



Guide Cyber Security Check of OT

A Guide for the Implementation of Cyber Security Checks of
Operational Technology (CSC-OT) in Industry and Automation

Publisher:

ISACA Germany Chapter e.V.
Storkower Straße 158
D-10407 Berlin

www.isaca.de
info@isaca.de

Team of authors:

- Martin Ennenbach
- Sebastian Fritsch
- Markus M. Lörsch
- Markus J Neuhaus
- Dirk Schugardt
- Christian Schwartz
- Andreas Teuscher
- Gregor Wittkowski
- Peter Böck
- Jordan Rahlwes
- Michael Krammel
- Mike Hofstetter
- Volker Reers
- Reinhard Erich Voglmaier
- Stefan Ahne
- Thomas Klir
- Markus Ruppel
- Detlef Hösterey
- Peter Loos
- Wolfgang Stadler
- Philipp Fath
- Erik Gremeyer
- Daniel Kastner
- Markus Müller
- Sven Super
- Alexander Junkermann
- Matthias Goeken

The contents of this publication was developed by members of the ISACA Germany Chapter in cooperation with the BSI and have been carefully researched. It reflects the views of the ISACA Germany Chapter. Despite the greatest possible care, this publication makes no claim to completeness. ISACA Germany Chapter accepts no liability for the content.

The latest version of this guide is available free of charge on the ISACA chapter Germany website:
https://www.isaca.de/de/veroeffentlichungen/cyber_security.

All rights, including the right to reproduce extracts, are reserved by the ISACA Germany Chapter e.V.
Edition: November 2021

Guide

CYBER SECURITY CHECK

OF OT

**A Guide for the Implementation of
Cyber Security Checks of Operational
Technology (CSC-OT) in Industry and
Automation**

Alliance for Cyber Security

With the Alliance for Cyber Security (ACS) founded in 2012, the Federal Office for Information Security (BSI) aims at strengthening the resilience of the business location Germany against cyberattacks. As of March 2021, this initiative comprises 4772 members, 152 partners and 100 propagators, who contribute to enhancing cyber security at the business location Germany.



With the Cyber Security Check V2 published in February 2020, ISACA Germany Chapter e.V. (Working Group Cyber Security) contributed to enhance the classic office IT. As a supplementary measure, ISACA Germany Chapter e.V. updated the “Cyber Security Practitioner” certificate course developed in cooperation with BSI.

Inspired by the positive user experience with the Guide Cyber Security Check V2, ISACA Germany Chapter e.V. decided to develop a Guide Cyber Security Check for Operational Technology (CSC-OT). The CSC-OT Guide is intended for persons and auditors who can use the six-step procedure to raise the operational security level of production systems and process systems.

Preface

German Electrical and Electronic Manufacturers' Association (ZVEI)

The threat of cybersecurity attacks has been growing for years. Cyberattacks and ransomware target increasingly not only traditional information technology (IT) but also operational technology (OT).

The Guide Cyber Security Check, which is available already in a second version, provides an excellent introduction to cyber security of IT of companies and government agencies. It is an important contribution to the topic as such and to raising awareness for cyber security.

The new guide CYBER SECURITY CHECK OT, as the next step, offers a reader-friendly way to understand the security of OT. The progressing interconnection between IT and OT, leading to the disappearance of boundaries between these fields, raises the challenges even more. Among the member companies of ZVEI, cyber security in business operations has become an ever more important topic. Cyberattacks pose an increasing threat to the workflows on the shop floor, where interruptions and downtime have an even greater impact and thus can cause higher losses. In addition, it is often impossible to quickly “reboot” the production, and troubleshooting requires more effort.

Many ZVEI members have pooled their expertise in the new guide, which provides substantial added value, particularly to small and medium-sized companies. Only through the continuous sharing of information and experience with networks such as the Alliance for Cyber Security (ACS), government agencies and associations such as ZVEI can we reach our common goal of a cyber-resilient industry.



“The resilience level in IT as well as OT must be adjusted to the increasing threats. The persons in charge of cybersecurity must take up this race and continuously expand their knowledge. The ISACA Guides make a very important contribution in this regard.”

Dr. Wolfgang Weber
Chairman of the Executive Board
ZVEI – German Electrical and Electronic
Manufacturers’ Association

German Mechanical Engineering Industry Association (VDMA)

The dependence on working IT/OT systems in global supply chains poses a central challenge to the networks of economy and society. Successful cyberattacks on critical infrastructure and its suppliers are not isolated incidents anymore. The cybercriminals' precision in attacks on medium-sized industrial companies has increased, whereas risk awareness and readiness to invest in cyber defence often struggle to keep pace.

Particularly the mechanical and plant engineering industry in its role as integrator of networked systems and functions needs a coordinated approach for a reliable defence against cyberattacks. Only the trustful cooperation between operator, mechanical engineer, component supplier and service provider enables the protection of production systems and industrial plants throughout the entire investment period.

In the field of IT, the ISACA Guide Cyber Security Check provides a good basis for medium-sized companies. However, the risks and their mitigation are not limited to the shop floor. Therefore, VDMA supports the development of a coordinated approach to industrial security.

To this end, experts from production, software development, and cybersecurity have been regularly discussing the topics of OT/industrial security within the VDMA network for about 10 years. The question of how to introduce the OT topic within one's own company, identify the risks and manage them lies at the heart of these discussions. The objective must be to prepare adequately for an emergency.

On behalf of the mechanical engineering industry, we thank the contributing experts for creating this guide. We wish the readers an interesting and informative read.



“Cybersecurity is not a sprint – it is a marathon on a constantly changing track. Only together can we protect production systems in an adequate and sustainable manner. The ISACA guides provide a good starting point for medium-sized companies to achieve this objective.”

Thilo Brodtmann
Managing Director
German Mechanical Engineering Industry
Association

Federal Office for Information Security (BSI)

Digitization shapes our lives day after day: An office without IT is already hard to imagine. The increasing automation and connectivity have found their way into production shop floors, machinery, and equipment. New potentials for the IT projects, production systems and business models of tomorrow have been opening here as well, for example, through the developments in the context of “Industry 4.0”. Technological development knows no rest and demands a great deal of decision-makers, administrators, developers, engineers but also all employees. Driven by this fast-paced change, we must not neglect security considerations. After all, control systems play an important role in many aspects of our lives, as we can see from the example of critical infrastructures. This dependency will further increase as digitalization progresses.

The impact of cyberattacks could be observed in the last few years in the numerous disruptions of production at small and large companies. The BSI report “Status of IT Security in Germany 2020” has also determined a high risk exposure for private users, companies, and government agencies. These threats are produced by increasingly professional perpetrators. There is a long victims list; in many cases, there has been massive damage, in some cases, there have even been business closures. We expect that production systems will also increasingly shift into the criminals’ focus.

In view of this situation, sound risk management must not only be a standard feature of corporate governance today but must also include cyber threats and cyber security controls. Focusing on IT alone is not enough, control and automation systems (OT) must also be considered in their entirety.

ISACA and BSI, the federal agency for cybersecurity in Germany, have been cooperating closely since 2014 to raise the awareness for cyber security in the IT as well as OT among the relevant stakeholders and to develop practical guidelines to determine the status quo. At the end of the day, it is impossible to separate digitalization and cyber security from each other.

With the Cyber Security Check of Operational Technology (CSC-OT), ISACA and BSI now take account of the rapid change in the cyber world and the increasing requirements for the protection of production systems. At the same time, the basic IT controls have been substantially revised and have been included in the control objectives.



“I am pleased that you are addressing this topic and I wish for this guide to assist you in the optimization of your cyber security controls as best as possible.”

Arne Schönbohm
President
Federal Office for Information Security (BSI)

International Data Spaces Association e.V. (IDSA)

In five years, the implementation of the EU Data Strategy will be completed and individuals and organizations will have regained control over their data. The basis for this vision is the concept of data spaces – secure environments where participants can freely share data by adhering to a fixed set of rules that ensures data sovereignty and guarantees transparency and fairness. Data spaces are the “level playing field” of the European Data Strategy. They enable interoperability and combine all kinds of data end nodes – countless sources and hollows consisting of smart objects, data marketplaces, cloud platforms, and the data of individuals, open sources, and databases. Data spaces can offer “data sovereignty by design” – this is a huge benefit in itself and paves the way for the data economy.

Data sovereignty is based on the premise that the data at every level of the data value chain have been assigned clearly defined user rights. This requires technical infrastructure and contractual regulations: Data linkage or data analysis may be prohibited or permitted; third parties may be forbidden or authorized to access data. In order to adequately protect data spaces against attacks from cyber space, we need technical and organisational controls.

The International Data Spaces Association (IDSA), as a non-profit organization with over 130 member companies from 22 countries, has defined a reference architecture and formal specifications which have been incorporated in the architecture of GAIA-X and in many data spaces of European design.

Well-proven and pragmatic cybersecurity controls that are widely accepted by companies lead to the creation of data spaces with thousands of participants who constitute an essential element of the national economy and the European market. This is the only way to implement the great visions of the European Data Strategy and enter a new era in the data economy.



“We need the commitment of the entire economy, robust standards and entrepreneurial thinking everywhere to secure a new competitive edge for Europe through the smart use of industrial data.”

Lars Nagel

CEO

International Data Spaces Association

ISACA Germany Chapter e.V.

ISACA Germany Chapter e.V. is the German branch of the worldwide leading professional association of IT auditors, IT security managers and IT governance officers. The association was founded in 1986 and, with more than 3,200 members, it is part of the international ISACA association, to which more than 140,000 experts in more than 180 countries worldwide belong. The association aims to promote understanding for the problems relating to IT auditing, IT security, cybersecurity and IT governance through discussions and exchange of information between members and interested parties and to share these insights with all members and interested parties through publications and seminars.

The Guide Cyber Security Check of Operational Technology (CSC-OT) has been created in cooperation with our partners and the members of the Working Group Cyber Security of ISACA Germany Chapter. I would specifically like to thank the experts of operational IT security for contributing their expertise, since, in addition to knowledge on information technology, this field requires further knowledge about production systems and process systems.

The CSC-OT thus reflects the reality of automation today having reached such a high level of connectivity that networked systems have become essential to production and controls. However, existing methods of isolating sensitive critical infrastructures and controlling dataflows are increasingly pushed to their limits. The future challenge related to the new requirements in Industry 4.0 environments with an even higher level of connectivity require trustful cooperation.



Guiding principle: “The security of information systems and communication systems is an integral part of modern production. Without security there can be no Industry 4.0 and no customer trust.”

Andreas Teuscher
Head of Working Group Cyber Security
ISACA Germany Chapter e.V.

