




Risk assessment of machinery system with respect to safety and cyber-security

Authors: Timo Malm, Toni Ahonen & Tero Välisalo

Confidentiality: Public

Report's title	
Risk assessment of machinery system with respect to safety and cyber-security	
Customer, contact person, address	Order reference
TecNetwork	
Project name	Project number/Short name
Advanced technologies for productivity-driven lifecycle services and partnerships in a business network	113057 TecNetwork
Author(s)	Pages
Timo Malm, Toni Ahonen & Tero Välisalo	26/
Keywords	Report identification code
safety, cyber-security, machinery	VTT-R-01428-18
Summary	
<p>This report is related to the concern that a cyber-security risk could cause a safety risk and furthermore an accident. There is already a tradition for how to treat safety risks related to automated machinery, but cyber-security is quite new aspect. A cyber-security issue can cause malfunction of a safety function or inherently safe design can be somehow bypassed. When looking the risks in details, it can be seen that the cyber-security/safety risk of automation is usually related to the safety integrity, availability or response time of the safety-related control system. Furthermore, the cyber-security issue is usually related to software and human access to the system.</p> <p>The risk assessment processes for safety and cyber-security have similar phases, but the point of view is different. The cause of an incident is from the safety point of view usually failure, misuse or disturbance of a system whereas from the cyber-security point of view an incident may originate from a threat and vulnerability and in most cases human is causing it.</p> <p>We conclude that it would be difficult to benefit from a complete integration of safety and cyber-security risk assessment processes into a single analysis, because there would be so many aspects to consider and only few mutual effects. It is recommended that the risks assessments are compiled separately, however, any identified safety-critical cyber-security issues should be added to the safety risk assessment process and associated risk treatment be validated according to safety process. The conclusion related to functional safety and cybersecurity can be mutual.</p>	
Confidentiality	Public
Tampere 19.3.2018	
Written by	Reviewed by
	
Timo Malm Senior scientist	Toni Ahonen Senior scientist
	Accepted by
	
	Päivi Kivikytö-Reponen Research team leader
VTT's contact address	
VTT, PL 1300, 33101 Tampere	
Distribution (customer and VTT)	
VTT + internet TecNetwork project partners	
<p><i>The use of the name of VTT Technical Research Centre of Finland Ltd 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></p>	

Preface

This research report is made in TecNetwork project (Advanced technologies for productivity-driven lifecycle services and partnerships in a business network). The main funder of the project is Tekes. Background to this text is Risk 2017 conference (2.-3.11.2017), which was organized by SRA (Society of Risk Analysis). The background for this report are the slides presented at the conference, but the subject is presented here in more details.

The main funder of the project is Tekes (Finnish Funding Agency for Technology and Innovation).

Tampere 19.3.2018

Authors

Contents

Preface.....	2
Contents.....	3
Definitions:	4
1. Introduction.....	5
2. Concepts related to safety and cyber-security.....	7
3. Risk assessment and reduction process.....	11
4. Conclusions	17
References.....	20
ANNEX A: Examples of safety measures related to cyber-security.....	21
ANNEX B: Risk assessment examples.....	23

Definitions:

Asset: Physical or logical object having either a perceived or actual value to a control system. [2]

Attack: Assault on a system that derives from an intelligent threat. [3]

Availability: Property of ensuring timely and reliable access to and use of control system information and functionality [6].

Availability can be defined formally as $(1 - (\text{down time} / \text{total time})) * 100\%$ [Wikipedia]

Conduit: Logical grouping of communication channels, between connecting two or more zones that share common security requirements [4].

Cyber-security: Measures taken to protect a computer or computer system against unauthorized access or attack (ISA 62443-3-2 proposal) [5]

Performance level (PL): Discrete level used to specify the ability of safety-related parts of control systems to perform a safety function under foreseeable conditions. [10]

Risk (machinery): Combination of the probability of occurrence of harm and the severity of that harm (ISO 12100).[9]

Risk (cyber-security): Expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular consequences (ISA 62443-3-2 proposal). [5]

Safety integrity: Probability of an E/E/PE safety-related system satisfactorily performing the specified safety functions under all the stated conditions within a stated period of time. [11]

Safety integrity level (SIL): Discrete level (one out of a possible four), corresponding to a range of safety integrity values, where safety integrity level 4 has the highest level of safety integrity and safety integrity level 1 has the lowest. [11], [12]

Security level: Measure of confidence that the system-under-consideration, security or conduit is free from vulnerabilities and functions in the intended manner. [5]

Threat: (1) 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. [2]
(2) Potential cause of an unwanted incident, which may result in harm to a system or organization.

Vulnerabilities: (1) Inherent weaknesses in systems, components, or organizations that could be exploited or triggered by a threat source. Vulnerabilities may be the result of intentional design choices or may be accidental, resulting from the failure to understand the operational environment.

(2) Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

(3) Weakness of an asset or control that can be exploited by one or more threats.

(4) A flaw or weakness in a system's design, implementation, or operation and management that could be exploited to violate the system's integrity or security policy. [2]

Zone: Collection of entities that represents partitioning of a system-under-consideration on the basis their functional, logical and physical (including location) relationship [4].

1. Introduction

There is a long tradition at machinery sector to make risk assessments considering safety issues. Currently, the assessment is made usually according to ISO 12100 and if the focus is on control systems then often according to ISO 13849-1. Cyber-security issues have emerged to publicity mainly because of the threat associated to expenses and confidentiality. It is evident that security may affect also safety. It is one reason why machine builders have increased their interest in security issues also. This paper is related to cases where cyber-security issues may have an effect on machinery safety. There are already several standard proposals related to the connection between cyber-security and safety, but the field is still evolving. The idea is that security issues must not impair safety, but on the other hand, the required resources must be in line with the risk.

This paper addresses the needs to combine risk assessments to cover both safety and related cyber-security issues. The security issues covered in this case are then limited to safety functions of control systems, communication, safety of machinery misuse (interfaces) and other safety-related situations that are found rare but possible. The information to this report is collected from standards and draft standards. Cyber-security aspects are mainly from drafts, since there are not yet so many standards related to the subject.

Safety-related risk is a function of severity and probability, whereas security risk is a function of negative impact and likelihood. There are similarities, but it is more difficult to put numbers on security risks. Safety risk is usually related to random events, whereas security risk is done on purpose. This means that probability of vulnerability associated to random events can be low, but if the vulnerability is searched on purpose, the probability is meaningless. Security risk may change as technologies or circumstances change, but it does not wear out and a long use history does not necessarily guarantee a secure system. There are some similarities with software and cyber-security validation. Safety software validation is often related to analyses, inspections, walkthroughs, design processes and testing in many phases of design against safety and functionality requirements. Validation of cyber-security of software is more related to how threats, vulnerability and assets are treated against target security levels (SL-T) and other cyber-security requirements.

Standard family IEC/ISA 62443 suggest that there should be target security levels (SL 1 – SL 4), which specify the general risk level and the target to quantify countermeasures against cyber-security risks. There is some similarity to Safety Integrity Levels (SIL according to IEC 61508 and IEC 62061 [12]) and to Performance Levels (PL according to ISO 13849-1) [10], which are applied to measure safety risk and related protective measures of machinery safety functions. All four of the mentioned standards ([5], [10], [11], [12]) are related to automation and control systems. In that field, there is a need to compare risks and risk reduction measures in order to direct resources according to the risk levels.

The classification of functional safety is relatively mature. The categories of machinery control systems (currently part of PL determination) were introduced 1996 (EN 954-1), SILs 1999 (IEC 61508-1) and PLs 2007 (ISO 13849-1). The history of safety classification dates back to 1980's as IEC 1508 development and some national standards (Germany and UK). Currently there is a development to merge SILs and PLs, but it is difficult. The security levels were introduced 2009 (IEC/TS/ISA 62443-1-1). Apparently, the security levels are not yet applied so widely in automation as SILs or PLs.

One aspect to the relation between safety and cyber-security risks is that according to Machinery Directive [8] the machine builder (or authorized representative) must consider in risk assessment "intended use and any reasonably foreseeable misuse thereof". Many

cyber-security risks can be associated to “reasonably foreseeable misuse”. Machinery Directive is related to safety, but if cyber-security issue can affect safety, it should be considered.

Although, the risk assessment from safety and security point of view have many similarities it is still difficult to integrate the security risk assessment to safety risk assessment. Many safety requirements are obligatory, but from the safety point of view measures against security risks are voluntary, unless there is a clear connection to a safety issue e.g. reasonably foreseeable misuse. Without systematic approach combining safety and security, it can e.g. be difficult to say that a specific security issue has no effect on safety. Current paper contributes to the development of the integrated approach and brings out its pros and cons. It can be said that safety and cyber-security have:

- Independent domains; different persons are dealing with the subjects.
- Little interaction; similarities in risk reduction are not noticed.
- Common infrastructure; safety and security issues are related to the same devices.
- Conflicting responsibilities? In many cases different persons are controlling the domains and responsibility of the entity is not clear.

