Federal Ministry
for Economic Affairs
and Energy

中国国家标准化管理委员会
Standardization Administration of the P.R.C.

中华人民共和国工业和信息化部

Sino-German White Paper on Functional Safety for Industrie 4.0 and Intelligent Manufacturing

bmwi.de

STANDARDIZATION COUNCIL INDUSTRIE 4.0

PLATTFORM INDUSTRIE 4.0

国家智能制造标准化总体组

GLOBAL PROJECT
Quality Infrastructure

List of Stakeholders

Standardization Council Industrie 4.0: The Standardization Council Industrie 4.0 (SCI 4.0) was founded at the Hannover Messe 2016 as a German standardization hub by Bitkom, DIN, DKE, VDMA and ZVEI. The initiative aims to initiate standards for digital production and to coordinate these standards nationally and internationally. SCI4.0 orchestrates the implementation of the standardization strategy of the German Plattform Industrie 4.0, which includes the coordination with standardization organizations (SDO) and international partners as well as the interlocking with Pilot projects. This coordinated approach will achieve that the norms and standards for the use of potentials of Industrie 4.0 are being developed in a coordinated manner. The SCI4.0 is supported by DKE and the German Federal Ministry for Economic Affairs and Energy (BMWi).

Plattform Industrie 4.0: Plattform Industrie 4.0 promotes the development of Industrie 4.0 in Germany. Companies, their workforce, trade unions, associations, science and politics have joined forces in the platform to promote the digital transformation of manufacturing in Germany and to strengthen the competitiveness of Germany as a production location. The platform is steered and led by the federal minister for economic affairs and energy, Peter Altmaier, the federal minister of education and research, Anja Karliczek, and high-ranking representatives from industry, science and the trade unions.

Intelligent Manufacturing Standardization Administration Group: The Intelligent Manufacturing Standardisation Administration Group (IMSG) was established to promote and accelerate the progress of intelligent manufacturing in China under the leadership of Standardization Administration of China (SAC) and Ministry of Industry and Information Technology (MIIT). It is responsible for carrying out the practical work on Intelligent manufacturing standardisation, such as taking part in the international standard-making on intelligent manufacturing as well as organizing the exchange and cooperation on international standards.

Global Project Quality Infrastructure: To promote the development of well-functioning and internationally coherent quality infrastructures, the German Federal Ministry for Economic Affairs and Energy (BMWi) has established the Global Project Quality Infrastructure (GPQI). GPQI supports the political and technical dialogues and implements bilaterally agreed activities in collaboration with all relevant stakeholders. The project aims to reduce technical barriers to trade and enhance product safety through bilateral political and technical dialogues on QI with some of Germany's key trading partners.

Imprint

Published by
Federal Ministry for Economic Affairs and Energy
Public Relations Division
11019 Berlin
www.bmwi.de

Text
Standardization Council Industrie 4.0
DKE Deutsche Kommission Elektrotechnik
Elektronik Informationstechnik in DIN und VDE,
60596 Frankfurt am Main

National Intelligent Manufacturing Standardisation
Administration Group
China Electronics Standardization Institute,
No.1 Andingmen East Street, Dongcheng District, Beijing, 100007,
China

Design
Iris Christmann, Wiesbaden

Status
July 2020

This brochure is published as part of the public relations work of the Federal Ministry for Economic Affairs and Energy. It is distributed free of charge and is not intended for sale. The distribution of this brochure at campaign events or at information stands run by political parties is prohibited, and political party-related information or advertising shall not be inserted in, printed on, or affixed to this publication.

CONTENTS

0 Introduction 5

0.1 Background and context 5
0.2 Compatibility with other Sino-German guidance 5
0.3 Related standardization committees 5

1 Scope 6

2 References to related standards and guidelines 6

3 Terms, definitions and abbreviations 6

4 History of safety in industry 7

4.1 Safety accidents 7
4.2 Safety-related legal requirements 7
4.3 Different safety domains 8

5 Current approaches to safety in industry 9

5.1 Risk reduction strategy for ensuring safety 9
5.2 Triggering of hazardous events 9

6 Introduction to Industrie 4.0 and IM 10

7 I4.0 and IM challenges and new risks to safety 11

7.1 Risks due to new technology 11
7.2 Creating a link between I4.0 and IM and Functional Safety 12
7.2.1 I4.0 and IM concept (axis 3 of RAMI) 12
7.2.2 Solution 14
7.2.3 Protection of the I4.0 and IM workspace and safety-related installations 14
7.2.4 Functional Safety for I4.0 and IM 15

7.3 Zones & conduits 15

7.4 Considerations for safe and secure communication 15

7.5 Risks due to system complexity and interconnectivity 18

7.6 Risks due to system interoperability 18

7.7 Risks due to lack of maturity of intelligent technologies and products 19

8 Safety in the context of security 19

8.1 Preconditions to be met by the security framework 19
8.1.1 Domain-specific knowledge 20
8.1.2 Security grading 20
8.1.3 Security requirements 20

8.2 Preconditions to be met by the functional safety framework 21
8.2.1 Domain-specific knowledge 21
8.2.2 Functional safety grading (extract from IEC 61508) 21
8.2.3 Functional safety requirements 21

8.3 Challenges of achieving safety while also considering security 22
8.3.1 Overview 22
8.3.2 Security from the perspective of safety 22
8.3.3 Safety from the perspective of security 22

8.4 Gaps in current standards and guidance 23

8.5 Safety management with consideration of security 24

8.6 Lifecycle with consideration of safety and security 24
8.6.1 General information 24
8.6.2 Risk assessment 25
8.6.3 System implementation 25
8.6.4 Engineering and systems integration 26
8.6.5 Operation and maintenance 26

Bibliography 28

0 Introduction

0.1 Background and context

Conventional Industrial Automation Control Systems (hereinafter: IACS) are based solely on mechanical and electronic technology. Different devices or systems are isolated or have limited connectivity. Typically, it is common to use functional safety measures to deal with safety issues, which are mainly based on the general functional safety standard IEC 61508 and domains-specific standards, e.g. IEC 61511 for the process industry, IEC 62061 or ISO 13849 for the machinery sector and ISO 26262/ISO 21448 for the automotive industry.

However, with the rise of Industrie 4.0 and Intelligent Manufacturing (hereinafter: I4.0 and IM), more and more intelligent and digital technology is required for IACS. To meet this need, an increasing number of information technologies, communication devices and smart devices are being integrated into modern control systems. This increases the degree of complexity and interconnection among systems. Although this can increase efficiency and reduce costs for industries, the overall infrastructure will become more susceptible to internal failures and more vulnerable to cyberattacks.

All of these new issues – including new hazards, e.g. security related attacks – therefore need to be considered to ensure that I4.0 and IM remain safe. Existing international standards need to be interpreted and amended to cover these issues. This paper surveys and analyses existing standards, specifications and research to give an overview of safety for I4.0 and IM.

0.2 Compatibility with other Sino-German guidance

This White Paper on Functional Safety is one of the research outcomes on I4.0 and IM under a programme by the Sino-German Standardization Cooperation Commission. It is compatible with other publications in the Sino-German programme, such as 'Security Standards White Paper for Sino-German Industrie 4.0/Intelligent Manufacturing', 'Alignment Report for Reference Architectural Model for Industrie 4.0/Intelligent Manufacturing System Architecture' etc.

0.3 Related standardization committees

Working group IEC/TC65/WG20 with the title 'Framework for safety and security' was specifically created within IEC/TC65 'Industrial-process measurement, control and automation' to jointly address both the safety and security requirements. Some results of this White Paper on Functional Safety may later be integrated into working documents of IEC/TC65/ WG20.

DKE working group **TBINK-AK IT-Security and Security by Design**, (hereinafter: TBINK-AK IT-Security) is currently focusing on rendering multipart-guidance on joint considerations of functional safety and cybersecurity.

Note: In the elaboration of this White Paper on Functional Safety, Germany's DKE/AK 914.0.6 has partnered with its Chinese counterpart the Instrumentation Technology and Economy Institute (hereinafter: ITEI).

SAC/TC124 is the Chinese Committee on Functional Safety and Industry Security, which has released many Chinese standards about functional safety, industrial security and the integration of safety and security.

1 Scope

This White Paper is used to research the safety issues in the I4.0 and IM application environment. It will explain the basic concept of conventional technical safety and consider the evolution of I4.0 and IM and its implications for safety techniques. Security will become a very important factor for I4.0 and IM safety. This White Paper will also discuss the potential integration of safety and security.

2 References to related standards and guidelines

IEC 61508 Functional safety of electrical/electronic/ programmable electronic safety-related systems – Parts 1 to 7

IEC 61511 Functional safety - Safety instrumented systems for the process industry sector – ALL PARTS

IEC 62443 All parts, industrial communication networks – Network and system security

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

ISO/IEC 27021 Information technology – Security techniques – Competence requirements for information security management systems professionals

ISO/IEC 27034-2 Information technology – Security techniques – Application security – Part 2: Organization normative framework

ISO 12100 Safety of machinery – General principles for design – Risk assessment and risk reduction

IEC 62061 Safety of machinery – Functional safety of safety-related electrical, electronic and programmable electronic control systems

ISO 13849 – 1 Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design

ISO 13849 – 2 Safety of machinery – Safety-related parts of control systems – Part 2: Validation.

ISO 26262 All parts, Road vehicles – Functional safety

3 Terms, Definitions and Abbreviations

Please refer to IEC 61508-4, IEC 62443-1-1 and IEC TR 63069 for the terms, definitions and abbreviations.

4 History of safety in industry

4.1 Safety accidents

What are accidents?

Accidents are unplanned and unintentional events that result in harm to humans, damage to the environment (safety incidents) or property, production outages, or nearly anything that has some inherent value (economic targets). These losses increase an organisation's operating costs because they raise production costs, reduce efficiency, and lead to lower employee morale and negative public opinion long term. Accidents are rarely simple and hardly ever result from a single cause. Most accidents involve multiple, interrelated causal factors. Accidents can occur whenever significant deficiencies, oversights, errors, omissions, or unanticipated changes are present. Any of these conditions can be a precursor for an accident; the only uncertainties are when the accident will occur and how severe its consequences will be.

How about protection?

Safety risk management prevents or mitigates accidents by identifying and implementing the appropriate controls and barriers. Controls help to prevent errors or failures that could result in an accident; barriers help to mitigate the consequences of potential errors or failures. Barriers to protect targets against loss can be physical barriers, such as machine guards and railings, or management barriers, such as work procedures, hazard analysis, requirements management, line management oversight, and communications. In a work environment, several barriers may be used in an effort to prevent accidents. Accidents occur when one or more barriers in a work system, including procedures, standards, and requirements intended to control the actions of workers, fail to perform as intended. The barriers may not exist, may not be adhered to, or simply may not be comprehensive enough to be effective. Personal performance and environmental factors may also reduce protection.

Accidents in industry

With the rapid development of industry, potential safety accidents are continuing to emerge. Although people have adopted various protection measures, safety accidents are still occurring. The Seveso II Directive Major Accident Reporting System (hereinafter: MARS) holds data on approximately 600 major accidents that have been notified since 1984, with approximately 30 notifiable accidents being reported on an annual basis since 2000.

4.2 Safety-related legal requirements

The European Commission (hereinafter: EC) has introduced a number of directives on health and safety matters. Some of these lay down minimum requirements, which are intended to form the basis of harmonised workplace health and safety laws throughout the Member States of the EU. New regulations have been introduced in the UK to implement these directives, including:

- The Management of Health and Safety at Work Regulations 1999
- The Provision and use of Work Equipment Regulations 1998 and
- The Health and Safety (Display Screen Equipment) Regulations 1992

Other EC directives, sometimes referred to as New Approach Directives, aim to remove barriers to trade that may arise from different design and manufacturing standards among Member States. The most significant of these is the Machinery Directive, which the Department of Trade and Industry has implemented in the UK as the Supply of Machinery (Safety) Regulations 1992 (as amended in 1994).

