied without calculating the actual values (e.g. PL and PFH) in detail. This enables merging communication related safety analysis (approach according to Industrial Communication Networks [24]) to safety analysis of other parts of the control system (approach according to Safety-related parts of control systems [35]), since the calculation methods are then similar according to ISO 13849-1 [35], EN 62061 [25] or IEC 61508 standard family.

Cybersecurity-related asset are described in the yellow blocks in Figure 13. Zone means grouping of logical or physical assets that share common security requirements. Conduit means logical grouping of communication channels, connecting two or more zones, which share common security requirements. According to IEC 62443-3-2 section 4.4.4 [28] (see also Figure 12, point 3 on the right side) system needs to be partitioned into zones and conduits and furthermore safety-related (as well as temporary, external, and wireless) assets need to be separated. It is also possible to define a larger entity (asset), which have similar security requirements according to the highest security level of the assets.

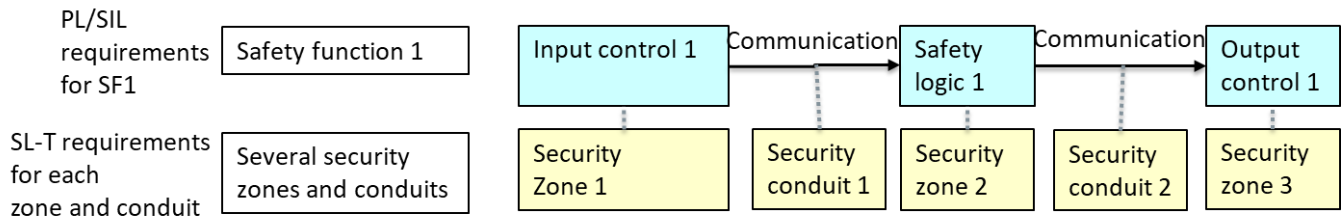


Figure 13. An example of single safety function and related security assets.

If the safety and security requirements for the zones 1, 2, and 3, and conduits 1 and 2 are similar, risk assessment can be done for them as a one asset (safety and security usually separately). If one asset had higher requirements, then more detailed analysis is required for that part. In Figure 13 there is one safety function and the parts have similar PL_r , but if there were other safety functions applying the same communication/conduits with higher PL_r , separation to different assets may be needed, since safety related assets need to be analysed separately according to IEC 62443-3-2 [28]. From safety viewpoint also the highest safety function requirements that are related to specific asset can be applied. For example, safety logic is usually related to several safety functions. The objective can be to optimize or minimize the amount of different safety and security analyses and requirements.

Figure 14 outlines different approaches for safety and security analysis for a single safety function. Solid blue and orange lines show a simple approach including only one analysis related to functional safety and one for cybersecurity. Usually there are several safety functions, which need to be analysed separately. However, some analysis methods, like FMEA (Failure Modes and Effects Analysis) are made to systems or subsystems and usually not to functions.

If the communication connections are realised using designed (not COTS) wireless or LAN (Local Area Network) a separate functional safety analysis is needed e.g., according to IEC 61784-3 fieldbuses [24]. The standard mentions also that security shall be considered in functional safety communication systems. The standard does not give any security requirements, but it refers to IEC 62443 standard family. In this case the analysis approach becomes more complicated because the fieldbus safety analysis differs from hardware functional safety analysis. Usually, a certified fieldbus is applied and no detailed analysis for the fieldbus is required. Also, the software of safety logic requires separate analysis and sometimes also the hardware logic. These analysed areas are marked using dotted blue lines in Figure 13.

Separate cybersecurity analyses may be required to different conduits and sometimes zones, if remote access is possible or the requirements for different conduits and zones differ. Basically, wireless, external and temporary conduits require separate analysis, but if the access and requirements look similar, the conduits may be analysed together.

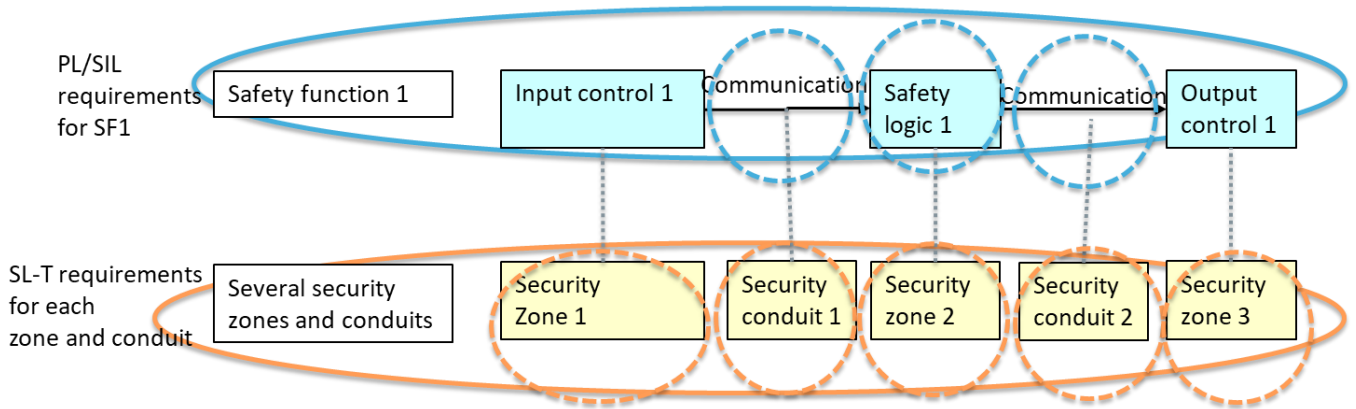


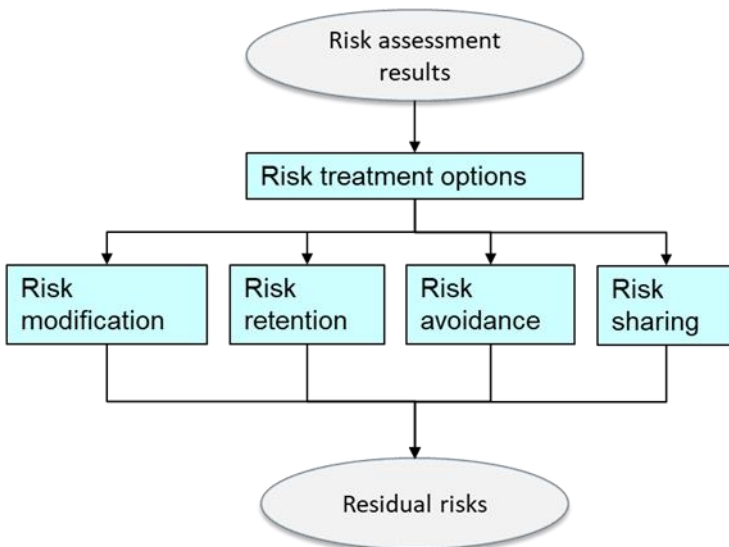
Figure 14. Proposed risk assessments for a single safety function.

This example showed that separate analysis may be needed for different parts of a single safety function. When there are several safety functions the simple approach with a merged analysis is often used, especially, when the required levels (PL, SIL and SL) are similar. However, the number of needed separate analysis depends on the case and no generic number of needed analyses can be declared even to this simple single function system.

4.4 Risk treatment

4.4.1 General risk treatment options

Risk modification and avoidance are typical ways to minimize safety or cyber security risks, but it is possible to share the risk to a party that effectively manage the risk. The fourth way is to check, does the risk meet the acceptance criteria and residual risk is adequately low. Figure 15 shows how security risks can be treated according to IEC 27005 [43] and ISO 22100-4 [8].



Risk modification

The level of risk should be managed by introducing, removing or altering controls so that the residual risk can be reassessed as being acceptable.

Risk retention

If the level of risk meets the risk acceptance criteria, there is no need for implementing additional controls and the risk can be retained.

Risk avoidance

The activity or condition that gives rise to the particular risk should be avoided.

Risk sharing

The risk should be shared with another party that can most effectively manage the particular risk depending on risk evaluation.

Figure 15. Cybersecurity risk treatment options. [43]

4.4.2 Risk treatment methods

Risk treatment or countermeasures against cyber security risks are part of risk assessment processes (see Figure 11). The viewpoint here is to identify needed risk treatment methods. For each risk treatment method there can be a separate process. Risk treatment methods can be categorized according to the lifecycle phases they are applied (Figure 17) [8], [26]. See the steps/phases the following list:

Identify step begins by considering machinery risks. Furthermore, risk reduction can lead to functional safety and safety functions. Cyber risks need to be identified separately, but synchronously with functional safety, since there may be interactions between safety functions and security countermeasures. Cybersecurity has also other objectives than accident prevention and therefore there are also other inputs in addition to safety analysis.

Protect step in machinery is related to mechanical protective measures like, guards, fences, or locks, which can be an option to a safety function. Cybersecurity countermeasures like, firewalls, access control and cryptography, are continuously on.

Detect step is related to situational awareness of functional safety and cybersecurity. The system needs to be aware of cyberattacks and functional safety situation. Machines have very limited capability to detect cyberattacks and therefore it is related more to IT security in higher system levels.

Respond step is related to triggering safety functions and security countermeasures according to situational awareness. Functional safety is related more to preventing harms and only sometimes a safety function only minimizes the damages. In many cases safety function triggers and operates until the risk is over (e.g. an obstacle has moved away).

Recover step is related to minimizing and repairing damages, which can be related to the equipment. After a failure, the control system may turn the operation to safety, limping or automatic mode, if according to risk assessment the operation can be restarted. The first objective of cybersecurity is to prevent damages, but if there are damages the system can restore capabilities and services. There can be a software copy of the damaged part of the system, which can be restored or the stopped services are reconnected.

Examples of risk treatment methods to improve machinery safety, functional safety and cybersecurity are presented in Figure 16.

Figure 17 shows examples of cyber security risk treatment methods categorized according to the applied life cycle phase. The methods are gathered from IEC/TS 62443-1-1 [26] and ISO TR 22100-4 [8]. The items marked with letters (a – h) refer to text in IEC/TS 62443-1-1 section 5.6.6 [26].

