The Relevance of Cybersecurity for Functional Safety and HCI

Sebastian Korfmacher(✉)

Commission for Occupational Health and Safety and Standardization (KAN), St. Augustin, Germany
Korfmacher@KAN.de

Abstract. Our world is being accelerated and changed massively by digitalization. We must therefore consider possible changes in the world of work and the impact on OSH. A changing world of work will also lead to changes in the work equipment. Digitalization will cause an increase in networked work equipment. If products are networked to the world wide web, possible threats originating from the web must be considered.

Cybersecurity is not only realized by technical solutions and requirements. Humans are also a key element for cybersecurity. The design of the HCI interface is therefore essential for minimizing the impact on cybersecurity and OSH.

The conference contribution gives a fundamental explanation of why functional safety & cybersecurity is important for OSH and HCI, especially in the context of digitalization and scenarios such as Smart Manufacturing or Industry 4.0.

The contribution of standardization and the current discussion concerning functional safety & cybersecurity will also be illustrated.

Keywords: Digitalization · Safety · Functional safety · Security · IT security · Cybersecurity · Standardization · Smart Manufacturing · Industry 4.0 · Work equipment · World of work

1 The Impact of Digitalization to the World of Work

Many developments are currently taking place in the context of digitalization: Homes are becoming smart, cars will be connected to one another and autonomous driving is being developed. In the healthcare sector, digitalization will make diagnostics more reliable and efficient. In the future robots will not only assist humans in their own home, but will also taking care of them.

Digitalization also has a strong impact on the world of work. There is an increase in "mobile work" and "crowd working", and their consequences are being discussed. We also see a massive change in work equipment due to digitalization. These changes must be considered adequately. This also leads to the question of whether digitalization affects safety (see Sect. 1.1).

V. G. Duffy (Ed.): HCII 2019, LNCS 11581, pp. 458–466, 2019.
https://doi.org/10.1007/978-3-030-22216-1_33

1.1 Possible Changes in Work Equipment

To answer the question regarding the effect of digitalization on safety, possible changes in work equipment must first be determined. The following example will illustrate this:

In the past, machines were controlled by the machine operator. Machine control systems did not exist. Today, processes are often automated and computers are essential for this.

Robots for example are often used within factories for process automation. The safety of the humans also working in this factory is ensured by a safety fence. When the door of the safety fence is opened the robot stops immediately. This safety function must function correctly at all times. This is guaranteed by the so called "functional safety", which refers to the safety of the control system.

Functional safety is a subsystem of safety and contributes to preventing hazards.

In view of the current progress in digitalization, we cannot however focus on machines or robots that are fenced in anymore. Robots are being developed which collaborate with humans to assist and support them. Robots will therefore no longer be fenced in at every workplace. Use of collaborating robots is not only conceivable in the industrial sector. They are also developed for the healthcare sector to assist humans in hospitals and in their homes.

In general, work equipment is changing and will increasingly be networked. Examples are drones used for transportation or smart personal protective equipment for firefighters intended to increase safety. Tablets are being used in various scenarios to provide additional information and can be used for setting up machine parameters.

As work equipment will be connected to the world wide web, possible threats originating from the world wide web must be considered. Possible consequences for functional safety must also be considered, because

- what happens if a collaborating robot makes unexpected moves due to a hacker attack?
- what happens if the speed of travel of a machine/robot is manipulated?
- what happens if functional safety is impaired by malware or a hacker attack?
- what happens if a machine or system can no longer be controlled because of malware or a hacker attack?

These questions lead to a new field which must be considered adequately if work equipped is being networked via the world wide web: cybersecurity.

A detailed description of why cybersecurity is relevant for functional safety is presented in the following chapter.