Table of Contents

1	Introduction	13
1.1	Motivation and Background	13
1.2	Objectives of This Guide	15
2	Cyber Security for Operational Technology (OT)	17
2.1	OT and Industrial Control Systems	17
2.2	Evolution of Technology and Industry 4.0	20
2.3	Risks and Cyber Threats to OT	21
2.4	Cyber Security Concepts of OT	25
3	Principles of the CSC OT	32
4	Implementation of a Cyber Security Check OT	34
4.1	Object of Assessment	34
4.2	Approach	35
4.2.1	Step 1 – Mandate	35
4.2.2	Step 2 – Risk Assessment	36
4.2.3	Step 3 – Information Review	39
4.2.4	Step 4 - Preparing the On-Site Assessment	40
4.2.5	Step 5 – On-Site Assessment	41
4.2.6	Step 6 – Follow-up Evaluation/Preparing the Report	41
4.3	Implementation Quality/Personal Certificate	42
4.4	Assessment Methods	42
4.5	Binding Control Objectives	42
4.6	Assessment Scheme	43
4.7	Preparing the Assessment Report	44
5	Glossary and Definitions	47
6	References	53
7	Control Objective	54

1 Introduction

In the current reporting period (2020), the trend towards targeted attacks on entire networks of companies or other organisations continues.

The attacks targeted, for instance, car manufacturers and their suppliers, various airports or airlines as well as less known companies with high sales volumes. Small companies with unique selling points, for example, manufacturers of specific components in the machine-building sector, or companies with poor protection mechanisms were also attacked.¹

1.1 Motivation and Background

Nowadays, also due to digitalization and Industry 4.0, everyone is talking about cyber security.

The Allianz Risk Barometer 2020² has named cyber security incidents as the most critical business risk for companies worldwide, followed by operational downtime caused, for example, by disruptions in digital supply chains. The World Economic Forum also classifies cyber security incidents as one of the highest global risks. Despite this, many organisations go about their business relatively free from suspicion.

A negative answer to the question “Am I a target at all?” must not give reason not to protect oneself. Incidents often occur as collateral damage of unspecified malware attacks (Petya, WannaCry, the hacker group “REvil”). More than 230,000 computers in over 150 countries were infected (by Petya and WannaCry, respectively). German companies such as Beiersdorf and Deutsche Bahn, the Danish shipbuilding company Maersk, the Russian oil company ROSNEFT, the US pharmaceuticals company Merck Sharp & Dohme and many more were affected by the attacks.

Often the primary focus is on technology and there particularly on information technology (IT) as presumable targets. However, another

-
1. Situation report on the IT security in Germany 2020 | Vulnerability, <https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2020.html>.
 2. <https://www.agcs.allianz.com/news-and-insights/news/allianz-risk-barometer-2020-de.html>

very important field of cyber security focuses on production systems and process systems controlled by industrial control systems, so-called operational technology (OT).

In 2010, the computer worm Stuxnet, which had been developed to target specifically the SCADA systems of the manufacturer Siemens, achieved widespread, albeit dubious, fame. It enabled the manipulation of frequency converters controlling, for example, motor speed. Stuxnet was presumably intended for the sabotage of the Iranian nuclear program, for infecting and destroying the relevant control systems. Although this attack was supposedly attributable to government circles, it shows drastically the technical possibilities of manipulating control systems of industrial systems. Further malware of Industroyer (2016) and Triton (2017) have demonstrated the permanent threat to OT systems/ industrial control systems (ICS). The frequency of security incidents in ICS environments has increased [see SANS 2019 State of OT/ICS Cybersecurity Survey] and the attack vectors have evolved at a dramatic pace in this relatively short period of time. However, despite prominent security incidents and improved exchange of information, there are still barriers between OT experts and cyber security experts of traditional office IT. This guide aims at building a bridge between them and thus removing obstacles to the further development of the cyber security of OT systems, especially in Industry 4.0 environments.

Due to the technological development, the risk exposure and the legal requirements, operators of process systems are directly confronted with the topic of cyber security and must know their cyber security risks. Among the relevant legal requirements, the German IT Security Act plays a major role. It requires operators to prove their security status. The requirements and the resulting obligations for operators of critical infrastructures aim to ensure that these operators' IT systems meet the highest security standards, since a disruption or impairment of the supply services would have drastic consequences for the economy, country, and society in Germany. This guide is not meant to fulfill the requirements for operators of critical infrastructures; however, it can create a basic understanding of where these requirements need to be considered when IT security controls are defined.

1.2 Objectives of This Guide

The Cyber Security Check of OT has been designed for all companies that use automation systems, for example in production, chemical industry, pharmaceuticals production, water supply, transport and traffic, healthcare, and technical facility management.

The intended readers are all persons responsible for, or working on, the security of process systems and production systems. This includes managing directors, plant managers, production managers, shift supervisors, and automation experts. Due to its practice-oriented style and compact presentation, this guide should be also of interest to persons who are not cyber security experts.

The term cyber security describes here the protection against threats from the Internet to the systems or processes connected to the Internet. The term sounds technical and suggests a technical solution for the security issues at the interface to the cyberspace. In practice, the focus of employees and management indeed often lies on the technical aspects. It is however important to point out that cyber security always requires collaboration between technology, individuals, and organisations.

With the help of the Cyber Security Check of OT (CSC-OT) companies can determine the current cyber security level of their industrial control systems. The objective is to create transparency regarding the implemented technical and administrative controls to ensure the cyber security of the systems assessed. The specific characteristics of industrial production systems and process systems are taken here into account.

The CSC-OT introduced herein enables analysis of the implementation level regarding the achievement of the control objectives (see section 7). This analysis makes it possible to directly identify initial technical and administrative controls to raise the cybersecurity level of OT systems. It can also serve as a starting point for a more in-depth analysis including other relevant industry standards, best practices, and norms. The control objectives forming the basis for the assessment have been designed to reduce cybersecurity risks if effectively implemented.

The approach described in this guide requires all relevant parties to have basic knowledge of IT, networks, and the special nature of the ICS environment. Assessors must be familiar with the IEC 62443 series of standards ([IEC62443-1-1], [IEC62443-3-3]), the ISO/IEC 27000 series (primarily [ISO27001]) or IT-Grundschutz ([IT-Grundschutz Compendium]) as a mandatory requirement.

2 Cyber Security for Operational Technology (OT)

2.1 OT and Industrial Control Systems

Operational Technology (OT) as an umbrella term means hardware and software that detects or causes changes through the direct monitoring and/or control of industrial systems, equipment, processes, and events³. OT systems thus include all forms of industrial process technology and its automation systems. Although the technologies used in OT and IT are similar to some extent, the areas of application and use are different.

Industrial control systems are a core element of OT. They automate the control of machinery and systems. To this end, sensors record operating parameters (e.g. temperature, fill levels, weight) and control systems process them into commands for actuators (switches and actuators, for example, for pumps and valves).

OT is found also in energy and water supply systems, traffic control and monitoring systems, medical technology, building services systems, and private home technology (smart home). The Internet of Things is also influenced by OT. Digitalisation and Industry 4.0 are the current buzzwords that focus on the increasing interconnection between IT and OT.

Industrial control systems are traditionally based on so-called PLC (programmable logic controllers) which have the interfaces to connect them and transmit process signals (input and output). Various transmission technologies are implemented. In the past, mostly serial connections or bus systems (e.g. fieldbus) were in use. Now, IP-based network protocols and connections have become the standard. Wired technology (e.g. Ethernet) as well as wireless systems (e.g. Wi-fi, Bluetooth, mobile communications technology) are implemented here.

3 Source: <https://www.gartner.com/en/information-technology/glossary/operational-technology-ot>

Two different information spheres with different perspectives come together in process systems. In addition to the mentioned control systems, IT systems from the office environment, for example for system-spanning or operational control, are also used. This includes, amongst others, ERP (enterprise resource planning) systems.

These different information spheres need to exchange information. The ISA-95 pyramid (hierarchies) [see image 2–1] illustrates this interdependency in a level structure. It consists of models and terminology which allow to determine which information needs to be exchanged between systems for sales, finances and logistics and systems for production, maintenance, and quality. The levels 0-2 are represented by control systems, level 3 encompasses process management. These levels include, for example operator terminals, monitoring and display components, programming devices, engineering workstations and databases to record production and process data (Data Historian). Level 4 represents the information sphere of the higher-level operational management with an interface to automation technology.

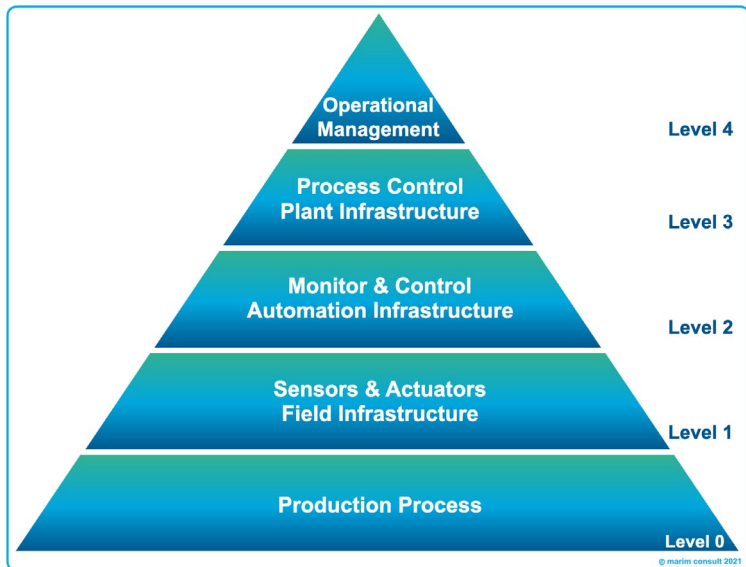


Figure 2-1 The ISA-95 pyramid (hierarchies)

The cloud computing topic is not included in the classic pyramid; however, it is growing in importance. Cloud computing describes the delivery of IT infrastructure and IT services such as data storage space, computing power or application software as services via the Internet.

In OT environments, components from traditional office IT become increasingly prevalent and are increasingly used. This applies to almost all levels of the pyramid. Although OT and office IT are growing closer, there are significant differences between them. The differences are essentially due to the nature of OT, namely the fact that intelligent systems control physical processes. One aspect is the requirement that partial processes must run in real time. This applies in particular to the levels 1-3. Availability of OT systems is another major requirement. This affects, for example, the maintainability (patch management) of these systems. Maintenance windows are often a problem. The aspect of operational safety is also of critical importance in OT environments. The objective here is to protect people and the environment from physical

harm, which is of little relevance in office IT. Another difference consists in the different lifecycles of OT systems and IT systems and components. While the average lifecycle of office IT ranges from three to five years, it is not unusual for OT to have lifecycles of 20 to 30 years (due to the associated production systems).

There are still some similarities between office IT and OT. In the case of OT, it is equally impossible to achieve cyber security only through technology; administrative and user-related controls (e.g. raising awareness) must also be taken into account. Many cyber security controls for office IT and OT follow the same principle. Often, they differ only in content and need to be adapted accordingly.