Suzuki describes in his text the relationship between security, safeguards and safety in nuclear industry [14]. Figure 1 describes how security, safeguards and safety are settled to frequency and law axis. It describes also how probabilistic means are applied to estimate different situations. The figure has heuristic features as Suzuki mentions, but yet there are historical incidents (35 incidents) behind it. Security incidents have been more rare than safety incidents, but all severe safety and security incidents are rare.

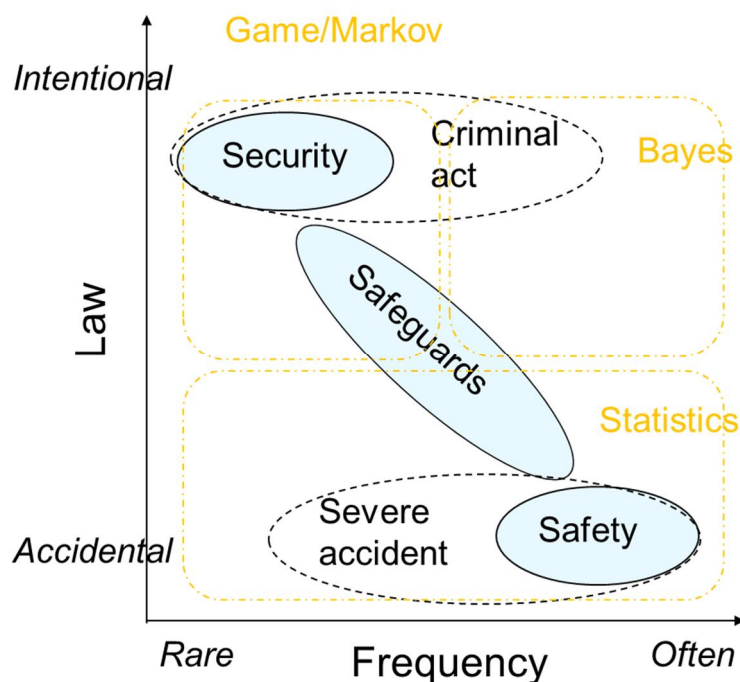
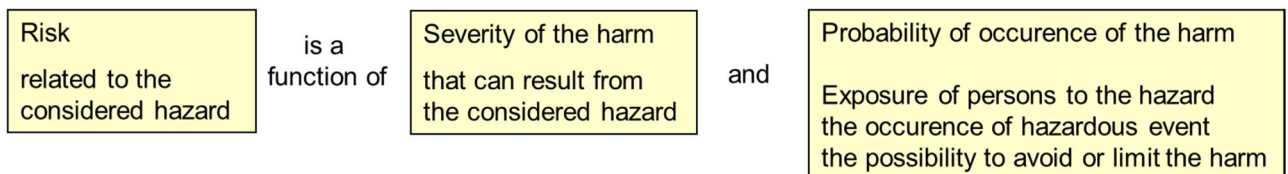


Figure 1. Relationship between Security, safeguards and safety. [14]

2. Concepts related to safety and cyber-security

The following text presents mutual issues in cyber-security and safety risk assessments from the machinery and their control system point of view. Figure 2 shows the definitions of machinery risk and cyber-security risk. It can be seen that severity of harm corresponds to negative impact (cyber-security) and probability of occurrence corresponds to vulnerabilities and associated threats. It can be easier to say probability of occurrence according to exposure to hazards, statistics of accidents, possibility to avoid hazard and probability of initial event to trigger accident. The history of events can predict the future, especially, in stochastic (random) cases. In cyber-security, the likelihood of a negative impact can usually be only estimated according to threat and vulnerability. There could be history data of threats related to amount of attacks, which could help in risk estimation [5]. Vulnerability is related more to design and procedures. One problem is that often vulnerabilities are kept secret to minimize threats. In general, cyber-security is usually related to human actions, which are more difficult to estimate than safety-related probabilities of failures.

Machinery safety risk



IT-security risk (Cyber security risk)

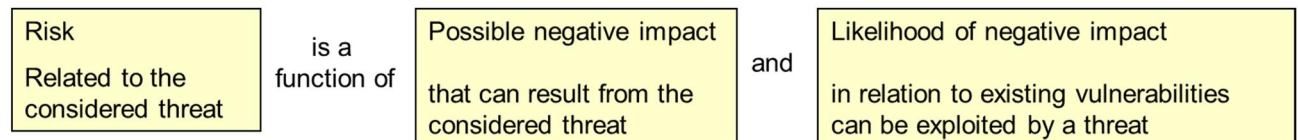


Figure 2. Definitions of machinery safety risk and cyber-security risk.[5]

The objectives related to machinery safety and cyber-security risk assessment are described at Table 1. The comparison of functional safety and cyber-security is presented at Table 2.

Table 1. Principle objectives of machinery safety and cyber-security. [7]

	Machinery safety	Cyber-security
Objectives	Injury/accident prevention, health (avoidance of harm)	Availability, integrity, confidentiality
Conditions (risks, methods, measures)	Transparent (not confidential)	Confidential (not shared with machinery user)
Dynamics	Rather static field (intended use, reasonable foreseeable misuse)	Highly dynamic field; moving target (intentional manipulation, criminal intent)
Risk property	Risk is often related to random events or software properties	The risk is often related to deliberate malicious human actions

	Machinery safety	Cyber-security
Risk reduction (mitigation) measures	Mainly by machine manufacturer at a dedicated time (when providing the machine for the first use)	By various actors (machine manufacturer, system integrator, machine user, service provider) at any time along the overall life cycle.

Table 2. Comparison of functional safety and cyber-security [4].

Lifecycle phase		Functional safety	Cyber-security
Risk analysis	Type of evaluation	Equipment under control	Zones and conduits based on logical grouping of assets
	Failure likelihood	Random failures due to operational and environmental stress Systematic failures due to errors during safety life cycle	Threats: internal, external or combination Vulnerabilities due to <ul style="list-style-type: none"> - component or system design flaws - making non-valid changes - not following security practices and procedures - threats exploiting vulnerabilities leads to failure
	Consequence severity	Impact on environment health and safety of personnel and the general public	Loss of availability and/or data integrity has direct impact and loss of confidentiality has indirect impact on functionality
	Risk categorization	Based on likelihood and severity; risk may be quantified	Based on likelihood and severity, risk is currently qualitative. Risk categorization for every security requirement Multi-dimensional problem Assigned to zone with target SL for each zone/conduit

Lifecycle phase		Functional safety	Cyber-security
	Risk mitigation measures	<p>Relies on independent protection layers concept</p> <p>Safeguards reduce likelihood of consequence evaluated</p> <p>Identifies integrity requirements for safeguards; for safety function assigns target SIL</p>	<p>Relies on security counter measures within zone, within conduits connected to the zone, and defense indepth concept</p> <p>Countermeasures reduce likelihood</p> <p>Identify requirements for countermeasures to meet the zone target SL for each threat vector</p>
	Implementation measures	<p>Safety manual for components</p> <p>Quantitative SIL verification for safety functions</p>	<p>Security manual for components</p> <p>Verification through different levels of testing for target SL</p>
	Operation and maintenance	<p>Restrict access to control system components to competent personnel with necessary access privileges</p> <p>Periodic testing of measures</p> <p>Demand rate and component failures to be monitored</p> <p>Awareness and training</p>	<p>Restrict access to control system components to competent personnel with necessary access privileges</p> <p>Periodic testing of measures</p> <p>Frequent reviews to identify new vulnerabilities and take appropriate action, necessary</p> <p>Awareness and training</p> <p>Cyber risk reassessment after each software or hardware change</p>
	Management system	<p>Defines requirements for competency, training, verification, testing, audit and documentation</p>	<p>Defines requirements for competency, training, verification, testing, audit and documentation</p>

The safety and cyber-security risk assessment and risk reduction process can be presented in block diagram format to see mutual phases. Similarities can be found also by looking attributes or properties of software.

Figure 3 shows mind map of cyber-security and functional safety. There are also other connections than shown in picture, but these are the main relations. Cyber-security is violated through assets, which are associated to design and systematic (software) failures and the cause is related to threat and vulnerability. Functional safety risk is associated to inherently safe system and safety function failure. Safety function failure means that the function is silent or its performance is hazardous. Furthermore, the reason to safety function failure is usually integrity, availability or response time change, which are initiated by software, design or hardware failures. The asset (see definition) can be associated to software and hardware, but here, since hardware failures are more associated to functional safety, no straight connection is drawn between them. Misuse prevention and deliberate human initiated attack may have some mutual aspects, like authentication, use control and encryption.