1.2 Why Cybersecurity Is Relevant for Functional Safety

To understand the relevance of cybersecurity for functional safety, a closer look should be taken at the history of electronics:

In the beginning, electronics (such as control systems) consisted purely of hardware components. Changes could only be made by changing the hardware. Then technology changed and electronic components became programmable. Today electronic

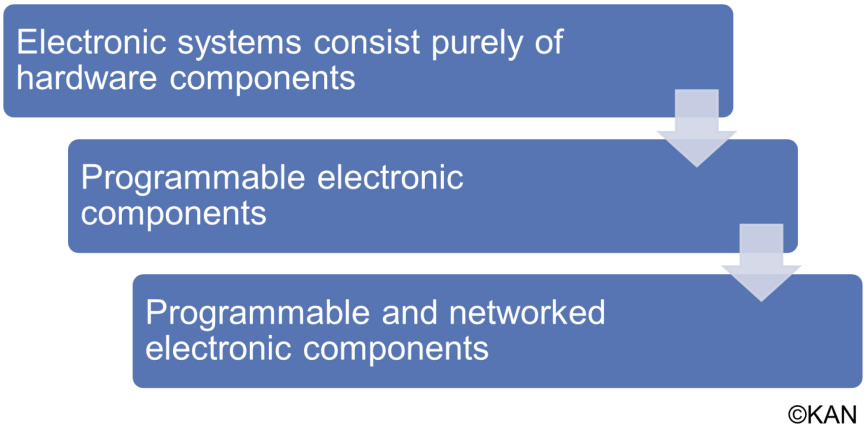

Fig. 1. Changes in electronic components

components are not only programmable, they are also connected to the world wide web (see Fig. 1).

This is the real problem, because cyberattacks or malware may have a negative impact on control systems – including those for safety. Safety functions may not perform correctly as result and humans could be at risk.

The types of attack can be differentiated and will be described in the following paragraph.

Types of Attack

Cybersecurity attacks can be differentiated into two groups: selective attacks and random attacks.

Selective attacks focus on one specific target. They are performed by a hacker who knows how to paralyse or manipulate machines or systems. However, they do not necessarily have an overview of possible negative effects on safety.

Random attacks do not focus on one specific target. They are intended to affect as many systems as possible and are called malware. Malware can lead to an unfavourable situation if machines or systems are paralysed.

Both types of attack can represent a possible hazard for humans. However, random attacks constitute a greater problem because in contrast to hacker attacks, targets are not selected based on attractiveness. Even small companies can be a target of random attacks. They should not suppose that they will never be affected by this kind of attack. Random attacks try to have a negative effect on the availability of systems of as many targets as possible. However, apart from the availability of the system, safety functions may also be affected negatively in case of an unfortunate combination of circumstances.

The different types of attack lead to the question of how significant cybersecurity is. The answer is given in the following paragraph.

Significance of Cybersecurity and the Relevance for HCI

Within the scenario of attacks coming from the world wide web, the question of the relevance and frequency of these attacks arises.

The German Federal Office for Information Security (BSI) communicates that 70% of companies and organisations in Germany were a target of cyber attacks in 2016 and 2017. Attackers did not only gain access to the IT system to influence them. Every second successful attack also led to a loss of production or a system breakdown [1].

There are also attacks which may not have been detected until now. Many companies will probably not admit a successful attack because this would have a negative impact on their image.

Cybersecurity is therefore very significant and must be considered adequately. Examples of possible gateways for hackers and malware are:

- insufficient security standards for hardware components
- remote maintenance
- unchanged standard passwords
- missing software updates
- obsolete operating systems
- vulnerable operating systems

This list of possible gateways for hackers and malware is by no means exhaustive. It can never be complete because threats for cybersecurity can change from one minute to the next. As possible ways of attacks are constantly changing, the cybersecurity will never cease to be relevant.

The aspects mentioned above focus on technical solutions and requirements to ensure cybersecurity. Humans and their behaviour and knowledge about the mechanisms employed by hackers and malware must not be ignored, however [2].