There are many guidelines and standards that provide important recommendations on this. They are included as references to the respective control objectives. They include IEC 62443 ([IEC62443-1-1], [IEC62443-3-3]), the [ICS-Security Compendium] of BSI, and ISO/IEC 27001 ([ISO27001]), which plays a major role in IT as well, and other industry-specific recommendations and requirements.

2.2 Evolution of Technology and Industry 4.0

A closer look at the historical evolution of OT, in particular of industrial control systems, shows that these were originally closed systems with proprietary technology. With the low level of connectivity, there were hardly any attack vectors from cyberspace. Therefore, cyber security in OT did not play any significant role if availability was not impaired. The simplest security mechanisms, as we know them in office IT (for example, encryption and authentication) were not implemented or if they were implemented, then only in a very basic form in terms of technology.

Increasing connectivity and increased use of standard components and protocols (Ethernet and IP instead of proprietary BUS systems) led to the convergence of OT networks and IT networks. Standard components of office IT became integral parts of OT networks, which in turn exchanged data with office IT. Moreover, office IT networks are by default connected to the internet and OT networks are increasingly connected. Thus, the still poorly protected OT systems are exposed to threats from office IT and cyberspace.

Industry 4.0 stands for the initiative to promote digitalisation in the production environment through the connectivity of industrial machinery and processes by means of information technology and communication technology.

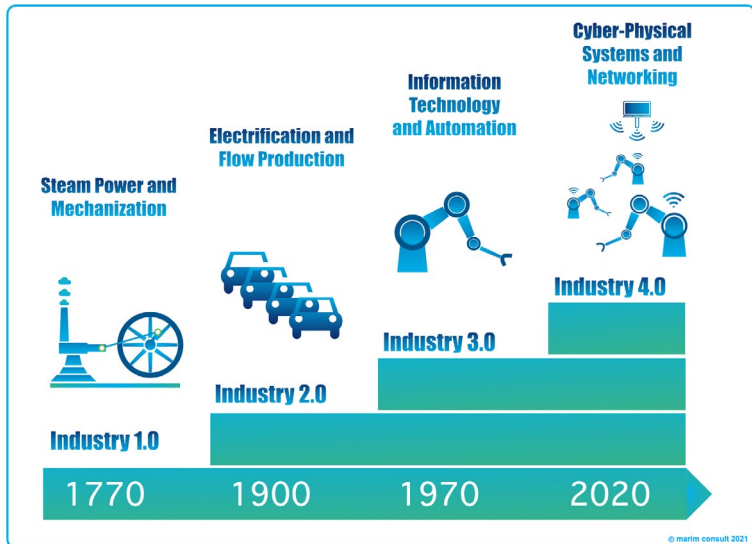


Figure 2–2 Evolution of industrial technology
(Source: ISACA Working Group Cyber Security)

2.3 Risks and Cyber Threats to OT

While the attacks on conventional IT cause primarily financial and operational damage, the risk of attacks on processing systems lies also in safety, that is in personal safety, Anlagen- and environmental safety. Attackers who gain access to the controls of a processing system can destroy it, pollute the environment, damage health and cause injuries. Therefore, when analysing cyber security in OT, it is also necessary to consider safety aspects.

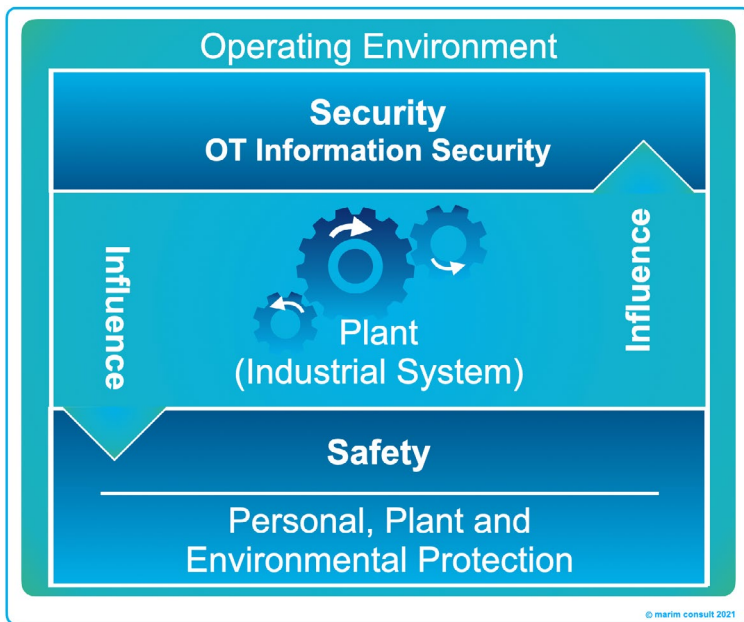


Figure 2-3 Safety and security (Source: ISACA Working Group Cyber Security)

Cyber security, cyberattack, cybercrime, and cyber espionage have long since become catchwords in the press and public discussions. In the context of information security, however, the term “cyber” requires an additional explanation since it is often misunderstood or generalised. It refers to “cyber space” as an open space, where information-processing systems are present and connected. With respect to this guide, cyber security refers the protection of interfaces to the information-processing systems of an organisation against threats from cyber space and, in particular, “the interface” between public cyber space and monitored business environments.

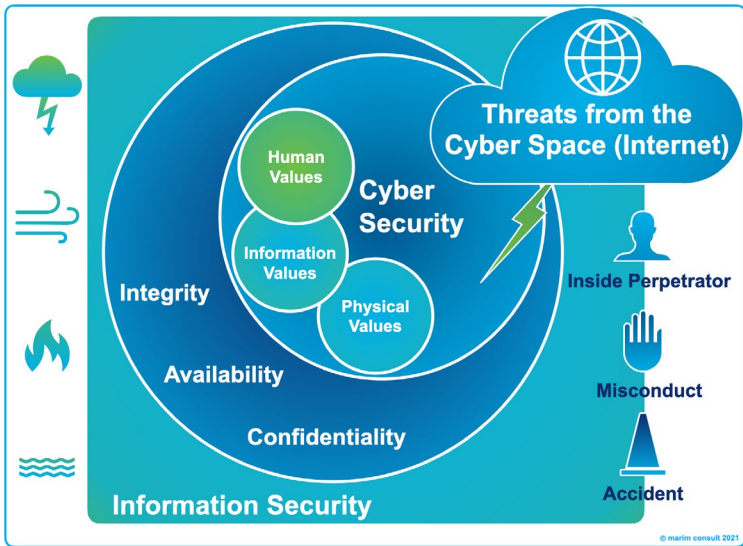


Figure 2–4 Cyber space and information security
(Source: ISACA Working Group Cyber Security)

Threats from cyberspace (see figure 2–4) pose a considerable risk to any industry. They can cause tremendous damage and threaten the continued existence of companies. Possible damage includes:

- ▶ Damage to the safety of people, the environment, and systems
- ▶ Production downtime or defective production
- ▶ Loss or unwanted disclosure of confidential information and intellectual property (patents, design data, etc.)
- ▶ Financial damage
- ▶ Reputational damage
- ▶ Liability claims
- ▶ Penalties (e.g., due to non-compliance with legal requirements)

Threats arise not only from intentional or targeted attacks. Significant damage is also inflicted on victims of random attacks, for example, with malicious code transmitted by email and activated by ignorant or negligent employees (Wannacry, Petya, NotPetya, etc.).

In principle, OT systems and their controls are subject to the same threats as IT systems. However, due to the requirements of an industrial environment and the different damage consequences and criticality, the risks and countermeasures need to be assessed differently. Many cyber threats have therefore a different impact on the industrial environment. The security structures existing in office IT cannot be adopted without adjustments due to the different structures and requirements.

BSI publishes regularly the Top 10 Threats and Countermeasures for Industrial Control System Security [ACS2]. The latest version was published in 2019; BSI plans to publish an update every two years. The document provides for each of the ten identified threats 1. a description of the problem and root causes, 2. possible threat scenarios and 3. countermeasures. It can be used as an additional reference to get a feel for an assessment. The Top 10 provides an overview of the threats, it is not an exhaustive list.











Top 10 Threats	Trend since 2016
Infiltration of Malware via Removable Media and External Hardware	
Malware Infection via Internet and Intranet	
Human Error and Sabotage	
Compromising of Extranet and Cloud Components	
Social Engineering and Phishing	
(D)Dos Attacks	
Control Components Connected to the Internet	
Intrusion via Remote Access	
Technical Malfunctions and Force Majeure	
Compromising of Smartphones in the Production Environment	

Figure 2–5 Top 10 Threats and Countermeasures [ACS2]

In practice, there are additional issues that result in special risks to OT and process systems:

- ▶ Partially “blind” trust in and inadequate control of suppliers and service providers
- ▶ Focus on main control technology and neglect of essential auxiliary systems
- ▶ Lack of cyber security awareness
- ▶ Inadequate or outdated system documentation
- ▶ Lack of clear roles and responsibilities
- ▶ Lack of regular and independent audits
- ▶ Continued operation of outdated networked systems without security measures
- ▶ Lack of network monitoring
- ▶ Poorly protected remote maintenance accesses
- ▶ Inadequate test and change management

The control objectives in section 7 describe holistic methods to mitigate the above threats.

2.4 Cyber Security Concepts of OT

As explained above, the approach to and concepts of cyber security for IT and OT are the same in many respects. However, the concrete implementation in the OT environment can differ considerably from the one in IT and requires the consideration of other aspects.

These specific aspects are addressed particularly well by the internationally accepted and applicable IEC 62443 series of standards. It stresses, for example, the importance of engaging all relevant parties in the construction, modification, and operation of process systems. Collaboration between the manufacturer, integrator and operator and their understanding of their respective roles is a basic prerequisite for a secure OT environment.

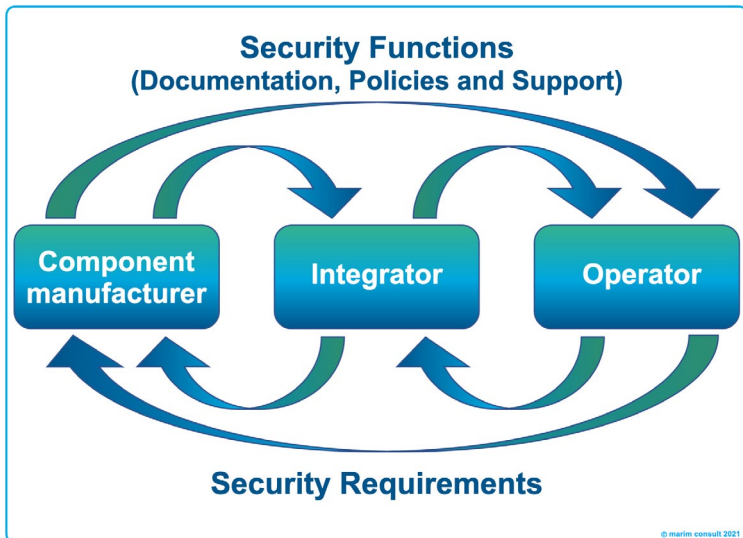


Figure 2-6 Collaboration between the relevant parties as defined in IEC 62443
(Source: ISACA Working Group Cyber Security)

Individual IEC 62443 standards describe the security requirements that the relevant parties must fulfill in the different phases of the system life-cycle, starting from the concept development phase until discontinuation.