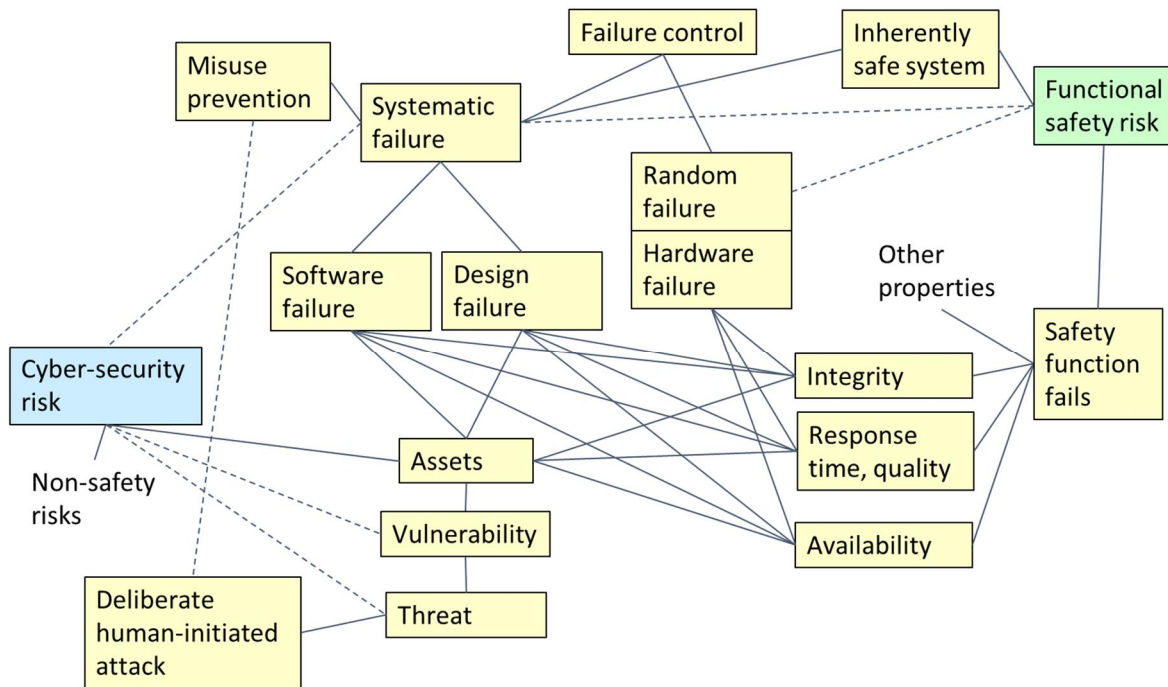


Figure 3. Mind map of cyber-security and functional safety.

One important issue related to control system and cyber-security risks is classification. Both the risks and means to minimize risks can be categorized according to risks and corresponding requirements. The requirements are associated to the rigor and extent to minimize the risk.

Figure 4 shows how performance level (PL_r) requirements are assigned by applying risk graph. The figure shows also the equivalence to safety integrity levels (SIL). SIL assignment is shown at Figure 5. Performance Level (PL) includes safe performance of electronics, hydraulics, pneumatics and mechanics and it is applied often in machinery sector. SIL is related to programmable safety systems in many branches of industry. When PL or SIL requirement for a safety function is known then the relevant parts of the control system can be designed according to the associated requirements.

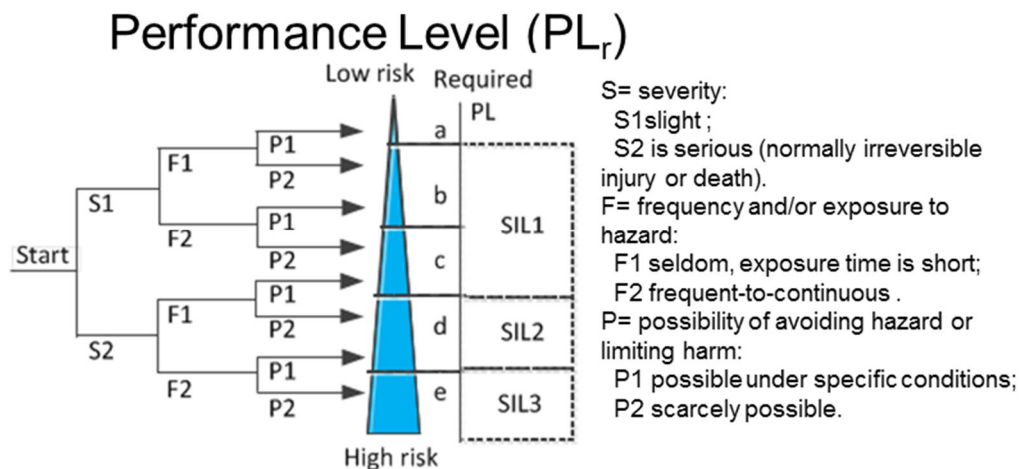


Figure 4. Risk graph shows how required performance level can be determined. [10]

Safety Integrity Level (SIL)

Consequences	Severity Se	Class Cl					Frequency and duration Fr	Probability of hazardous event		Avoidance	
		3-4	5-7	8-10	11-13	14-15		Pr	Av		
Death, losing an eye or arm	4	SIL 2	SIL 2	SIL 2	SIL 3	SIL 3	<= 1 hour	5	Very high	5	
Permanent, losing fingers	3			SIL 1	SIL 2	SIL 3	> 1 h - <= day	5	Likely	4	
Reversible, medical attention	2			SIL 1	SIL 2		>1 day - <=2 weeks	4	Possible	3	Impossible 5
Reversible, first aid	1				SIL 1		>2 weeks - <=1 year	3	Rarely	2	Possible 3
							> 1 year	2	Negligible	1	Likely 1

Figure 5. Risk matrix shows how required Safety Integrity Level (SIL) can be defined. [12]

The security levels or actually target security levels (SL-T) are estimated according to estimated risk. Table 3 describes the security levels.

Table 3 Security levels. [5]

Security level	Description
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, IACS (Industrial Automation Control Systems) specific skills and moderate motivation
SL 4	Protection against intentional violation using sophisticated means with extended resources, IACS specific skills and high motivation.

3. Risk assessment and reduction process

Figure 6 shows the risk assessment and risk reduction process according to ISO 12100. The described process can be associated to machinery. The part on the left shows the risk assessment and on the right risk reduction. If the risk is not tolerable, it is possible to go back to the beginning and change, for example, the intended use (e.g. forbid a specific use). Designers (or manufacturer) apply the main process of risk assessment and reduction. At the bottom right are the tasks, which are targeted for the user.

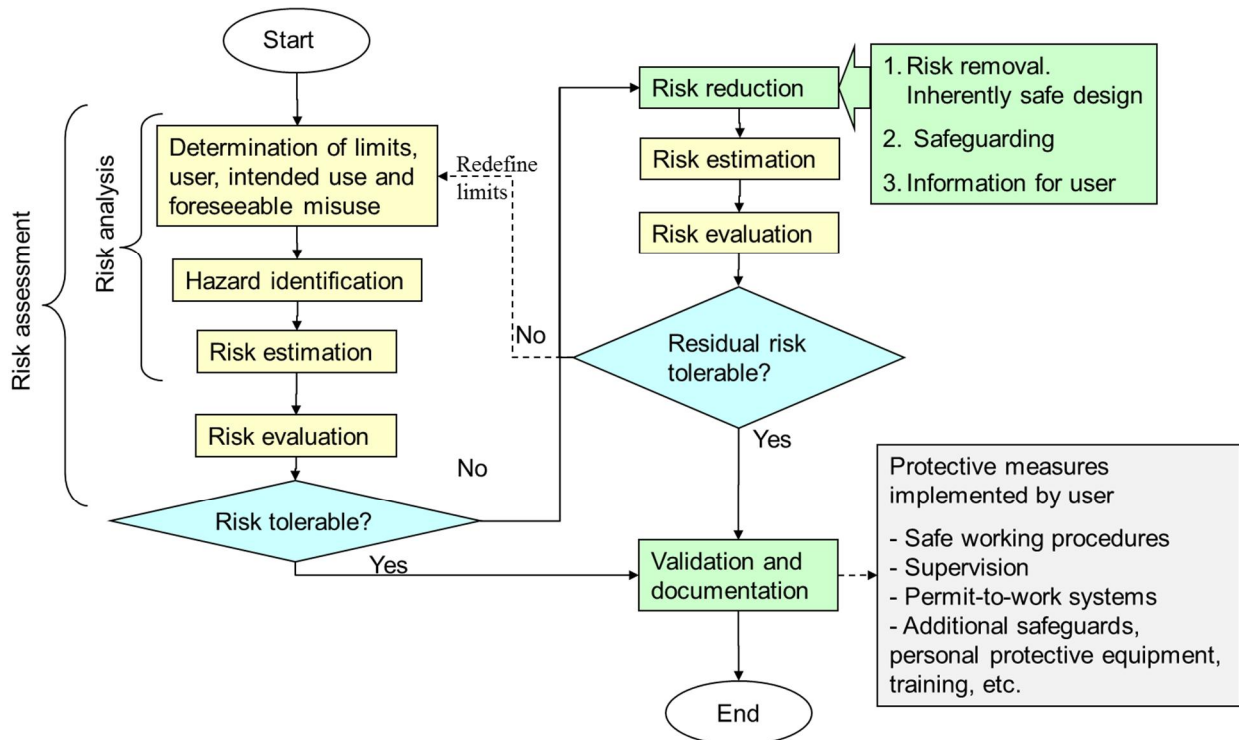


Figure 6 Risk assessment and risk reduction process (ISO 12100). [9]

Cyber-security standard proposal for machinery (ISO TR 22100-4 proposal) “Guidance to machinery manufacturers for consideration of related IT-security (cyber-security) aspects” describes shortly the process for cyber-security (see Figure 7) [6].