Humans are often a key element for the success of malware or hackers. Clicking on a faked link that was sent by e-mail, for example, can open doors to hackers. Likewise, the execution of malware can be started and the computer be encrypted until a ransom is paid. The design of the HCI interface is therefore essential not only for office computers, but for any kind of machine and system. Furthermore, HCI has the opportunity to take account of cybersecurity and to facilitate the prevention of wrong decisions made by humans which would open the door to potential threats (e.g. malware, hacker attacks).

Standardization contributes to cybersecurity and functional safety. Section 2 will illustrate important documents and the current progress of standardization activities concerning cybersecurity of industrial automation and control systems and functional safety.

2 Contribution of Standardization to Functional Safety and Cybersecurity

Standardization documents provide a contribution to functional safety and cybersecurity. Functional safety and cybersecurity are two independent spheres that are being brought together through the increasing development of systems that are connected to

the world wide web. Functional safety and cybersecurity use different mechanism however to achieve their particular aims.

The following chapters will illustrate the different mindsets and methodologies.

2.1 Standardization of Functional Safety

The safety of a system as a whole is achieved by different individual systems. These systems can consist of different technologies such as hydraulic, mechanical, electrical, electronic or programmable electronic components.

ISO/IEC Guide 51 defines safety as the freedom from unacceptable risk. Functional safety applies to all kinds of control systems and is aimed at the reduction of unacceptable risk. Functional safety guarantees that safety functions (see example of Sect. 1.1) are functioning at all times. Only then is functional safety able to contribute to safety and to ensure human health.

The key element of safety is the risk assessment, during which the necessary input of every safety function in the control system is defined.

In the event of a fault, the safety function must perform correctly. Necessary methods are described in full detail by standardization documents:

- IEC 61508 series: Functional safety of electrical/electronic/programmable electronic safety-related systems (generic standard) [3]

  – IEC 61508-1:2010: Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 1: General requirements
  – 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
  – IEC 61508-3:2010: Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 3: Software requirements
  – IEC 61508-4:2010: Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 4: Definitions and abbreviations
  – IEC 61508-5:2010: Functional safety of electrical/electronic/programmable electronic safety related systems - Part 5: Examples of methods for the determination of safety integrity levels
  – IEC 61508-6:2010: Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3
  – IEC 61508-7:2010: Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 7: Overview of techniques and measures [4]

- IEC 61511 series: Functional safety - Safety instrumented systems for the process industry sector (process industry)

  – IEC 61511-1:2016 + AMD1:2017 CSV Consolidated Version: Functional safety - Safety instrumented systems for the process industry sector - Part 1: Framework, definitions, system, hardware and application programming requirements [5]
  – IEC 61511-2:2016: Functional safety - Safety instrumented systems for the process industry sector - Part 2: Guidelines for the application of IEC 61511-1:2016 [6]

- IEC 61511-3:2016: Functional safety - Safety instrumented systems for the process industry sector - Part 3: Guidance for the determination of the required safety integrity levels [7]
- ISO 13849 series: Safety of machinery – Safety-related parts of control systems (machinery)
- ISO 13849-1:2015: Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design [8]
- ISO 13849-2:2012: Safety of machinery – Safety-related parts of control systems – Part 2: Validation [9]

and

IEC 62061: Safety of machinery - Functional safety of safety-related electrical, electronic and programmable electronic control systems [10]
(machinery)

2.2 Standardization of Cybersecurity

Cybersecurity describes the resistance of an IT system to attacks and the disruptions and malfunctions caused by them. To reach cybersecurity different strategies can be applied, e.g. security by design or defense in depth. All strategies and measures which can be applied depend on the motivation of the attacker, however. A distinction between coincidental maloperation and intentional attacks is therefore drawn and expressed by different security levels (SLs) specified in the international (draft) standard IEC 62443-3-3: Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels.

The IEC 62443 series constitutes very important standardization documents for IT security for industrial automation and control systems. The series is currently under development and not all parts have been published yet.

Comparison of the strategies of functional safety (Sect. 2.1) and cybersecurity (Sect. 2.2) illustrates the different mindsets: Security is faced with continually changing attack scenarios. By contrast threats addressed by functional safety will not change unless the state of the art changes. Owing to the described change of digitalization (see Sect. 1), functional safety and cybersecurity must be applied at the same time to guarantee safe products.

