Comparing cybersecurity and functional safety risk assessments

Malm T[1]., Tiusanen R[1]. & Berger J. [1]

1 : VTT Technical Research Centre of Finland

KEYWORDS: Risk assessment, cybersecurity, functional safety, safety of machinery

ABSTRACT

As number of cyberattacks have increased, safety systems in machines can also be endangered. This means that in safety assessments also cybersecurity issues need to be considered from the safety viewpoint. This can be done in a single mutual analysis or in separate analyses by considering the domain specific risks. Risk assessment is the tool to identify and assess the threats and vulnerabilities of the safety related systems.

There are many new standards, requirements and proposals, which give guidelines for cybersecurity. New Machinery Regulation (EU) 2023/1230 of June 2023 gives some cybersecurity requirements, which were not in the current Machinery Directive (2006/42/EC). The new Machine Regulation makes a safety conscious connection between safety and cybersecurity. There are also many new cybersecurity requirements and standards, which machine manufacturers need to consider in the near future. These new requirements can cause a lot of work, but they can also show new business opportunities. All providers related to machinery systems need to show that their customers can rely on the cybersecurity measures and documentation that the subsystem or the service provider has delivered.

The primary objective of safety analyses is to avoid accidents and the primary objective of cybersecurity analyses is to prevent or minimize the effects of cyberattacks. The primary objectives are different and it affects the risks that need to be considered in the analysis.

The main objectives of functional safety attributes are to maintain integrity and, in many cases, also availability of the control system. The main objectives of cybersecurity attributes are to maintain integrity, availability and confidentiality. Impaired integrity means that the system is not operating as it should and for example a safety function can be lost. Impaired or reduced availability means that the access into the system is limited and the system does not operate as intended. This can be a safety issue or violation of cybersecurity objectives depending on the system and its operations. Confidentiality is not straight a safety issue, but it is cybersecurity matter. However, confidentiality issue can change the threats and vulnerabilities of the system, and therefore the system may need to be to be reevaluated.

It is practical to make the cybersecurity and safety analyses separately, but cooperation is needed, especially, in risk identification and risk mitigation phase. Risk identification is the most important phase of the risk assessment and therefore cooperation and resources are needed in this phase. In risk mitigation phase the safety and security measures need to be considered in order to have congruent measures and to avoid conflicts between objectives.

1 INTRODUCTION

Cyberattacks can cause various damage to many stakeholders. As number of cyberattacks is increasing it comes more probable that also, safety systems in machines can 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.

There are many new standards, requirements and proposals, which give guidelines for cybersecurity. New Machinery Regulation (EU) 2023/1230 of June 2023 gives some cybersecurity requirements, which were not in the current Machinery Directive (2006/42/EC). Other new requirements will be set, for example, in Network and Information Security Directive II [4] and in Cyber Resilience Act proposal [5]. There are also some cybersecurity standards related to industrial automation and machinery, such as, IEC 62443 family (automation), IEC TS 63074 (functional safety, machinery) [8] and ISO/TR 22100-4 (machinery) [9]. The number of new requirements and guidelines show that cybersecurity domain is developing, and all processes are not yet mature compared to safety and functional safety engineering processes.

The main objective of the study is to find out is it practical to merge completely or partially cybersecurity and safety risk analyses or does it just increase work without major benefits. Another objective is to point out phases of the cybersecurity and safety analyses, when cooperation increases effectiveness of the analyses. The study is described more detailed VTT Research Report (published in Summer 2024) "Comparison of cybersecurity and functional safety risk assessments" [1].

2 COMPARING CYBERSECURITY AND FUNCTIONAL SAFETY RISKS

The differences between cybersecurity and functional safety attributes, methods and objectives can show which factors are important to consider in each risk analysis. If the analyses differ from each other then analysis, which considers all items similarly, can cause inefficient laborious work. In this case separate security and safety analysis is more practical, since risk items can be considered according to the domain.