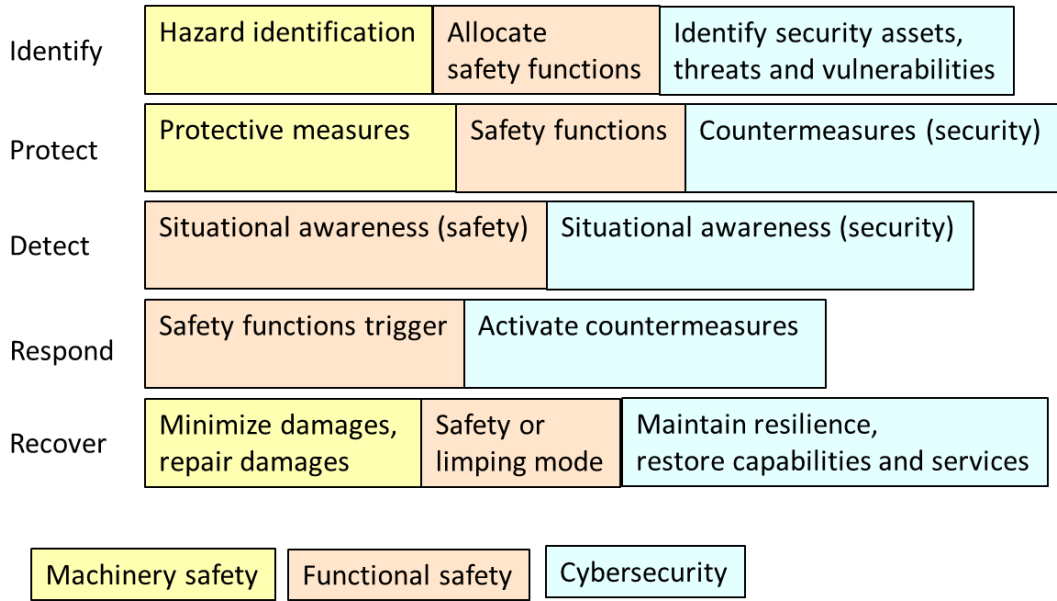


Figure 16. Risk treatment protective methods to improve cybersecurity, machinery safety and functional safety. [8]

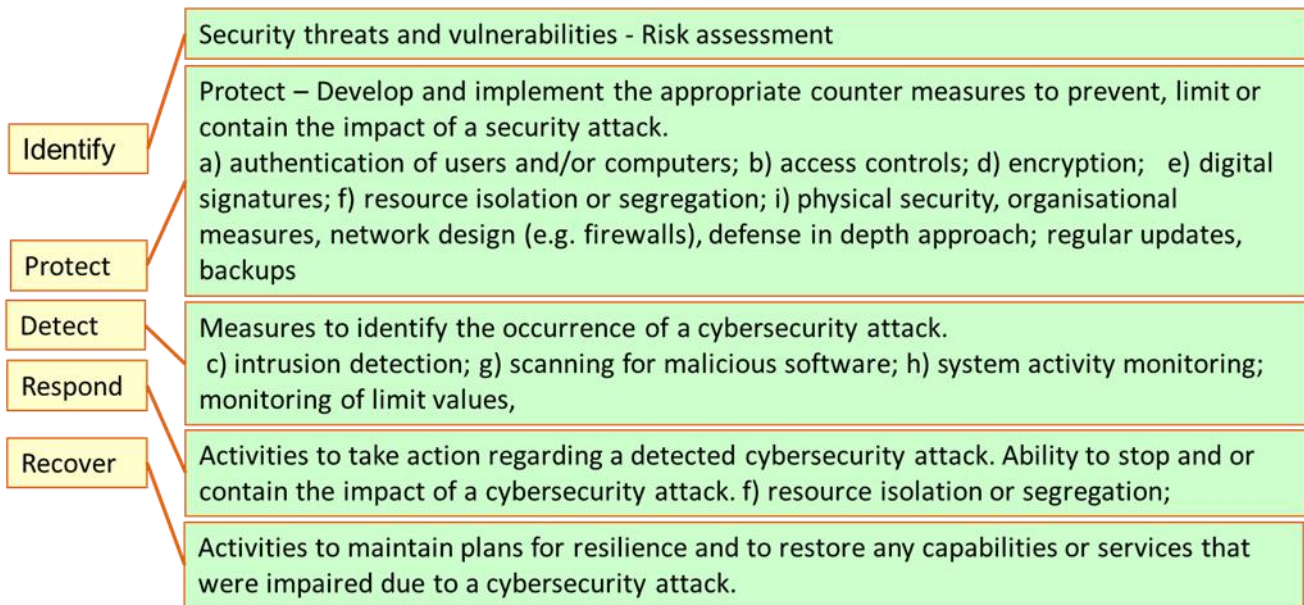


Figure 17. Examples of cyber security risk treatment measures related to the risk treatment methods. [26], [8]

4.4.3 Possible conflicts between risk treatment measures

Security risk treatment measures can possibly have unwanted compromising effects on safety-related control systems. Security foundational requirements (FR) defined in [33] and how they may affect safety-related control system are presented in Table 3. The first column on the left can be considered as basic measures to build cybersecurity defence. Influence on safety integrity means that safety can be compromised. Influence on availability means that in systems, where availability is critical safety can be compromised, but otherwise it means that production may be affected. Indirect influence on safety



integrity means that safety is not compromised immediately, but the system has become more vulnerable and security need to be reconsidered.

As seen in Table 3, security foundational requirements may have effects on safety-related system and these aspects need to be under control. The cyberattack can happen in any layer of protection. In practice, this means that defence in depth (See section 4.4.4) is important approach to get adequate protection in all layers.

Table 3. Overview of security foundational requirements (FR) and possible influences on a safety-related control system. [33]

Security foundational requirements (FR)	Brief description	Possible influence(s) on a safety-related control system
Identification and authentication control	Identify and authenticate all users (humans, software processes and devices) before allowing them to access to the control system.	Influence on safety integrity by modification or manipulation.
Use control	Enforce the assigned privileges of an authenticated user (human, software process or device) to perform the requested action on the control system and monitor the use of these privileges.	Influence on safety integrity by modification or manipulation.
System integrity	Ensure the integrity of the control system to prevent unauthorized manipulation.	Influence on safety integrity.
Data confidentiality	Ensure the confidentiality of information on communication channels and in data repositories to prevent unauthorized disclosure.	Possible indirect influence on safety integrity (e.g., inaccessible information on the safety configuration).
Restricted data flow	Segment the control system via zones and conduits to limit the unnecessary flow of data.	Influence on safety integrity.
Timely response to events	Respond to security violations by notifying the proper authority, reporting needed evidence of the violation, and taking timely corrective action when incidents are discovered.	Possible indirect influence on safety integrity (e.g., by ignoring security violations that prevent the application of the appropriate counter measures).
Resource availability	Ensure the availability of the control system against the degradation or denial of essential services.	Influence on availability.

4.4.4 Defence in depth

One obvious reason to defence in depth is that cyberattack is often made to the found weak link. Therefore, cybersecurity needs to be controlled in several operational levels or layers. If one operational level is not well under control it is possible that there is a weak point, which is vulnerable for an attack. For example, if password management is poor, but firewall is excellent, then attacker may use the weak point (pass the firewall with the password) and overall security is compromised. According to defence of depth strategy all operational levels need to be adequate. Usually, one stakeholder does not have means to operate in all layers, but cooperation with other stakeholders is needed to cover all layers.

Figure 18 shows examples of defence in depth approach. According to IEC 62443-4-1 “Defence in depth strategy is a key philosophy of the secure product lifecycle” [30].

In functional safety the safety function can rely e.g., on very reliable switch system or light curtain for detection, but in cybersecurity domain single good countermeasure is not enough if there are other vulnerabilities to make a cyberattack. The right side of the Figure 18 shows some requirement sources (standards) related to the defence in different operational levels. The left side of the figure shows examples in different operational levels for protection against cyberattack.

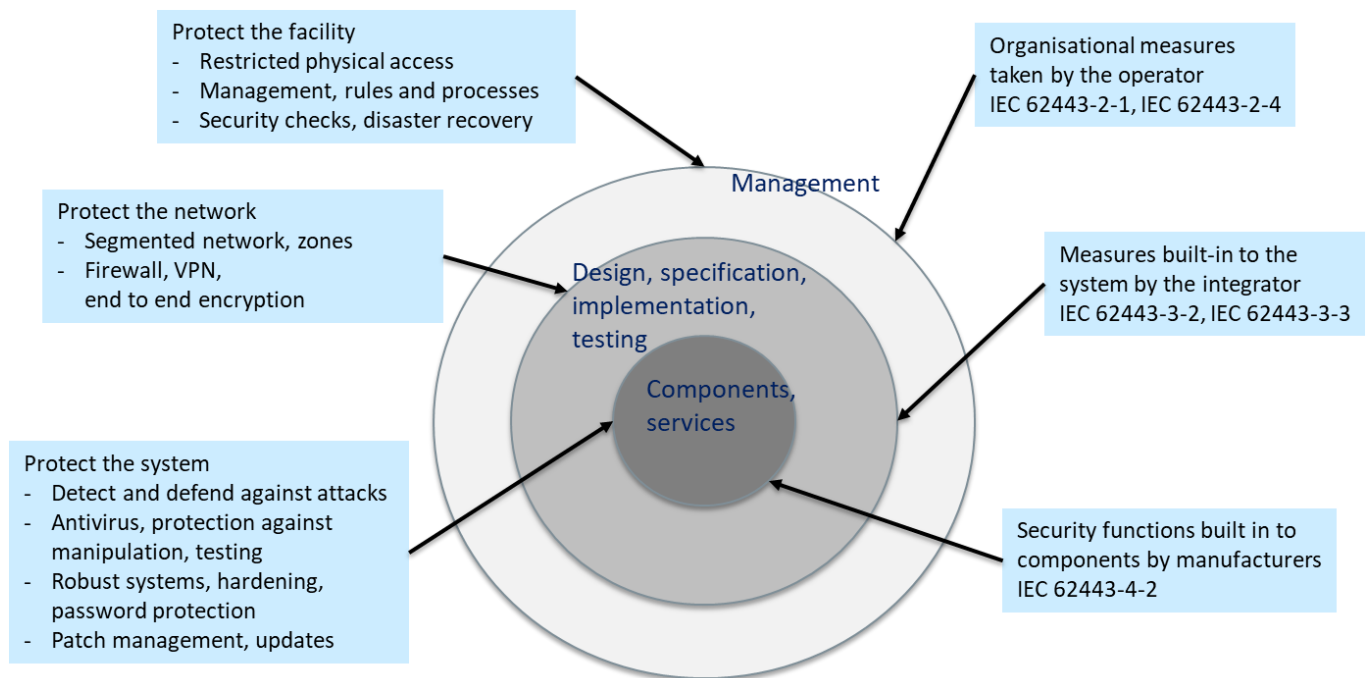


Figure 18. Examples of protection layers and countermeasures according to the defence in depth strategy [30] (modified).