The basic legislative framework in the European Union is as follows:

- EU directive (European law), e.g. Seveso Directive, Machinery Directive, Pressure Equipment Directive, Low Voltage Directive, EMC Directive etc.
- Definition of underlying standards (harmonised standards attached to EU directive), e.g. for machinery ISO 12100, IEC 62061, EN/ISO 13849, etc.
- Local implementation, e.g. in Germany the Safety at Work Act (Arbeitssicherheitsgesetz), Hazardous Incident Ordinance (Störfallverordnung).
- Local implementation rules, e.g. in Germany VDI/VDE 2180 as the implementation rule for IEC 61511.

In China, production and manufacturing safety is the responsibility of the Ministry of Emergency Management of the eople's Republic of China. Its responsibilities also include:

- Organising the preparation of overall national emergency plans
- Establishing a disaster reporting system and dealing with the disaster situation
- Guiding the prevention and control of fires, floods and droughts, geological disasters, etc.
- Undertaking comprehensive supervision and management of safety production and safety production supervision and management of industrial and mining safety

The State Administration for Market Regulation is responsible for product safety, safety inspection/tests and safety approval, including responsibility for

- product quality and safety supervision and management
- food safety supervision and management
- unified management of standardisation
- unified management of inspection and tests

The basic legislative framework in China is as follows:

- National law, e.g. People's Republic of China Safety Production Law, People's Republic of China Mine Safety Law, etc.
- Regulations or national orders, e.g. Hazardous Chemicals Safety Management Regulations, Safety Production License Regulation, State Council Order No. 639: Railway Safety Management Regulations, etc.
- Ministry order, Ministry of Emergency Management of the People's Republic of China (No. 1) on safety evaluation testing and inspection agency Management, etc.
- Standards, including mandatory standards and recommended standards, GB/T 20438-2017 (IEC61508 idt), GB/T 21109-2007 (IEC 61511 idt), GB 18218-2018, identification of major hazard installations for hazardous chemicals
- Local implementation, e.g. for coal mines, oil and gas, transportation and in other areas

4.3 Different safety domains

Safety has a very wide meaning for different applications in industry. As a result of the last three industrial revolutions, the issue of safety is also constantly evolving.

Mechanical safety

Example:

- *To protect a vessel against overpressure*
- *A well-known mechanical safety measure is to attach a safety valve to such a vessel. For this application, a spring is used to keep the valve closed. In the event that the pressure inside the vessel exceeds a predefined limit, the valve opens and the pressure is released.*
- *It has to be ensured that the valve is directly attached to the pressurised vessel. If the valve is connected via a piece of pipe only, the desired safety measure will not work correctly.*
- *The correct function of the valve is to be tested at regular intervals. Depending on the size of the valve (mechanical dimensions, rated pressure), the location of the valve (e.g. at the bottom of the sea), it might be challenging to perform such testing.*

Electrical safety

Example:

- *To protect users from electrical shock*
- *To protect users from electrical shock in the event of an isolation fault, all conductive elements of a housing are galvanically connected to protective earth*

When designing an electrical supply system, a protective earth conductor of sufficient dimension has to be installed so that every electrical device can be connected to such a conductor.

In order to guarantee correct functioning, the functionality of such a protection conductor system might need to be checked at regular intervals. Due to the amount of connections (every outlet socket) and the amount of devices (every cord connected device), this can be a significant undertaking.

Functional safety:

Example:

- *Reduce the probability of the occurrence of a hazardous event*
- *In order to prevent the unwanted occurrence of a hazardous event (e.g. overheating of a vessel), a functionality is implemented that stops a process (e.g. supply of heat to a vessel) in the event that pre-defined limits (e.g. the maximum temperature of such a vessel) are violated*

There are 2 design challenges:

1. To properly define all conditions that will cause the safety functions to be activated
2. To define all conditions that may hinder the safety function from functioning once triggered

There are 2 maintenance challenges:

1. To ensure that the correct function can be guaranteed
2. To make sure that no modifications are made that n egatively impair the safety function throughout its entire lifetime

5 Current approaches to safety in industry

5.1 Risk reduction strategy for ensuring safety

Risk management and risk reduction are commonly accepted processes for maximising safety. These processes seek to reduce risk using different protection measures to achieve tolerable risk targets.

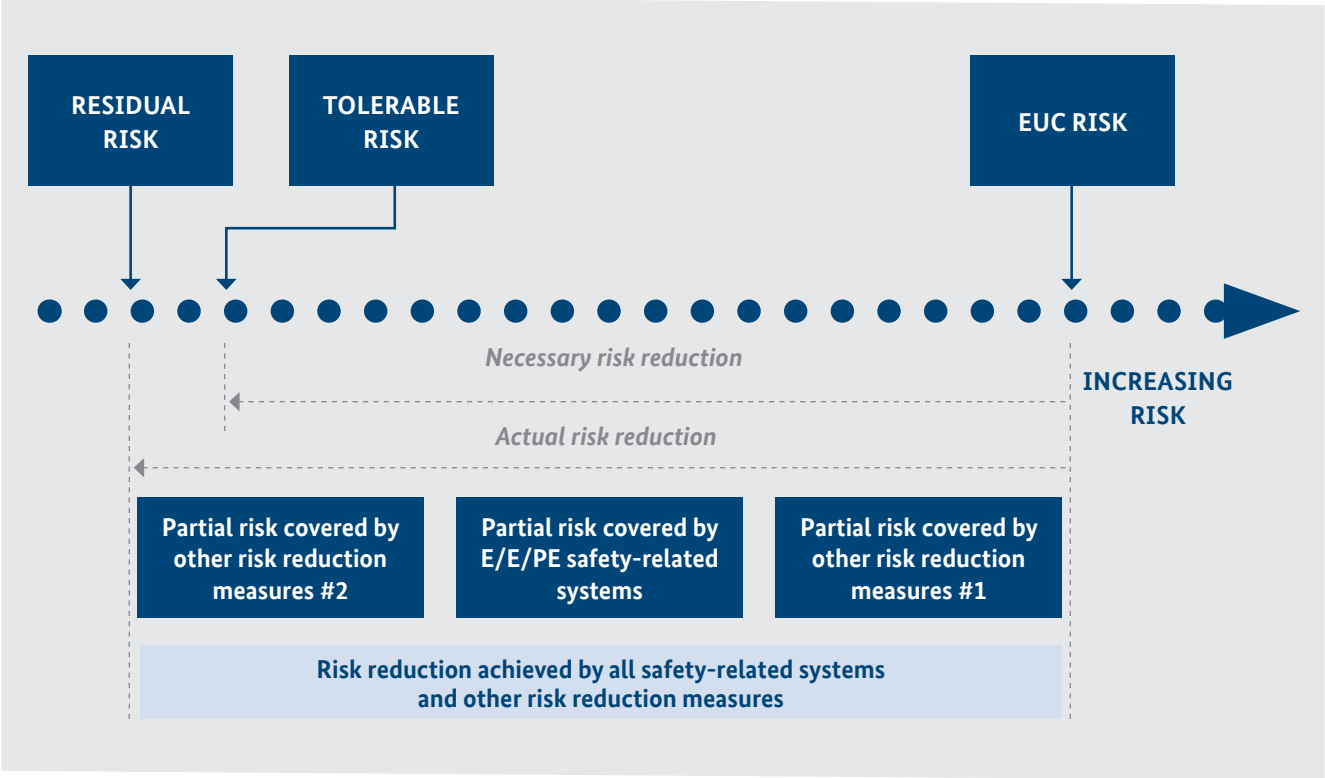
The necessary risk reduction is the reduction in risk that has to be achieved to meet the tolerable risk targets for a specific situation (which may be stated either qualitatively or quantitatively). The notion of necessary risk reduction is of fundamental importance in the development of the safety requirements specification for the E/E/PE safety related systems. In particular, this concerns the Safety Integrity Level (SIL or Performance Level (hereinafter: PL)) part of the safety requirements specification. The purpose of determining the tolerable risk for a specific hazardous event is to state what is deemed reasonable with respect to both the frequency (or probability) of the hazardous event and its specific consequences. Safety-related systems are designed to reduce the frequency (or probability) of the hazardous event and/or the consequences of the hazardous event [IEC61508-5].

5.2 Triggering of hazardous events

Industrial accidents and disasters are caused by a chain of faults causing errors and resulting in failures. The thinking behind traditional safety strategies is to prevent hazards by designing systems which are fail-safe. This can be done through redundancy or the use of technical measures for safety critical technical components (e.g. separation, diversity, oversizing) according to IEC 61508 for safety systems (see chapter 5.1). Additionally, hazards resulting in accidents can be prevented by organisational measures.

By means of interconnected systems, hazardous events can also be influenced by security attacks and not only by technical failures related to the system design. To prevent attacks, we have to understand the systems and manage their complexity (see chapter 7). To detect security vulnerabilities, risk assessments have to be done (see chapter 8.1) and technical and organisational measures have to be in place. The method of implementing different barriers for security is called Defence in Depth (including technical and organisational measures). The challenge to protect a critical safety system with completely interconnected systems is very high and safety cannot be guaranteed under all circumstances (as there is also no 100% safe system).

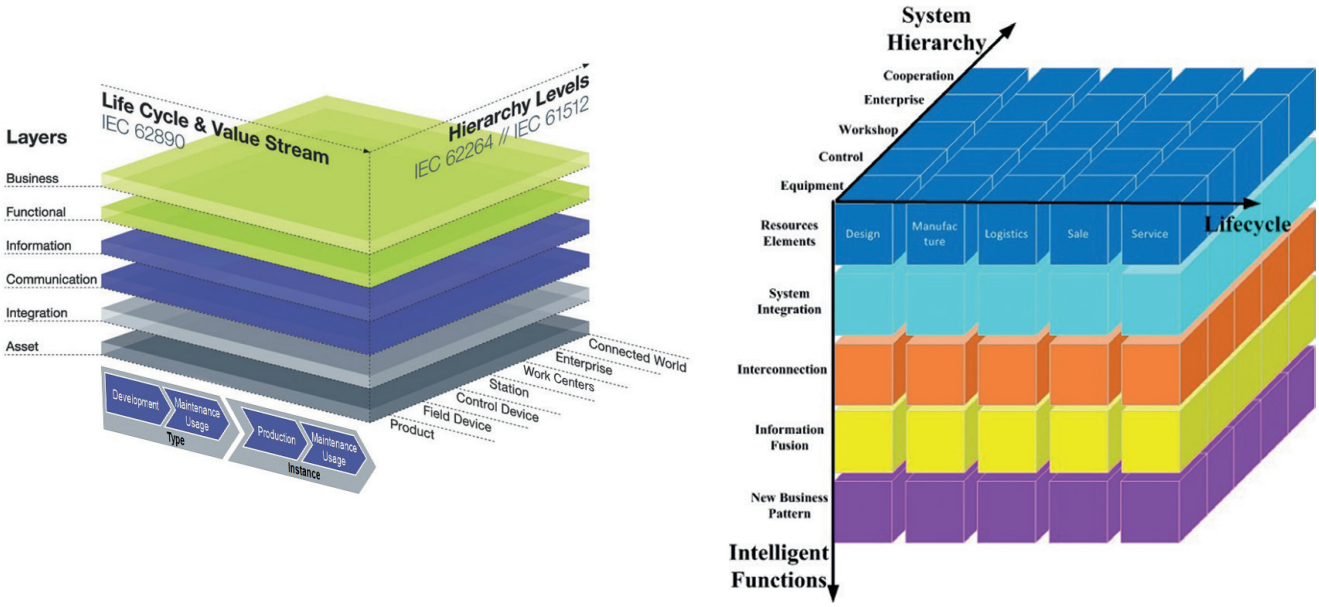
Figure 1: Risk reduction concept for low demand operation mode (from IEC61508-5)



6 Introduction to Industrie 4.0 and IM

The 4th industrial revolution has arrived in the industrial sector. It is characterised by the increasing digitisation and interconnection of production, systems, value chains and business models. The Chinese and German governments have each published respective Reference Architecture Models (Germany: RAMI and China: IMSA). The alignment of both models was agreed upon (see the White Paper entitled 'Alignment Report for Reference Architectural Model for Industrie 4.0/Intelligent Manufacturing System Architecture').