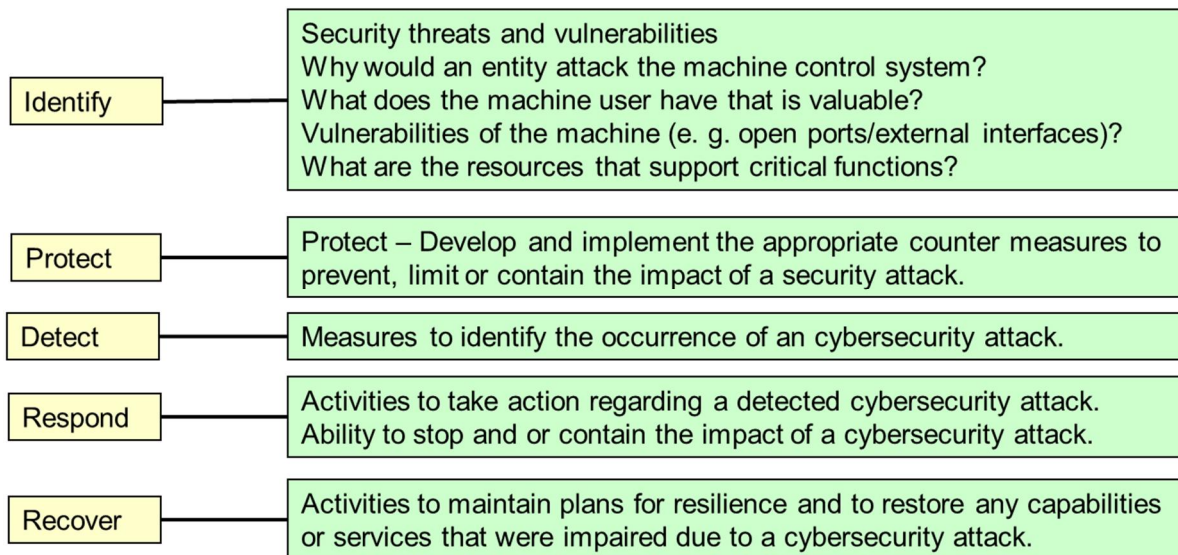


Figure 7 Steps to provide cyber-security for machinery. [6]

Figure 8 shows the comparison between risk assessment of machinery and information technology. Both processes have identification, estimation and evaluation tasks, but the names and targets differ. The process for cyber-security is here obtained from information technology, since the process seems, currently, more mature than the machinery sector process (cmp. ISO TR 22100-4 proposal).

Machinery safety risk

Cyber-security risk

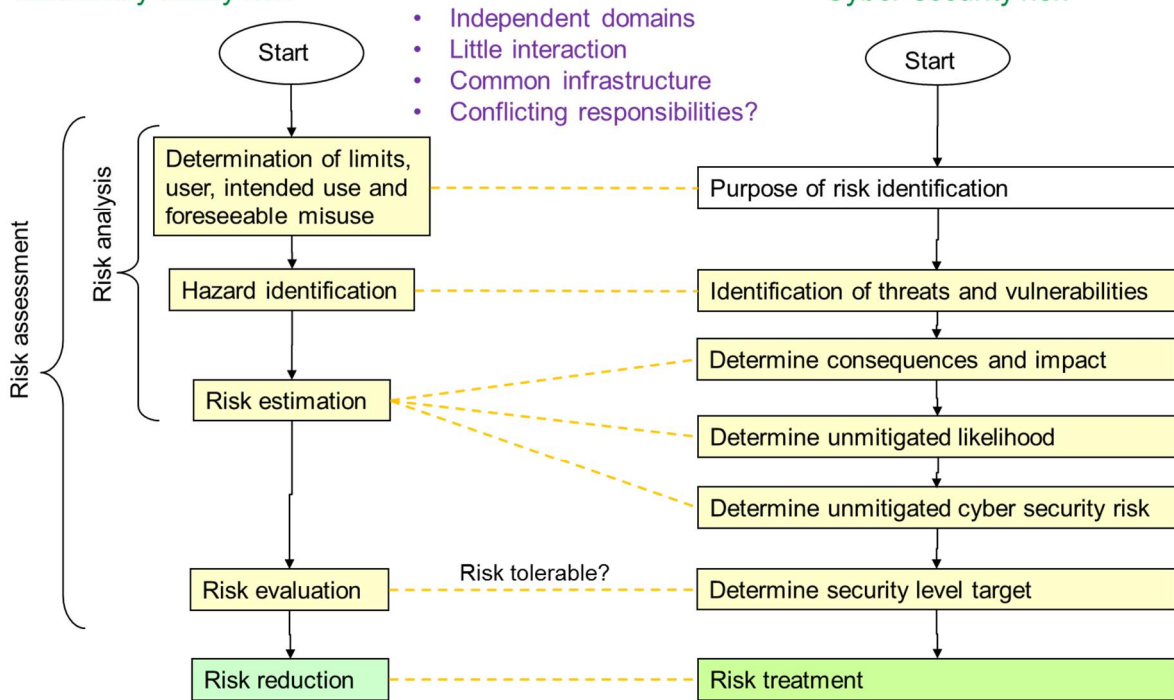


Figure 8 Comparing risk assessment process for machinery and information technology. [9], [5]

Figure 9 shows the risk reduction process of safety related machinery control system and cyber-security process related to functional safety of control systems. One can see that after or during the risk assessment process the target safety/security level is defined. This needs to be done in order to define the extent and rigor of the safety/security measures. The security levels are described at Table 3, safety integrity levels at Figure 5 and performance levels at Figure 4. The cyber-security process at Figure 9 shows also that in some cases a safety function may have safety and cyber-security features and then both requirements need to be fulfilled.

Machinery control system safety risk

Cyber-security risk

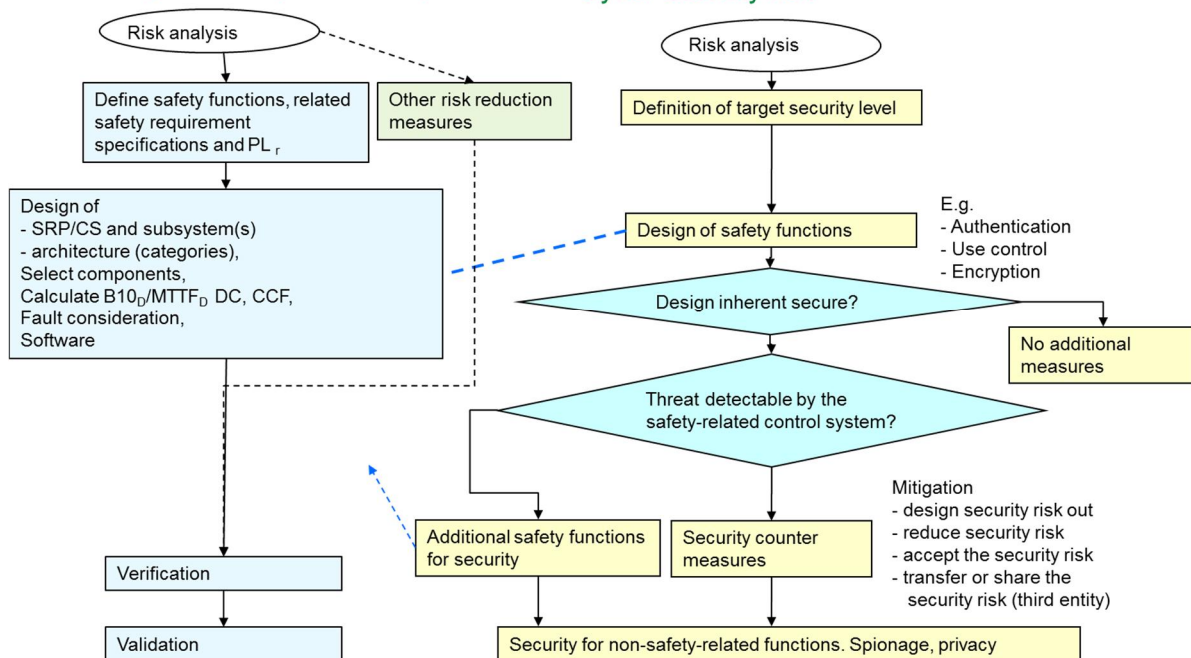


Figure 9 Comparing safety and cyber-security risk reduction processes related to functional safety of control systems. [10], [2]

Cyber-security affects many domains, but only some issues are related to safety. Here are two lists of cyber-security topics:

Security categories should cover (IEC 62443-2-1 / IEC 27001) [2]:

Information security policies, Organization of information security, Human resource security, Asset management, Access control, Cryptography, Physical and environmental security, Operations security, Communications security, System acquisition development and maintenance, Information security, aspects of business continuity management, Compliance, Supplier relationships.