Defence in depth levels can be selected also according to system lifecycle. Security management covers all lifecycle phases and then there are security guidelines for different lifecycle phases, such as specification of security requirements, security by design, secure implementation, and security V&V testing. [30]

Many companies present seven layers of cybersecurity (E.g., [Mindsight](#), [MicroAge](#)). The layers resemble a little bit OSI model (Open Systems Interconnection Model, ISO, [Wikipedia](#)) for communication, but it is changed towards cybersecurity. The presented layers are often:

- Mission Critical Assets layer,
- Data Security layer,
- Application Security layer,
- Endpoint Security layer,
- Network Security layer,
- Perimeter Security layer,
- The Human layer.



The responses to attacks can be divided in terms people, process, and technology. Table 4. shows response elements and some examples related to each element. The technology examples are foundational requirements according to IEC 62443, which are presented also at Table 3.

Table 4. Response elements. [3]

People	Process	Technology
management	policies	Identification and authentication control (FR1)
staff	procedures	Use control (FR2)
contractors	guidelines	System integrity (FR3)
...	security culture	Data confidentiality (FR4)
	...	Restricted data flow (FR5)
		Timely response to events (FR6)
		Resource availability (FR7)

4.5 Cybersecurity and functional safety differences

There are many differences between (cyber)security and (functional) safety related to important topics as Table 5 shows. The table shows safety and security viewpoints to each case and ideas why there can be conflicts between safety and security.

Table 5. Safety and security viewpoints to important topics and conflicts between objectives.

Topics, situation, or system design	Safety viewpoint	Security viewpoint	Conflict? Trade-off?
Primary targets (ISO/TR 22100-4:2020 [8]).	Injury/accident prevention, health	Negative impacts like, service operates in wrong way or not at all, confidential information leak, information is changed etc. Related to preventing or minimizing cyberattack effects.	Primary objectives differ, but in principle there is no conflict.
Principle	Functional safety: Part of the overall safety relating to the machine and the machine control system that depends on the correct functioning of the safety-related control systems and other risk reduction measures. (IEC TS 63074:2023 [33]) Safety functions are the tool of functional safety.	Cybersecurity: Set of activities necessary to protect network and information systems of the machine control system, the users of such systems, and other persons from cyber threats, typically regarding the aspects of confidentiality, integrity and availability (IEC TS 63074 [33]) Measures taken to protect a computer or computer system against unauthorized access or attack (IEC 62443-3-2 [28])	Primary principles differ, but in principle there is no conflict.



Topics, situation, or system design	Safety viewpoint	Security viewpoint	Conflict? Trade-off?
Risk dynamics (ISO/TR 22100-4:2020 [8])	Rather static field (intended use, reasonably foreseeable misuse)	Highly dynamic field; moving target (intentional manipulation, criminal intent)	Primary principles differ, but in principle there is no conflict.
Risk reduction stakeholder	Mainly machine manufacturer and user	Various actors, like, machine manufacturer, user, service provider. Asset owner approval required (IEC 62443-3-2:2020 [28])	In safety sector roles and timing are clear, but in security sector all actors need to be considered along the overall life cycle. (ISO/TR 22100-4:2020 [8])
Risk target, victim, or sufferer	User (direct effect), bystanders	User and other stakeholders when the negative impact affects other parties.	In safety sector main sufferer is user or victim. In cybersecurity sector the negative impact can be often wider.
Risk definition (IEC TS 63070:2023)	Combination of the probability of occurrence of harm and the severity of that harm	Expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular consequence	Risk definitions differ, but there are no straight conflicts.
Risk analysis (target to be analysed)	In functional safety domain functions are analysed. Analysis may include analyses related to a specific structure of the system.	In cybersecurity analyses zones, conduits and systems are analysed. These have relation to the structure of the system.	The target to be analysed may be different.
Risk analysis (qualitative or quantitative).	Random failures are studied with quantitative or qualitative analysis. Design/software failures are studied with qualitative analysis.	Deliberate acts or sometimes also mistakes, equipment failures and natural disasters are analysed. (IEC TS 63074:2023 [33]). The definition causes depend on the standard. Typically, qualitative analysis is applied.	Qualitative analysis can be applied in safety and security studies. Quantitative analysis suits mainly to the study of random failures.
Risk reduction management (ISO/TR 22100-4:2020 [8])	Specific safety organization (user organization, and discussions with e.g. notified body, authorities, subcontractors)	Various actors (user, service provider, manufacturer, integrator, security guards etc.)	Safety management is often more focused than security management. Information delivery need to be considered.
Failure	Random failures or systematic/design/software flaws, which can furthermore cause a hazard. Dangerous failure prevents a safety function from operating when required or decreases the probability that the safety function operates correctly when required (IEC TS 63070:2023 [33]).	Usually design flaws, i.e. vulnerability, which can allow threat to cause negative impact. The failure is associated to machine control system vulnerability and makes cyberattack possible. Failure is not the only consequence of cyberattack, but consequences can be in addition, for example information leakage	Failure is termination of the ability of a device to perform a required function (ISO 13849-1:2023 [35]). Cyberattack can have also other consequences than failure, which can lead to final consequences (see Figure 5).



Topics, situation, or system design	Safety viewpoint	Security viewpoint	Conflict? Trade-off?
		(confidentiality) or service denial.	
Failure causes	Random failures or systematic/design/software flaws. The causes are related for example to environment, circumstances, and wear.	Attack, assault on a system that derives from an intelligent threat. (IEC 62443-3-3:2019 [29]) Threat is typically intentional, but unintentional threats are not always excluded. (IEC 62443-3-2:2020 [28])	Failure causes differ. In safety domain failure cause is typically unintentional. In security domain, in addition to failure causes, also causes to other consequences, like information leakage and service denial need to be considered. All of these (security) causes are typically intentional.
Categories	SIL (Safety Integrity Level), PL (Performance Level). Associated to safety functions, their integrity and performance. SIL/PL requirement levels are associated to the risk of harm. Safety performance is associated to integrity (stability to perform safety functions) of safety functions. (ISO 13849-1:2023 [35])	SL (Security Level). Associated to zones (grouping of logical or physical assets), conduits (communication channel) or systems, that share common security requirements. Security level: measure of confidence that the control system is free from vulnerabilities and functions in the intended manner. (IEC 62443-3-2:2020 [28])	There is no direct correlation between SIL or PL and SL. (IEC TS 63074:2023 [33])
Integrity decrease	The most important functional safety target. Integrity decrease is a risk. If integrity decrease is detected, a specific safety function is triggered.	Integrity is an important security target. Integrity decrease is a risk.	Integrity is important for safety and (OT systems) security. Integrity checking in data transfer and management can support both safety and cybersecurity (e.g. safety code, CRC).
Availability decreases or timely response becomes longer (IEC TS 63074:2023 [33])	Availability decrease can be a risk. If response time increases and it is detected (watchdog timer) this triggers safety function, which typically stops the machine and safe state is reached. If continuous control is required (e.g. cooling or stability control), then decreased availability or increased response time is an immediate hazard.	Availability is an important security target (OT systems). In some cases, access denial may be applied as a counter measure to prevent cyberattack (e.g. too many password trials).	Safety system can stop the system if it is needed to prevent a harm. Security system can deny access to prevent cyberattack (rare cases, since cyberattacks are difficult to detect). Availability conflicts between security and functional safety need to be considered. Access denial must not affect safety (e.g. e-stop must always be available).
Confidentiality decreases (IEC TS 63074:2023 [33])	Confidentiality is not a safety target. If confidential cyber vulnerability information of safety system is revealed (e.g. passwords, weak points, threat vectors), then	Confidentiality can be important cybersecurity target. It is more important in IT systems than OT systems.	Confidentiality is related to security, but not to safety.