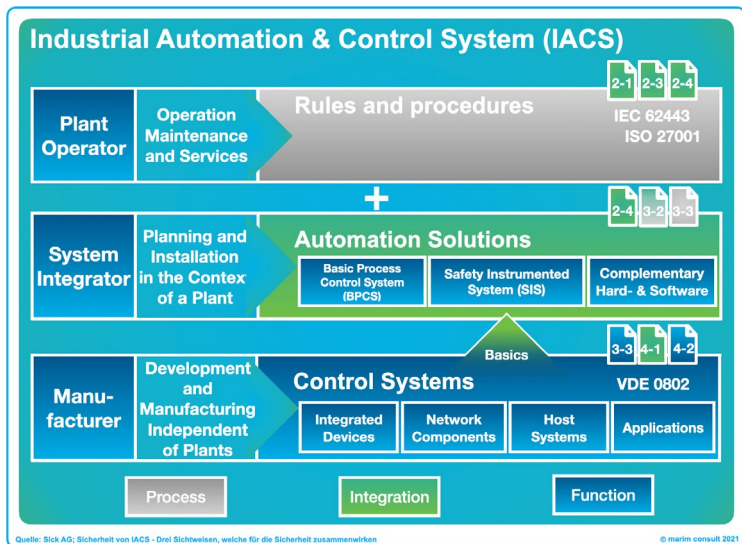


Figure 2-7 Overview of responsibilities as defined in IEC 62443

(Source: SICK AG, A. Teuscher)⁴

This guide is intended for operators. Requirements for integrators and manufacturers are addressed indirectly from the operator's perspective (as requirements for suppliers). Direct requirements for manufacturers are not covered by this guide. Nevertheless, when selecting manufacturers, the operator should consider or demand their conformity with the IEC standard requirements.

4 The colors used in the figure have the following meaning. Grey stands for the responsibility for operational processes at the system operator. Green stands for the responsibility of components and systems and for the integration into secure operation. Blue stands for the function that industrial cyber security must include. The responsibility and collaboration between manufacturer, system integrator and system operator should be stressed here.

The integrator also plays a special role, which is addressed in this guide. He plans, implements and configures the entire system by assembling the manufacturers' components according to the operator's specifications. The quality of the integrator's execution lays an important foundation for the secure operation of the system, including in terms of cyber security. In addition to sound implementation, the integrator must consider all controls that would enable secure operation by the operator (e.g. documentation, training, patch management and maintenance agreements). Operators should call integrators to account during the implementation and acceptance by means of adequate cyber security specifications and well-managed quality assessments.

Furthermore, during the commissioning the integrator often assumes the role of a "quasi-operator". In some cases, he also operates the systems in the production. As a rule, however, he assumes the role of the warranting party and often long-term service partner who performs the system maintenance. Here, the operator often gets the wrong idea of the responsibility being vested in the service partner as well.

The defence in depth concept for OT systems across the value-added chain is a fundamental component of OT cyber security. It is based on several security controls that are aligned with each other and implemented by manufacturers, integrators, and operators. These controls are implemented as several layers. The attacker must breach several lines of defence to succeed. For the best possible protection, the relevant parties should therefore implement coordinated controls in the areas of component security, planning, and processes.

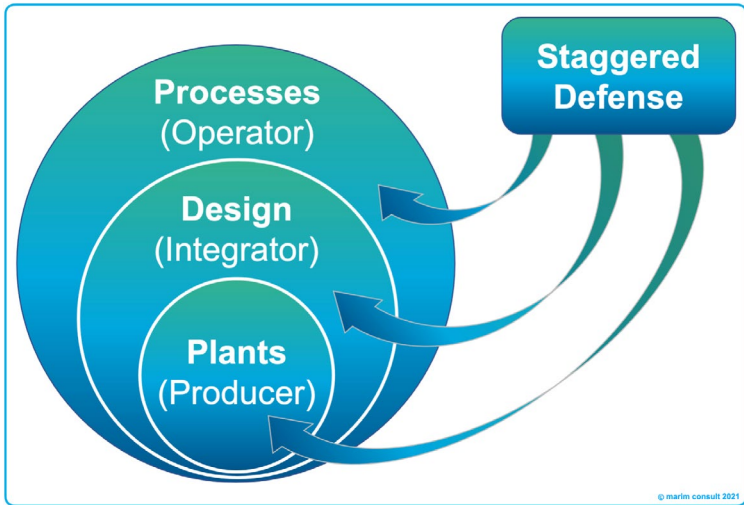


Figure 2-8 Responsibilities of the relevant parties
(Source: ISACA Working Group Cyber Security)

In short, the primary task of manufacturers is to develop and supply secure components (security by design, see section 7. control objectives C and D). Secure development forms already a major cornerstone. The challenge in the planning stage is to develop a secure system by selecting secure components. In the end, the operator must align his processes in a manner that ensures the comprehensive implementation of the security requirements. The “Foundational Requirements” of IEC 62443 provide a good basis for this.

For the OT, it is of particular importance to have an adequate segmentation of systems that takes into consideration the requirements and risks. The “Zones & Conduits” concept of the IEC62443 shows such a segmentation.

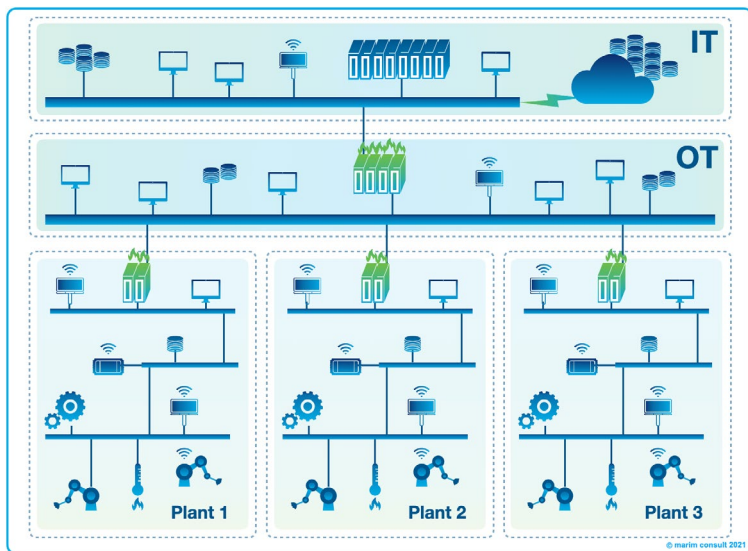


Figure 2-9 Zones & Conduits: the cell protection concept

(Source: ISACA Working Group Cyber Security)

The cell protection concept and the segmentation concept are both elements of the defence in depth. Due to the proper segmentation of the network infrastructure, the different levels (field level to production management) are separated from each other and secured by adequate protection mechanisms (firewalls, gateways, conduits) (see Control Objectives A). A potential cyber attack from the Internet would have to breach several zones and misuse conduits to reach critical areas. Moreover, the individual zones can constitute separate security zones; thus, potential attacks on one zone cannot easily spread to other zones (analogously to fire compartments in a fire protection concept). Designing and implementing an adequate cell protection concept within the system is a major task in the design phase and thus the responsibility of the integrator. The operator and integrators are responsible for designing and implementing such a concept between the systems and in the OT environment. The

control objectives include references to the fundamental requirements of IEC 62443. Other controls refer to ISO/IEC 27001, as the standard reference for the description of an information security management system (ISMS), and to the BSI IT-Grundschutz Compendium. An ISMS describes a systematic, holistic, risk-oriented approach to organising and defining core controls (Annex A) for information security. ISO/IEC 27001 is therefore equally applicable and recommendable in the IT environment as well as the OT environment; however, the respective controls differ.

3 Principles of the CSC OT

In order to build trust in an objective assessment, individuals as well as organisations providing services in the field of cyber security must meet the following requirements [ISACA2]:

- ▶ Formal mandate for the CSC-OT by the organisation
(see also ISACA IT auditing standard 1001 – Audit Charter) [ISACA2]
- ▶ Independence
(see ISACA IT auditing standard 1002 – Organisational Independence and 1004 – Personal Independence) [ISACA2]
- ▶ Integrity and confidentiality
(see ISACA IT auditing standard 1005 – Professional Due Diligence) [ISACA2]
- ▶ Professional expertise
(see ISACA IT auditing standard 1006 – Proficiency) [ISACA2]
- ▶ Evidence and traceability
(see ISACA IT auditing standard 1205 – Evidence) [ISACA2]
- ▶ Objectivity and diligence
(see ISACA IT auditing standards 1207 – Irregularities and Illegal Acts and 1204 – Materiality) [ISACA2]
- ▶ Objective and factual representation
(see ISACA IT auditing standard 1401 – Reporting) [ISACA2]

When planning and conducting assessments in the environment of OT and industrial systems, it is essential to ensure that the persons responsible have the necessary expertise in IT security as well as substantial practical experience with industrial control systems (ICS), the equipment and the technical and administrative processes.

The basic prerequisite for each assessment within the framework of the CSC-OT is an unrestricted right to information and inspection. This means that no information may be withheld from the assessor. This also includes the inspection of sensitive or officially confidential information relating to IT operation, information security management and IT operation if the assessor can substantiate corresponding legitimate interest. A confidentiality agreement between the assessor and the organisation should formally clarify this.

The CSC-OT controls have been developed based on various cyber security standards and compendia. The overview of controls (see section 7) contains references to these documents for a more in-depth examination of each control.

If his document does not contain any specifications on individual parts of the assessment, other relevant regulations, laws, standards or specifications by manufacturers or professional associations such as VDMA or ZVEI should be used. The use of these sets of rules must be documented and the reasons for the use explained in the assessment report.

The on-site assessment can be performed by a single assessor or by a team. It is important to ensure that there is sufficient expertise available to adequately assess the specific cyber security requirements for the OT system and its components, if any.

In principle, already at the planning stage of an CSC-OT, the assessor should take care to avoid any major interruptions in the organisation's running operations due to the assessment. The assessor never actively accesses the systems and does not give any instructions to modify IT systems, infrastructures, documents, or administrative processes. The assessor needs only reader access if necessary.

4 Implementation of a Cyber Security Check OT

4.1 Object of Assessment

The object of a CSC-OT is in principle the entire organisation. The focus of the CSC-OT lies on the level 0- to level 3-systems (process control and its networks including fieldbuses and input/output modules). This includes the actual OT systems but also machine-related systems (e.g. MES) and their interfaces to office IT, direct interfaces to external networks and to the internet.