The main objectives of functional safety attributes are to maintain integrity and, in many cases, also availability of the control system. The main objectives of cybersecurity attributes are to maintain integrity, availability and confidentiality. Confidentiality is not considered in functional safety, since it has no straight connection to accidents. In many cases, detected jeopardized safety integrity (e.g. failure) initiates machine stopping as a safety function, which may violate security objectives (reduced availability). Different objectives of cybersecurity and safety analyses is one reason to keep the analyses separate. However, it is important to compare safety measures and security countermeasures to match adequately both cybersecurity and functional safety objectives.

Figure 1. shows how cyberattack can affect objectives related to integrity, availability and confidentiality. In specific cases the objective can be jeopardized, but in many cases situation or countermeasures can minimize or remove the damages. Figure 1. shows the basic situations, when impaired objective can cause a hazardous situation or a safe state. The idea how these objectives can be affected, can give cybersecurity analysis help to consider safety issues. Cybersecurity analysis have also other risks than safety risks and they need to be analysed separately from the safety items.

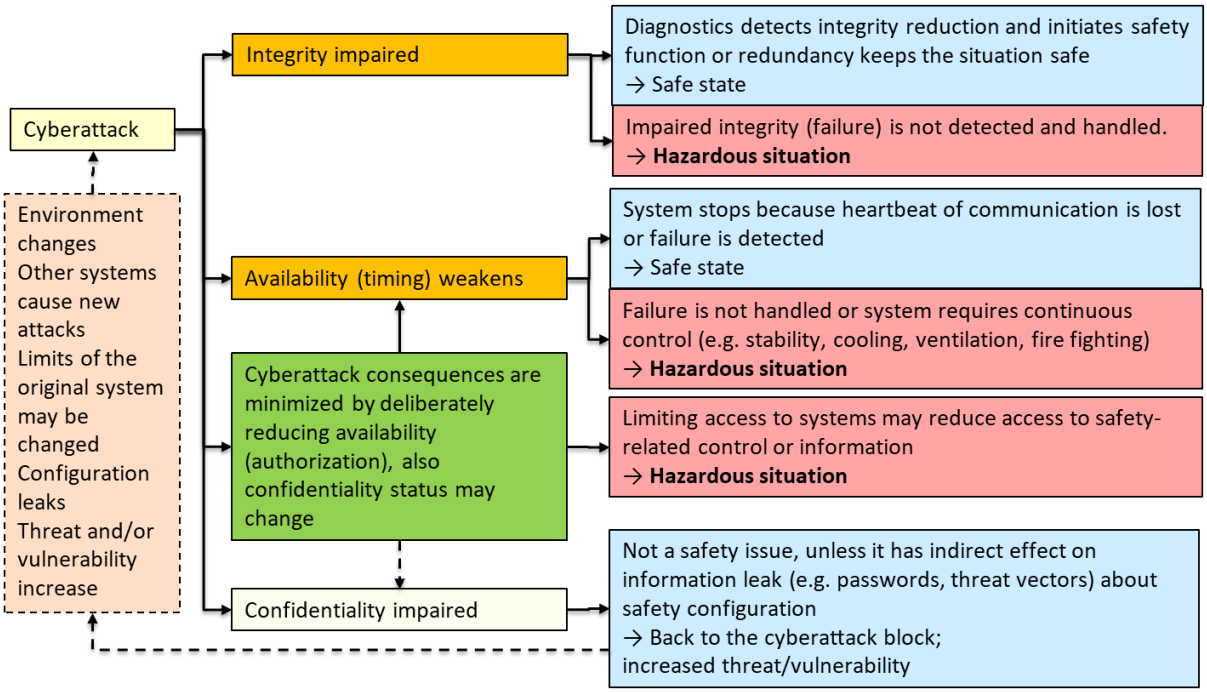

Figure 1. *Effects on safety attributes during cyberattack. [1]*

Figure 2 shows mind map of cybersecurity and functional safety items. In upper level there is categorization, which includes SL (Security Level, cybersecurity) and PL/SIL (Performance Level/Safety Integrity Level, functional safety). Then downwards the figure shows primary objective, examples of project phases, some examples of common technological interests, legislation