Figure 2: RAMI vs. IMSA



As shown in the figure, the RAMI 4.0 model maps the whole lifecycle and working scope of an industrial product or service along three axes. In the hierarchy axis, a smart factory can be abstracted as a pyramid model in which the enterprise stays on the top and is refined down to the control device level, the field device level and so on. The architecture axis represents different views of the product or service, such as the business view, the functional view, the communication view and the asset view. The production lifecycle axis covers the full lifecycle of a product/service while taking all participants such as supplier and integrator into account. RAMI 4.0 provides a standard framework for tracking details of a product or a service. For example, a safety function in the hierarchy axis can be mapped to relevant devices. In the architecture axis, the function is described in detail in the functional layer. To achieve the required safety goal, different production phases might be involved, e.g. the material quality needs to be defined in the design phase while being guaranteed in the purchase phase.
However, considering security requirements within the RAMI or IMSA model is even more complex. Firstly, the compromising target may not be the described product or service directly but only be a feature of it (e.g. availability/integrity or just an involved control device in the hierarchy axis). Secondly, a comprehensive attack can be achieved within the whole scope of the RAMI model. It may start from a lower hierarchy level to compromise a higher-level target (e.g. a factory station). In the architecture axis, it comes with its own business purposes, compromises important functions as well as goes through a specific communication topology. At last, the attack can be deployed in the beginning of the lifecycle and will be only triggered at a given point, as part of an Advanced Persistent Threat (APT). Accordingly, the security analysis should not be limited within a single level, layer of phase of the RAMI model, which means the search space is significantly increased. However, for a given attack, the RAMI or IMSA model provides a break-down view to analyse, discover and prevent or mitigate the attack with the knowledge of the product/service.

7 I4.0 and IM challenges and new risks to safety

7.1 Risks due to new technology

of functional safety, there is a wide range of challenges to be mastered. In this chapter, key aspects are highlighted and recommendations made for further evaluations.

In general, there is a potential conflict between I4.0 and IM applications and the conventional way of implementing functional safety solutions.

Conventional solutions for functional safety are implemented with a static scenario in mind, while the basic idea of 4.0 applications is a seamless integration with more dynamic changes among the elements making up an overall business application, not limited to automation solutions only but also covering business applications. It needs to be kept in mind that solutions for functional safety are implemented in order to bring the risk on a dedicated application down to an acceptable level.

This objective has top priority for all applications of functional safety and shall not be influenced by either the technology used or the individual application.

When thinking about functional safety and I4.0 and IM, the key factor is to make sure that the safety integrity required for attaining the anticipated risk reduction is achieved (see Figure 1 and description in Chapter 5).

This needs to be maintained during the entire lifecycle during all phases of operations, including patching and all other sorts of modification. That said, it needs to be kept in mind that for applications with very low safety requirements, the commercial benefits of an I4.0 and IM applications may prevail over safety considerations.

This, however, has to be looked at critically because even low-level safety solutions may cause hazards and legal implications when such a function does not work correctly.
A solution designated to realise a dedicated SIL recommendation has to be able to comply with the related safety recommendations irrespective of whether it is realised via hard-wiring, programmable, isolated or integrated into an I4.0 and IM environment.

Nevertheless, this does not mean that integrating solutions of functional safety into an I 4.0 and IM environment is not possible. However, the desired risk reduction capability needs to be maintained under all relevant aspects.

However, the interaction between safety and security, and their different requirements and types of implementation, are much more diverse. To take account of this fact, the IEC has set up a working group under the Technical Committee TC65 which has taken on the task of defining a framework for safety and security (project IEC TR 63069 Ed1). Within this framework, recommendations are given that arise from the interaction of these two complex topics.

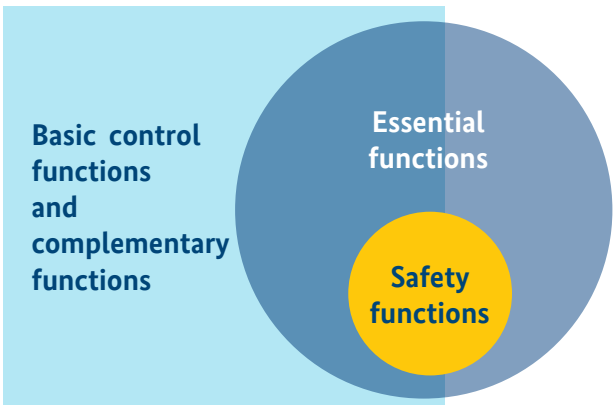
In order to develop this framework and provide recommendations, a dedicated risk analysis is needed so that new risks can be identified, and both safety and security aspects are considered in an adequate manner (see IEC TR 63069).

According to the rules applicable for the implementation of functional safety, the following main areas are to be looked at:

- The capabilities of the products to be used
- The design processes at application level
- The lifecycle support activities incl. testing and maintenance activities with a special focus on updating/ upgrading processes

Taking account of the applicable security standards (IEC 62443), the plan is to develop an overall concept under which different security recommendations are required in order to trigger action (zones and conduits) at different functional levels of an application. Safety functions are “essential functions” as per IEC 62443 and as such require particular attention (see below figure 3).

Figure 3: Correlation between different functional layers as per IEC 62443 (from IEC 63069)



In this document, the various situations that are encountered today are considered and a description of methods will be given on how functional safety can be realised and maintained in an I4.0 and IM workspace and protected against security threats through the implementation of security standards.

7.2 Creating a link between I4.0 and IM and Functional Safety

7.2.1 I4.0 and IM concept (axis 3 of RAMI)

When it comes to standard control devices and devices providing functional safety, the difference is as follows: for functional safety devices, additional attributes are defined.

These are:

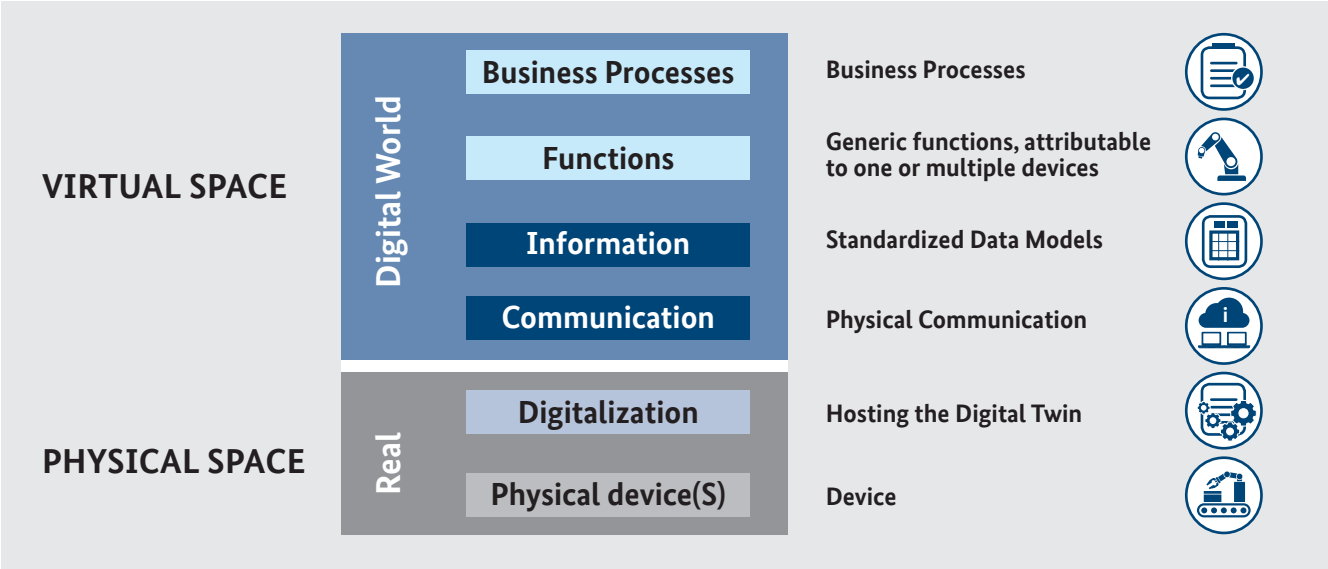
- Dedicated reliability recommendations (low probability of failures or sufficient fault tolerance)
- Modes of operations (low demand mode or high/continuous demand mode)
- Systematic capability, leading to dedicated recommendations for design, software and usage of a device

Anticipating that functional safety in general is a kind of an attribute of physical devices (or the way such devices are used), we have to look at axis 3 of RAMI, the dimension in which the physical layering of I4.0 and IM applications is described.

A given device is connected to an administration shell that is handling functions required to establish the functions of the 'digital twin'. The administration shell may be part of every device or may be hosted by a dedicated piece of equipment handling the digital twins of one or multiple devices.

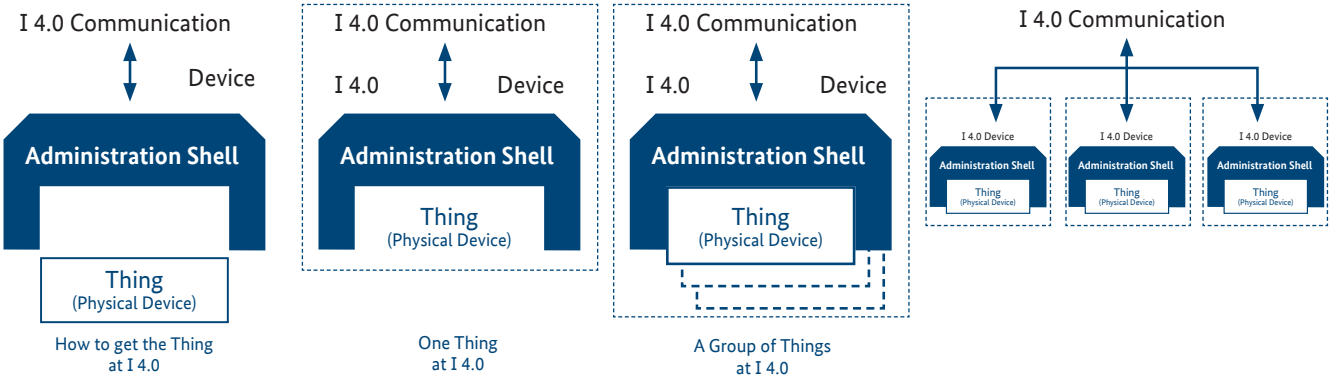
This administration shell covers all functions required to integrate devices into an I4.0 and IM application. Such a shell may cover either a single physical device (e.g. a sensor), a functional group of devices (e.g. a PLC including its field devices) or a complete production unit (e.g. a machine or a process unit).