Additionally, all systems and services with physical, logical or functional interfaces must be analysed in terms of their impact on secure system operation. Therefore, the analysis must also include auxiliary and ancillary systems even if they have only an indirect impact on secure system operation. Relevant systems include but are not limited to:

- ▶ Heating/air-conditioning/ventilation
- ▶ Station automation and electric protective technology (electric energy supply)
- ▶ Self-sufficient auxiliary system controls (e.g. fuel depot, energy supply and waste disposal)
- ▶ Building automation
- ▶ Online monitoring and diagnostics systems, process data management and storage
- ▶ Engineering and system documentation
- ▶ Connected systems (fire alarm system, video surveillance, etc.)
- ▶ Safety systems
- ▶ External services such as the Cloud

If essential systems, system parts and technical and organisational processes are excluded from the assessment, this must be documented and justified in the assessment report as boundaries of the assessment scope.

4.2 Approach

The approach to the implementation of a CSC-OT is explained step by step below.

4.2.1 Step 1 – Mandate

Inquiry and object of assessment

When performing a CSC in the OT environment, the scope and complexity of the object of assessment (hereinafter referred to as “Scope”) determine the time and cost required. To calculate the time and cost of the CSC-OT, it is necessary to define the Scope.

Representatives of various parties should be involved in this. For example:

- ▶ Executive management
- ▶ Company management
- ▶ Site management
- ▶ Production management
- ▶ Persons responsible for the control systems
- ▶ IT management
- ▶ IT service providers

It must be determined which OT components and networks should be assessed as the object of the CSC. Here, it is important to establish a common understanding of what counts as components. The Scope must be documented and approved by the management level (executive management, site management, client) with due consideration of the participants.

Scoping can be already be part of the assignment and the time frame can be already fixed. It can happen that not all the areas to be audited can be analysed. In case of very complex and extensive environments, it is expedient to order and perform the scoping as an additional step in advance.

Mandate

To ensure a comprehensive and effective assessment, the mandate to perform a CSC-OT should be given by the site manager or the management of the respective organisation. Lower- or same-level management cannot grant the mandate to assess a same- or higher-level unit. The object of assessment should also be defined in the mandate.

It is possible to initiate a CSC-OT at any stage of an organisation's security process. Neither documents on the OT security organisation and on the organisation nor the completion of a specific implementation level of the OT security measures are necessary.

4.2.2 Step 2 – Risk Assessment

To determine the risk exposure of the assessed organisation and the respective Scope, a risk assessment must be performed prior to the on-site assessment. This includes the calculation of a key risk indicator based on the damage and probability of incident occurrence. Based on this indicator, the estimated required time, the assessment depth as well as the selection of samples for the performance of the CSC-OT can be determined in a risk-oriented manner.

If the risk assessment has been performed before by the organisation, the assessor can accept it without any further activities of their own (provided that the damage and probability of incident occurrence have been determined) if the assessor considers it to be understandable and adequate.

If the risk assessment has not been performed before for the respective organisation, it should be carried out for the first time by the organisation or in cooperation with the assessor according to the following scheme.

The starting point of the risk assessment is the determination of damage for each protection objective (availability, integrity, and confidentiality,) according to the following table 4–1.

	Availability		Integrity		Confidentiality	
Value of data and processes ⁵	low	0	low	0	low	0
	normal	1	normal	1	normal	1
	high	2	high	2	high	2
	very high	3	very high	3	very high	3
Damage = value per protection objective						

Table 4-1 Determination of damage

The next step is to determine the probability of incident occurrence according to table 4-2.

5. The values low, normal, high, very high must be defined by the organisation itself according to its risk appetite.

	Availability		Integrity		Confidentiality	
Dependency on OT, IT, and level of connectivity (attractiveness for attackers)	local ⁶	1	local	1	local	1
	partially connected ⁷	2	partially connected	2	partially connected	2
	fully networked ⁸	3	fully networked	3	fully networked	3
Expertise (knowledge) of the attackers	general ⁹	1	general	1	general	1
	moderate ¹⁰	2	moderate	2	moderate	2
	specific ¹¹	3	specific	3	specific	3
Attacks in the past	blocked undetected/ successful	1 3	blocked undetected/ successful	1 3	blocked undetected/ successful	1 3
	Probability of occurrence = addition of the values for each protection objective					

Table 4-2 Determination of the likelihood of incident occurrence

6. IT-supported processes, which can also be performed manually, in a verifiably closed network without any internet connection.
7. IT-supported processes, which can be performed manually for a limited period, separate networks with monitored data exchange (remote maintenance) and limited internet use (e.g. remote maintenance).
8. Completely IT-based processes, separate networks with monitored data exchange (remote maintenance) and internet use (e.g. e-mail, internet search, use of cloud services, mobile applications).
9. The attacker has basic knowledge, resources and tools to access data and processes in an unauthorized manner and to modify or delete them, as the case may be.
10. The attacker has knowledge about the organization and suitable resources and tools to access data and processes in an unauthorized manner and to modify or delete them.
11. The attacker has specific knowledge about the organization, substantial resources and specific tools to access data and processes in an unauthorized manner and to modify or delete them.

Now, the key risk indicator is calculated for each protection objective by multiplying the damage with the probability of incident occurrence (sum of the individual values for each protection objective).

Formula for each protection objective (AIC):
(Dependency + Expertise + Attacks) × Damage = Key Risk Indicator

In the CSC-OT, the highest value of the three key risk indicators is used to determine the cyber security exposure and in the subsequent steps.

This results in the following risk exposures:

Numeric value 0 – 9 = Normal

Numeric value 10 – 18 = High

Numeric value 19 – 27 = Very High

The risk exposure (normal, high, very high) is used in the CSC-OT to determine the adequacy of the controls assessed in the on-site assessment (step 5) and of the report (step 6).

4.2.3 Step 3 – Information Review

The information review allows the assessor to get an overview of the tasks, the organisation itself and the OT infrastructures. The information review consists merely of a rough inspection of the documents provided. Here, the OT and IT framework concepts, the list of the critical OT processes, the security guidelines for OT and IT, the OT and IT security concepts (including network plan) and the safety concepts are assessed.

Ideally, the following information is provided in advance to prepare the on-site assessment:

- ▶ **Organisation, processes, personnel, and responsibilities**
 - OT specifications and information security specifications (directives, standards, policies)
 - Organisation chart and OT as well as information security organisation

- ▶ **Technical documentation**
 - Network structure as a physical and logical network plan (incl. IP network addresses and netmasks, IP addresses of all network interfaces, MAC addresses, computer name and the systems' functionalities, (if available) DNS name, zones)
 - Inventory of all programmable components of the system (incl. boundaries and interfaces to other systems)
 - Process chart (overarching process, all sub-processes)
 - Security concepts for operational technology

- ▶ **Previous audit reports and risk analyses**

If there are no adequately informative documents available, the document review is supplemented by interviews which allow the assessor to obtain the required overview. Based on the knowledge gained, the assessor defines the samples and foci of the assessment in a risk-oriented manner.

4.2.4 Step 4 - Preparing the On-Site Assessment

In preparation of the on-site assessment, a program that takes the cyber security risk exposure into consideration should be prepared. This program should define the contents to be assessed, the time/date of assessment, and the contact persons (roles/functions) who are needed for the assessment. The program must be forwarded in advance to the relevant organisation.

4.2.5 Step 5 – On-Site Assessment

All assessments are derived from the control objectives in section 7. The on-site assessment always starts with a short kick-off meeting and ends with a final meeting. During the kick-off meeting, the assessor explains to the organisation (e.g. production managers, site management) the approach and objective of the CSC-OT. In addition, organisational issues are clarified, such as access control, meeting room or changes to the schedule, if any.

As part of the on-site assessment, the assessor conducts interviews, closely inspects the OT environment, in particular the production systems and IT systems, and, if necessary, reviews additional documents. The contact persons to be interviewed on the respective topics should be available at the time of the on-site assessment. The assessor should document the samples assessed (e.g. documents, production systems, and IT systems) and the facts established in a sufficiently detailed manner to be able to adequately use this information later for the preparation of the report.

During the final meeting, which the organisation's management level should also attend, the assessor provides a first general estimate of the cyber security level in the organisation's OT environment. In addition to this, the assessor discloses any serious security deficiencies which put the organisation's cyber security at an immediate high risk and should thus be dealt with and remedied promptly.

4.2.6 Step 6 – Follow-up Evaluation/Preparing the Report

The CSC-OT is concluded with an assessment report. The report provides an overview of cyber security in the organisation's OT environment and contains, in addition to a cyber security assessment, a list of the detected deficiencies. For each control objective (see section 7), the assessment result should be documented. The report provides general recommendations on how to deal with the detected deficiencies. These recommendations show the areas where additional actions are required to increase the cyber security level of the organisation's OT environment. More information on how to prepare the report is provided in section 4.7 "Preparing the Assessment Report".

4.3 Implementation Quality/Personal Certificate

An organisation can conduct a CSC-OT either by using its own qualified personnel or by contracting a qualified service provider. In both cases, however, it must ensure that the assessors have the necessary expertise (minimum requirement: Cyber Security Practitioner OT, Cyber Security Practitioner IT or equivalent qualification as well as basic knowledge of OT and IT environments) and take the approach outlined in this guide.

4.4 Assessment Methods

The term “assessment methods” refers to all actions taken to examine a situation. During a CSC-OT, the assessor can use the following assessment methods:

- ▶ Interview
- ▶ Visual inspection of IT systems, sites, premises, and objects
- ▶ Monitoring (experiences during the on-site assessments)
- ▶ File analysis (this includes the analysis of electronic data or statistical analysis)
- ▶ Data analysis (e.g. configuration files, log files, analysis of databases, etc.)
- ▶ Written questioning (e.g. questionnaire)
- ▶ Assessment reports and certifications of third parties

It depends on the specific situation and must be determined by the assessor which of these methods are to be applied. The assessor must also ensure that the principle of proportionality is observed in all cases. It is also possible to use a combination of several assessment methods to examine a situation. Access to the object of the examination itself is not permitted in any case.

4.5 Binding Control Objectives

Defining binding control objectives shall ensure the consistently high quality of the CSC-OT as well as the comparability of the activities of different assessors.

The binding control objectives for a CSC-OT are based on the most critical security deficiencies detected in the OT environment and on the references to the “Basic Controls for OT Cyber Security” (see reference sheet in the appendix).

The assessment depth (intensity) is adjusted by the assessor in a risk-oriented manner depending on the level of cyber security risk exposure.

4.6 Assessment Scheme

If any security deficiencies are detected within the framework of a CSC-OT, the assessor must determine, at the latest when preparing the report, how to assess the deficiencies in terms of their criticality.

Security deficiencies must be classified as follows:

“No security deficiency”

At the time of the assessment, no security deficiency could be detected. There is no supplementary information.