Owing to the different histories and strategies of functional safety and cybersecurity, further standardization documents exists that are very important in this context and will be described in the next chapter.

2.3 Developments Within Standardization of Functional Safety and Cybersecurity

Standardization documents for functional safety have existed for a very long time, but they do not consider possible threats arising due to the fact that machines are connected directly or indirectly to the world wide web. Dedicated standards for cybersecurity are therefore being developed.

Many standardization activities are currently taking place regarding functional safety and cybersecurity. Some of them will be presented in this chapter and can be categorized as follows:

The documents are categorized into “Guides” and “Technical Reports” (TR). Guides represent an internal rulebook of the particular standardization organization and assist standards writers during the developing process [11, 12].

Technical reports contain collected data, e.g. regarding the “state of the art”, and are entirely informative and not normative [13, 14]. They can also serve as an aid for people applying standards.

Some key facts on some of the documents in Fig. 2 are given below to demonstrate the wide range of topics covered by these documents:

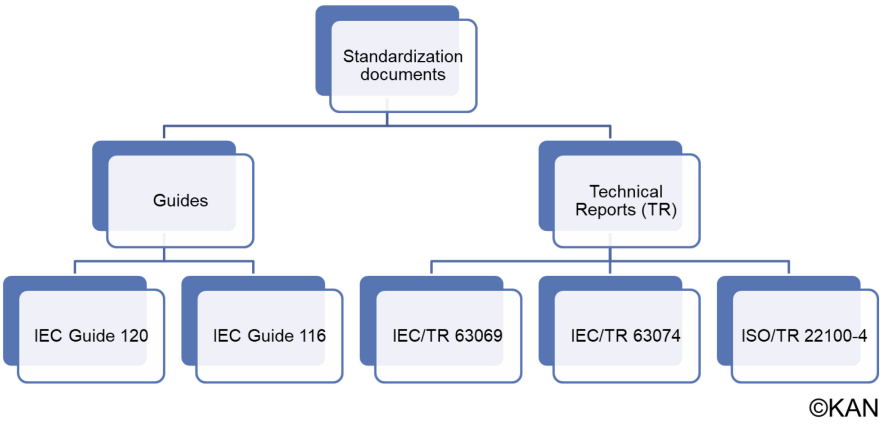

Fig. 2. Documents for functional safety and cybersecurity

- **IEC/TR 63069: Industrial-process measurement, control and automation – Framework for functional safety and security**

As mentioned in (Sect. 2.1) the standard IEC 61508 describes generically the safety of a whole system. In contrast, IEC 62443 describes security for industrial automation and control systems (Sect. 2.2).

Today’s challenge is to apply both standards at the same time to guarantee functional safety & security.

“This Technical Report (TR) explains and provides guidance on the common application of IEC 61508 and IEC 62443 in the area of industrial-process measurement, control and automation. This document may apply to other industrial sectors where IEC 61508 and IEC 62443 are applied.” [15].

- **IEC/TR 63074:2017-12 Draft (44/793/CD:2017): Safety of machinery - Security aspects related to functional safety of safety-related control systems**

This draft TR contains general requirements regarding such aspects of security threats and vulnerabilities that could affect functional safety (realized by the safety-related control system (SCS)) and lead to a loss of the ability to maintain the safe operation of a machine [16].

- **ISO/TR 22100-4:2018: Safety of machinery – Relationship with ISO 12100 – Part 4: Guidance to machinery manufacturers for consideration of related IT-security (cyber security) aspects**

"This document gives machine manufacturers guidance on potential security aspects in relation to safety of machinery when putting a machine into service or placing on the market for the first time. It provides essential information to identify and address IT-security threats which can influence safety of machinery.

This document gives guidance but does not provide detailed specifications on how to address IT-security aspects which can influence safety of machinery.

This document does not address the bypass or defeat of risk reduction measures through physical manipulation." [17].