Figure 4: Axis 3 of RAMI



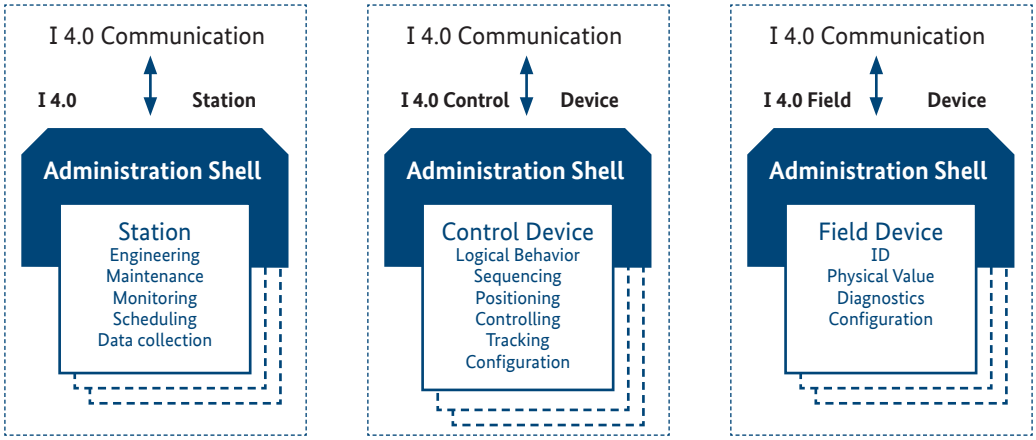
Looking at possible ways to integrate things (physical devices) in I4.0 and IM, the following can be anticipated:

Figure 5: Integrating things in I4.0



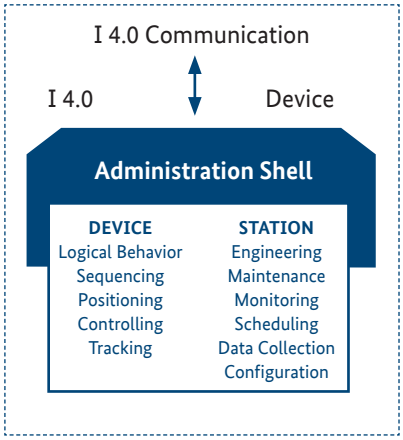
Looking at the I4.0 and IM definitions, there are in principle three kinds of I4.0 elements of relevance to the subject matter discussed here:

Figure 6: Different kinds of communications related I4.0 elements



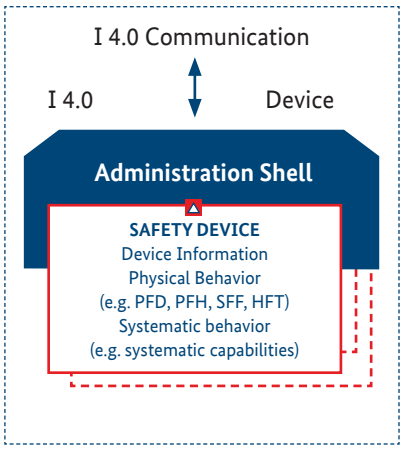
When looking at the specific constraints of functional safety, the following should be anticipate:

Figure 7: I4.0 Device



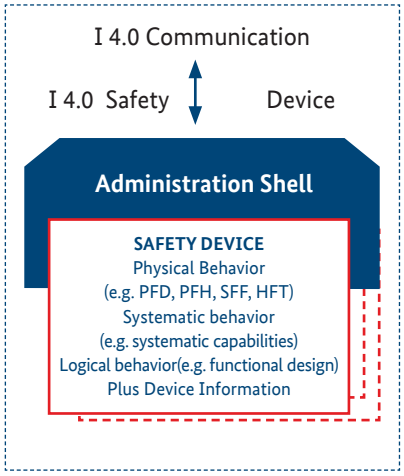
As described above, an I4.0 and IM component in the context of this document is either a device or a station. Each device/station is either equipped with an administration shell. Such an administration shell can either be used to handle an individual component or, alternatively, multiple components can be hosted in the same shell.

Figure 8: I4.0 Safety device



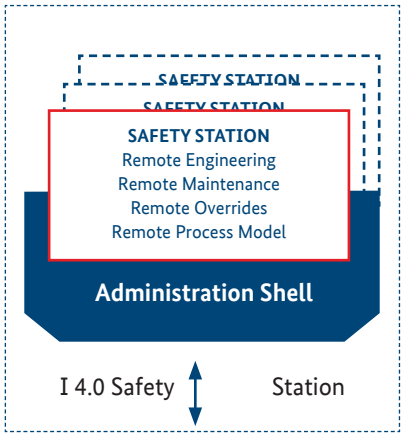
In the event that a safety related device (device with relevance for the safety application) is connected to an I4.0 and IM workspace, it is also attached to an administrative shell. The difference between safety and non-safety applications is that safety functions should not be negatively affected by non-safety functions (free from interference).

Figure 9: Safe Administration Shell



Generally, it is also feasible to define a safety related administration shell. In this case, the integrity of the safety function is also related to the administration shell. Such a shell might provide safe and non-safe communication.

Figure 10: Safe I4.0 Station



Based on that functionality, safety related devices and safety stations can be allocated in the I4.0 and IM workspace. A safety station is in essence built up following the same concept applied for a safety device too, however a station is connected to the area of business processes and interfaces between this part of the I4.0 and IM workspace and the data-handling domain.

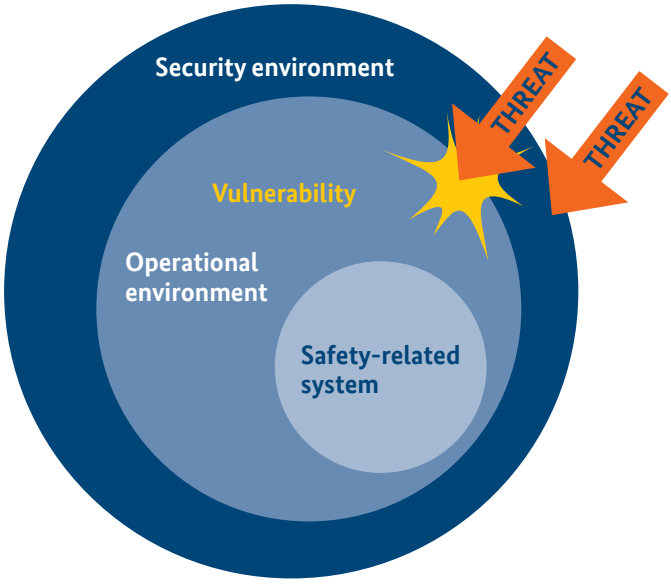
Looking at the specific safety constraints, the safety parameters will be attributed to the physical device(s). Either the physical device or the administration shell or a combination of both is protected by the security aspects.

7.2.2 Solution

Based on the special considerations for an I4.0 and IM workspace and the specific application, the relevant environment and perimeter need to be defined. This is necessary because achieving the overall safety and the dedicated risk reduction realised though functional safety requires a sufficient level of security to be achieved.

IEC TR 63069 introduces the concept of the security environment, which provides all security countermeasures necessary to sufficiently protect the operational environment of an I4.0 and IM workspace (see Figure 10a below).

Figure 10a: Security environment and its coverage of the operational environment of the system (from IEC 63069)



The security countermeasures are defined based on a security risk assessment of the security environment for the SM control system. This is required in order to ensure all relevant security protection targets, Confidentially, Integrity and Availability (CIA), the safety of the system under consideration (I4.0 and IM workspace) and the implemented safety functions.

The security risk assessment relies on the safety risk assessment of the I4.0 and IM workspace for determining the safety criticality. This is of particular importance, because for the time being, many of the applications will be realised by products that have rather different levels of security and also different safety features implemented.

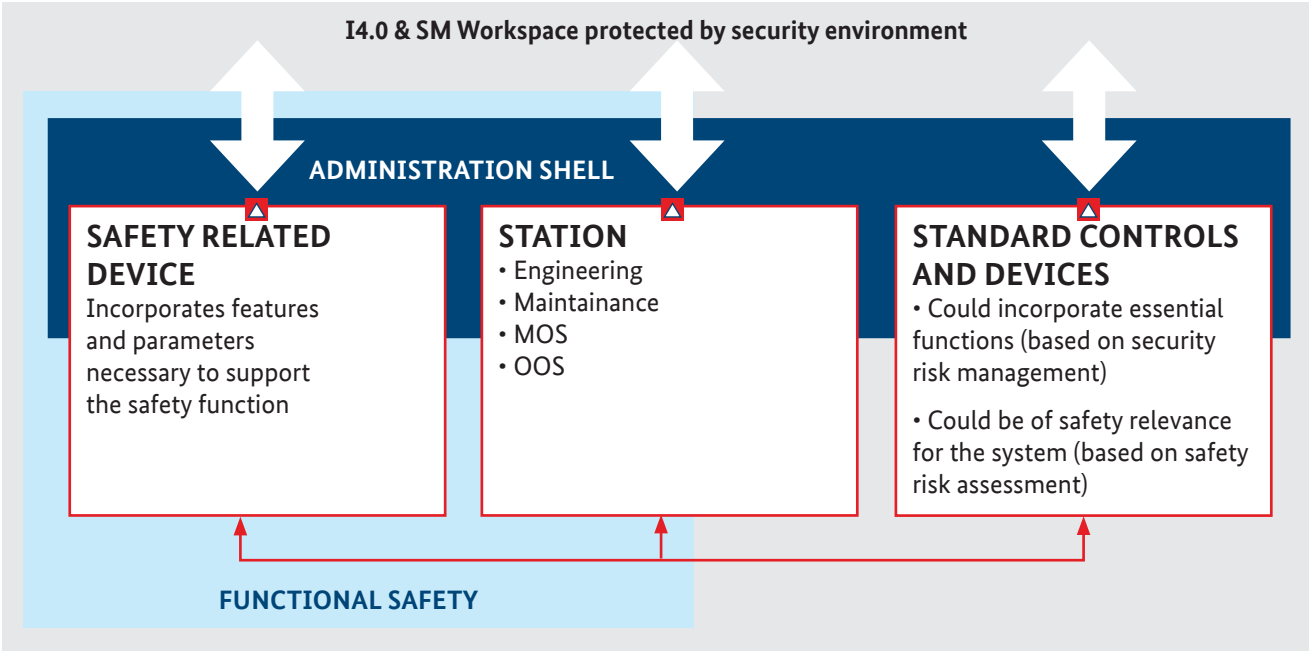
7.2.3 Protection of the I4.0 and IM workspace and safety-related installations

When transforming the stipulations of IEC 62443 and IEC TR 63069 into the terminology of I4.0, one of the options is outlined in Figure 11 (see picture below).

It is emphasised that the security environment does not correspond to a security zone, but to all security (counter) measures necessary to ensure sufficient security protection of an I4.0 and IM system, including aspects like defence in depth and the zone concept. These security (counter)measures might be within or external to physical devices in the system.

The essential communication (incl. safety communication) is covered by the (counter)measures of the security environment (see IEC TR 63069).

Figure 11: I4.0 & IM security environment for IM operational environment



7.2.4 Functional Safety for I4.0 and IM

Figure 12: I4.0 & IM workspace

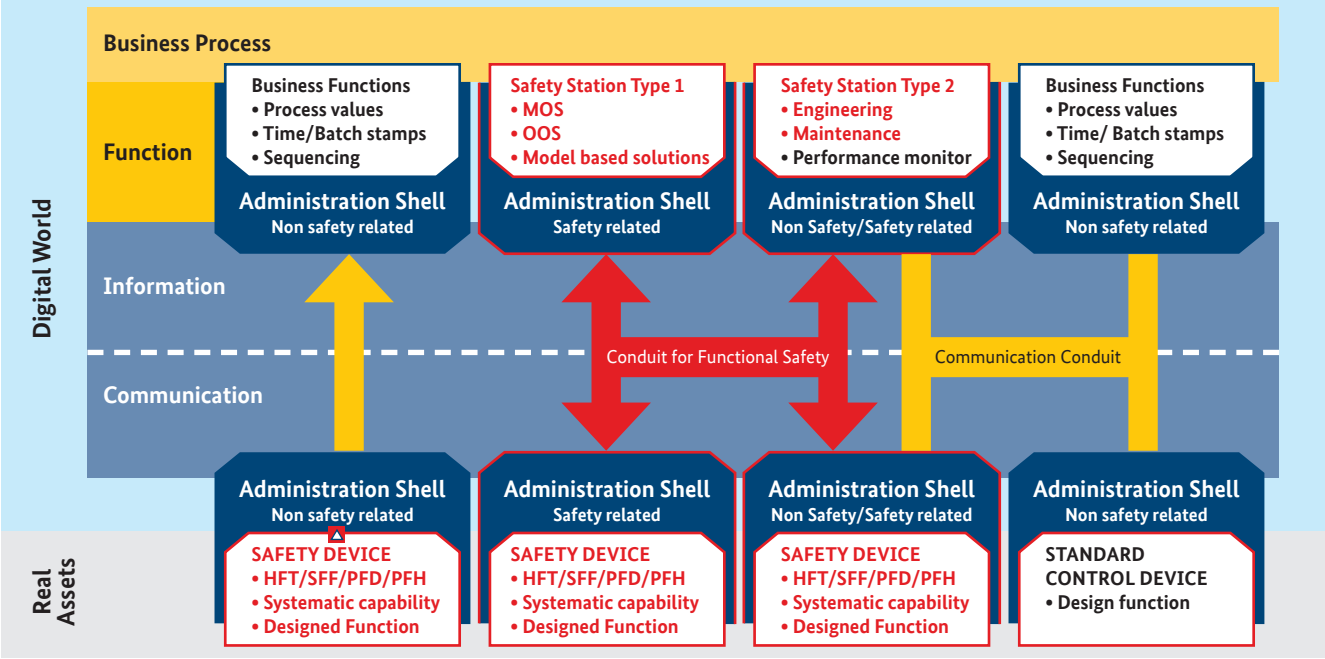


Figure 12 shows an installation of safety-related components in an I4.0 and IM workspace constituting the operational environment within the meaning of IEC TR 63069.