IEC 62443-3-3 [6]: Identification and authentication, Use control, System integrity, Data confidentiality, Restricted data flow, Timely response to events, Resource availability.

It is clear that at least timely response to events and resource availability have a connection to safety. In both cases, if a safety function cannot be performed in time, then a hazard is possible. Other aspects in the list may have indirect effects on functional safety.

Also Machinery safety standard proposal considers the threats related to cyber-security and machinery safety. It gives also examples of counter measures (see Annex A). The following list considers cyber-security threats and relevance to machinery safety [7]:

- Access to data/know-how from the machine manufacturer or from the machine user (process know-how) – No machinery safety relevance.
- Creation of economic damage to the machine user – unlikely, but possible.
- Creation of hazard of machinery and/or people (operator, bystanders) – unlikely, but possible
- Creation of damage to infrastructure and/or people (operator; bystanders), e.g. a terroristic act – relevant.

Figure 10 shows the dependencies of dependability and cyber-security associated to software. Fault and error can lead to failure, which can cause problems to dependability. The problems can be related to reliability, safety, maintainability, integrity and availability. The preventive actions are related to prevention (e.g. testing, validation), tolerance (e.g. redundancy), removal (e.g. diagnostics) and forecasting (maintenance). In cyber-security domain, threat and associated vulnerability can cause negative impact (cmp. failure). Negative impact can be mitigated by designing risk out, by limiting the risk, by accepting risk or by transferring the risk to a third entity. The negative impact can effect on confidentiality, availability and integrity. Integrity and availability may have a connection to safety and furthermore dependability.

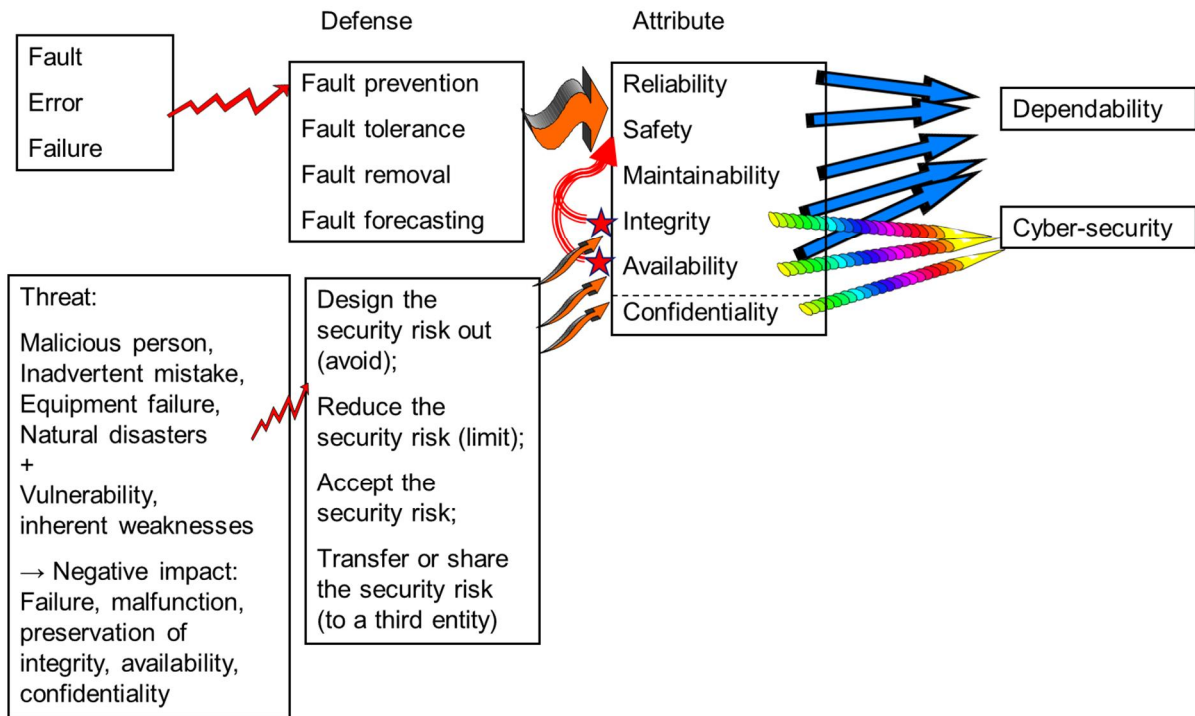


Figure 10 Taxonomy related to dependability and cyber-security in software domain. [1], [2]

Figure 11 shows how security threat can lead to failure or malfunction of safety-related control system. Typical cyber-security aspects to be considered are [2]:

- identification/authentication; all users are identified/authenticated before access to the system,
- use control; assigned privileges,
- system integrity; prevent unauthorized manipulation,
- data confidentiality; not relevant for safety integrity,
- restricted data flow; limit unnecessary flow of data,
- timely response to events; respond to security violations,
- resource availability; ensure availability against denial of essential services.

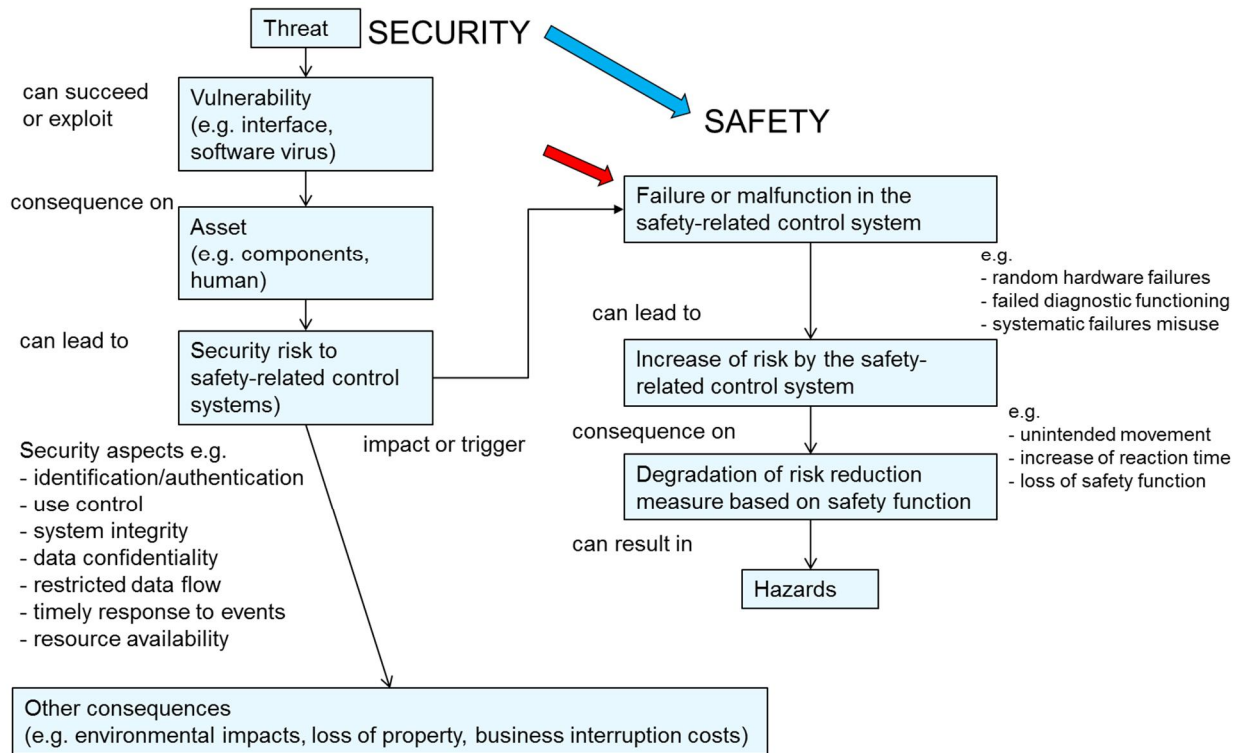


Figure 11 Security threat may lead to safety issue. [2]

Figure 12 shows how security threat can affect a machine [6]. A threat can exploit a vulnerability of the safety-related control system, which can lead to malfunction or inadequate performance of a safety function. The safety functions are affecting clearly safeguarding or complementary safety measures. In addition, the standard sees a possibility to affect also inherently safe design measures; this this can be related e.g. to deliberate removal of a structure or change of circuits. The machine cyber-security standard [6] points out following aspects to be considered carefully: identification/authentication, system integrity, timely response to events and availability.