Topics, situation, or system design	Safety viewpoint	Security viewpoint	Conflict? Trade-off?
	this may have an indirect effect on safety and additional study may be needed.		
Conditions/environment (ISO/TR 22100-4:2020 [8])	Transparent	Confidential	Open versus confidential information. Users must be informed about safety risks. Security vulnerabilities are more confidential.
Restriction of logical/physical access to the IT-system (with possible influence on safety) (ISO/TR 22100-4:2020 [8])	Restrictions to access are common for safety reasons (authorized use, e.g. use of a crane or a machine line). In emergency situations, like fire, some restrictions may need to be overridden.	Restrictions of access are typical security countermeasures.	Restrictions related to access need to be coordinated between safety and security.
Detection and reaction on IT-security incidents (with possible influence on safety) (ISO/TR 22100-4:2020 [8])	Provisions to detect unavailable (safety) services and failures are associated to safety.	Monitoring of cyberattacks and relevant countermeasures. However, countermeasures like firewalls, are typically on all the time on and single machines do not usually have capabilities to detect attacks.	Unavailable safety services cause typically a safety function. In principle cooperation between safety and cybersecurity systems could be useful.
In the case of remote maintenance and service (ISO/TR 22100-4:2020 [8])	Provisions for remote access. Remote operations require specific safety rules (e.g. to avoid collisions).	Setting rules, monitoring, and priorities for remote access.	Remote maintenance and control are both safety and security sensitive operations.
Identify (ISO/TR 22100-4:2020 [8])	Hazard identification. Allocating safety functions to the complete system or subsystems.	Identify IT-security assets, threats, and vulnerabilities.	Risk identification is most important phase in risk assessment. Cooperation is beneficial for both security and safety, but the analyses can be separate.
Protect (ISO/TR 22100-4:2020 [8])	Order of safety measures: First inherently safe solution – Secondly safeguarding/safety functions – Thirdly information for users (ISO 12100 [34]). Safety functions are defined in functional safety process (PL/SIL and description).	Determine SL-T for subsystems or each zone and conduit and countermeasures accordingly. (IEC 62443-3-2:2020 [28])	Cooperation is beneficial for both security and safety, although the protective objectives are different.
Detect (ISO/TR 22100-4:2020 [8])	Hazardous situations are detected, and a specific safety function is triggered when needed.	In machines, countermeasures, like firewalls, and access control are continuously on, and there is only small capability to detect cyberattacks. Fleet control may have specific countermeasures to detect cyberattacks, like	It is useful to share common situational awareness during incidents.



Topics, situation, or system design	Safety viewpoint	Security viewpoint	Conflict? Trade-off?
		intrusion detection, scanning for malicious software, system activity monitoring and monitoring of limit values.	
Respond (ISO/TR 22100-4:2020 [8])	During service failures safety function(s) usually trip to prevent harm(s).	Single machines do not usually have capability to detect cyberattacks and apply additional countermeasures.	Cooperation could be beneficial for both security and safety.
Recover (ISO/TR 22100-4:2020 [8])	If a hazardous situation begins a person may have possibilities to avoid harm by applying slow speed, situational awareness etc. If a harm has happened then the situation is related to management, medical care, and rescue operations.	Appropriate activities to maintain resilience and to restore any capabilities or services that were impaired due to a cyberattack.	Functional safety usually considers aspects before harm, but also reduced capability mode (limping mode) may be applied for rescue purposes. Machinery safety also considers minimizing damages. Cybersecurity covers restoring services and connections.
Cyberattack and legislation	Currently cyberattacks are not considered in Machinery Directive. "Reasonably foreseeable misuse" is considered in current Machinery Directive (ISO/TR 22100-4:2020 [8]). New Machinery Regulation requires protection against accidental or intentional corruption. [13]	Every kind of intentional violation (sabotage/spying) of a machine is de facto a criminal act. Cyberattack is considered as criminal act and considered according to criminal legislation. (ISO/TR 22100-4:2020 [8]). New legislation for cybersecurity is coming and there are many acts to refer to, such as, NIS2 [14] and Cyber Resilience Act [11].	Machinery safety and cybersecurity have different legislation.
High level design process (case: automotive discipline) (CySec , FuSa , TARA , HARA , ASIL ... , Functional safety vs. cybersecurity in the automotive industry , see links for more information related to automotive discipline)	Define – identify – evaluate – realise – validate. HARA ASIL (SIL/PL) Safety requirements HW and SW design process according to functional safety requirements.	Define – identify – evaluate – realise – validate TARA AcSIL (SL) Security requirements During the design process take into account cybersecurity aspects.	The high-level process of functional safety and cybersecurity looks similar, although the details are different.

5 Cybersecurity risk assessment

To perform an in-depth assessment and mitigation of cybersecurity risks for mobile machines and cyber physical systems, it is important to look at how such assessments can not only protect such systems from cyber threats, but also allow them to operate securely under all conditions. This section therefore looks at various methodological approaches and tools to provide flexible and reliable cybersecurity risk assessment of critical operational technologies as well as systems of systems.

5.1 Examples of cybersecurity risk assessment methods

This section introduces cybersecurity tools valued for their ability to assess cybersecurity issues while also considering potential impacts on the safety domain of Operational Technology (OT). In recent years, there has been a growing recognition of the need for safety and security co-analysis. This attributed to the increasing complexity of modern systems, characterized by high interconnectivity, open communications, increased automation, and vulnerability to physical harm due to cyberattacks. These systems, known as Cyber-Physical Systems (CPS) [6], cannot be deemed safe unless they are also secure. Therefore, CPSs require a comprehensive analysis approach.

By conducting a unified safety and security analysis, one can achieve the dual goal of creating systems that are both safe and secure, while also gaining insight into the interrelation between these two aspects. This includes understanding the impact of security measures on safety, as well as the impact of safety considerations on security [6].

5.1.1 STPA-SEC

In 2013, Young and Leveson [46] introduced (System-Theoretic Process Analysis for Security) STPA-Sec, an extension to STPA (System-Theoretic Process Analysis) aimed at incorporating security considerations. STPA and STPA-Sec recognize that systems have dynamic properties in which system elements engage and impact each other potentially leading to new, non-obvious ways of how undesired situations can emerge. Whereas STPA considers such interactions from safety perspective, STPA-Sec extends its analysis to include security concerns. To do so, Unsafe or Unsecure Control Actions (UCAs) are identified, and their causes determined.

The process of STPA's and STPA-Sec's methodology can be viewed in Figure 20. As indicated in blue, STPA-Sec seamlessly integrates safety and security considerations and does not distinguish between the analysis stages of security and safety. The method is characterized by requiring a hierarchical visualization of command / Control Action (CA) and feedback flows among system elements. This so-called control structure (generic example in *Figure 19* depicts all system elements and whether they transmit or receive CAs or feedback.

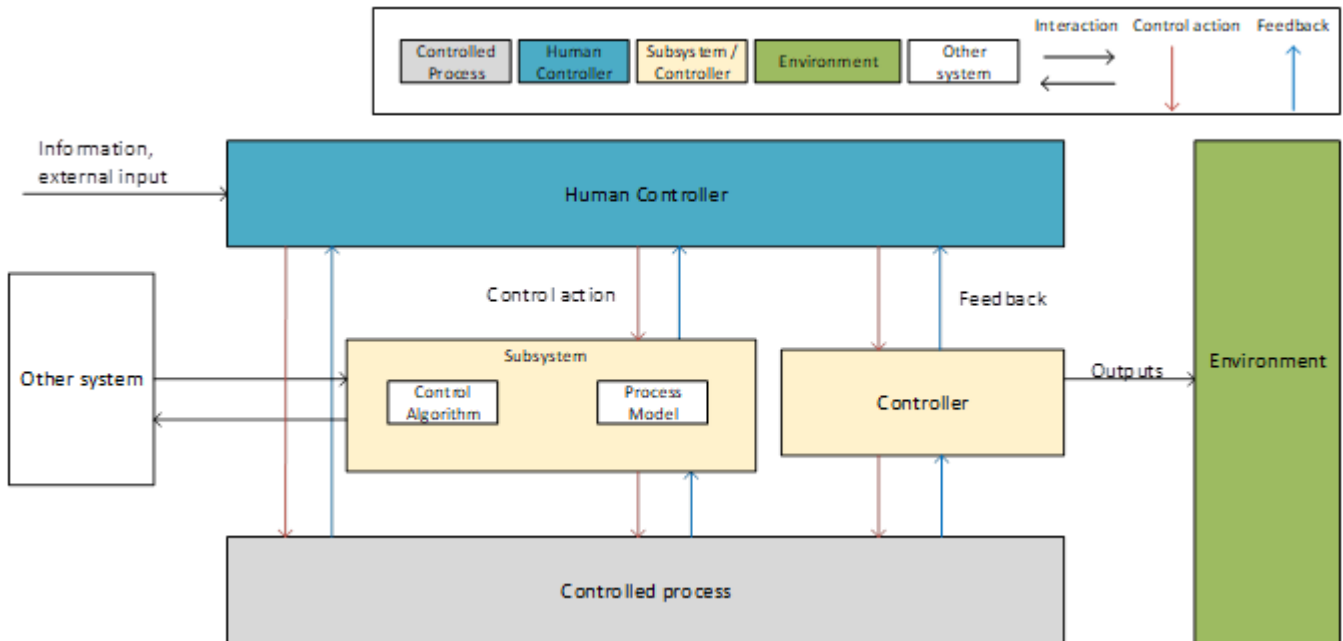


Figure 19. Generic STPA / STPA-Sec control structure.

Although STPA-Sec does not deliver specific countermeasures, it serves as a valuable tool for identifying critical scenarios, so called loss scenarios, and steers cybersecurity efforts on proactive prevention [1]. However, it's important to note that STPA-Sec alone cannot guarantee full analysis of system security. This is because it does not examine the impacts of externally imposed threats [7].

5.1.2 STPA-Sec + STRIDE

Developed by Microsoft in the late 1990s, STRIDE is a practical and straightforward model used for threat analysis. It aids in identifying potential threats to a system and revealing security design flaws. The acronym 'STRIDE' stands for 'Spoofing of user identity, Tampering, Repudiation, Information disclosure, Denial of service, and Elevation' of privilege, representing the six threat categories of the method. The hint words guide in considering how each threat category impacts the system and its connections with other systems. Each threat is numerically rated and thus, the most relevant threats can be identified. To utilize STRIDE effectively, it is essential to model the system accurately and comprehensively including its components, data flows, data stores, processes, and interactions [1].

Combining STRIDE with STPA-Sec serves in overcoming the earlier mentioned weakness of STPA-Sec and provides cybersecurity threat analysis from the attacker's perspective. This leads to identification of additional loss scenarios caused by intentional threats, which have the potential to breach confidentiality, integrity, and availability. Furthermore, when STPA and STRIDE are used together collaboratively, they enable the interactive discovery of loss scenarios that might not have been identified when either method is used alone [7]. The additional steps that STPA-Sec and STRIDE bring to the generic STPA are visualized in Figure 20.