If the administration shell is safety-related, safety-related communication through the I4.0 and IM workspace is possible, allowing the connection of safety-related devices and stations allocated somewhere in the I4.0 and IM workspace. If such solutions (as per IEC 62443) are used, the related communication must be investigated for potential attack surfaces regarding security threats. Following the concept of defence in depth and in consideration of the criticality of essential functions as per IEC 62443, different architectural decisions on the implementation might be made.

7.3 Zones & conduits

In an I4.0 and IM workspace, the different components allocated at the different levels each communicate with one another using open protocols, such as Open Platform Communications United Architecture (hereinafter: OPC UA).

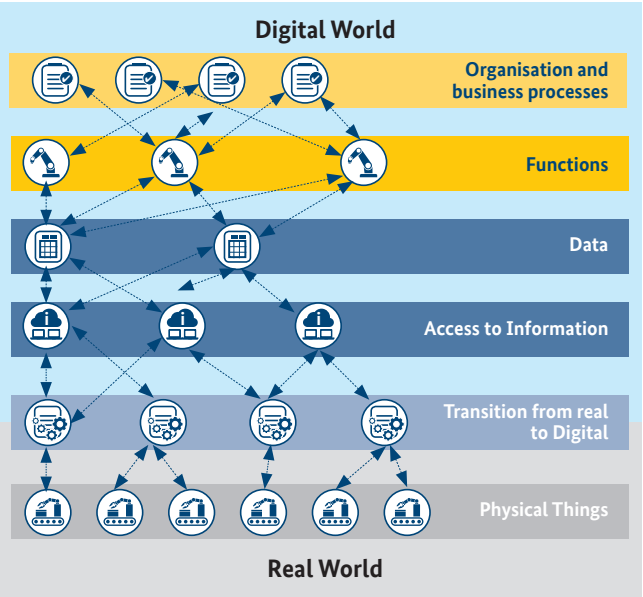
The communication can be organised either in 1-to-1 or m-to-n relations as required by the related business functionalities.

The infrastructure design and the layout of zones and conduits in such solutions need to be developed in line with the results of the security risk assessment, which has to consider the possible impact on the safety risk reduction required by the I4.0 and IM workspace.

7.4 Considerations for safe and secure communication

One of the key elements required to create a digital world is communication. Looking at the integration of safety functions, safety-related communication and its integration into a non-safety related communication environment is one of the most important aspects to consider. In addition to the individual I4.0 and IM recommendations, such communication needs to be protected by security measures that cover the recommendations defined for the security environment of the safety devices/stations.

Figure 13:Zones and conduits in I4.0



Due to the constantly escalating threat of cyber-attacks, not least due to enormous attacks conducted in recent years on industrial facilities worldwide, but also the thoughts on I4.0 and IM applications, the demand for secure and safe transmission protocols is growing.

The interaction of safety and security plays an important role for the entire automation system, or at least for the safety part of the system, and this applies in particular to industrial communication. In fact, this communication is the link to surrounding systems and from a security point of view is therefore a highly sensitive area in need of protection.

It is IEC 61508 Part 2 which deals with the safety of electronic systems in general and refers to functionally safe communications. This purpose is addressed in IEC 61784-3, which is part of the IEC 61784 series of standards and deals with the communication in industrial processes in general. Other sector-specific standards, such as IEC 61511 or ISO EN 13849, refer to IEC 61508 for functionally safe communication or, more recently, to IEC 61784-3 as well.

According to IEC 61784-3, functionally safe protocols have to be able to deal with the following communications errors in line with the black channel principle:

- Corruption (of messages)
- Unintentional repetition (of messages)
- Incorrect sequence (of messages, e.g. commands in the wrong sequence)
- Loss (of messages)
- Unacceptable delay (message data too old)
- Insertion (messages from unexpected sources)
- Masquerade (messages generated by functionally non-safe elements and treated as functionally safe messages)
- Addressing (delivery of messages to wrong recipients)

IEC 61784-3 also lists several measures for dealing with these errors, including sequence numbering, time stamping, time expectation, and connection authentication. An essential point is data redundancy, e.g. by means of Cyclic Redundancy Checks (hereinafter: CRC).

Along with the characteristics of the actual backup procedure, e.g. CRC, an evaluation of the data redundancy efficiency must take the Bit Error Probability (hereinafter: BEP) within the communication channel into account. Standard-compliant implementation of the indicated error control is highly non-trivial.

Secure communication is always relevant when leaving protected networks (protected by the security environment) and passing through public or semi-public networks. This does not only apply, for example, if the internet or GSM is used for communication. It must also be assumed that external access is possible when WLAN (Wi-Fi) routes are used.

Security communication in the area of industrial communication is covered by the IEC 62443 series. Overall, the origins of the various methods vastly vary. However, all cryptographic methods have one thing in common: they have to withstand critical analysis by other recognised cryptologists in order to gain general acceptance.

Ultimately, it is assumed that, when passing through a public (note: the specification analysis performed has shown that OPC UA, in contrast to many other industrial protocols, provides a high level of security) communication infrastructure, encryptions and decryptions taking place at various points (e.g. provider transition) beyond operators' control are to be applied. 'Public' in this sense means that communication between different devices and/or stations (see Figure 13) is routed through infrastructure components that are not under control of the I4.0 and IM workspace operator (black channel principle), but that still need to be considered when carrying out the security risk assessment and to be protected by countermeasures from the security environment.

Currently, OPC UA is the only industrial protocol that has comprehensively integrated security features. The German Federal Office for Information Security (*Bundesamt für Sicherheit in der Informationstechnik,* hereinafter: BSI) has conducted a security analysis of OPC UA. The report of this analysis was published in April 2016.

OPC UA relies on established, modern cryptography and has decided to use TLS. The 'Main results' section of the above-mentioned BSI report clearly identifies a basic problem of secure communication:

No systematic errors could be detected.
When analysing the reference implementation, basically the following problems were identified: [...]"

Such work is currently being done in the development of the OPC UA Safety communication protocol (a joint activity by the OPC foundation and the PNO), which will subsequently be transferred to the IEC. The key aspects of the work for OPC UA safety are:

- Uses OPC UA client/server (OPC UA pub/sub with or without TSN later on)
- Unidirectional, bidirectional, and multicast communication patterns
- Arbitrary network topology: line, tree, star, ring, mesh, ...
- ·Arbitrary structured user data, length: 1-1500 bytes
- Dynamic establishment of safe connections during runtime
- No requirements on regular (i.e. non-safe) network participants
- No need for synchronised clocks
- Unlimited number of network components and terminals
- Unlimited data rate

The concept is based on IEC 61784-3 series standards (functional safety for fieldbus)

- Cyclic communication, watchdog (local clock of the consumer suffices)
- 32-Bit CRC-polynomial:
- "Properness" shown for all data lengths between
- 1-1500 bytes
- calculated PFH-value suffices for SIL4
- IDs are used to detect authenticity errors such as misdirected telegrams
- A Monitoring Number (MNR) is used to detect timeliness errors

In respect to the new complexity of I4.0 and IM, it has to be ensured that fault models (see encryption example below) of functional safe communication are state of the art and are furthermore compatible with the cryptographic methods used to secure communication.

In the meantime, all so-called interferences have to be handled by the safety communication. IEC TC65 SC65C WG12 is about to work on a corresponding amendment.

Example of encryption for safe communication:
In this example, we consider an issue that impacts on the performance of the safety-related protocol transmission: adding a HASH to the transmitted data which keeps the safe protocol untouched and enables standard communication infrastructure to be used. The benefit of such a strategy is that if vulnerability is detected in the HASH, only the infrastructure can be updated, while the safety protocol remains untouched.

This leads us to the following considerations:
Imagine that a short safety telegram is transmitted, which is encrypted. Many safety telegrams only contain 12 bytes. To simplify matters, we will not consider the entire protocol with the associated CRC, headers, etc., but only the pure data content of 12 bytes (1 byte = 1 ASCII character).

- An error is inserted into the encrypted Data 1.
- The information is then decrypted.

After the decryption, it becomes visible that the decrypted text is very different from the original message. If this had been a piece of safety-related information, the bit failure mechanism of the protocol used would have been challenged to address this situation. In our example, 66 out of 128 bits are impacted by the change of 1 bit. The IEC SC65C WG12 is working on this and other issues related to safety communication use cases of the I4.0 and SW workspace.

Table 1: Example of data 1 failure in the safety telegram

	ASCII	Hexadecimal
Original text	123456789a12	31-32-33-34-35-36-37-38-39-61-31-32-00-00-00-00
Encrypted information	Ëç .cSZ.£;É«Òee.	Cb-a2-88-8c-63-53-5a-11-a3-3b-c9-ab-d2-65-65-13
Impacted by transmission error	Ëç .cRZ.£;É«Òee.	Cb-a2-88-8c-63-52-5a-11-a3-3b-c9-ab-d2-65-65-13
Decrypted text	i.¸ÓÜ"^Àoú.ÇÅ.w	69-00-b8-d3-dc-22-5e-c0-6f-20-fa-87-c7-c5-1a-77

7.5 Risks due to system complexity and interconnectivity

The increased complexity of automation solutions for an I4.0 and IM environment may potentially lead to an increased level of risk that would need to be considered. On the other hand, itis anticipated that the application of I4.0 and IM will create commercial benefits due to the more flexible, seamlessly integrated engineering and production processes used.

The future challenge will be to identify the optimal combination for flexibility, design complexity and maintainability. The most effective way in which this can be done is by defining individual use cases including related structures.

However, even in an integrated I4.0 and IM workspace there will need to be clustered structures so that different areas of applications can be handled as required.

Example: process industry:
The engineering process requirements for a Safety Instrumented Function (hereinafter: SIF) as per IEC 61511 requiring a lot of activities for the implementation and monitoring of

- Training of people, functions and equipment
- Design reviews
- Safety assessment

Based on this assumption, the implementation of the SIF, even in an I4.0 and IM environment, will be different from the implementation of a standard automation (non-safety) function.

In order to make sure the additional functionality (which is in effect what I4.0 and IM is) of I4.0 and IM does not lead to uncontrollable complexity, appropriate structural approaches need to be developed and implemented. Especially when looking at axis 3 of RAM,I it can be maintained that the implementation of I4.0 and IM does not necessarily affect the complexity at the functional safety level at all. However, this strictly y depends on how such implementation is done and how different functional aspects are taken into consideration during the process of designing a solution.

Example:
When applying the black channel communication principle to interconnect a safety device and a safety station, there will be no difference between an I4.0 and IM application and a conventional one; if you decide, however ,to integrate the safety related administration shell required at functional level, you will end up with a level of complexity that is tremendously higher.

In fact, the overall complexity of an I4.0 and IM application is higher than the complexity of an application that does not follow I4.0 and IM principles. By applying an appropriate design process, such complexity can be mastered

Example: cloud computing:
When using cloud computing, there are 2 possibilities in terms of the underlying principle:

A: If the safety devices connected to the cloud do not support such applications, the cloud needs to be analysed and in this case will be part of the safety system. The cloud will need to comply with the same SIL requirements applicable for the safety devices and stations.
B: If the safety functions connected to the cloud maintain sufficient fault detection algorithms, a kind of black channel principle may apply when the cloud is not investigated to meet SIL requirements.

Mastering complexity is the key challenge – especially when talking about functional safety. This can be achieved based on more intense cooperation between experts in the areas of functional safety, information technology (hereinafter: IT) and operational technology (hereinafter: OT) security. IEC TR 63069 addresses this by introducing a joint security risk assessment and management process making sure that an appropriate security environment can be formed so that systems of functional safety can be operated securely during their entire lifecycle.

7.6 Risks due to system interoperability

In the event that security vulnerabilities are detected, it is beneficial to be able to eliminate these as quickly as possible. Such corrective action (e.g. patching) may or may not have an impact on the safety function.

Based on this, there are areas where robust (time consuming) development processes are not the highest priority. An example of this kind of application is the software for devices in the communication infrastructure. In the event that a switch or a router has vulnerability, this has to be corrected as soon as possible. If such a device goes on to be integrated into a safety device, such a correction would mean the safety device being modified.

