Federal Office
for Information Security

BSI-Publications on Cyber-Security

RECOMMENDATION: IT IN PRODUCTION

Industrial Control System Security

Top 10 threats and countermeasures 2022

Systems for manufacturing and process automation - summarized under the term Industrial Control Systems (ICS, IACS) - are used in almost all infrastructures that handle physical processes. This ranges from energy generation and distribution to gas and water supply, factory automation, traffic control technology and modern building management. Such ICS are increasingly exposed to the same cyberattacks as conventional IT. Operators need to urgently address this issue in light of an increasing frequency of incidents and newly discovered vulnerabilities.Hence, they have to consider the risk and damage potential of untargeted malware as well as targeted, high-quality attacks against ICS infrastructures. This applies both to systems that are directly connected to the Internet and to those that can be attacked indirectly by cyberattacks.

As part of its cyber security analyses and industry collaborations, BSI has compiled the current threats with the highest criticality to which ICS are currently exposed. The identified threats are presented according to the following scheme:

1. Problem description and causes: the causes and underlying conditions contribute to the existence of the vulnerability or a threat situation
2. Possible threat scenarios: Possibilities are explained with which the previously mentioned problems can be abused for an attack.
3. Countermeasures: Measures are identified that are currently considered appropriate to mitigate the threat or to help minimize residual risks.

The present summary document can not and should not be considered as a complete list of threat scenarios and countermeasures. Rather, the scenarios listed are intended to illustrate the scope of the respective threat. The countermeasures listed represent starting points for countering the respective threats and allow an initial assessment of the overall measures required to defend against the respective threats.

Whether or which measures are specifically suitable and which alternative measures may be necessary must ultimately be examined in the respective application and evaluated within the framework of a risk analysis. In doing so, attention must be paid to effectiveness and economic efficiency, among other things. In all case compatibility with the operational business as well as applicable real-time and safety requirements must be ensured. Furthermore, the implementation of security measures must not lead to the loss of warranty or support services.

As a first step, the present Top 10 include a simple assessment of the resulting risks as well as a self-check for initial individual evaluation of your own security level.

Threats and their consequences

Risks for an ICS result from threats that can cause damage to the ICS and thus to a company due to existing vulnerabilities. The most critical and frequently occurring threats to ICS are summarized in the following table.

A differentiation is made between primary and secondary attacks. The focus is placed on primary attacks, with which attackers penetrate industrial systems and companies, while secondary attacks allow access to other internal systems.

Top 10 Threats	Trend since 2019
Infiltration of malware via removable media and mobile systems	→
Infection with malware via Internet and Intranet	↑
Human error and sabotage	→
Compromise of extranet and cloud components	↗
Social engineering and phishing	→
(D)DoS attacks	→
Internet-connected control components	↗
Intrusion via remote maintenance access	↗
Technical failure and force majeure	→
Soft- and hardware vulnerabilities in the supply chain	↑

Starting from most of these primary attacks, an attacker can successively spread throughout the company by means of follow-up attacks. The following sketch illustrates the connection:

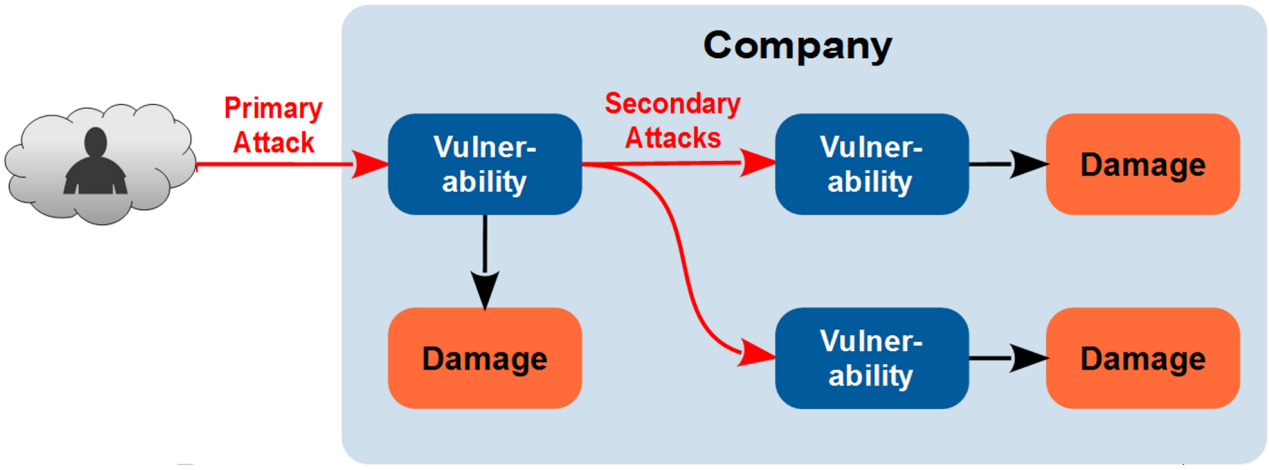

Figure 1: Sequence of primary and secondary attacks and consequences of damage

Secondary attacks specifically include:

- Privilege Escalation: In the industrial environment, existing standard IT components such as operating systems, application servers or databases often contain bugs and vulnerabilities that can be exploited by attackers.
- Unauthorized access to other internal systems: In particular, internal perpetrators or follow-up attacks after a penetration from the outside have an easy job if services and components in the corporate or control network do not use sufficient methods for authentication and authorization or basic hardening measures are missing.
- Manipulation of fieldbus communication: Since most control components currently communicate via plain text protocols and are therefore unprotected, it is often possible to read, manipulate or import control commands without much effort.
- Manipulation of network components: Components such as routers or firewalls can be manipulated by attackers to, for example, disable security mechanisms or redirect data traffic.
- Deployment of ransomware: This often encrypts data and systems. If no backups are available, recovery is often not possible, as paying a ransom is discouraged.
-

The implementation of measures against such follow-up attacks should be carried out after establishing basic protection against the primary attacks in the course of a so-called defense-in-depth concept.[1]

Organizational deficiencies, as well as ignorance or human error, encourage attacks and facilitate follow-on attacks. They also make it more difficult to detect attacks and to clean up and restore systems after a successful attack. The potential associated damage can take many forms and has to be assessed as rather critical:

- Triggering or manipulation of safety procedures or systems
  → Damage to people and the environment, production losses
  → Causing physical damage to equipment
- Disruption of the availability of parts or the entire ICS
  → Production losses
- Data leakage
  → Loss of know-how (intellectual property)
- Manipulation of systems or parameters
  → Reduction of the quality of the products

The corresponding countermeasures listed further below form the first line of defence and their implementation should be assigned the highest priority.

1 https://us-cert.cisa.gov/ics/Recommended-Practices

Assessment criteria

The basis for the evaluation is experience from concrete security incidents, threat and feedback from the industry. The ten most frequent threats are described, and a trend indicator shows the current development. Even if the trend remains the same or is even falling, there is still a threat to IT security and a holistic view of the company is required.

The evaluation criteria of the past years 2014 and 2016 were deviated from, as the criterion of prevalence seems to be the most essential for the evaluation of the risk. This is mainly due to the fact that the other criteria used previously (exposure, exploitability and detection) change only insignificantly, whereas the degree of prevalence can change significantly due to the activity of the offender groups. Thus, the order in this document does not represent a ranking.

In order to assess the resulting threat and risk for one's own company, the respective countermeasures should be evaluated according to technical or organizational feasibility for the identified threats. This assessment should be done together with a cost estimate of the respective measure. This cost estimate should then be compared and evaluated with the business impact, i.e. the economic effects for the company, for the respective case. As a rule, this can only be carried out by the operator himself, taking into account the general conditions and possible subsequent attacks.

Overview of changes

Compared to the last edition, no change can be seen for many threats in terms of exploitation. However, this does not mean that the threat posed by these has been reduced and that less attention should therefore be paid to them. Overall, a high level of danger can be assumed for all the threats listed.

The threat from smartphones is no longer a standalone item. This chapter is now part of the threat from removable media and mobile systems. The essential points have been integrated there.

A new addition is the threat posed by hardware and software vulnerabilities in the supply chain. More attention must be paid to this point in the future.