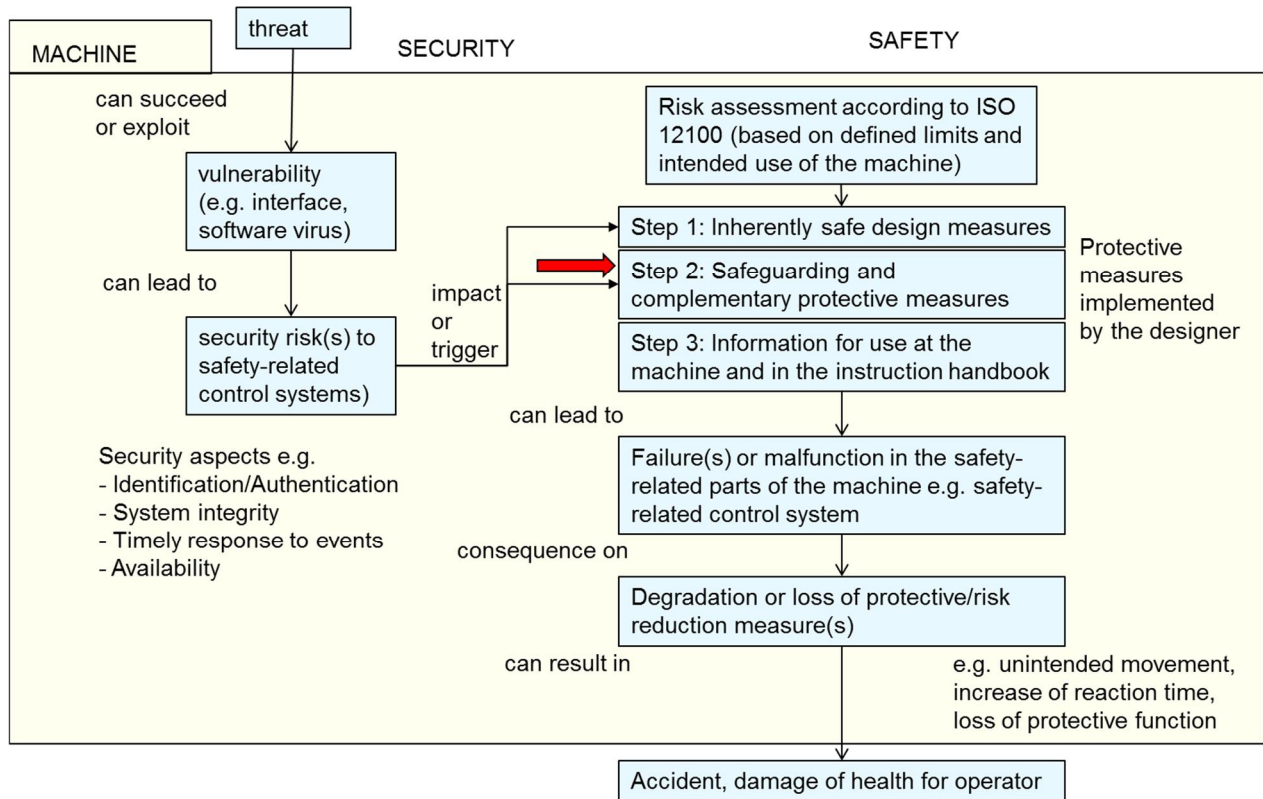


Figure 12 Security threats and consequences to safety. [6]

4. Conclusions

Figure 13 shows the conclusion of safety and cyber-security process for safety-related machinery control system. On the left side is the basic design process according to ISO 13849-1. On the right side are the cyber-security aspects, which need to be considered. When a safety function has both safety and cyber-security dimensions, one needs to categorize safety level (SIL or PL) and security level (SL-T). Then the safety and cyber-security measures correspond the defined risk. The final verification and validation are included in the safety process. It is possible that some cyber-security counter measures need to be validated also in the safety process, because counter measures might block the availability of a safety function.

Standards [13], [6], [2] and [5] offer checklists among others for cyber-security threats, vulnerabilities and counter measures. It is advisable to apply such checklist when identifying the cyber-security risks. The standards show also, which factors should be considered for each cyber-security risk. The list of factors can include e.g. threat, vulnerability, asset, consequence, SL-T and counter measures.

Functional safety of machinery control systems and cyber-security have common risks, which are related mainly to timely response, availability, restricted data flow and integrity. Other aspects, like, reliability is possible. For example Stuxnet¹ worm did affect speed of

¹ Wikipedia: <https://en.wikipedia.org/wiki/Stuxnet>

centrifuges and therefore also reliability. Safety aspect may be indirect. In some demos, car brake control was hacked² and it did have an effect on safety and other dependability factors.

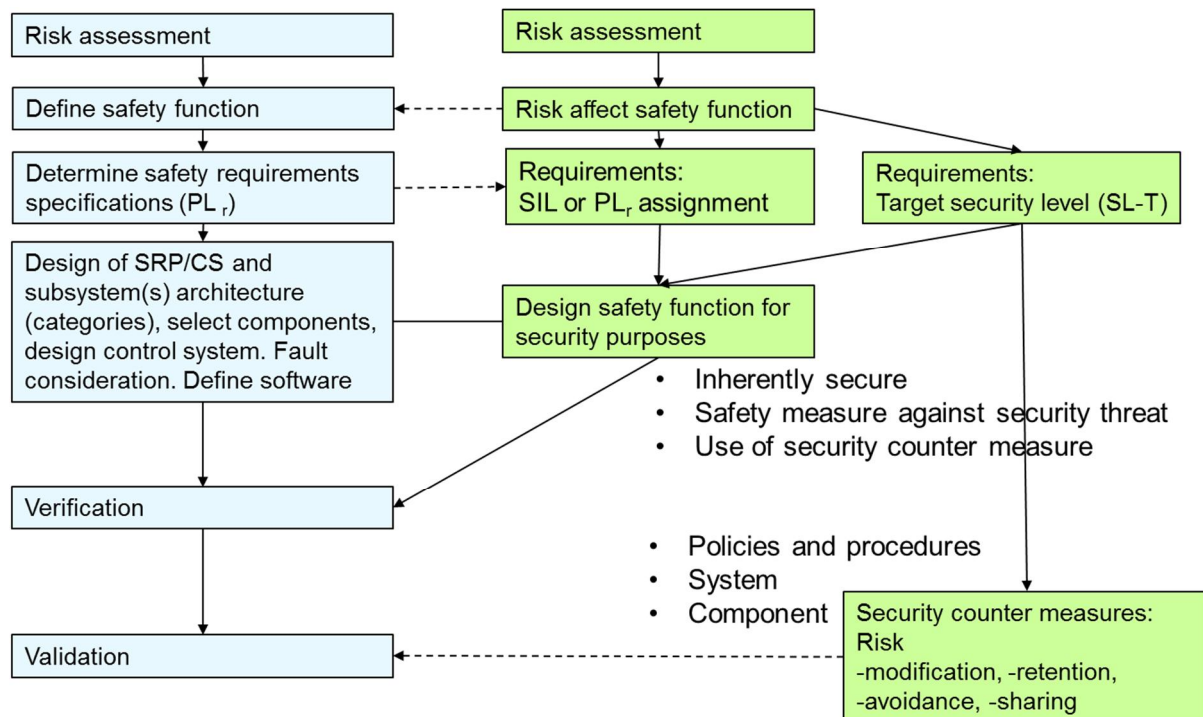


Figure 13 Cyber-security aspects added to machinery control system process. [10]

Functional safety risks are related to random (stochastic) and systematic failures. Random failures can be estimated when there is knowledge of component failure data and model and environment of the device. Such aspects can only seldom be linked to cyber-security, since malicious attacks search vulnerabilities, which may have low probabilities if they are associated to random events, but probability is meaningless, if the vulnerability is applied on purpose.

Systematic failures are related to design and software failures. Systematic failures may well have a connection to vulnerability of a device and furthermore to cyber-security. Especially, software can have a lot of vulnerabilities and also possibilities for defense. Cyber-security aspects should be considered in the assessment of software. Cooperation of safety and cyber-security experts would be beneficial, especially, when the safety and cyber-security demands are high.