If such measures are kept separated (e.g. by using the black channel communication concept), it would be possible to modify the communication infrastructure without modifying the safety implementation.

By following the concept of protecting the operating environment incl. the essential functions and safety functions from simulation systems hosting the digital twin in the digital space , flexibility can be maintained and even technology that has not yet been proven in use may be utilised, without the operation and the safety of the I4.0 and IM application being harmed.

When implementing functional safety and big data, artificial intelligence (hereinafter: AI), internet technology and a new generation of information technology – including fuzzy boundaries – may create an additional risk. However, if they are implemented using a proper strategy as described above, such additional risks can be minimised.

7.7 Risks due to lack of maturity of intelligent technologies and products

Where new technologies such as AI (or cognitive systems) are used, it is essential to develop a risk determination process for these technologies.

As long as such processes are not available, the application of current AI solutions requires restrictions to be placed on the scope of their supervised or unsupervised actions. Currently, initial activities are under way to look at the integration of AI in safety applications. This, however, is an area where further research need to be undertaken before safety applications relying on AI are used in an industrial setting.

8 Safety in the context of security

8.1 Preconditions to be met by the security framework

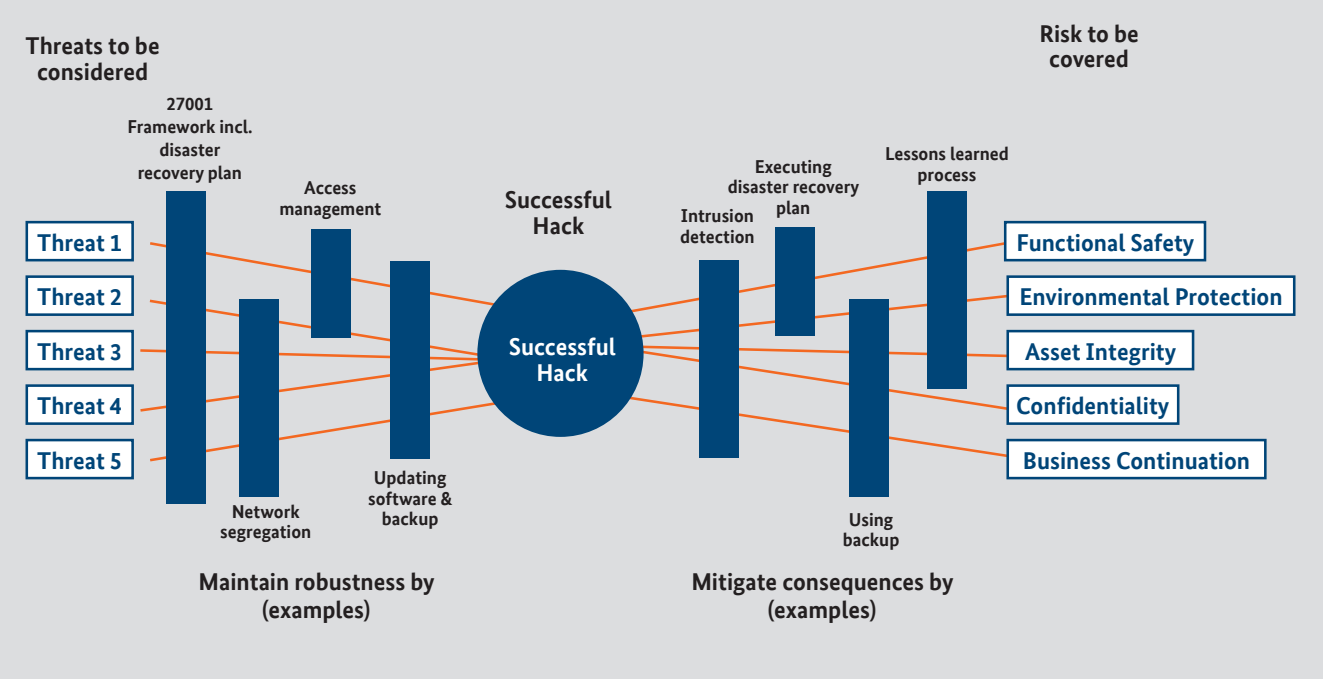
8.1.1 Domain-specific knowledge

The figure below shows a generic security-related threat-risk model.

- Threats exploit the vulnerability of ICS
- No countermeasures might represent an intolerable risk (for assets)
- Generally, countermeasures are required to minimise risk (for assets)

In addition, in the event that a successful attack takes place on a system, measures to mitigate the consequences of such an attack should be defined.

Figure 14: Context element relationships for security (from IEC 62443-1-1:2009)



8.1.2 Security grading

Security grading is essential for setting up a comprehensive security framework, as needed in the context of intelligent manufacturing and digital plants. Security grading is a key concept for expressing graded security needs, security requirements and, following this , adequate security architectures, security by design and graded security tests.

The IEC 62443 standard series provides the adequate basis for this. These standards in particular do not just address Security Levels (hereinafter: SL), but also the contribution of maturity levels towards IACS protection levels.

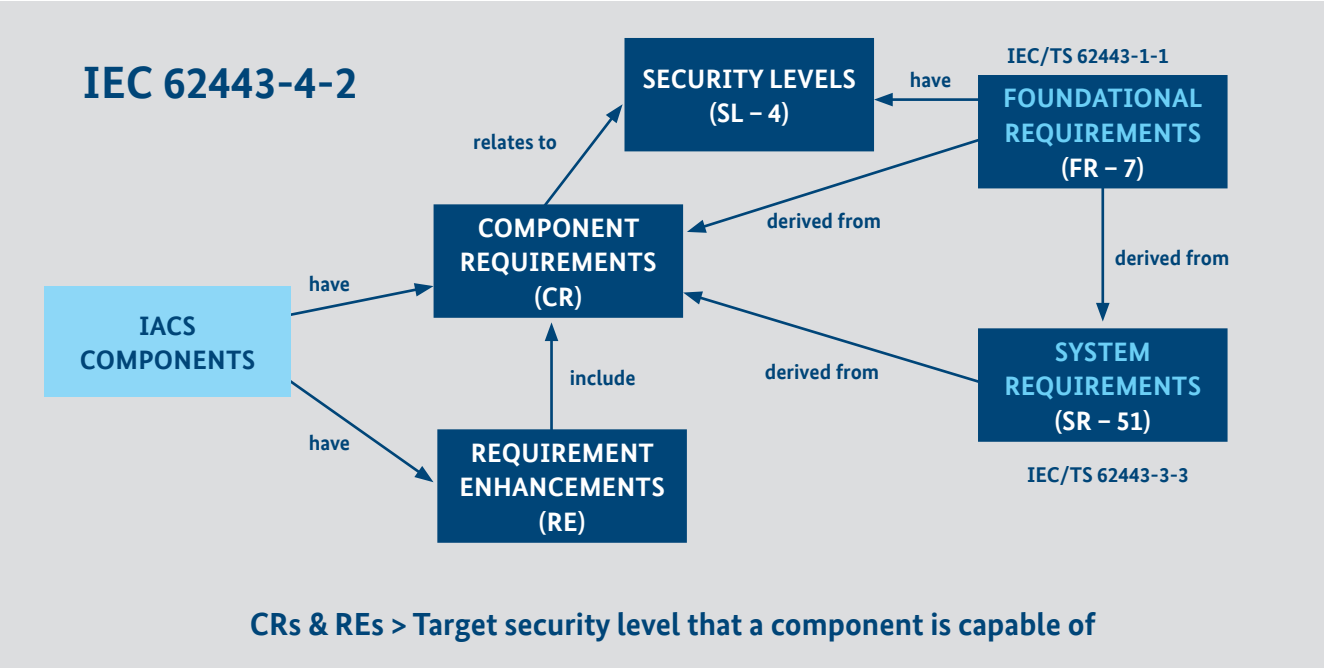
Three different types of security levels can be defined by the IEC 62443 series:

- SL (target) – target security level for a zone or conduit
- SL (achieved) – achieved security level of a zone or conduit
- SL (capability) – security level capability of countermeasures associated with a zone or conduit or inherent security level capability of devices or systems within a zone or conduit.

8.1.3 Security requirements

The subsequent figure indicates several types of security-related requirements that are addressed by IEC 62443.

Figure 15: Different requirement types in the IEC 62443 context



In general, the correlation is as follows:

- The solution or parts of the solution (based on different threat environment considerations) need to comply with a dedicated target security level (SL-T)
- Relevant components / functions based on their functionality need to comply with requirements for a dedicated Security Level (SL-A)

A potential gap between SL-T and SL-A needs to be covered via configuration and additional measures like firewalls or encryption devices etc. In addition to security grading, other pre-conditions that need to be met by a security framework include considerations of security requirements and support for meeting these requirements. In order to meet these requirements, the following aspects should be supported by a security framework in particular:

- It should be possible to refine security requirements.
- Security requirements should relate to the security grading, e.g. the SL indicated in the above figure.
- Security requirements should be specific to the main lifecycle phases.
- It should be possible to trace security requirements to security objectives and security controls, in order to demonstrate that all security requirements have been addressed.
- Security requirements should be sufficiently precise and self-contained so that selected requirements can be grouped and forwarded to sub-suppliers along the supply chain.
- Security requirements should take safety requirements into consideration, where applicable. This may similarly relate to quality requirements for the implementation of security controls as to the implementation of safety related software, firmware, FPGAs, mixed criticality system (virtualised hardware) etc.

8.2 Preconditions to be met by the Functional Safety framework

8.2.1 Domain-specific knowledge

A production process may be understood as a system whereby, based on a controlled process, raw materials and energy are converted into products and energy. In order to control the inherent risk in the production process, safety measures are implemented. The role of the safety measure is to make sure that in the event of a malfunction either in the production process or the controlling device, dangerous situations can be avoided by reducing the risk in the production process to a value smaller than the tolerable risk. The way in which the safety device is planned, designed and analysed is key to achieving functional safety.

8.2.2 Functional Safety grading (extract from IEC 61508)

SIL is used for functional safety grading and is the most core index for this purpose. Safety integrity levels are used for specifying the safety integrity requirements of the safety functions to be allocated to the E/E/PE safety-related systems. A SIL is not a property of a system, subsystem, element or component. The term "SIL n safety-related system" (where n is 1, 2, 3 or 4) is often referred to on the business markets. The correct interpretation of the phrase "SIL n safety-related system" is that the system is potentially capable of supporting safety functions with a safety integrity level up to n. There are 4 SILs specified by 2 kinds of target failure measures:

8.2.3 Functional Safety requirements

To achieve functional safety, first a safety lifecycle and a safety management system need to be established. Then the design of the safety-related system is to meet all of the following requirements:

a. The requirements for hardware safety integrity comprising;
   - the architectural constraints on hardware safety integrity, and
   - the requirements for quantifying the effect of random failures

b. The requirements for systematic safety integrity (systematic capability), which can be met by following one of the compliance routes set out below:
   - Route 1S: compliance with the requirements for avoiding systematic faults and with the requirements for controlling systematic faults, or
   - Route 2S: compliance with the requirements for furnishing evidence that the equipment is proven in use, or
   - Route 3S (pre-existing software elements only): compliance with the requirements of IEC 61508-3, (see chapter 7.4.2.12).

c. he requirements for system behaviour on detection of a fault.
d. The requirements for data communication processes.

Table 2: Safety integrity levels – target failure measures for a safety function operating in low-demand mode of operation

Safety integrity level (SIL)	Average prohability of a dangerous failure on demand of the safety function (PFD_{avg})
4	$\geq 10^{-5}$ to $< 10^{-4}$
3	$\geq 10^{-4}$ to $< 10^{-3}$
2	$\geq 10^{-3}$ to $< 10^{-2}$
1	$\geq 10^{-2}$ to $< 10^{-1}$

Table 3: Safety integrity levels – target failure measures for a safety function operating in high-demand mode of operation or continuous mode of operation

Safety integrity level (SIL)	Average frequency of a dangerous failure of the safety function h^{-1} (PFH)
4	$\geq 10^{-9}$ to $< 10^{-8}$
3	$\geq 10^{-8}$ to $< 10^{-7}$
2	$\geq 10^{-7}$ to $< 10^{-6}$
1	$\geq 10^{-6}$ to $< 10^{-5}$

8.3 Challenges of achieving safety while also considering security

8.3.1 Overview

It's not an easy task to consider safety and security at the same time. Safety focuses on the potential result of an occurrence defined as a risk. This means that something is identified as a safety problem if there is an unacceptable risk of damage to people, property or the environment. A security problem is independent of the result of the occurrence. A security problem refers to illegal or unwanted penetration, interference with proper operation or inappropriate access to confidential information regardless of the motivation (intentional or unintentional) or consequence (result).