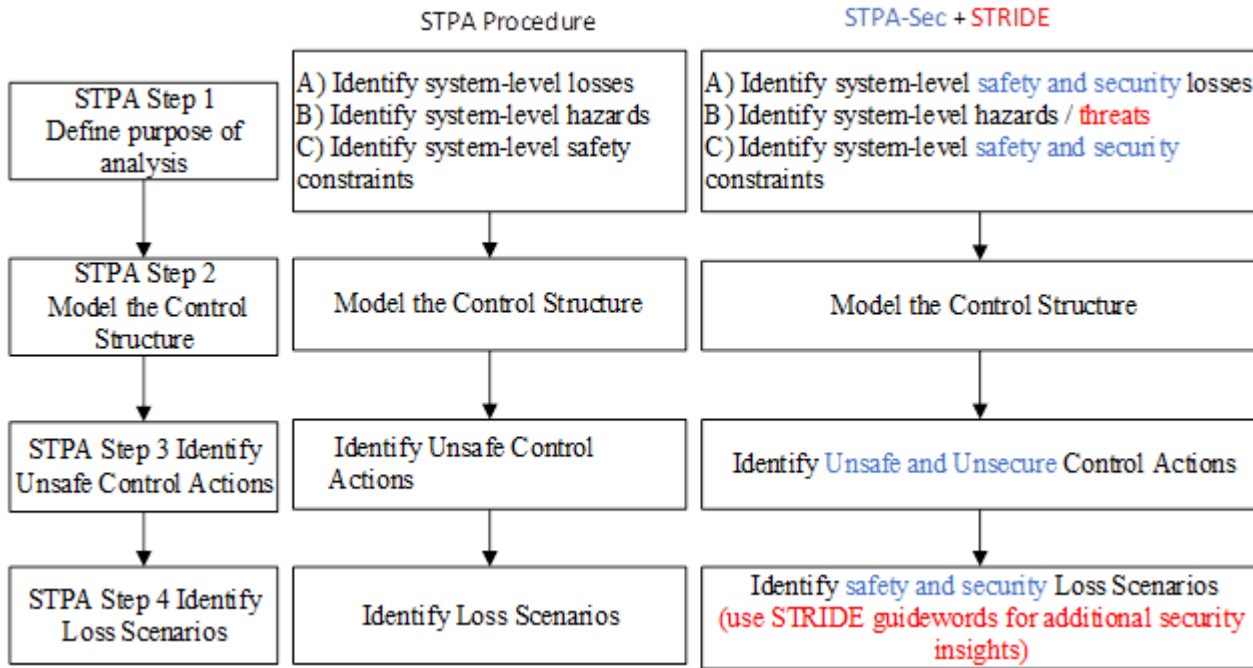


Figure 20. Process of STPA-Sec + STRIDE. (Modified from [36]).

5.1.3 Security Threat Analysis (STA)

STA, a cyber security risk assessment method was published in 2022 by VTT Technical Research Centre of Finland Ltd [2]. It is applicable to industrial instrumentation and control (I&C) systems of any domain, and it is targeted for use in early design phases.

Primarily focusing on cyber security, it is a hybrid method utilizing reliability, availability, maintainability, safety, and security (RAMSS) information, and it delivers a data model with harmonized fundamental concepts between dependability, safety, and security. While it does not define a cyber security risk assessment procedure it comes with an ontology for each of the three discipline’s input and output artefacts (e.g., Risk evaluation result, RAMSS Hazard (Threat), Negative impact, Imperfection (Vulnerability), Asset, Requirement, etc).

Nevertheless, ontology and the derived data model give enough structure to the process to integrate STA into typical risk assessment procedures, such as presented in ISO 31000 [44], or IEC 62443–3–2 [28]. Regarding IEC 62443–3–2 [28], STA is especially tailored to execute certain Zone and Conduit Requirements (ZCR): ZCR-1(Identify the system under consideration), ZCR-2 (Perform an initial cyber security risk assessment) as well as ZCR-5 (Perform a detailed cyber security risk assessment). Zone and Conduit Requirements (ZCR) are groupings of logical or physical assets (zones) and groupings of logical communication channels (conduits) that share common security requirements and connect two or more zones.

In [2] the authors implemented STA using ‘Polarion REQUIREMENT’ requirements management tool. Other programs that allow traceability links between data objects (specific preconfigured data fields available for inserting assessment data), suspect flagging for impact analysis and document version control are also suitable.

5.1.4 Uncontrolled Flows of Information and Energy (UFoI-E)

In 2020, Carreras Guzman [7] introduced the tool UFoI-E (Uncontrolled Flows of Information and Energy), which is an integrated method for analyzing safety and security. It addresses the limitations of current methods that co-analyze safety and security. Unlike some methods that focus mainly on systems in the early requirement and concept phase and are suitable only for simple system architectures, UFoI-E offers more in-depth analysis by showing relationships between the energy and information flows exchanged between the cyber and physical environments of the system. [7]

UFoI-E builds on a basic principle also known as UFoI-E causality concept in which "Energy" encompasses various forms of energy streams, including kinetic, chemical, and thermal, among others, which enter, move within, and exit the system [7]. These energy streams are initiated through commands (information) and have a direct impact on the physical layer of the system. The tool comprehensively considers how potential hazards and vulnerabilities may arise from uncontrolled or unintended flows of both energy and information.

To enhance understanding, UFoI-E requires modeling of information and energy streams within the system under investigation into what is known as a CPS master diagram. This diagram consists of three layers: the Cyber layer, the Cyber-physical layer, and the Physical Layer (PL) [7]. Through this structured approach, UFoI-E systematically analyzes the interactions between information and energy, providing a robust framework for assessing safety and security risks within complex systems.

Furthermore, UFoI-E incorporates the Cyber-Physical Harm Analysis for Safety and Security (CyPHASS), which serves as an accident causation model and can be thought of as a "harm scenario builder". CyPHASS extends the bow-tie method and conducts risk identification backwards starting at the safety consequence at the PL. It provides a database of checklists and guidewords to show how different risk sources affect one layer and then cascade backwards throughout the connected layers, simultaneously aiding in identifying barriers (layers of protection) to prevent and mitigate propagation [7]. Figure 21 below illustrates the three main elements of the UFoI-E methodology.

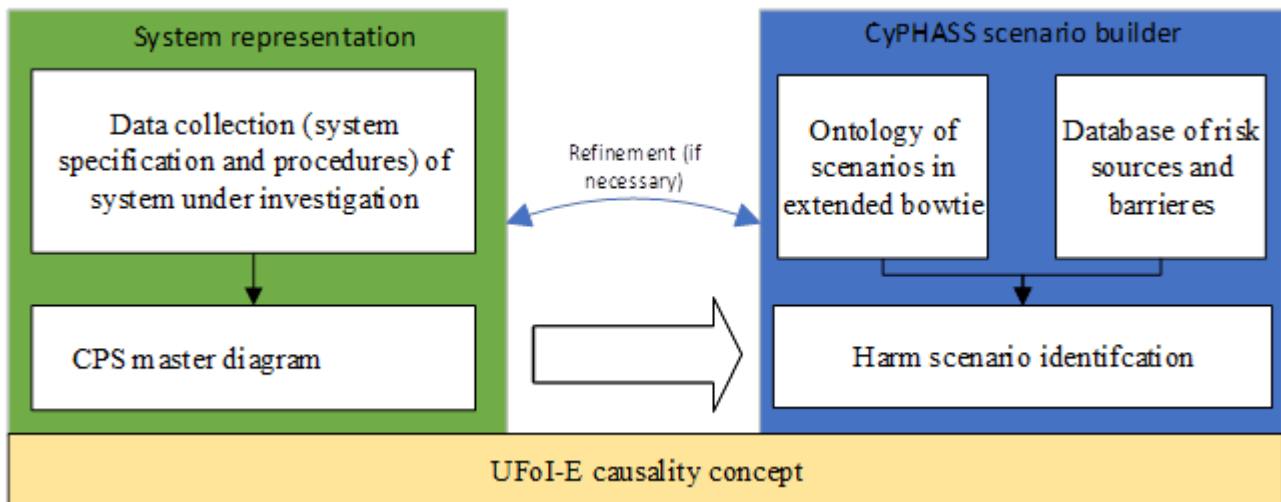


Figure 21. UFoI-E method. (Modified from [6])

5.2 Risk assessment of System of Systems

System of Systems (SoS) can be defined as set of systems or system elements that interact to provide a unique capability that none of the constituent systems can accomplish on their own. System elements can be necessary to facilitate the interaction of the constituent systems in the system of systems. (ISO/IEC/IEEE 21839, 2019) [37].

The risk assessment of System of Systems (SoS) resembles risk assessment of Stand-alone Systems (SaS) very much. However, the SoS layer can add new objects to the analyse. Compared to SaS, SoS can be more complex and much larger, and a lot of communities can be involved. This means usually that the analyst needs to pay attention more to humans, communities and safety cultures rather than systems. The ideas are described more in VTT report “System of systems modelling for safety and cyber-security assessments” written by Joonas Linnosmaa, Jarmo Alanen, Risto Tiusanen, Josepha Berger, Sami Karadeniz, and Timo Malm. The report will be published during Autumn 2024. [37]

5.3 Cybersecurity perspective on risk assessment

In order to gain an understanding of risk assessment from the perspective of cybersecurity best practices, several factors need to be taken into account. In addition to potential Advanced Persistent Threats (APTs) and the ability for connected machines to be remotely compromised via existing IT infrastructure by threat actors, manufacturers must also consider regulatory and legislative compliance as well as potential disruptions and the robustness of the entire supply chain. Recommendations and guidance for these issues are described in the following paragraphs.

Industrial machinery equipped with semi-autonomous operations, advanced sensors, and 4G/5G connectivity face significant cybersecurity risks. These include remote hacking, data interception, and the potential for malicious firmware updates, which could disrupt operations or compromise safety. The supply chain is also vulnerable to tampering, especially with software and hardware components. Manufacturers should conduct regular risk assessments, implement secure communication protocols, and ensure robust cybersecurity measures are in place to mitigate these threats.