A common means to reduce cyber-security and safety risks is isolation of machine control system and safety control system. Isolation can guarantee that unauthorized or sometimes even authorized modifications are not possible. Total isolation is often too hard requirement, since authorized modifications are needed. On the other hand, integrated safety/machine control system allows access to control system and it may be difficult to prevent access to the safety control system. Anyway, separated safety control system is more expensive to establish (more components), easier to modify (separated validation process for safety system) and cyber-security issues are easier to control. In many cases, communication between safety and ordinary control system requires a channel for data exchange.

High cyber-security requirements may urge the designer to separate safety and machinery control systems. Then from the safety point of view, if there is vulnerable access to the

² <https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/>

machine control system, but not to the safety control system, it is assumed that machinery control system does not affect safety or at least safety system can handle all safety issues. This may be true when the machine is not very quick and safety system has enough time to respond.

The safety and cyber-security risk assessment and risk reduction processes have many similar phases and the target is often the same, but major part of the risks do differ. If only one analysis were made, it would mean that all risks should be considered from both safety and cyber-security point of view. Since the risks differ so much, this would mean that for most cases the considerations would be done in vain i.e. it is not practical to consider cyber-security issues, like threat and vulnerability, related to e.g. all relay failures. Therefore, it is good to separate cyber-security and safety analysis. This is the case, especially, in bottom-up type analyses (e.g. HAZOP, FMEA, PHA), which intend to find new risks. One aspect is that cyber-security threats are related assets or larger units, and a vulnerability can be associated to many threats and consequences. Safety risk factors have typically more focused causal relationships. It is good to have both safety and cyber-security experts in the processes. It would be difficult to benefit from complete integration of safety and cyber-security risk assessment.

Acknowledgements:

The main funder of the project is Tekes (Finnish Funding Agency for Technology and Innovation).

References

- [1] Avizienis, Algirdas; Laprie, Jean-Claude; Randell, Brian; Landwehr, Carl. 2004. Basic Concepts and Taxonomy of Dependable and Secure Computing. In: IEEE Transactions on Dependable and Secure Computing (Volume: 1, Issue: 1, Jan.-March 2004) pp. 11-33.
- [2] EN ISO/IEC 27001:2017. Information technology - Security techniques - Information security management systems – Requirements. 27 p.
- [3] IEC proposal 2016. Security aspects related to functional safety of safety-related control systems. 24 p.
- [4] ISA 62443-1-1: 2017. Security for industrial automation and control systems. Models and concepts. 114 p.
- [5] ISA/IEC 62443-3-2: 2017 draft. Security for industrial automation and control systems -Security risk assessment, System partitioning and Security levels. 36 p.
- [6] ISA/IEC 62443-3-3: 2013. Security for Industrial automation and control systems. Part 3-3: System security requirements and security levels. 81 p.
- [7] ISO/DTR22100-4 proposal: 2018. Safety of machinery – Relationship with ISO 12100 – Part 4: Guidance to machinery manufacturers for consideration of related IT-security (cyber security) aspects. 15 p.
- [8] 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.
- [9] SFS-EN ISO 12100. 2010. Safety of machinery. General principles for design. Risk assessment and risk reduction. Finnish Standards Association SFS. 172 p.
- [10] SFS-EN ISO 13849-1. 2015. Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design. Finnish Standards Association SFS. 193 p.
- [11] SFS EN 61508-4:2010. Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 4: Definitions and abbreviations. 67 p.
- [12] SFS-EN 62061. 2005. Safety of machinery – Functional safety of safety-related electrical, electric and programmable electronic control systems. 198 p.
- [13] SFS-ISO/IEC 27005:2013. Information technology - Security techniques - Information security risk management. 126 p.
- [14] Suzuki, Mitsuo. 2018. Integrated Risk Assessment of Safety, Security, and Safeguards. In: Risk assessment. Ed. Svalova, Valentina. Pub. InTech. pp. 133-151. ISBN 978-953-51-3799-3.

ANNEX A: Examples of safety measures related to cyber-security

Table A4. Example of protective measures related cyber-security of machinery. [7]

Protective area	Protective measure	Responsibility
General	Using pertinent standards	Machine manufacturer, system integrator or end user
Restriction of logical/physical access to the IT-system (with possible influence on safety)	Physical separation of safety relevant IT-system from overall IT-system	Machine manufacturer, system integrator or end user
	Provision of IT-system with risk reduction measures (e.g. firewalls, antivirus tools)	Machine manufacturer, system integrator or end user
	Preservation of the risk reduction measures of the IT-system in an actual secure mode (e.g. update of antivirus tools)	End user
	Provision of means allowing a software upgrade	Machine manufacturer or system integrator
	Provision of separate authentication and access control mechanisms (e.g. card readers, physical locks)	Machine manufacturer or system integrator
	Provision of a network topology with multiple and independent layers	Machine manufacturer or system integrator
	Restriction of IT-system user privileges to only those that are required for each person's role	End user
	Disabling of all unused ports and services	End user
	Responsibility for individual user accounts and the account management (e.g. update of passwords)	End user
	Provision of the machine with means for an authorization check of the players/services after every authentication.	Machine manufacturer or system integrator
	Provision of the machine with physical hardware measures to bring it into safe state in the case of a severe security attack. (e.g. emergency stop, shut down button)	Machine manufacturer or system integrator
	Physical restriction of access or use of IT connection points (e.g. USB or Ethernet sockets)	Machine manufacturer, system integrator or end user

Protective area	Protective measure	Responsibility
	Disconnection or deactivation of accessible IT connection points (e.g. USB or Ethernet sockets)	Machine manufacturer, system integrator or end user
	Observation of instructions for use of component manufacturers regarding <ul style="list-style-type: none"> — the use of IT connection points, — the phase of the life cycle of the machine in which the connection is required, — the duration of the required connections, — the IT interface (HW/SW) specified by the component manufacturer, — the access restriction to the application SW specified or recommended by the component manufacturer. — the use of (turn on) passwords and antivirus tools — changing the initial default password at installation, and frequently thereafter. 	Machine manufacturer, system integrator or end user
Detection and reaction on security events and incidents (with possible influence on safety)	Provision of the machine with capability to detect failed IT-system components or unavailable services	Machine manufacturer or system integrator
	Provision of the machine with means for monitoring of vulnerabilities	Machine manufacturer or system integrator
	Responsiveness and reaction to vulnerabilities	End user
In the case of remote maintenance and service	Provision of means for setting up and ending of a remote access session Provision of means on the machine that have priority over remote access commands. Provision of means independent of software so that they cannot be bypassed remotely. Provision on incoming access limits to specific times or individuals rather than leaving the lines continuously open (an arranged rendezvous between two people).	Machine manufacturer or system integrator
	Monitoring of any remote access session (restriction of duration for remote access)	End user
	Means for use of encryption for initiating a remote maintenance/remote service	Machine manufacturer or system integrator

ANNEX B: Risk assessment examples

Risk assessment associated to safety of machinery system

Safety risk assessment is required for a system during design phase and during modification. Usually the risks are not changing unexpectedly and therefore modifications are good phase for risk assessment. Sometimes, a new risk may become known, for example, because of an accident or incident and therefore a specific risk needs to be assessed between modifications. Also a change in responsibilities related to, for example, company acquisition, can initiate risk assessment, since new owner wants to know the current risks from their point of view.

Preliminary hazard analysis (PHA) is typical analysis to find risks related to machinery (see Figure B14). The analysis is often made according to the list of potential hazards given in standard ISO 12100. In all of these risk assessments all factors at the same row are associated to each other i.e. the described consequences and preventive actions are related to the same risk.

	Type of group	Origin	Potential consequences	Hazard	Consequences	Risk Index	Preventive actions
1	Mechanical hazards	<ul style="list-style-type: none"> - movements of any part of the robot arm (including back), end-effector or mobile parts of robot cell - movements of external axis (including end-effector tool at servicing position) - movement or rotation of sharp tool on end-effector or on external axes, part 	<ul style="list-style-type: none"> crushing shearing cutting or severing entanglement drawing-in or trapping impact stabbing or puncture friction, abrasion high-pressure fluid/gas 	Robot arm can move when a person is beside the robot.	Robot arm or load crushes the worker against a rigid object.	High	Distance from the robot can be increased by locating the pendant to suitable distance from the suction cup. The distance can be arranged by

Figure B14. Example of PHA (Preliminary hazard analysis) analysis.

HAZOP (Hazard and operability study) resembles PHA, but the items are considered according to guide words, which can help to consider hazards. Guide words can be related to specific field of technology. It is not necessary to consider the causes an accident (only guide words) and this may speed up the analysis process. Figure B15 shows an example of HAZOP analysis.