related to cybersecurity and machinery (related also to functional safety) and typical stakeholders related to cybersecurity and machinery. The mind map shows how items can have relations or how, for example, categorizing items (SL and PL/SIL) have similar purpose, but there is no correlation between them, i.e. high SL does not require high PL/SIL or vice versa [8].

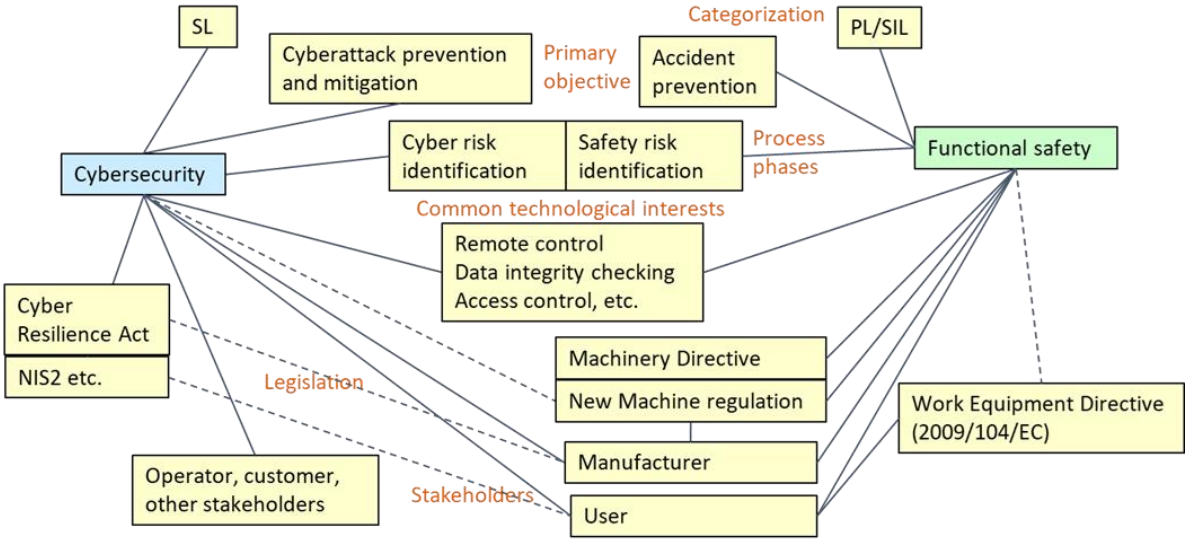

Figure 2. *Mind map of general cybersecurity and functional safety dependencies and differences. [1]*

3 RISK ANALYSIS

The primary objective of safety analyses is to avoid accidents and the primary objective of cybersecurity analyses is to prevent or minimize the effects of cyberattacks. The causes of functional safety failure are random failures or design/systematic (e.g. software) faults, whereas cybersecurity failures are related to intentional attacks, which exploit vulnerability. Safety risk victim is typically the system user, whereas cybersecurity victims are often many stakeholders. These factors show that the basis for cybersecurity and safety analyses can be different and therefore it is more practical to keep the analyses separate.

Risk assessment tries to find also critical, but improbable failures/risks, kind of "devil in the details". The question is: Can these kinds of risks be found in separate cybersecurity and safety analyses or in one single merged analysis. In separate analyses same amount of resources could give more focused analyses to both safety and security, which could reveal more weaknesses. On the other hand, if "the difficult to find" risk were between safety and security, then cooperation with safety and security analysts could reveal the risk. This case is related to risk identification and discussions with safety and security analysts are needed both in merged and separate analyses.