Manufacturers operating in the EU must comply with stringent cybersecurity regulations, including the EU Cybersecurity Act, which mandates certification for connected devices. GDPR compliance is crucial for handling personal data collected by machinery sensors. Upcoming legislation, such as the Cyber Resilience Act and the NIS2 Directive, will likely impose additional cybersecurity obligations on manufacturers and their supply chains. Staying informed and preparing for these changes is essential for continued compliance and market access.

Ensuring cybersecurity compliance across the supply chain is critical. Manufacturers must conduct thorough assessments of services from suppliers and third-party vendors to avoid introducing vulnerabilities. Compliance with EU cybersecurity standards and guidelines, such as ISO/IEC 62443, should be mandated for all partners to maintain consistent and secure practices throughout the manufacturing and supply process.

To address cybersecurity challenges, manufacturers should adopt security by design principles, integrating robust security measures from the outset of product development. Developing tailored incident response plans for industrial machinery and engaging in industry collaboration and information sharing will further enhance resilience against emerging threats. Proactively addressing these areas will ensure that machinery is not only compliant but also secure against the evolving cybersecurity landscape.



6 Discussions with companies

The discussion topics have been related to cybersecurity risk assessment and some related machinery safety aspects. Table 6 includes information from three companies that were in these workshops/discussions and in addition four companies, which presented their views in seminars. The three companies in workshops are all related to mobile machine manufacturing and in all cases, there were persons, who know about safety and persons, who know about cybersecurity. The companies related to seminars are related to the following domains: machinery, machinery/radio, process industry and IT-security. The presenting persons were all cybersecurity experts, and they have answers only to general cybersecurity questions.

Here are some related topics: related regulations and standards, risk assessment process model, ideas about cybersecurity and safety cooperation, steps to analyse the system, defence in depth applicability and limiting factors in combining analyses. One discussion topic has also been possible checklist to detect items, which may cause cybersecurity/safety conflicts.

Table 6 shows observations from workshop discussions and seminars. The left column shows the subject and right column shows the observations. The numbers in parenthesis show how many companies were familiar with the requirement. Some requirements were only proposals or new publications and therefore companies have not yet had time to get acquainted with them.

Table 6. Observations from the discussions with companies.

New Machinery Regulation (EU) 2023/1230 Link	It is important for companies in machinery domain. Companies from other domains did not mention it. (5/7)
Cyber Resilience Act. Brussels, 15.9.2022. Proposal Link .	Only a proposal, but it will have more importance and it affects products. (3/7)
NIS2: Network and Information Security Directive II, (EU) 2022/2555 . Proposals: AI act (Link), Data Act: Link	Is important. Affects company actions. Most of the companies did mention. (6/7) Both are proposals, but they will be important (3/3).
NIST Special Publication NIST SP 800-82r3 Link	Not yet well known. Could be important (only) to some customers. (0/7)
CEN ISO/TR 22100-4:2020. Part 4: Guidance to machinery manufacturers for consideration of related IT-security (cyber security) aspects.	It is important for companies in machinery domain. (4/7)
IEC TS 63074:2023. Security aspects related to functional safety of safety-related control systems.	Not yet well known. Maybe some importance in machinery domain. (1/7)
IEC 62443 Security for industrial automation and control systems (standard family)	It is important for companies in automation domain. All companies have mentioned. (7/7)
SFS-ISO/IEC 27005:2018. Information technology. Security techniques. Information security risk management. 55 p.	Important in IT security. Some machinery domain companies have mentioned. (4/7)
Most useful cybersecurity risk assessment process?	IEC 62443-3-2, some methods were mentioned only briefly.
Methods?	No solid process to apply a specific method.
Can cybersecurity and safety risk assessment processes be combined?	They are separate. Maybe in the future?



Are there several stakeholders/asset owners in risk assessment process.	Usually, machine manufacturer makes the analysis alone. In many cases the asset owner gives requirements. Only in some cases, there can be many stakeholders in the same analysis.
How important is Defence in depth approach?	Defence in depth approach is important in cybersecurity domain, but single stakeholder cannot usually operate in all layers. The cybersecurity related customer requirements do vary a lot.

General remarks, which were not said straight in discussions are that cybersecurity requirements are not yet ready, there is not yet solid process for security risk assessment, there is not yet a leading risk analysis method and due to lacking requirements and methods it is difficult to prove adequate level of cybersecurity. Currently companies related to automation apply mainly IEC 62443 standard family for cybersecurity guideline.

7 Discussion

Requirements

Safety and security have many differences in objectives and requirements. Functional safety standard ISO 13849-1 mentions that the standard has no security requirements, but the requirements need to be checked at ISO/TR 22100-4 and IEC/TS 63074. Respectively, IEC/TS 63074 refers to functional safety standards to find safety requirements. New standards will be published, and the technical report and the technical specification will be replaced with more powerful requirements. Harmonised standards are needed to get more firm support to the requirements.

Currently cyberattacks are not considered in Machinery Directive. “Reasonably foreseeable misuse” is described in current Machinery Directive, but it is not related to cyberattacks (ISO/TR 22100-4:2020). New Machinery Regulation will consider also reasonably foreseeable malicious attempts [13]. This means that if a cyberattack causes a harm, the liability of the cyberattack can be considered also according to the new Machinery regulation. Currently, cyberattacks are considered as criminal act and therefore liability is according to criminal legislation (not harmonized in EU). New legislation related to cybersecurity means that the liability of cyberattacks can be considered also according to new coming legislation (e.g. NIS2 [14], Cyber Resilience Act proposal [11]). The new legislation means that not only the attacker, but also for example system provider can be liable for inadequate actions.

Risk assessment

The primary objective of safety is to prevent accidents and primary objective of cybersecurity is to prevent or minimize effects of cyberattacks. The primary objectives are different, and this also affects the risk assessments. The focus in the analysis should be in the most potential risks and if the security and safety analyses were merged, it could mean that too much attention is put to improbable events. It is laborious to search security events from detailed safety risks and safety risks from detailed security events. In risk assessments the workload depends among others, on the approach type (here: bottom-up and top-down).

- In bottom-up approach (e.g. failure mode and effects analysis) all details are analysed systematically, and the result can give good confidence on finding single-point failures/cases. Usually simultaneous failures/events (e.g. common cause failures) are not considered. In bottom-up analysis each item is analysed, and it causes a lot of work, if both safety and security properties are estimated for each item.
- Top-down approach (e.g. fault tree analysis) begins with top event and the initial causes are concluded. All causes and items are found according to the knowledge of the analysts, but the items are not found systematically. Top-down methods can merge simultaneous failures/events/threats and it can give a good overview of the risks. The analysis can also handle many simultaneous causes. In top-down analysis the number of initial items is not so large compared to bottom-up analysis, since all initial items are related to top event. The analysis can focus on the case, how it can initiate series of events to cause the top event. The same top-down analysis (e.g. fault tree) can have security and safety causes.

The above reasoning shows that it is easier to merge safety and security analyses when top-down approach is applied. Top-down approach is illustrative, and it can consider simultaneous failures/events/threats, but one do not know whether all items are considered systematically. Quite often a bottom-up analyses are done first to find all items that need to be considered. This means that first separate security and safety analyses are done and then the results are merged in top-down analysis, if needed. There are also specific analysis methods, which are designed to be used with cybersecurity and safety systems, like UFoI-E (see 5.1.4).

One objective of risk assessment is to find also critical, but improbable failures, kind of “devil in details”. The question is, can these kinds of risks be found in separate analyses or in merged analysis. In separate analysis same amount of resources could give more focused analysis, which can reveal more weaknesses. This is relevant, especially, in bottom-up approach, when finding rare risks. On the other hand, if “the difficult to find” risk is between safety and security, then discussions with safety and security analysts could reveal the risk. This means that discussions with safety and security analysts are needed both in merged and separate analyses, especially, in risk identification phase. Top-down approach can give additional information in redundant systems, where considering several simultaneous risk causes can be important.

Risk identification is usually considered to be the most important step in risk assessment according to Debra Patterson’s book (section 6.3) [40]. Unidentified risk is often not under control, especially, if the risk differs from other risks and designed risk reduction methods do not cover the unidentified risk. Since risk identification is so important it is obvious that cooperation between cybersecurity and safety analysts is needed to identify effectively risks. Some risks may be related to both cybersecurity and functional safety.

Another phase, when cooperation between analysts is essential is risk treatment/reduction. In this phase it is important to check that the methods do not violate safety or security objectives. However, safety requirements may not be violated.

Risk estimation phase is usually done separately in cybersecurity and safety domains. One reason is that PL/SIL and SL values have no direct correlation [33]. One can say more generally that high risk in cybersecurity does not mean that there is high risk in functional safety or vice versa. When there is no correlation between risks, it means that it is practical to make risk estimations separately. This is related also to different objectives (accident prevention versus cyberattack minimization), which are considered separately.

Remote control and maintenance are critical for safety and cybersecurity. These operations need to be considered carefully from both security and safety viewpoint. The objectives can be mutual.

Risk assessments related to cybersecurity are made more often than to safety. Safety risk assessment is made typically in the beginning, when the system or part of it is changed or a new risk is discovered due to for example an accident, close call or manufacturer’s risk notifications. Security risk assessment is made in addition, when the environment, stakeholder or threat changes without any modifications of the system. Different frequencies of the analyses are not supposed to make any conflicts.

Risk assessment is related to uncertainties. Can we say that a specific risk assessment method gives an adequate confidence on cybersecurity, perhaps according to required SL and asset owner policy. IEC 62443-3-2 and ISO 12100 shows general principles for the risk assessment, but they do not specify by name a specific analysis method for safety or cybersecurity. Specific risk analysis methods have their own strong and weak points it may be good to choose a specific method on case-by-case basis.

There can be advantages to make cybersecurity and safety risk assessments simultaneously when all these factors are true:

- System to be analysed is the same. The system includes safety functions, security zones, and conduits.
- Hazard identification has also cybersecurity aspects, otherwise the analyses should be separate.
- Stakeholders (asset owner, user) are same for safety and security. The motivation to make the analyses need to be mutual, especially, when several companies are involved.
- The objective to find risks is similar (e.g. prevent accidents).
- Risk of losing integrity or availability is the main focus.
- Need for risk analysis is at the same time (new system, changes in the system). Security risk analysis is done more often, since it is needed usually also when operator or thread changes.