Product, system:		Koe		Version: 2.3 eng				Annex 1			
Analysis:		HAZOP						8.4.2013			
Compilers:											
No	Component	Guide word	Deviation, scenario, consequences	Risk rating beginning			Preventive actions and residual risk	Risk rating			Remarks, responsible person
				C	P	R		C	P	R	
A1	Camera	No	No signal, the failure can be seen immediately.	1	c	L		1	c	L	
A2	Camera	Other than	Wrong camera connected.	4	b	M	Guidance and cable markings are required to avoid wrong assembly. The system must be tested before use.	4	a	L	
A3	Camera	More	Camera is sending still picture.	4	b	M	The camera cannot generate a valid still picture.	4	a	L	
A4	A/D	No	No signal, the failure can be seen immediately.	1	b	L	Time stamp is added to the picture.	1	b	L	

Figure B15. Example of HAZOP analysis.

Fault tree analysis (FTA) is applied to see what a combination of events can cause. Usually the basic events are already known and they are not invented in the analysis. Analysis begins at top event and the causes are then considered and drawn in the fault tree (see Figure B16). FTA can be applied also to calculate the probability of the top event.

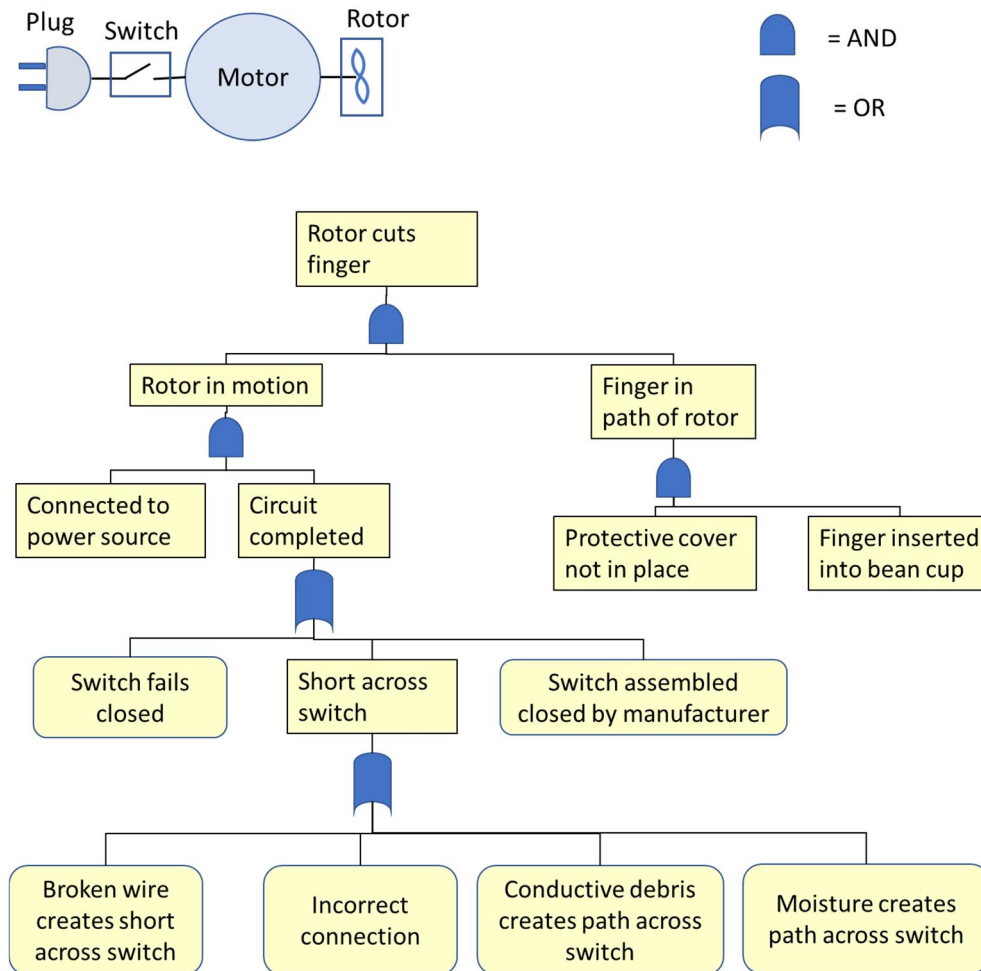


Figure B16. Fault tree analysis to a coffee mill.

Risk assessment associated to cyber-security of machinery system

Cyber-security risk assessment is required for a system during design phase, during modification and also if some circumstances change. The threat may change even if the system remains same. For example, importance of a system may change or a vulnerability may be revealed in public and therefore the system may become a target for a malicious attack without any changes to the system. This means that cyber-security audits are needed more often than safety estimations. The cyber-security life cycle is presented at Figure B17. The reasoning for tasks are presented at Figure B18.

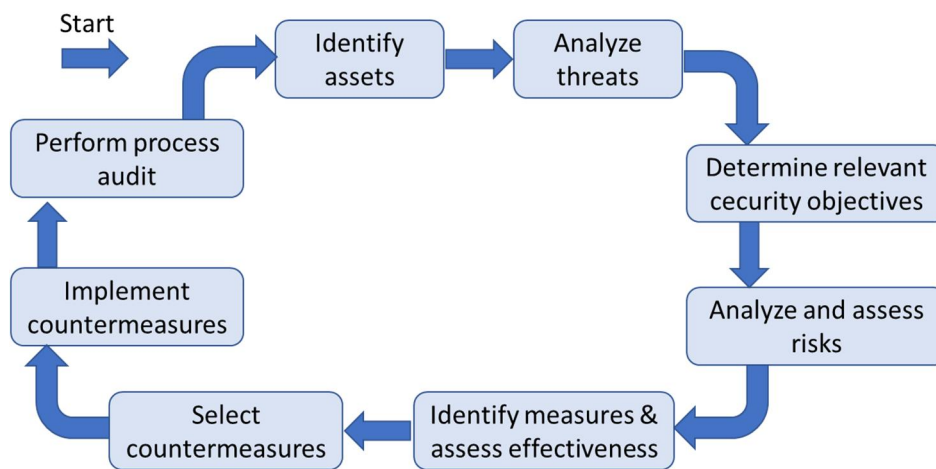


Figure B17. Life cycle steps. [4]

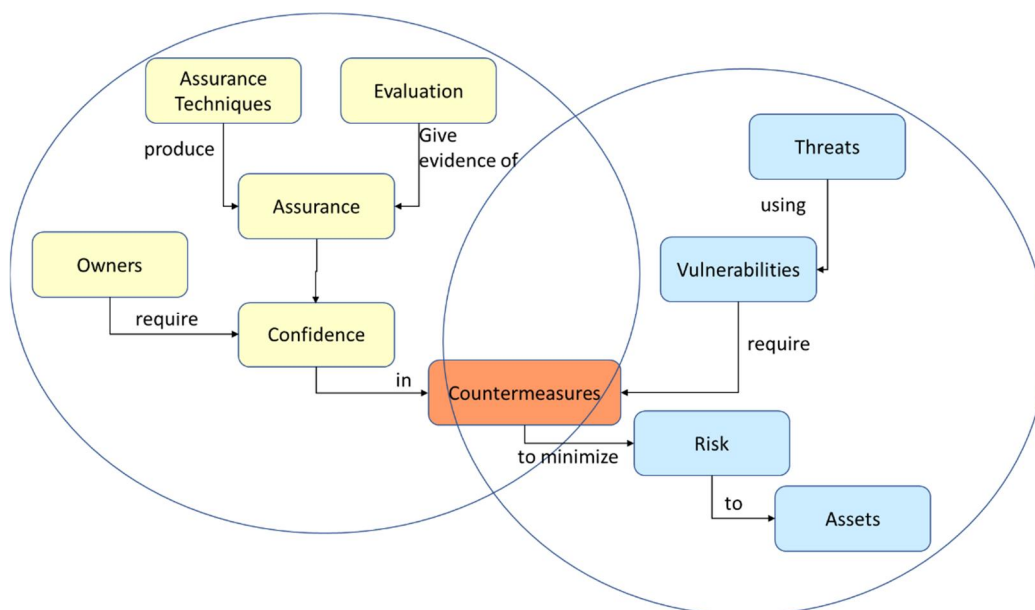


Figure B18. Context model. [4]

The risk assessment related to cyber-security is made in many phases. Threats, vulnerabilities, consequences and risk mitigations are treated in different phases. In many cases each threat is associated to many vulnerabilities and furthermore the worst

consequences can be similar to many threats and vulnerabilities. This means that the phases are typically separate or they can be related to a specific asset or a larger unit. An example of risk analysis related to cyber-security is presented at Figure B19. It shows the analysis from the risk treatment point of view.

Designer of safety-related control system (SCS) performing functions for safety of machinery				Use of machinery
Source of security lack (threat, vulnerability)	Safety function (impacted SCS)	Potential consequences	Description of proposed security measure(s)	Implemented security measure(s)
Unauthorized access (identification) and use control				
Unauthorized modification of safety function Only common password for use and modifications.	Overload detection	Machine falls down and the pilot and by-stander die.	Authentication, 6 digit password for function modification	Authentication, 4 digit password for machine use.

Figure B19. Example of cyber-security analysis.