Figure 3. shows general risk assessment processes related to machinery (on the left) and cybersecurity (on the right). Some phases of the processes resemble each other and therefore some cooperation in specific phases can be useful. The thicker dotted lines (identification and risk reduction) in the figure show the phases when cooperation is specifically needed.

In bottom-up approach (e.g. failure mode and effects analysis, FMEA) all details are analysed systematically and the result can give good confidence on finding single-point failures/cases. In bottom-up analysis each item is analysed, and it causes a lot of work, if both safety and security factors are estimated for each item. The analysis is thorough, but often not very effective compared to needed resources. On the other hand bottom-up approach can be thorough and it can give confidence on the analysis. Top-down approach (e.g. fault tree analysis, FTA) 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 usually not searched systematically, but more like intuitively. This means that in top-down approach simultaneous safety and security analysis does not necessarily need additional work compared to separate analyses with domain specific item considerations. Top-down methods can merge simultaneous failures/events/cyberattacks and it can give a good overview of the risks. It can also reveal well events, which are related to two or more causes. These cases are often related to redundant systems.

In this study, basic cybersecurity and safety risk assessment processes have been compared to see similarities of the analyses and which phases have mutual interests. In all risk assessments perhaps the most important phase is risk/vulnerability/threat identification. Unidentified risk is not under control or actually it increases uncertainty of the risk. Identified risks should be known as potential input in other analyses to increase the possibility to identify hazards. Cooperation between analyses is important also in other phases in order to estimate and evaluate relevant risks and to avoid conflicts between objectives. Especially, in risk reduction (safety) and risk treatment

(cybersecurity) phase, when protective measures (safety) and countermeasures (security) are designed to reduce or avoid risks. These conflicts are often related to reduced availability, such as, machine or communication is stopped as a protective measure after a failure or cyberattack, in order to avoid further hazards or damages.