Due to the diversity of different standardization activities, a coordinated procedure must be followed to avoid duplication or overlap in the development of standards. Close cooperation between experts and standardization organizations must continue for this purpose [18].

3 Conclusions

In conclusion, the proportion of networked machines and systems is going to increase. As a result, the probability of successful attacks will also increase – especially in scenarios of Industry 4.0 or Smart Manufacturing. Cybersecurity can no longer be ignored because a cybersecurity problem can lead to a potential risk for humans if functional safety is affected.

Standards are an appropriate resource for the consideration of functional safety and cybersecurity. During the current development of functional safety and cybersecurity standards, documents overlapping and duplication of work must be avoided.

As cybersecurity is relevant for a broad range of products, some organisations propose a horizontal implementation of a cybersecurity directive. The German Electrical and Electronic Manufacturers Association (ZVEI) has recently published a whitepaper regarding this proposal [19]. The idea behind this proposal is that cybersecurity problems would affect not only one component or product. The problem can have a negative impact on a whole system. ZVEI therefore considers it necessary to have a common horizontal solution which is valid across the European Union.

Independent of the solution for cybersecurity it is necessary that manufacturer, user, integrator and operator are adequately involved to prevent that only one of them bears responsibility. Only then can cybersecurity be applied holistically.

In addition, questions of liability and guarantee must be resolved. This lies outside the scope of standardization, however.

Technical measures and concepts are essential for cybersecurity. Humans are equally important, however. In consequence, the design of HCI interfaces is not negligible. The opportunity to design HCI interfaces such that they consider cybersecurity and the possible consequences for the safety of humans should therefore be taken.

References

1. BSI. https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2018/Cyber-Angriffe_haben_erhebliche_Konsequenzen_fuer_die_Wirtschaft_31012018.html. Accessed 26 Nov 2018
2. Moallem, A.: Human-Computer Interaction and Cybersecurity Handbook, pp. 18–19. CRC Press, Boca Raton (2019)
3. IEC. https://www.iec.ch/functionalsafety/explained/page1.htm. Accessed 23 Jan 2019
4. IEC. https://www.iec.ch/functionalsafety/standards/page2.htm. Accessed 23 Jan 2019
5. IEC. https://webstore.iec.ch/publication/61289. Accessed 23 Jan 2019
6. IEC. https://webstore.iec.ch/publication/25521. Accessed 23 Jan 2019
7. IEC. https://webstore.iec.ch/publication/25479. Accessed 23 Jan 2019
8. ISO. https://www.iso.org/standard/69883.html. Accessed 23 Jan 2019
9. ISO. https://www.iso.org/standard/53640.html. Accessed 23 Jan 2019
10. IEC. https://webstore.iec.ch/publication/22797. Accessed 23 Jan 2019
11. IEC. https://www.iec.ch/standardsdev/publications/guide.htm. Accessed 12 Dec 2018
12. ISO. https://www.iso.org/iso-guides.html. Accessed 12 Dec 2018
13. IEC. https://www.iec.ch/standardsdev/publications/tr.htm. Accessed 12 Dec 2018
14. ISO. https://www.iso.org/deliverables-all.html#TR. Accessed 12 Dec 2018
15. Danish Standards Foundation. https://standards.globalspec.com/std/10392180/dsf-iec-tr-63069. Accessed 16 Jan 2019
16. Beuth. https://www.beuth.de/de/norm-entwurf/din-en-63074/280563956. Accessed 16 Jan 2019
17. ISO. https://www.iso.org/standard/73335.html. Accessed 16 Jan 2019
18. KAN. https://www.kan.de/en/publications/kanbrief/digitalization-and-industry-40/aspects-of-safety-and-security-in-the-emergence-of-industrie-40/. Accessed 16 Jan 2019
19. ZVEI. https://www.zvei.org/presse-medien/publikationen/horizontale-produktregulierung-fuer-cybersicherheit-whitepaper/. Accessed 26 Nov 2018