- Knowledge to make both analyses is adequate.
- Information is transparent inside the analyst team. No restrictions to access adequate information.
- In cybersecurity defence in depth means that risks need to be estimated in different layers. It is difficult to include several layers also to the safety analysis. One security layer at a time is easier to analyse anyway.

Attributes of a system

Impaired integrity is often the most important attribute in functional safety (safety integrity level). Impaired integrity means that software, data or hardware has changed unintentionally causing, for example, failed operations or faulty information. The concern of integrity is mutual in safety and security, and it may be possible to have common means to reveal unintentional data integrity changes in communication or data storage, for example, by using CRC or other safety code. The safety code may include cryptography.

Another common attribute for safety and security is availability. In OT systems availability is the most important attribute [26]. Reduced availability can be a result of cyberattack or safety/security measure. Reduced availability can be applied as a countermeasure to minimize hazardous effects by stopping the machine or denying access. If attacker knows, how safety function triggers easily, information may be used in service denial attack. Reduced availability cases need to be studied and checked that risk level is adequately low.

Persons and liability

Persons who are qualified to implement security countermeasures are not necessarily the same people who are qualified to implement safety-related control systems [33]. This means that in cybersecurity and functional safety risk assessment processes, there are often different persons, which indicates often separate analyses, but mutual exchange of information and support becomes more important.

The stakeholders and victims related to risks can be different in safety and security domain. In safety domain victim is typically user (person) and liable stakeholders are usually the user (organisation) and the machine manufacturer. In security domain victims (receive negative impact) and liable stakeholders can vary from case to case and the liable stakeholder can even change during the lifetime of the system. Examples of stakeholders are service provider, asset owner, system integrator, system supplier and insurance company. Different stakeholders may have different objectives and countermeasures may be biased.

Liability has an effect on risk assessment too. Apparently, the liable stakeholder is eager to have successful risk assessment. On the other hand, the stakeholder, which has knowledge of the system has best capability to do the risk assessment. Probably there is no conflict between stakeholders, but it is often important to have NDA (non-disclosure agreement) and an agreement, about the tasks and responsibilities of each stakeholder. According to IEC 62443-3-2 the asset owner approves the risk assessment.

Categorizing items

It is useful to categorise and differentiate items to understand better their relations. In this report the following aspects have been differentiated and categorized:

- Functional safety - cybersecurity risk definition and parameters Figure 1 and Figure 2.

- Safety – security relation to integrity, availability, and confidentiality, Figure 5 and Figure 6.
- IT and OT systems differences, Table 1.
- Overview of security foundational influences on risks and possible influences on a safety-related control system, Table 3.
- Risk treatment (lifecycle), safety – security, Figure 16 and Figure 17.
- Categorizing risk treatment methods, Table 2.
- Defence (principal) types against risks in safety – security, section 4.1.2.
- Categorizing defence in depth layers and methods, section 4.4.4.
- Categorization functional safety (PL/SIL) – cybersecurity (SL) risks, requirements, section 4.2.
- Risk assessment processes, IT-security – OT security – safety, section 4.3.
- Safety and security viewpoints to some important topics, Table 5.

Figure 22. shows a summary of cybersecurity and functional safety dependencies and differences. The figure shows examples of important relations related to subjects. The corresponding topics in cybersecurity and functional safety are drawn horizontally and named with orange colour. In the figure, “Process phases” include only risk identification phases, since in that phase the cooperation between cybersecurity and functional safety is necessary. In other process phases cooperation is possible, but not so obvious. In the figure, “Common technological interests” show some examples of technologies, which typically need both cybersecurity and functional safety consideration (remote control, data integrity checking and access control).

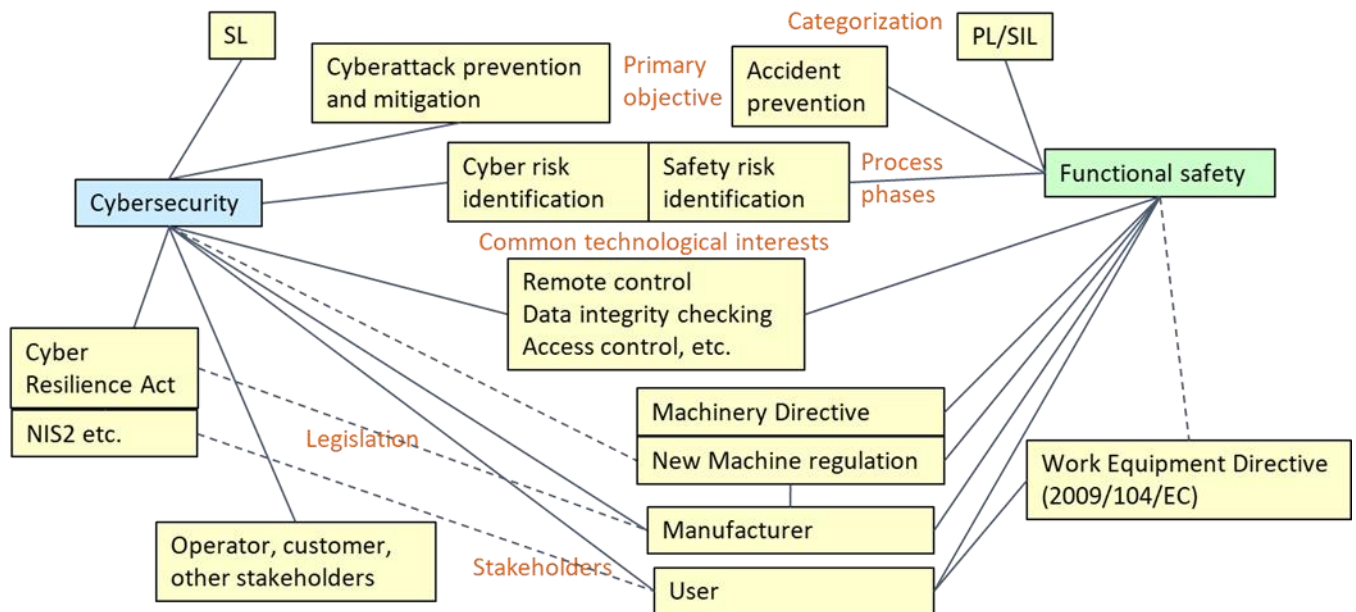


Figure 22. Mind map of general cybersecurity and functional safety dependencies and differences related to requirements, risks, and risk control.

8 Conclusions

Cybersecurity and functional safety have different objectives and there are differences in risk assessments. List of essential differences can be found in Table 5. The list is not exhaustive, but it gives an overview of different types of differences. It is practical to make the cybersecurity and safety analyses separately and especially risk estimations need to be separate. However, cooperation between the analyses can be beneficial especially in risk identification and risk treatment phases. Also, a common summary and perhaps fault tree analysis (top-down analysis methods) can be illustrative result of the analyses. Risk identification is the most important phase of risk assessment [40] and mutual resources are needed to find essential risks. The communication between domains in risk treatment phase (see section 4.3.1) is important to minimize possible conflicts between countermeasures (cybersecurity) and protective measures (safety).

It is useful to consider cybersecurity risk treatment actions from many perspectives and levels, like, lifecycle phase (Figure 17), properties of the target (Figure 6) and risk treatment strategy (Figure 15). In addition, also defence in depth strategy (section 4.4.4) need to be applied. This kind of approach can make it more probable to avoid the weak links of the cybersecurity.

New cybersecurity requirements have already been published (e.g. NIS2) and some coming soon (e.g. Cybersecurity Resilience Act). Also new Machinery Regulation (EU) 2023/1230 of June 2023 determines some requirements related to cybersecurity. These all regulations mean that machine manufacturers and system providers need to consider cybersecurity objectives. This is relevant, especially, in complex systems with, for example, remote control, cloud services, wireless communication and fleet control.

On the other hand, the requirements are made, because the number of cyberattacks is increasing and actions are needed to prevent and minimize the impacts of cyberattacks. The requirements are also related to the level of confidence. The better machine manufacturers and system providers fulfil the requirements, the more confident customer can be on adequate cybersecurity measures, and this can be good for business. The user organization and asset owner need to have adequate cybersecurity measures, since they are often the first ones to suffer consequences of the cyberattack. All of this can be considered as a new expense item, but it can be seen also as an opportunity to new business.

In cybersecurity domain it is typical that responsibility of the overall cybersecurity is divided to several stakeholders. In safety domain the user and manufacturer take the main responsibility, but in cybersecurity domain, in addition, operator and communication/data system provider may have responsibility. Many aspects related to responsibility can be stated in agreements. Also, NDA agreements (non-disclosure agreements) are common in cybersecurity domain.

Risk assessment is a tool to find out vulnerabilities of the products and operations and furthermore to get confidence on solutions. Risk identification is the most important phase of the risk assessment. Currently cybersecurity domain and cyberattacks are developing so quickly that new approaches are needed to find new kinds of threats and vulnerabilities. This can be related to case examples, checklists or even new methods.