“Security recommendation”

Even a fully implemented security safeguard can be supplemented by a security recommendation. By implementing the recommendations described in the situation, the security can be increased. Security recommendations can include suggestions how to improve the implementation of safeguards, additional safeguards that have been successful in practice, and comments regarding the adequacy of safeguards.

“Security deficiency”

A “security deficiency” is a security gap that should be closed in the medium term. The availability and integrity but also the confidentiality of OT and IT systems and of information might be compromised.

“Serious security deficiency”

A “serious security deficiency” is a security gap which should be closed immediately, since the availability and integrity but also the confidentiality of OT and IT systems as well as information are exposed to a high risk and considerable damage can be expected.

All types of security deficiencies and recommendations must be documented in the assessment report in a way that allows for verification by an expert third party.

4.7 Preparing the Assessment Report

The assessment report of a CSC-OT must be made available in written form to the head of production, the management and/or to the client. A draft version of the report should be submitted in advance to verify whether the issues detected (only the issues detected – without any assessments and recommendations) were recorded correctly and objectively.

The assessment report consists at least of the following three parts:

- ▶ the framework data including the detailed description of the object to be assessed
- ▶ an executive summary (including the cyber security risk assessment)
- ▶ a detailed assessment (detailed description of the deficiencies detected, their assessment and recommendations to remedy the deficiencies)

The assessment report must be prepared as deficiency report without appreciating any positive aspects.

Part I – Framework Data

This part contains organizational information:

- ▶ Object of the assessment
- ▶ Limits/scope of the assessment
- ▶ Assessor
- ▶ Contact persons of the organization assessed
- ▶ Bases for the assessment
- ▶ Schedule of the assessment
- ▶ List of the recipients of the assessment report
- ▶ Framework data of the assessment document and/or document control
 - File name
 - Print date
 - Document status

Part II – Executive Summary

This part includes a summary for the management. The main deficiencies and recommendations resulting therefrom should be summarised in a brief and understandable manner.

- ▶ Summary
- ▶ Cyber security risk assessment
- ▶ Overview of the assessment results for all control objectives

Part III – Detailed Assessment

This part of the report contains a detailed description of the topics assessed, the deficiencies detected, their assessment as well as the control objectives to remedy the deficiencies. For the assessment of the detected deficiencies, the scheme shown in section 4.6 must be used.

- ▶ Control objective (see section 7)
- ▶ Result including assessment
- ▶ Sample(s)
- ▶ Description of the deficiencies including control recommendation(s)

Formal aspects of the assessment report:

When preparing the assessment report, the following formal aspects must be respected:

- ▶ The pages must be marked in such a way that each page can be clearly identified (for example, with a page number and version number and the title and date of the report).
- ▶ All terminology or abbreviations used in the report that are not in general use must be summarised in a glossary and/or index of abbreviations.
- ▶ The report must clearly specify the organisational units audited and assessed, the recipients of the report, and any restrictions of use.
- ▶ The report must be signed by the assessor.
- ▶ The form and contents of a report might vary depending on what kind of assessment work was contracted; however, the minimum requirements for the assessment report for CSC-OT¹² and the ISACA IT Audit and Assurance Standard 1401 (see [ISACA1]) must be met.

12 A template for a CSC-OT report is available on the ISACA Germany Chapter e.V. website (see section 7).

5 Glossary and Definitions

The following terms are used in this document:

Actuator is a technical component that converts an electric signal into a physical variable (electric signal into mechanic movement, etc.) and is therefore used for process control.

AIC better known as the CIA triad (confidentiality, integrity, and availability) is a model designed to guide information security activities within an organization. For OT the sequence is changed to consider the operation requires in an better way.

APT (Advanced Persistent Threat) refers to a very complex, specific, intensively prepared and implemented cyberattack. Due to the high technical complexity, the precise aim at the target and the required technical expertise, APTs are considered extremely complex and have often considerable negative effects on the affected location.

Asset/Inventory: In general, an item of material or immaterial value which deserves to be protected, including people, information, infrastructures (e.g. hardware, software, etc.), finances or reputation. (ISACA CSX Nexus).

Asset Register/Inventory (financial asset, fixed asset¹³) is a list of hardware (e.g. servers and switches), software (e.g. business-critical applications and support systems) and confidential information in an IT environment. They are integral parts of the systems and network infrastructure of a company. Information security, computer security and network security are IT assets such as data, devices or other components of the environment that support information-related activities.

Control Objectives are specifications for the aspects that are to be achieved with the controls, i.e. they allow to assess the effectiveness of the controls. They include security management topics as well as technical aspects.

13 Definition from the BSI Compendium for Operators, VDI 2182

CPS (Cyber-Physical System) means a complex structure in which IT components are permanently connected to mechanical/electronic components. Such structures can become very extensive, as in the case of smart grids.

CPS-Plattform is the basis for the assembly and integration of a CPS

CPPS (“Cyber-Physical Production System”) is a CPS used in industrial production.

Cyber Crime refers to criminal activities using cyberspace as source, target and/or tool.

Cyber Security in the OT environment pursues the protection of confidentiality, integrity and availability of OT systems and information against threats from cyberspace.

Cyberspace comprises all information infrastructures that can be reached through the Internet worldwide across territorial borders.

Data Historian (also Process Historian, Operational Historian) refers to a program that receives and records time series of production data or process data. The data are used, among other things, for status checks, quality assurance or cost and performance monitoring.

DCS refers to “distributed control system” and thus to a distributed, typically hierarchical system of control units connected in a network. Such systems are typically used for complex larger systems (plants, process chains).

Embedded System is a system, typically a machine, “embedded” into another system. The latter refers to a computer that has a specific monitoring or control function within the overall context. Usually, the embedded system cannot be recognized as such by the user. The variations range from highly specialized modules to “embedded PCs”.

FCS is a Field Control Station and thus a component such as a *PLC* in a control system directly connected to a *sensor* or an *actuator*.

Flash Memory is actually a flash *EEPROM*; however, it can also take the form of an USB flash drive or SSD drives and be rewritten by the user. Often, it contains the *firmware* of a component. The information is

stored as charges that cannot flow away (non-volatile storage) because a charge can flow into the storage layer only through an insulating layer with a high electric field and only due to the quantum-mechanical tunnelling effect.

Firmware is software more or less firmly embedded in electronic devices. Nowadays, it is mostly held in a *flash memory* or *EEPROM* and thus basically modifiable without any exchange of the hardware. It may also be permanently stored in *ROM* or *EPROM*. Firmware and hardware can only work together as a unit. It lies below the operating system in the layer architecture.

HMI refers to human-machine interaction, that is the communication and interaction between a human and a machine. The abbreviation HMI is also used for human-machine interface, which is a device or software that enables the user to communicate with machines or production systems.

ICS is the abbreviation of industrial control system and refers to control systems for industrial equipment, ranging from individual displays to extensive systems with thousands of field-level connections.

Industry 4.0 means the transformation towards a *smart factory*. It is preceded by the transition from Industry 0.0, (no industry) to Industry 1.0 (factory through mechanisation), 2.0 (electrification) and 3.0 (electronification). The uniqueness of the transition to 4.0 is that the production tools, now connected in a network, are “getting to know each other” thus can optimise themselves. The boundaries of the factory are becoming blurry because they cannot be defined only physically anymore. Several factories can become a “meta factory” through networking, with production and logistics growing together (with the logistics unit taking on parts of final production), and even the consumer can become part of the factory, because they can directly control product customizing (e. g. via a “car configurator” or by printing of posters/T-Shirts with individual designs through the Internet).

IoT, Internet of Things is the collective term for the technologies of a global infrastructure of information societies. This infrastructure enables the networking of physical and virtual devices and their collaboration by means of information and communication technologies.

Integration, horizontal means connecting components across system boundaries within a functional or organisational hierarchy level.

Integration, vertical means connecting components within a system across functional or organisational hierarchy levels.

KRITIS (critical infrastructures) are organisations and facilities of major importance for society whose failure or impairment would cause a sustained shortage of supplies, significant disruptions to public order or other dramatic consequences.

Legacy System. The term refers in computer science to a well-established enterprise software application, which has historically evolved.

MTU is a Master Terminal Unit that sends commands to *RTUs* in a *SCADA* context and requests information for the *RTUs*, with the *MTU* initiating the connection. The information is pooled and processed at the *MTU* in the control centre so that control decisions can be made.

Office IT as opposed to “production IT” (see definition) means for the purposes of this guide all IT components outside of production and thus the classic office IT as well as IT components in the data processing centre.

Orchestration can refer to services or systems and means combining various individual components in a flexible manner for a designated purpose.

OT refers to operational technology. It is a collective term for any kind of control system in industrial production. It comprises *ICS*, *SCADA*, *DCS* and *PLC* systems and makes decisions based on sensor data (automatically or via operator) which control actuators.

PLC “Programmable logic controller” is a programmable control unit, which records digital or analogue input via sensors, processes it and creates digital or analogue output by means of actuators. It is therefore a computer with *I/O* capabilities, which has been typically “hardened” for industrial applications and has a real-time operating system.

Production IT as opposed to “*office IT*” (see definition) refers to all IT components used in a production plant, for example, system controls,

sensors, actuators, and robotics. It should not be confused with the similar or even identical term for the “staging level” in IT, meaning a development, test, and production environment when new components go live.

ROM, EPROM, EEPROM are forms of “read-only memory”. This form of memory contains data that the user can only read but not write or modify. The initial recording of a ROM is called programming and is very different from the writing access to random-access memory (RAM). Forms of ROM include programmable ROM (PROM), the erasable programmable ROM (EPROM) that can be erased by UV light, and electrically erasable PROM (EEPROM). Nowadays, flash memory is often used instead of a ROM.

RTU is a “remote terminal unit” and, therefore, a terminal for remote control and/or remote maintenance.

SCADA refers to “supervisory control and data acquisition” and thus to the monitoring and controlling of technical processes by means of an IT system.

Senior Management is used to refer to the executive boards, management boards, managing directors, and the management of government agencies.

Sensor is a technical component that measures physical or chemical data and transforms them into electrical signal for the purpose of process monitoring.

Smart Factory refers to an environment where production and logistics are connected based on CPS in self-organizing networks down to a product that autonomously communicates with the production system (“Smart Product”).

Smart Product refers to a part that communicates with its production system and with other CPS in the logistics chain or with other products.

Smart Production is the production process at a smart factory that entails, amongst others, communication between this factory and smart products.

VDE is the German Association of Electric and Electronic Information Technology. It develops, amongst others, rules for standardization, testing and certification of electric and electronic information technology.

VDMA is the German Mechanical Engineering Industry Association. It represents the interests of its predominantly medium-sized member companies in the capital goods sector.

ZVEI is the German Electrical and Electronic Manufacturers' Association. It represents the interests of its predominantly medium-sized member companies in the electrical and electronic components sectors.