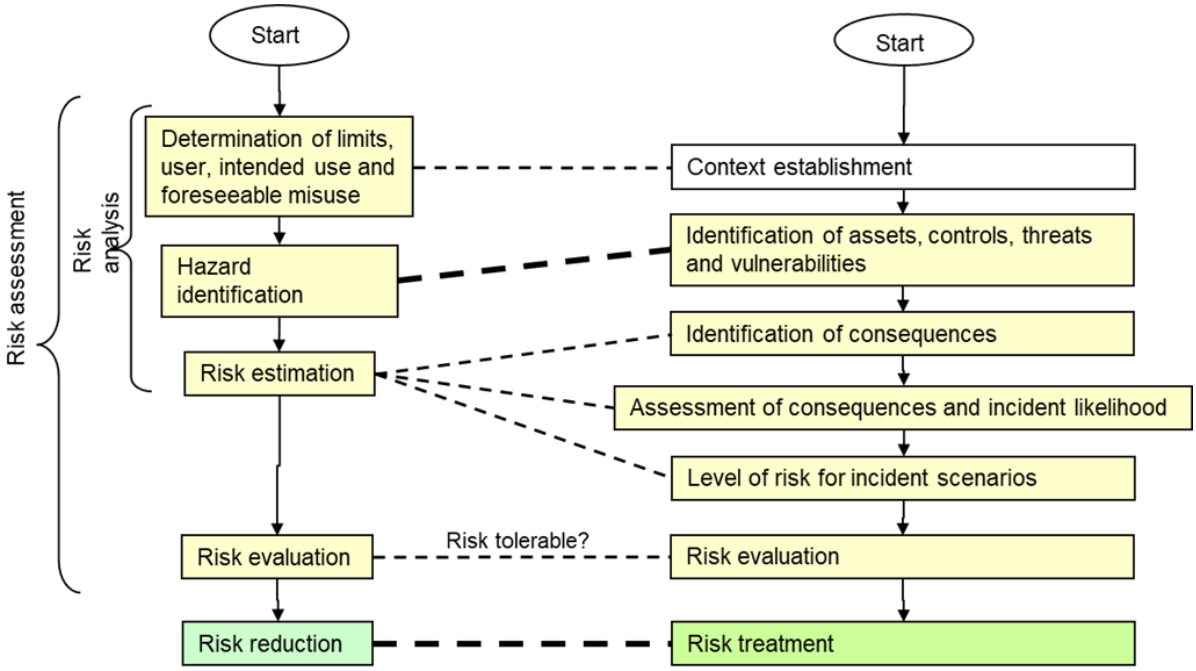

Figure 3. *Comparison of machinery safety and information security risk assessment processes. [1], [2], [3]*

Figure 4. compares information security and automation security risk assessment processes. There are some differences. Information security risk assessment is often done to a complete system or subsystem and it gives a good overview of the risks. In automation security assessment, the risk assessment process is more often divided into smaller processes according to requirements (SL and other requirements) and specific features of subsystems. Higher requirements (SL) lead typically to more detailed analysis. The SL is related also to the level of risks and countermeasures for relevant parts of the system.

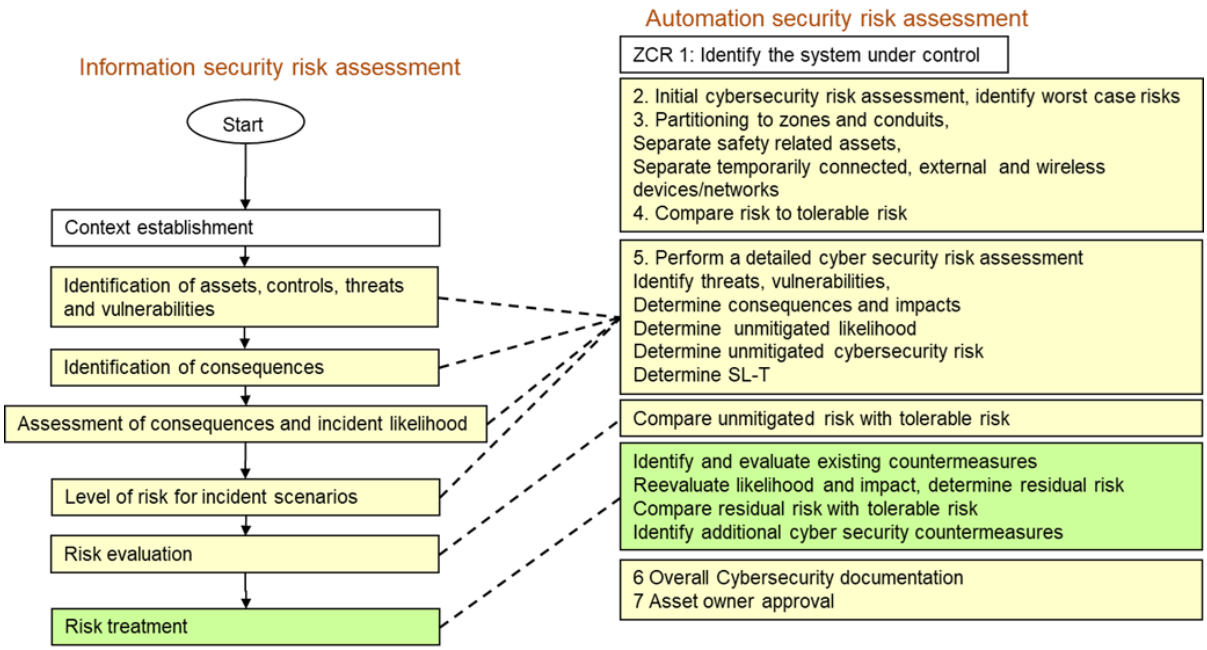

Figure 4. *Comparison of information security and Automation security risk assessment processes. [1], [3], [4].*

4 CONCLUSIONS

Cyberattacks have already caused financial, reputational and destructive occurrences and the number of attacks is increasing. The cyberattacks have been more common in IT security domain (close to office systems), but also OT security (closer to devices and automation) has got its share. One aspect is that IT and OT security are partly applying similar systems and therefore the difference between them is getting smaller in many ways.