It can be said that both safety and security imply the need for protection. However, the chosen protection must address risks that are radically different in nature. There is an important similarity: neither safety nor security is a one-time event. As indicated in IEC 61508 and ISA 99, a common mistake is to address safety and cyber security as a project with a start and end date. When this occurs, the safety and the security level will tend to decline over time. Risks to cyber security constantly change in particular as new threats and vulnerabilities surface along with the implementation of ever-changing technology. It is no longer possible to be truly safe without also being secure. However, the challenge is to not only address security issues, but to also get the most from the ability to connect systems and share data. There seems to be a fine line between security and productivity.

8.3.2 From the Perspective of Safety Concerning Security

In IEC 61508:2010 and IEC 61511-1:2016, there are some clauses mentioning security, for example:

- IEC 61508-1:2010 Sub-clause 7.4 Hazard and risk analysis (sub-clause 7.4.2.3)
- IEC 61511-1:2016 (sub-clause 8.2.4)

However, there are no specific cybersecurity requirements in IEC 61508:2010 and IEC 61511:2016 and these standards are not designed to address related threats, such as insiders introducing malware, software updates and default passwords. IEC 61508 does not set out the requirement for any specific action to be taken to enhance or ensure cybersecurity. IEC 61511 just lays down the requirement for access control to critical systems.

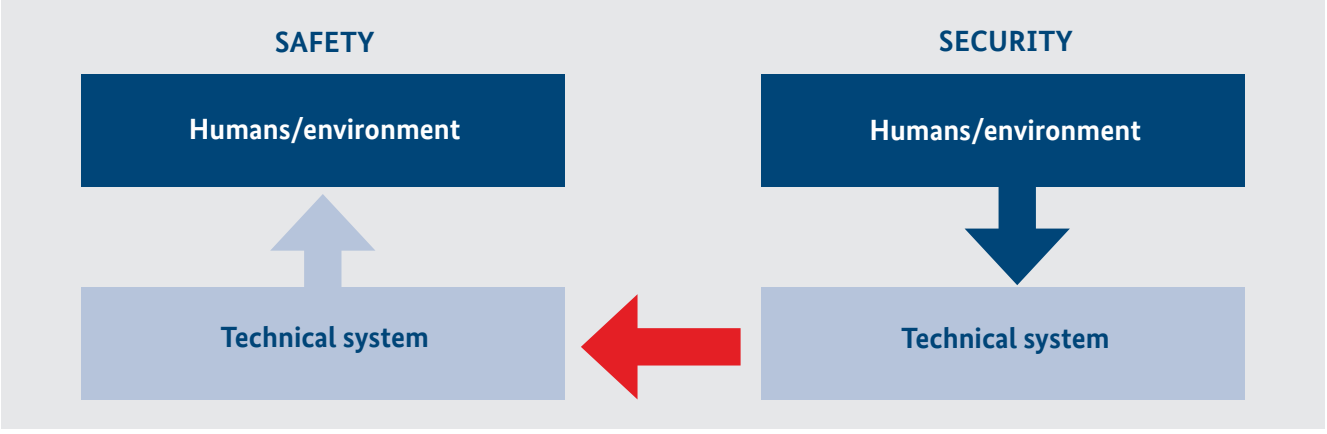
There are continuing discussions in the expert community as to whether specific requirements on cybersecurity would be appropriate and effective in these standards. ACSEC Guide 120 does not recommend the inclusion of such requirements (see also 8.3.3).

8.3.3 From the Perspective of Security Concerning Safety

Some parts of the IEC 62443 series sometimes use the structure of the Basic Process Control System and the Safety Instrumented System within an IACS and describe a way of installing these in the process industry. However, such architecture descriptions and wording anticipate a certain implementation which is not deemed necessary to meet the needs for safety or security. In IEC 62443, safety functions are treated as parts of the whole IACS, without taking into account the special safety property. In draft IEC GUIDE 120 security aspects – guidelines for their inclusion in publications (not yet officially published), sub-clause 7.3 sets out the points of security documents.

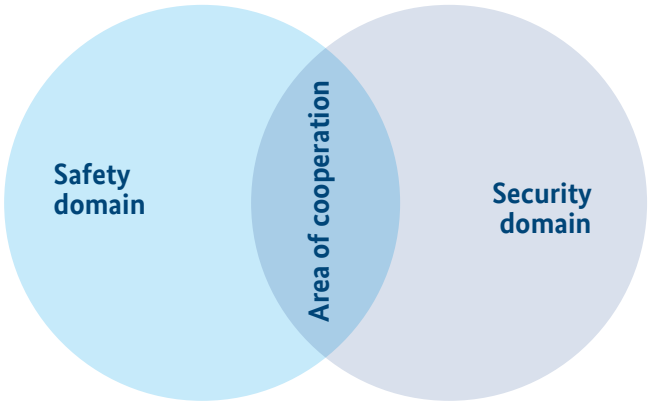
The viewpoints of Guide 120 are very clear. If we consider the process from threat to hazard as an "event chain", the first half is the responsibility of security policy (before invading the systems), the latter half is the responsibility of safety (capability of system to prevent and control failures from random, to systematic, even to intended). But the de facto scenario is more complex, for example the threat may attack the End-User Control (hereinafter: EUC) or EUC control systems instead of safety-related systems to trigger shutdown frequently and result in the field operators wrongly thinking that the problems do not lie with the safety-related systems.

Figure 17: Interrelation between functional safety and security (from IEC GUIDE 120)



8.4 Gaps in current standards and guidance

Figure 18: High-level view of functional safety and cybersecurity



Standard series **IEC 61508 r**equires **unauthorized behaviour and manipulation** to be considered within the **Hazard and Risk Analysis**. **IEC 61508** refers to standards series IEC 62443 which does not directly refer satisfactorily to functional safety. IEC 62443 defines "essential functions" and defines safety functions as essential functions.

Possible vulnerabilities of such safety-related systems (the term safety-related systems in this context can relate to more parts of the I4.0 and IM than just the functional safety-related systems) have come into question in industry as some sectors have been cyberattacked and organisations and governments attempt to secure important infrastructure against such cyberattack. For I4.0 and IM, interconnection and interoperability are the basic requirements, so conventional industry control networks need to connect to the plant information system, even the internet. Whilst the IT industry is further ahead in relation to cybersecurity, the priorities for IT are different from those of OT, and the solutions and mechanisms used are not necessarily applicable to industry and industrial control systems (CIA or AIC). There are some international standards on the joint use of safety and security technology published in recent years, but the viewpoints of different documents vary. A simple list is provided in Table 4.

Table 4: Documents related the joint consideration safety and security

Organization	Title of the documents	Main context
IEC/TC65/WG20	IEC/TS 63069 Ed. 1.0 Industrial-process measurement, control and automation framework to bridge the requirements for safety and security	Develops recommendations for applying safety standards and security standards in parallel for IACS, which is the scope of TC65. The safety standards addressed can include IEC 61508, which is a basic safety standard. The output of WG20 can include suggested priority for applying requirements of safety and security, but WG20 does not intend to modify existing standards for the time being. The concept and approach of WG20 may be referenced by other TCs.
ISA84 WG9: Security in safety	ISA 84.00.09 Cybersecurity related to the functional safety lifecycle	Provides guidance on the work process and countermeasures used to reduce the likelihood of a security breach of the process control system, SCAI and SIS that degrade the ability of the IACS to perform its function(s) in order to satisfy company-specified risk criteria.
IEC/TC44 Safety of machinery - electrotechnical aspects	IEC TR 63074 ED1 Security aspects related to functional safety of safety-related control systems	This technical report considers aspects of security threats and vulnerabilities that may lead to the loss of the ability to maintain safe operation of a machine (safety measures) in relation to safety-related control systems.
IEC/TC121A Low-voltage switchgear and controlgear equipment	IEC TS 63208 Low-voltage switchgear and controlgear security aspects	This technical specification contains information on the topic of security for the low-voltage switchgear and controlgear industry.
IEC/TC45/SC45A Nuclear instrumentation & control and electrical power systems	IEC 62859:2016 Nuclear power plants – Instrumentation and control systems – Requirements for coordinating safety and cybersecurity	This international standard establishes requirements and guidance to integrate cybersecurity provisions into nuclear I&C architectures and systems which are fundamentally tailored to safety; to avoid potential conflicts between safety and cybersecurity provisions; to aid the identification and the leveraging of potential synergies between safety and cyber security.

8.5 Safety management with consideration of security

Functional safety management is essential for all safety-related systems and for all stages of the overall safety lifecycle. In claiming conformance (irrespective of the target SIL), it is necessary to show that the management of the design, operations and maintenance activities and of the system implementation is itself appropriate and that there is adequate competence for carrying out each task. This involves two basic types of assessment. The first is the assessment of management procedures. The second is an assessment of the implementation of these procedures. Hence, the lifecycle activities are audited, for one or more projects, to establish that the procedures are being put into practice.

Security also requires many management activities to achieve security goals. Some of them could be aligned with safety while others need additional measures to avoid conflicts

There needs to be co-engineering to organise safety and security, especially in:

- Security risk assessments to appropriately consider the impact on safety
- Processes which facilitate the co-engineering activities; it needs to be ensured that the efficiency of both the safety as well as the security measures defined during the design of an application are kept efficient during the entire lifecycle
- Human competence, especially a new category of experts familiar with industrial security
- Modification management. Modification management should be established. Procedures should be developed to assess the potential for adverse effects on both safety and security when changes are made to the EUC or EUC control system (including configuration, execution status, etc.).

8.6 Lifecycle with consideration of safety and security

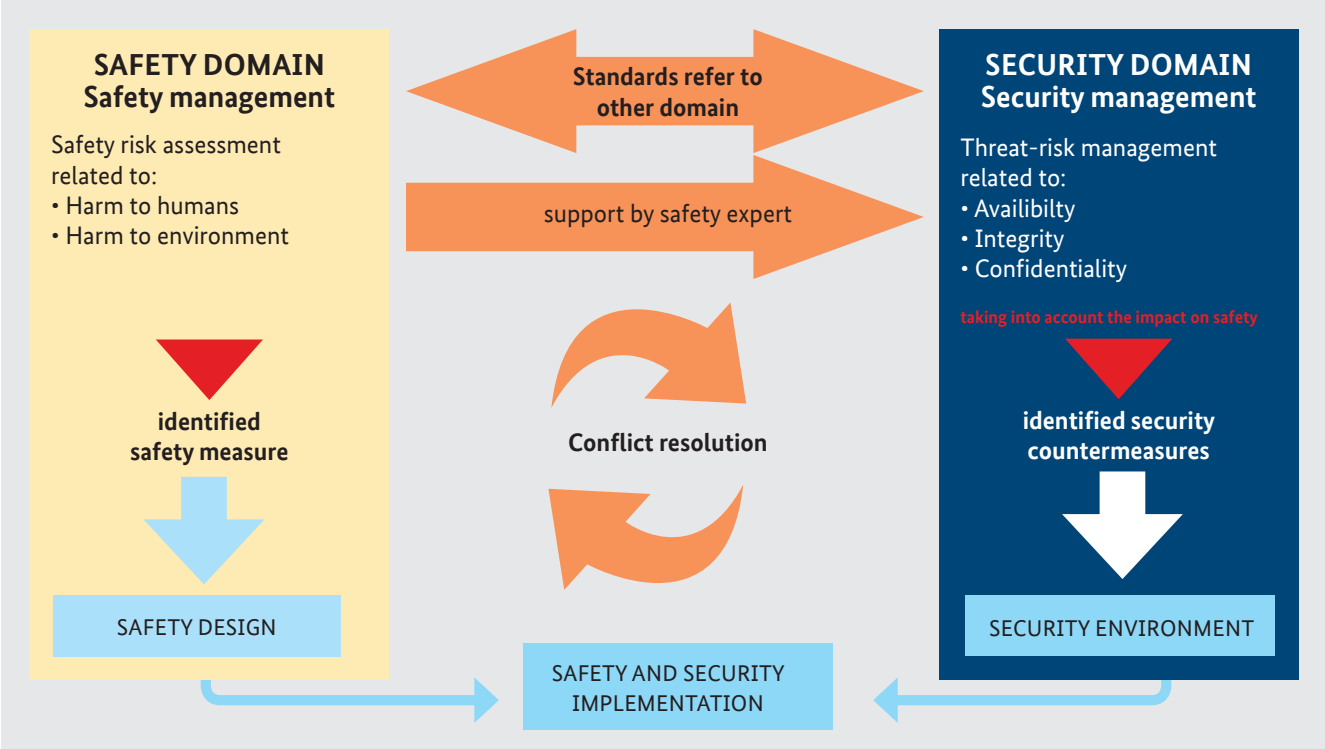
8.6.1 General information

From the high-level view, engineering the safety and security of control systems does have similarities. Both are concerned with attempts to prevent unwanted things happening, with assuring the absence of those events.1 General processes can be summarised as follows

- Determine the objective and scope (device, data, human, environment, etc.)
- Find the weak points (hazard, vulnerability) and their extent (risk)
- Provide measures to control the weak points

Although there are no mature solutions for safety and security integration during the main lifecycle phases, it should be noticed that some tools and methods are helpful to facilitate this. IEC TR 63069 provides some basic concepts for this.