References

- [1] Alanen, J. Linnosmaa, J. Pärssinen, A. Kotelba, and E. Heikkilä, "Review of cybersecurity risk analysis methods and tools for safety critical industrial control systems," 2022.
- [2] Alanen J. *et al.*, "Hybrid ontology for safety, security, and dependability risk assessments and Security Threat Analysis (STA) method for industrial control systems," *Reliab Eng Syst Saf*, vol. 220, Apr. 2022, doi: 10.1016/j.ress.2021.108270.
- [3] Avizienis A, Laprie J-C, Randell B, and Landwehr C. 2004. Basic Concepts and Taxonomy of Dependable and Secure Computing. *IEEE Transactions on Dependable and Secure Computing*, VOL. 1, NO. 1. 23 p.
- [4] Berger J. 2024. STPA Guide. VTT Technical Research Centre of Finland. VTT Research Report No. VTT-R00848-23. 43 p. https://cris.vtt.fi/ws/portalfiles/portal/98296189/Complete_with_DocuSign_2024-1-2_STPA_guide_F.pdf
- [5] Bicaku. A. Security Standard Compliance in System of Systems. Doctoral Thesis at Luleå University of Technology. 2020. 90 p. ISBN 978-91-7790-633-9
- [6] Carreras Guzman N. H., Wied M., Kozine I., and Lundteigen M.A.. "Conceptualizing the key features of cyber-physical systems in a multi-layered representation for safety and security analysis," *Systems Engineering*, vol. 23, no. 2, pp. 189–210, Mar. 2020, doi: 10.1002/sys.21509.
- [7] Carreras Guzman N.H., I. Kozine, and M. A. Lundteigen, "An integrated safety and security analysis for cyber-physical harm scenarios," *Saf Sci*, vol. 144, Dec. 2021, doi: 10.1016/J.SSCI.2021.105458.
- [8] CEN ISO/TR 22100-4:2020. Safety of machinery. Relationship with ISO 12100. Part 4: Guidance to machinery manufacturers for consideration of related IT-security (cyber security) aspects. 23 p.
- [9] EN 60204-1. 2018. Safety of machinery - Electrical equipment of machines - Part 1: General requirements. 150 p.
- [10](EU) COMMISSION DELEGATED REGULATION (EU) 2022/30 of 29 October 2021 supplementing Directive 2014/53/EU of the European Parliament and of the Council with regard to the application of the essential requirements referred to in Article 3(3), points (d), (e) and (f), of that Directive. 5 p. <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R0030>
- [11] (EU) Cyber Resilience Act. Brussels, 15.9.2022. Proposal for a regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU). 103 p. <https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act>
- [12] (EU) Machinery Directive 2006/42/EC. Directive 2006/42/EC of the European Parliament and of the Council of 17 May 2006 on machinery, and amending Directive 95/16/EC (recast). 63 p.
- [13] (EU) Machinery Regulation (EU) 2023/1230 of 14 June 2023. <https://eur-lex.europa.eu/eli/reg/2023/1230/oj>
- [14] (EU) NIS2 Directive. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive). [EUR-Lex - 32022L2555 - EN - EUR-Lex \(europa.eu\)](https://eur-lex.europa.eu/eli/dir/2022/2555/oj) 73 p.
- [15](EU) Critical Entities Resilience Directive. Directive (EU) 2022/2557 of the European Parliament and of the council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC. <https://eur-lex.europa.eu/eli/dir/2022/2557/oj> 35 p.

- [16](EU) Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on liability for defective product. 33p. + 3 att. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2022%3A495%3AFIN>
- [17](EU) Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive). 29 p. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022PC0496>
- [18](EU) REGULATION (EU) 2024/1689 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence). 144 p. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R1689>
- [19](EU) REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act). 55 p.
- [20](EU) Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act). 71 p. <https://eur-lex.europa.eu/eli/reg/2023/2854/oj>
- [21] Giaconia M., Bignalet X. 2021. Demystifying ISA/IEC 62443 and Secure Elements. AN3983. Microchip. 17 p. Retrieved 13.7.2021. <http://ww1.microchip.com/downloads/en/Appnotes/Demystifying-ISA-IEC-62443-and-Secure-Elements-DS00003983.pdf>
- [22] Hauet J-P. 2012. ISA99/IEC 62443: a solution to cyber-security issues? ISA Automation Conference – Doha (Qatar) - 9 & 10 December 2012. 52 p. Retrieved 13.7.2021. http://www.kbintelligence.com/Medias/PDF/ISA_Doha_hauet.pdf
- [23] IEC 61508-2:2010. Functional safety of electrical/electronic/programmable electronic safety-related systems. Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems. 167 p.
- [24] IEC 61784-3:2021. Industrial communication networks – Profiles – Part 3: Functional safety fieldbuses – General rules and profile definitions. 214 p.
- [25] IEC 62061. 2021. Safety of machinery – Functional safety of safety-related control systems. 143 p.
- [26] IEC/TS 62443-1-1:fi:2009. Industrial communication networks. Network and system security. Part 1-1: Terminology, concepts and models. 153 p.
- [27] IEC/TR 62443-3-1:fi. Industrial communication networks. Network and system security. Part 3-1: Security technologies for industrial automation and control systems. 182 p.
- [28] IEC 62443-3-2:2020. Security for industrial automation and control systems - Part 3-2: Security risk assessment for system design. IEC 40 p.
- [29] IEC 62443-3-3:2019. Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels. IEC. 88 p.
- [30] IEC 62443-4-1:2018. Security for industrial automation and control systems - Part 4-1: Secure Product Development Lifecycle Requirements. 60 p.
- [31] IEC 62443-4-2:2019. Security for industrial automation and control systems - Part 4-2: Technical security requirements for IACS components. 100 p.
- [32] IEC 62859:2020. Nuclear power plants - Instrumentation and control systems - Requirements for coordinating safety and cybersecurity. 36 p.
- [33] IEC TS 63074:2023. Safety of machinery – Security aspects related to functional safety of safety-related control systems. IEC 34 p.

- [34] ISO 12100. 2010. Safety of machinery. General principles for design. Risk assessment and risk reduction. 77 p.
- [35] ISO 13849-1. 2023. Safety of machinery Safety-related parts of control systems Part 1: General principles for design. ISO 164 p.
- [36] Kaneko T., Sasaki R., and Takahashi Y. "Threat analysis using STRIDE with STAMP/STPA," 2019.
- [37] Linnosmaa J., Alanen J., Tiusanen R., Berger J., and Malm T. System of systems modelling for safety and cyber-security assessments. VTT Research Report. to be published Autumn 2024.
- [38] Malm T., Ahonen T & Välisalo T. 2018. Risk assessment of machinery system with respect to safety and cyber-security. VTT Research Report VTT-R-01428-18. 26 p.
- [39] Malm T., Heikkilä T. and Ahola J M. Safety Assessment Process for Human-Robot Handling Tasks. 2015 ASME/IEEE International Conference on Mechatronic and Embedded Systems and Applications (MESA). MESA-9 Mechatronics for Advanced Manufacturing August 2-5, 2015, Boston, Massachusetts, USA.
- [40] NIST Special Publication NIST SP 800-82r3. 2023. Guide to Operational Technology (OT) Security. Keith Stouffer, Victoria Pillitteri, Michael Pease, Suzanne Lightman, CheeYee Tang, Timothy Zimmerman, Adam Hahn, Stephanie Saravia, Aslam Sherule and Michael Thompson. 316 p.
<https://doi.org/10.6028/NIST.SP.800-82r3>
- [41] Patterson D. Strategic Project Management: Theory and Practice for Human Resource Professionals. 600 p. <https://ecampusontario.pressbooks.pub/hrstrategicprojectmanagementtheory/>
- [42] SFS-EN ISO/IEC 27000:2020. Information technology. Security techniques. Information security management systems. Overview and vocabulary.
- [43] SFS-ISO/IEC 27005:2022. Information security, cybersecurity and privacy protection. Guidance on managing information security risks. 134 p.
- [44] SFS-ISO 31000:2018. Risk management – Guidelines. 39 p.
- [45] de Souza N. P., C. de César A. C., de M. Bezerra J., and Hirata C. M., "Extending STPA with STRIDE to identify cybersecurity loss scenarios," *Journal of Information Security and Applications*, vol. 55, Dec. 2020, doi: 10.1016/j.jisa.2020.102620.
- [46] Young W. and Leveson N, "Systems thinking for safety and security," in *ACM International Conference Proceeding Series*, 2013, pp. 1–8. doi: 10.1145/2523649.2530277.

Certificate Of Completion

Envelope Id: 8D6366489A9F4B659DE90DC095AA3278	Status: Completed
Subject: DocuSign: CyberFunctionalSafetyComparisonReportFinal	
Source Envelope:	
Document Pages: 56	Signatures: 1
Certificate Pages: 1	Initials: 0
AutoNav: Enabled	Envelope Originator:
Envelopeld Stamping: Enabled	Anne Räsänen
Time Zone: (UTC+02:00) Helsinki, Kyiv, Riga, Sofia, Tallinn, Vilnius	Tekniikantie 21, Espoo
	.., . P.O Box1000, FI-0204
	Anne.Rasanen@vtt.fi
	IP Address: 130.188.17.16

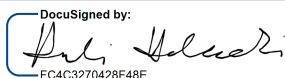
Record Tracking

Status: Original	Holder: Anne Räsänen	Location: DocuSign
20 September 2024 12:26	Anne.Rasanen@vtt.fi	

Signer Events

Heli Helaakoski
Heli.Helaakoski@vtt.fi
Vice President, Cognitive production industry
Security Level: Email, Account Authentication (None), Authentication

Signature

DocuSigned by:

FC4C3270428F48E...
Signature Adoption: Drawn on Device
Using IP Address: 130.188.17.16

Timestamp

Sent: 20 September 2024 | 12:30
Viewed: 20 September 2024 | 12:42
Signed: 20 September 2024 | 12:43

Authentication Details

SMS Auth:
Transaction: 223e0b31-a652-498f-ba1a-27e27958b065
Result: passed
Vendor ID: TeleSign
Type: SMSAuth
Performed: 20 September 2024 | 12:42
Phone: +358 40 5108619

Electronic Record and Signature Disclosure:
Not Offered via DocuSign

In Person Signer Events	Signature	Timestamp
Editor Delivery Events	Status	Timestamp
Agent Delivery Events	Status	Timestamp
Intermediary Delivery Events	Status	Timestamp
Certified Delivery Events	Status	Timestamp
Carbon Copy Events	Status	Timestamp
Witness Events	Signature	Timestamp
Notary Events	Signature	Timestamp
Envelope Summary Events	Status	Timestamps
Envelope Sent	Hashed/Encrypted	20 September 2024 12:30
Certified Delivered	Security Checked	20 September 2024 12:42
Signing Complete	Security Checked	20 September 2024 12:43
Completed	Security Checked	20 September 2024 12:43
Payment Events	Status	Timestamps