Risk assessment is a tool to find out vulnerabilities of the products and operations and furthermore to get confidence on solutions. Currently cybersecurity and cyberattacks are developing so quickly that new approaches are needed to find and respond to new kinds of threats and vulnerabilities.

The main attributes to maintain in automation cybersecurity are typically integrity, availability and confidentiality. The main attributes to maintain safety are integrity and in some cases availability. If integrity violation is detected, then the system is designed so that typically it can be stopped safely. This means reduced availability, which is often against cybersecurity objectives. Also cyberattacks or too many access trials can cause cybersecurity countermeasures and reduced availability. Since reduced availability can be applied to reduce risks, its effects need to be considered from both security and safety viewpoint. One important factor is that no safety function may be impaired due to cybersecurity countermeasures.

There are many differences in objectives, risk assessments and requirements of cybersecurity and functional safety. In cybersecurity the main objective is to mitigate risks related to cyberattacks. The main objective of safety is to mitigate and avoid accidents. Although there are differences, cooperation in specific phases of risk assessment can be beneficial. However, it can be laborious and inefficient to consider all risks from both safety and security perspective, especially, in bottom-up type analysis (e.g. FMEA, Failure Modes and Effects Analysis). One related aspect is that both safety and cybersecurity risk assessment processes have some requirements, which aspects need to be considered related to all items (see Figure 3 and Figure 4) and this could mean additional work in a mutual analysis. Separate cybersecurity and safety analysis can better focus on specific properties and attributes of each domain and each item is considered according to the domain specific requirements.

It is practical to make the cybersecurity and safety analyses separately, but cooperation is needed, especially, in risk identification and risk mitigation phase. Risk identification is the most important phase of the risk assessment and therefore resources are needed in this phase. In risk mitigation phase the safety and security measures need to be considered in order to have congruent measures and to avoid conflicts between objectives. It is useful to consider cybersecurity risk treatment actions from many perspectives and levels, like, system of systems lifecycle phase, properties of the target and risk treatment strategy. A defence in depth strategy need to be applied. This approach can make it more probable to avoid the weak links of the cybersecurity.

New legislation and standards have already been published and new publications are coming. In the near future, companies need to consider cybersecurity effects on their operations, policy and products. This can be considered as a new expense item, but it can be seen also as an opportunity to new business.

Many companies are preparing themselves to new requirements. 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.

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.

4 REFERENCES

1. Malm T., Berger J., Tiusanen R., Ranta A., Seppälä J., Linnosmaa J., Alanen J., Salonen J., Dalla Costa A., Silverajan B., Zhao H. *Comparison of cybersecurity and functional safety risk assessments*, VTT Research Report (To be published 2024), Finland. 51 p.
2. ISO 12100. 2010. *Safety of machinery. General principles for design. Risk assessment and risk reduction*. 77 p.
3. *Machinery Regulation* (EU) 2023/1230 of 14 June 2023. https://eur-lex.europa.eu/eli/reg/2023/1230/oj
4. *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. EUR-Lex - 32022L2555 - EN - EUR-Lex (europa.eu) 73 p.
5. *Cyber Resilience Act proposa*l. 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
6. SFS-EN ISO/IEC 27000:2020. *Information technology. Security techniques. Information security management systems. Overview and vocabulary*.
7. IEC 62443-3-2:2020. *Security for industrial automation and control systems - Part 3-2: Security risk assessment for system design.* IEC 40 p.
8. IEC TS 63074:2023. *Safety of machinery – Security aspects related to functional safety of safety-related control systems.* IEC 34 p.
9. 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.