6 References

- [ACS1] Alliance for Cyber Security, website,
www.allianz-fuer-cybersicherheit.de
- [ACS2] TOP 10 Cyber Threats to ICS,
https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_005E.html
- [ISACA1] ISACA, IT auditing standards,
<https://www.isaca.org/resources/isaca-journal/issues/2020/volume-5/standards-guidelines-tools-and-techniques>
- [ISACA2] ISACA, Knowledge Center,
www.isaca.org/resources/frameworks-standards-and-models
- [IEC 62264-3] IEC 62264-3:2016-12 Enterprise-control system integration – Part 3: Activity models of manufacturing operations management
- [IEC62443-1-1] IEC TS 62443-1-1:2009 Industrial communication networks – Network and system security – Part 1-1: Terminology, concepts, and models
- [IEC62443-3-3] IEC 62443-3-3:2013 Industrial communication networks – Network and system security – Part 3-3: System security requirements and security levels
- [ICS Compendium] ICS-Security Compendium for manufacturers and integrators, BSI, 2014
- [ISO27001] DIN EN ISO/IEC 27001:2017-06 Information technology – Security techniques – Information security management systems – Requirements
- [IT-Grundschutz Compendium] IT-Grundschutz Compendium, BSI, 2020
- [SANS Survey] SANS 2019 State of OT/ICS Cybersecurity Survey
Page 7: / Figure 4. Comparison of OT/Control System Incidents
2017 vs. 2019

7 Control Objective

Assessing the control objectives A to N listed below is mandatory when implementing an industrial cyber security check. The order of the control objectives is thus not to be considered as prioritisation or mandatory order to be complied with during the assessment, but solely serves structuring purposes. In order to assess a control objective, the basic controls associated with the respective control objective must be examined. The samples for the on-site assessment must be checked in a risk-oriented approach. Apart from the threat situation and the probability of incident occurrence associated therewith, the criticality of the impact on the production processes must be considered.

Letter	Block of controls
A	Network segmentation and zoning, and protection of network gateways
B	Protection against malware and security gateways
C	Procurement and cataloguing of systems
D	Prevention of security gaps, system hardening and change management
E	Secure communication with systems outside of automation networks and remote maintenance
F	Log data recording, analysis, and system monitoring
G	Ensuring an up-to-date level of information
H	Management of security incidents
I	Secure identification and authentication, in particular of human users
J	Ensuring availability of resources, cyber security organisation
K	Implementing user-oriented measures, raising awareness and training of personnel
L	Secure use of social networks
M	Analysis of vulnerabilities and configuration audits
N	Secure use of cloud services

Control objectives	Basic controls	References
<p>A Network segmentation and zoning, and protection of network gateways</p> <p>The production networks are split into security zones and separated from each other by suitable gateways. Network zoning aims to prevent easy spread of Internet attacks into automation levels.</p> <p>Ideally, each system constitutes an individual security zone, higher levels such as Level 2, Level 3, IT, cloud, and remote access are cascaded according to the “onion skin principle” and thus constitute an adequate defence-in-depth concept.</p>	<ul style="list-style-type: none"> – All production networks are split into segments and separated from the IT networks. All transitions are identified and documented and protected by gateways. – The data flow from and to the production networks must be routed and monitored through a DMZ. This applies in particular to connections to untrusted networks. – Wireless and mobile connections require special protection (encryption and access control). – Network access is granted only to authorized mobile end devices which must not have any other active network connection (bridge to IT or Internet via second network interface). 	<p>ISO/IEC 27001:2013 A.6.2.1, A.9.1.2, A.12.1.4, A.13.1.1, A.13.1.2, A.13.1.3, A.14.1.2, A.14.1.3</p> <p>IEC 62443-1-1 IEC 62443-3-3</p> <p>FR 5: SR 5.1, SR 5.2, SR 5.3</p> <p>BSI IT-Grundschutz 2021: IND.1.A5, IND.1.A16, IND.1.A20, IND.1.A21, IND.2.1.A1, IND.2.1.A2, IND.2.1.A6, IND.2.1.A11, IND.2.1.A16, IND.2.1.A17, IND.2.2.A3, IND.2.3.A3, IND.2.4.A1, IND.2.7.A7, IND.2.7.A9, DER.1.A8, CON.1, NET.1.1, NET.1.2, NET.2.1, NET.2.2, NET.3.1, NET.3.2, NET.3.3, OPS.3.1.A11, OPR.4.A16, SYS.3.2.2.A10</p>



	Control objectives	Basic controls	References
A		<ul style="list-style-type: none"><li data-bbox="405 187 638 319">– Components from the levels 0-2 should get only external network access if this is essential for the function. <li data-bbox="405 344 638 505">– The network segmentation is effective in preventing DoS attacks, especially in real-time communication environment.	

	Control objectives	Basic controls	References
B	<p>Protection against malware and security gateways</p> <p>For the purposes of a defence in depth against attacks by malware, several successive security gateways that detect and prevent the spread of malware must be implemented.</p> <p>The objective is to bring the last line of defence as close as possible to the system or to implement it there.</p>	<ul style="list-style-type: none"> – Firewalls or application layer gateways (ALGs) used between the zones should include functionalities for the detection and blocking of malware. – Different technologies such as signature-based identification, heuristics, machine-based learning, ... should be used. Server and operator systems should have adequate antivirus protection. Systems without such protection should be isolated. – In addition to the above technical controls, administrative requirements for protection against malware and misuse, amongst others, for the use of external maintenance notebooks and removable storage devices, should be established. 	<p>ISO/IEC 27001:2013 A.12.2.1 IEC 62443-3-3</p> <p>FR 3: SR 3.2, SR 3.3, SR 3.4, FR 7: SR 7.1</p> <p>BSI IT-Grundschutz 2021: IND.1.A3, IND.1.A10, IND.2.1.A8, DER.1, DER.2.1, DER.2.2, OPS.1.1.4</p>

Control objectives	Basic controls	References
<p data-bbox="135 182 386 261">C Procurement and cataloguing of systems</p> <p data-bbox="182 297 366 546">In order to identify risks and plan the implementation of countermeasures on the systems used, a complete inventory of the systems and software used must first be performed.</p> <p data-bbox="182 568 377 925">Already during procurement, a classification should be made so that the devices can be selected and protected according to their intended purpose. When selecting the devices, manufacturers and products with relevant security certificates should be preferred.</p>	<ul style="list-style-type: none"> <li data-bbox="403 182 640 375">– All systems (incl. hardware and software) have been fully catalogued and classified in terms of their criticality with regards to the system where the data a processed. <li data-bbox="403 396 636 561">– Versions and patch versions are documented and version changes are tracked. Tools for automated inventory management are used. <li data-bbox="403 582 632 689">– When purchasing new systems, a classification regarding the intended use should be performed. <li data-bbox="403 711 636 982">– New components are catalogued prior to commissioning. This means we create a digital twin and its asset inventory must contain the software, the configuration incl. the security settings, and the cyber security-relevant documentation. 	<p data-bbox="656 182 857 204">ISO/IEC 27001:2013</p> <p data-bbox="656 211 860 261">A.8.1.1, A.8.1.2, A.8.1.3, A.8.2.1, A.8.2.3</p> <p data-bbox="656 282 780 304">IEC 62443-2-1</p> <p data-bbox="656 325 783 347">IEC 62443-3-3</p> <p data-bbox="656 368 759 389">FR 7: SR 7.8</p> <p data-bbox="656 411 897 432">BSI IT-Grundschutz 2021:</p> <p data-bbox="656 439 904 604">IND.1.A11, IND.1.A23, IND.2.1.A13, OPS.1.1.3.A1, ORP.4.A3, IND.1.A12, IND.1.A3, DER.4.A14, ER.1.A9, ORP.1.A2, ORP.3.A3, ORP.1.A7</p>

	Control objectives	Basic controls	References
D	<p>Prevention of security gaps, system hardening and change management</p> <p>In order to minimise the risk of successful cyber attacks, security gaps must be consistently avoided.</p>	<ul style="list-style-type: none"> – An effective change management process should be established. – When planning and purchasing components, security features and related certifications are taken into account. – Communication interfaces should be deactivated if they are not used. Active interfaces should be hardened before use if possible, i. e. services that are not used should be deactivated. – Patch and update capability of the components is ensured for the intended lifecycle. – Known security gaps are closed quickly by means of workarounds and security updates. 	<p>ISO 27001:2013 A.12.1.2, A.12.5.1, A.12.6.1, A.14.1.1, A.14.2.2, A.14.2.3, A.14.2.4</p> <p>IEC 62443-4-1</p> <p>Practice 7 – Security-Update-Management</p> <p>BSI IT-Grundschutz 2021: IND.1.A3, IND.1.A6, IND.1.A12, IND.1.A17, IND.2.1.A4, IND.2.1.A13, IND.2.7.A2, IND.2.7.A3, CON.1.A1, CON.1.A3, CON.1.A4, CON.1.A5, CON.1.A15, CON.5.A1, CON.5.A3, CON.5.A4, CON.5.A6, CON.5.A9, OPS.1.1.3, OPS.1.1.4.A1, OPS.1.1.4.A6, OPS.1.1.3.A1, OPS.1.1.3.A15, ORP.4.A3, IND.1.A12, IND.1.A3, DER.4.A14, DER.1.A9</p>



	Control objectives	Basic controls	References
D		<ul style="list-style-type: none"><li data-bbox="405 187 639 291">– Operating systems, server services and applications are hardened prior to commissioning.<li data-bbox="405 315 639 419">– A process ensuring secure software development has been established.<li data-bbox="405 444 639 548">– An efficient vulnerability and patch management process has been established.	