Figure 19: Comparison of lifecycle phases based on IEC 61508 and IEC 62443 (from IEC 63069)



1 *A High-Level View of Safety and Cybersecurity*

8.6.2 Risk assessment

A unified risk assessment (threat-risk assessment in IEC TR 63069) that contains both safety and security aspects should be performed to identify potential impacts (on safety) and vulnerabilities (for security). The aspects of smart factory/digital plants should be part of the consideration.

Generally, the safety function could be jeopardised by security threats, which may result in the safety function becoming inoperative. Possible security threats that could affect functional safety are usually affected by human attackers. Further possibilities are from other devices/systems connected to the EUC CONTROL SYSTEM or safety-related system, or from the reaction/failure of a security countermeasure itself.

Malicious external hackers/insiders could attack the critical infrastructure or even the safety-related system directly if they have the possibility to operate directly in the plant or operate the device itself (in the event that there is a lack of physical and organisational protection). In addition, well-meaning employees who have privileged access to the IACS could for example bring in security threats through unintentional operation. Security vulnerabilities in corporate networks/personal computers could result in security threats to the EUC control system and the safety-related systems that are connected to it.

These security threats could be based on the vulnerabilities caused by hardware failures and systematic failures, e.g. software bugs in the EUC control system and safety-related system.

8.6.3 System implementation

To achieve safety and security compatibility, the following could be considered (the specific security (counter)measures for I4.0 and IM are to be defined in the risk assessment):

a. Physical compensation measures might be necessary for access control. Key areas such as central control rooms, cabinet rooms, and engineer rooms are protected by physical access control (guards, access control, room locks), video surveillance, etc. Only certain types of known people are allowed to visit. Visitors need to be accompanied by authorised personnel and to be registered.
b. Usage of locked cabinets. Unnecessary interfaces such as USB, optical drives, and wireless devices on the industrial host should be removed or closed. The user should closely monitor the important security devices such as software dogs and authorised U-disks in the management system.
c. Segmentation into zones and border protection. Safety networks may be connected to the EUC CONTROL SYSTEM and corporate networks for the required interconnectivity and interoperability. Therefore, additional considerations to ensure boundary protection may need to be made for the network interfaces of safety-related systems, including dedicated firewalls for safety-related systems, authentication and authorisation for access from networks, read-only access for the safety-related system, input validation/integrity check on data/commands sent to the safety-related system from networks.

   Particular attention has to be paid to the management systems of the communication infrastructure in use. In the event of unauthorised access, it is possible that a critical security gap is present.

d. Usage of safety and security communication protocols. Conventional safety-related systems normally use proprietary communication protocols for safety communication. However, a general communication protocol, e.g. Ethernet-based protocol, could be widely used in the smart factory/digital plant. This threat surface requires specific attention and might require the use of specific technology. Security countermeasures designed to protect the data in transit should be enhanced especially.
e. Remote access control. Remote access is not common in conventional safety applications but could be widely supported in smart factory/digital plants. This situation increases the risk of eavesdropping and spoofing threats in particular, e.g. man-in-the-middle attacks. Security countermeasures for remote access control should be supported, and security could be improved by detailing policies and procedures for each deployment.

8.6.4 Engineering and systems integration

To truly ensure functional safety, it is necessary to integrate security protection measures.

a. In order to ensure that the commands executed by the safety system come from legitimate users, there are 2 different paths to be followed:
   – The network used for transmitting such commands is sufficiently protected from unauthorised users.
   – The users accessing the system must be authenticated, and commands issued by uncertified users are not executed. In the control protocol communication process, it is necessary to add the constraints of the authentication to prevent the attacker from establishing a session by intercepting the packet and obtaining the legal address, thus affecting the process safety.
b. Different types of operations are to require the authentication of users with different permissions to operate.
c. In the design of safety communication protocols, appropriate encryption measures need to be used for sensitive information to ensure that the information exchanged between both parties is not used for preparation of a man-in-the-middle attack or other harmful undertakings.
d. The safety control system should be code tested before it is put into use to check the public defects in the software. The integrity check measures are used to verify the safety control software, and software tampering is discovered in a timely manner. Make backups of safety control software and configuration programmes. For further details please refer to IEC 61508/ GB/T 20438.
e. Measures for the detection, prevention and recovery of malicious code could be implemented, making sure the safe state can be maintained even under influence of malicious code.
f. Changes and upgrades of the safety-related system need to be carefully tested in a test system and a detailed rollback plan developed. Important patches need to be tested and deployed as soon as possible. For general patches, only the necessary patches are tested and deployed.
g. The safety-related system vendors should in a timely manner repair the vulnerabilities in the control system or provide other alternative solutions, such as closing the ports that may be used.
h. In-depth filtering of protocols using industrial firewalls to track the content of communications between safety control systems and devices in real time.
i. Security monitoring and auditing can detect network security incidents in time to avoid security incidents and provide detailed data support for investigation of security incidents.

8.6.5 Operation and maintenance

Efforts to realise both functional safety and security in the phase of operation and maintenance can be closely related and interwoven because the objectives of both security and safety activities in this phase are the same, i.e. achieving the required safety. The security activities should therefore consist of enhancements to the mature operation and maintenance procedures for safety in a plant, and security risks should be considered as part of the organisation's risk management processes. In normal operation and maintenance operations, the activities generally involve response to safety/security events and possible modification of safety-related systems. The measures for monitoring, logging and response to both safety and security events set out below should be applied.

Monitoring of normal operation

During the normal operation of safety-related systems, online monitoring of safety-related systems takes place continuously via the Human-Machine Interface (hereinafter: HMI), and user access to the safety-related system for programming is usually inhibited via the system configuration. In the context of the smart factory/digital plant, the use of remote access e.g. via mobile devices for the monitoring of information at an HMI may be common, but should be limited in such a way that safety is not harmed by it (e.g. read only, limitations of values to be written to a dedicated value etc.). In this case, confidentiality of the monitored data is of the most concern from a security point of view. All flows via public networks should be confidentiality protected, e.g. encrypted, remote access should be logged, and proper authentication and authorisation for remote access control should be applied, making sure a man-in-the-middle attack is prevented.

Routing maintenance and inspection

Concerning aspects of safety, routing maintenance on safety-related systems involves activities including proof testing, inspection, bypassing and any preventive maintenance activities. In general, these activities should be performed by trained personnel as planned and also properly documented.

- Proof testing should be performed as planned using a written procedure to prove that safety functions work as defined in the SRS, and inspection should be performed periodically to detect any unauthorised modifications. Actual demand rates and causes of demand should be recorded to check whether discrepancies exist between actual and expected application.
- Bypassing should only be permitted if compensation measures are in place to provide adequate risk reduction. The bypass operation should be authorised, logged and time-limited (for further Information please refer to IEC 61511 / GB/T 21109).

Regarding aspects of security, inspection of system software and security countermeasures should be performed periodically, e.g. to check whether the security configuration has been changed. In addition, security mechanism verification should be performed periodically to check whether all security counter-measures are configured and work as designed.

Response to failure/security event

If a failure is detected in the safety-related system, the maintenance procedure should be performed in line with the maintenance plan, including response to the diagnostic information, repair and re-validation after repair. In the event of security event triggering the safety system, the event and the response of the counter-measure should be logged and monitored. It should be analysed in such cases whether the system response was in line with the SRS.

In addition, an override mechanism should be in place for emergency responses because security countermeasures need to ensure that operator intervention is not forbidden (hindered) by the security design if immediate failure response is required

Modification

Modification of any part of the safety-related system should be analysed for its possible impact on safety. Normally, this is covered by a mature modification management procedure for safety. When security is considered, additional modification management for security countermeasures should be included. This includes monitoring, testing and release of updates/patches for security countermeasure software, as well as re-validation after modification.
A concept should be prepared describing how this can be achieved during the entire lifecycle of the application.

Bibliography

C. Baylon, R. Brunt and D. Livingstone, Cyber Security at Civil Nuclear Facilities: Understanding the Risks. The Royal Institute of International Affairs (Chatham House), October 2015. Retrieved from https://www.chathamhouse.org/publication/cyber-security-civil-nuclear-facilitiesunderstanding-risks, accessed 2015-05-23.

UK Health and Safety Executive, Cyber Security for Industrial Automation and Control Systems (IACS), March 2017. Retrieved from http://www.hse.gov.uk/foi/internalops/og/og-0086.pdf, accessed 2017-05-23.

P. Bieber, J.P. Blanquart, G. Descargues, M. Dulucq, Y. Fourastier, E. Hazane, et al., Security and safety assurance for aerospace embedded systems. In: Proceedings of the 6th international conference on embedded real time software and systems (ERTS2 2012), Toulouse, France; 2012.

T.J. Cockram, S.R. Lautieri, Combining security and safety principles in practice. In: Proceedings of the 2nd institution of engineering and technology international conference on system safety; 2007.

Security and safety modeling – D2.1 specification of safety and security mechanisms, vol. 1; 29 May 2013.
Security and safety modeling – D3.1 specification of safety and security analysis and assessment techniques, vol. 1; 29 May 2013.

T Novak, A Treytl, A Gerstinger, Embedded security in safety critical automation systems. In: Proceedings of the 26th international system safety conference (ISSC 2008), Vancouver, Canada; 2008

Conducting Accident Investigations Revision 2 ,
U.S. Department of Energy Washington, D.C. 205851999]

Table of Abbreviations

Industrial Automation Control Systems	**IACS**
Industrie 4.0 and Intelligent Manufacturing	**I4.0 and IM**
TBINK-AK IT-Security and Security by Design	**TBINK-AK IT-Security**
Instrumentation Technology and Economy Institute	**ITEI**
Standardization Administration of the People's Republic of China	**SAC**
Chinese Committee on Functional Safety and Industry Security	**TC124**
Major Accident Reporting System	**MARS**
European Commission	**EC**
Safety Integrity Level	**SIL**
Performance Level	**PL**
German Reference Architecture Model	**RAMI**
Chinese Reference Architecture Model	**IMSA**
Advanced Persistent Threat	**APT**
Confidentially, Integrity and Availability	**CIA**
Cyclic Redundancy Checks	**CRC**
Bit Error Probability	**BEP**
Open Platform Communications United Architecture	**OPC UA**
German Federal Office for Information Security / Bundesamt für Sicherheit in der Informationstechnik	**BSI**
Safety Instrumented Function	**SIF**
Artificial Intelligence	**AI**
Information Technology	**IT**
Operational Technology	**OT**
Security Level	**SL**
End-User Control	**EUC**
Human-Machine Interface	**HMI**