Control objectives	Basic controls	References
<p data-bbox="128 182 373 318">E Secure interaction with areas outside of automation networks and remote maintenance</p> <p data-bbox="174 358 373 682">Communication processes between automation networks and areas outside of these networks (e.g. Level 2 and 3, Cloud, IT area, remote accesses and remote maintenance accesses) must be protected with adequate controls to prevent attacks.</p> <p data-bbox="174 708 373 925">These controls should be based on a risk assessment. It should be considered that attackers could use the systems as a relay station to run attacks on other targets.</p>	<ul style="list-style-type: none"> <li data-bbox="394 182 629 318">– Communication with areas outside of automation technology is restricted. The number of gateways is minimised. <li data-bbox="394 339 629 504">– The default rule DENY-ANY prevents transparent IP communication. Only expressly authorized communication is permitted. <li data-bbox="394 525 629 632">– Personal communication, IT services such as Internet, email, chat is not possible. <li data-bbox="394 654 629 789">– In secure protocols which contain known vulnerabilities, or which are targeted by many attack vectors, are avoided. <li data-bbox="394 811 629 1025">– Ideally, the protocols that are used can be reliably restricted and protected by application layer gateways. Connections should be established from inside to the outside insofar as possible. <li data-bbox="394 1046 629 1153">– There is a feasible concept for secure remote accesses and remote maintenance. 	<p data-bbox="650 182 895 318">ISO/IEC 27001:2013 A.13.2.1, A.13.2.2, A.13.2.3, A.13.2.4, A.14.1.2, A.14.1.3, A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2</p> <p data-bbox="650 339 774 361">IEC 62443-3-3</p> <p data-bbox="650 382 767 432">FR 5: SR 5.1, SR 5.2, SR 5.3</p> <p data-bbox="650 454 891 561">BSI IT-Grundschutz 2021: IND.1.A21, IND.2.1.A16, IND.2.4.A1, IND.2.7.A9, ORP.1.A12</p>

Control objectives	Basic controls	References
<p data-bbox="135 182 379 261">F Log data recording, analysis, and system monitoring</p> <p data-bbox="182 297 379 489">To detect attacks and perform subsequent analyses, it is necessary to access log data. These data must be protected against manipulation.</p> <p data-bbox="182 511 379 1118">Security incidents often go undetected as they cause no visible or obvious damage in the short term. However, a well concealed and sufficiently careful approach may enable attackers to control the target systems for extended periods of time without these attacks being detected immediately due to singular events. Therefore, it is necessary to also develop procedures for detecting inconspicuous security incidents and attacks planned for the long term.</p>	<ul style="list-style-type: none"> <li data-bbox="405 182 638 375">– Relevant log data is recorded completely according to the relevant statutory, regulatory, and organizational requirements and evaluated at regular intervals. <li data-bbox="405 396 638 532">– The use of privileged accounts and administrative accesses, in particular write accesses, is monitored continuously. <li data-bbox="405 554 638 632">– Log data are adequately protected against manipulation and destruction. <li data-bbox="405 654 638 818">– Changes to configurations must be monitored, automatically if possible, and alerts of relevant incidents must be enabled. <li data-bbox="405 839 638 946">– consistent date and time synchronization in the entire network must be ensured. 	<p data-bbox="658 182 905 261">ISO/IEC 27001:2013 A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4</p> <p data-bbox="658 282 783 304">IEC 62443-3-3</p> <p data-bbox="658 325 864 404">FR 2: SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12</p> <p data-bbox="658 425 760 475">FR 3: SR3.3, SR 3.4</p> <p data-bbox="658 496 897 604">BSI IT-Grundschutz 2021: IND.1.A10, DER.1, DER.2.1.A2, PS.1.1.5, ORP.5.A3</p>



Control objectives		Basic controls	References
F	Configuration files should be also monitored; this allows to track changes, in particular unwanted changes and to quickly respond to them..		
Control objectives		Basic controls	References
G	<p>Ensuring an up-to-date level of information</p> <p>The ability to plan efficient cyber security safeguards is predominantly determined by the quality and the scope of your own level of information. Therefore, the availability of up-to-date and technically reliable information about cyber security, in particular on OT environments, must be ensured.</p>	<ul style="list-style-type: none"> – Current information on cyber security is continuously obtained from reliable sources and analysed. – Based on the information available, cyber security controls are regularly checked and adapted with respect to their effectiveness 	<p>ISO/IEC 27001:2013 A.6.1.4, A.16.1.3</p> <p>BSI IT-Grundschutz 2021: IND.1.A12, IND.2.7.A4, DER.1.A12, DER.2.1.A2, DER.2.1.A9, OPS.1.1.3.A1</p>

	Control objectives	Basic controls	References
H	<p>Management of security incidents</p> <p>Adequate processes and procedures for security incident management must be established and drilled to ensure the fast and adequate management of security incidents, thus maintaining continuous business operations..</p>	<ul style="list-style-type: none"> – There are established processes and procedures for the fast and adequate handling of security incidents (crisis management). – Data back-up must be performed regularly. – The management of security incidents is drilled at regular intervals (recovery test). In particular, the effectiveness of the emergency measures is tested. – Completed security incidents are examined regarding their causes and possible consequences. – Security incidents are reported to responsible government agencies for criminal prosecution purposes and for an assessment of the situation. 	<p>ISO/IEC 27001:2013</p> <p>A.12.3.1, A.16.1.1, A.16.1.2, A.16.1.3, A.16.1.4, A.16.1.5, A.17.1.1, A.17.1.2, A.17.1.3, A.17.2.1</p> <p>IEC 62443-3-3</p> <p>FR 6</p> <p>BSI IT-Grundschutz 2021:</p> <p>IND.2.1.A7, IND.2.1.A18, IND.2.7.A5, CON.3, DER.2.1, DER.2.2, DER.2.3, DER.4</p>

Control objectives	Basic controls	References
<p>I</p> <p>Secure identification and authentication, in particular of human users</p> <p>Authentication is necessary to prevent unauthorized access by users and to track and categorise activities.</p>	<ul style="list-style-type: none"> – Access to the system must be limited to identified and authorized persons only. – particularly secure passwords or multi-factor authentication (MFA) are used in critical areas. – Access codes and the associated rights are managed centrally, reviewed regularly, and adapted or revoked if necessary. – Sessions are locked when the operator leaves the terminal. Unsuccessful log-in attempts are logged and analysed. – Authentication data for areas with different protection requirements are separated from each other. 	<p>ISO/IEC 27001:2013</p> <p>A.9.1.1, A.9.1.2, A.9.2.1, A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.2.5, A.9.2.6, A.9.4.2, A.9.4.4</p> <p>IEC 62443-3-3</p> <p>FR 2: SR 2.1, SR 2.2, SR 2.3, SR 2.5, SR 2.6, SR 2.7</p> <p>BSI IT-Grundschutz 2021:</p> <p>IND.1.A8, IND.1.A14, IND.1.A15, IND.2.2.A2, APP.2.1, APP.2.2, ORP.4, NET.1.2, NET.2.1, NET.2.2, NET.3.1, NET.3.2, NET.3.3, OPS.1.1.2, OPS.1.2.5.A3, OPS.1.2.5.A7, OPS.1.2.5.A17, ORP.1, ORP.4, SYS.1.1, SYS.2.1, SYS.3.2.1</p>

	Control objectives	Basic controls	References
J	<p>Ensuring availability of resources, cyber security organisation</p> <p>To counter cyber security threats effectively, the organisation should make available sufficient financial and personnel resources.</p>	<ul style="list-style-type: none"> – There is a cyber security organisation with an information security officer for automation technology (ISB-OT). – There must be sufficient financial and human resources available to counter to cyber security threats. – If necessary, qualified and reliable external service providers are contracted. – When allocating resources, the organization must account for test and development environments. 	<p>ISO/IEC 27001:2013 A.6.1.1, A.6.1.2, A.12.1.1, A.12.1.4, A.12.3.1</p> <p>IEC 62443-2-1</p> <p>ORG 1.1, ORG 1.3</p> <p>BSI IT-Grundschutz 2021: IND.1.A1, ISMS.1, PS.1.1.2, ORP.1</p>

	Control objectives	Basic controls	References
K	<p>Implementing user-oriented measures, raising awareness and training of personnel</p> <p>The organisation's personnel must also shift into the focus of a cyber security strategy. All technical controls can become ineffective due to human error or deliberate acts.</p>	<ul style="list-style-type: none"> – Operators and service and OT personnel are regularly made aware of the dangers of a cyber attack and instructed on the correct behaviour. – Standard security principles are implemented, for example, passwords and system details are only made available to persons with a need to know. – Personnel and management are familiar with their roles and responsibilities. – There is a clear separation of roles. The concentration of too many responsibilities in one role is avoided. 	<p>ISO/IEC 27001:2013 A.6.1.1, A.7.2.2, A8.1.2</p> <p>BSI IT-Grundschutz 2021: ORP.3</p>

	Control objectives	Basic controls	References
L	<p>Secure use of social networks</p> <p>Employees must be made aware that no confidential information (images, projects, system documents, etc.) may be published in social media.</p>	<ul style="list-style-type: none"> – There are binding specifications (social media guidelines) for the secure and respectable presence of the organization and the employees' professional profiles in social networks. – Employees are regularly made aware of the risks and instructed on the correct behaviour in social networks. – There must be no direct interfaces between social networks and operational infrastructure. 	<p>ISO/IEC 27001:2013: A.7.2.2, A.8.1.3, A.8.2.3, A.13.2.1, A.13.2.2, A.13.2.3</p> <p>BSI IT-Grundschutz 2021: APP.1.4.A2, CON.9.A1, CON.9.A2, CON.9.A3, CON.9.A4</p>

	Control objectives	Basic controls	References
M	<p>Analysis of vulnerabilities and configuration audits</p> <p>Regular vulnerability assessments and configuration audits should be performed by qualified and experienced persons who were not involved in the planning or implementation of the system in question to detect sources of errors at an early stage.</p>	<ul style="list-style-type: none"> – The systems are regularly checked by independent, qualified persons for secure configuration, resiliency and vulnerabilities. New developments should be tested for vulnerabilities prior to commissioning. – The scope and intensity of the penetration tests correspond to the cyber security exposure. – The results of the audits are used consistently to minimize risks. 	<p>ISO/IEC 27001:2013: A.14.2.8, A.18.2.1, A.18.2.3</p> <p>BSI IT-Grundschutz 2021: IND.1.A12, IND.1.A17, IND.2.1.A19, OPS.1.1.6.A14</p>

	Control objectives	Basic controls	References
N	<p>Secure use of cloud services</p> <p>The use of cloud applications should be regularly reviewed. Dependencies between the process control and cloud services should be known and their risks should be assessed to prevent unauthorized data loss.</p>	<ul style="list-style-type: none"> – There are binding specifications for the storage, use and processing of data in cloud applications. – Cloud providers should be selected based on their ability to optimally meet the organisation's security requirements in consideration of commercial aspects. – In the selection process, the aspects relating to a change of the cloud provider should be considered. – The way of how to properly manage the cyber risks of a cloud solution must be determined in a risk assessment. – Cloud services are professionally provisioned, managed and monitored. The use of cloud services should be subject to a release process. 	<p>ISO/IEC 27001:2013: A.14.2.8, A.15.1.1, A15.1.2, A15.1.3, A15.2.1, A15.2.2, A.18.2.1, A.18.2.3</p> <p>BSI IT-Grundschutz 2021: IND.2.1.A1, IND.2.1.A4, IND.1.A21, IND.2.1.A16, ISMS.1, ORP4.A23, OPS.1.1.6, OPS.2.2,</p>



	Control objectives	Basic controls	References
N		<ul style="list-style-type: none">– Employees are regularly familiarized with the risks and trained on the correct use of cloud services.– Direct interfaces between cloud applications and the organisation's own OT, if any, are adequately protected. – Prohibited cloud applications should be blocked, permitted applications should be protected by adequate controls.	



ISACA Germany Chapter e. V.
Storkower Straße 158
D-10407 Berlin

www.isaca.de
info@isaca.de