Infiltration of malware via removable media and mobile systems

Problem description & causes

Notebooks, smartphones, tablets, programming devices or removable data carriers such as USB sticks are often used for configuring and maintaining ICS components or transferring data between the ICS and office networks. In the case of these devices, it is not always clearly regulated or apparent to the operator where they are used. For example, private use is possible with laptops or smartphones. External personnel also usually carry their own devices with them. The use of notebooks with external data and maintenance software, which may be used in different companies by external maintenance personnel, also harbors risks.

Possible threat scenarios

1. Removable media may have been infected in the office network or in the private environment, for example. Malware can thus find its way directly into the ICS networks.
2. Notebooks or smartphones used for maintenance may have be infected when accessing the Internet, in office networks or in the infrastructure of the respective external service provider. As soon as these are then operated in the ICS network, the systems and components there are infected with malicious code.
3. Project files or executable applications may contain malicious code that leads to infection or data leakage.
4. Theft or loss of mobile systems (such as smartphones) or devices containing sensitive information (e. g. passwords or configured remote access to the ICS network).

Countermeasures

1. Establish strict organizational policies and technical controls for removable media:
   a. Taking inventory and whitelisting of approved removable media.
   b. Security perimeter for mobile devices (virus protection and file whitelisting, deployed on a machine that uses a different operating system than the maintenance devices).
   c. Exclusive use of company-owned, possibly personalized removable media.
   d. Exclusive use in the ICS network.
   e. Physical barriers against (unauthorized) connection of USB devices by e.g. resin, USB locks or removal of the ports.
   f. Full encryption of data carriers.
2. Establish strict organizational policies and technical controls over external devices, smartphones, tablets, etc. used for maintenance:
   a. Restriction of access or restriction of use
   b. The exchange of data takes place exclusively via removable media and is subject to the aforementioned controls.
   c. Establishment of quarantine networks for access by external service providers.
   d. Virus scan of the devices brought in before accessing the actual system.
   e. Full encryption of maintenance notebooks kept with the operator.
   f. Restriction and control of software/apps.

Infection with malware via Internet and Intranet

Problem description & causes

Enterprise networks use standard IT components such as operating systems, web servers and databases. Browsers or e-mail clients and are usually connected to the Internet. Every day, new vulnerabilities are discovered in these components. An attacker may exploit them to penetrate the systems and infect them with malware. This malware can also be placed in the intranet by an inside offender, for example.

The spread is also facilitated by the increasing prevalence of Ethernet-based networks and protocols in the ICS environment and their connection with systems in the corporate network (file servers, ERP, MES, etc.). If an attacker succeeds in penetrating the office network or is already on the intranet, he can often work his way into the ICS network directly or with follow-up attacks. Employees are not always aware of these connections.

Access from the ICS network or an ICS-related network to other networks - especially the Internet - can also lead to direct infection of the systems with malware.

Possible threat scenarios

1. Infection of systems via office communication software, e.g. as an attachment to an e-mail or a manipulated Office document
2. Manipulation of external websites, e.g. in order to carry out a drive-by download and thus infect the victims without user interaction, i.e. by simply calling up the website. One example would be browsing the internet using systems that are part of the control room or other operating controls.
3. Undocumented or unprotected connections between corporate network and ICS network.
4. Conducting attacks on enterprise web pages (e.g. SQL injection, cross-site scripting etc.).
5. ICS Components contain known vulnerabilities that can be exploited by malware for manipulation.
6. Installation of private hardware (e.g. Wifi router for smartphone, gaming PC, game console) by staff that is infected with malware or enables infection paths (see also Human error and sabotage).

Countermeasures

1. Maximal isolation of the different networks (segmentation) by firewalls and VPN solutions in order to largely exclude attack paths to the ICS network. Sealing off unprotected / non-patchable systems (so called "secure islands").
2. Use of conventional safeguards at the perimeter (e.g. firewalls, anti-virus software, Intrusion Detection Systems) or at the ICS (e.g. firewalls, application allowlisting).
3. Limitation of available information within the enterprise (e.g. on file servers or in databases) in order to impede leaking of critical information (need-to-know principle)
4. Regular and timely patching of the operating systems as well as the applications in the office and backend network and, where possible, in the ICS network.
5. Monitoring of the network and systems for unusual connections and transfer volumes, connection attempts and activities by network- and host-based IDS.
6. All IT components (services, computers) used in the Office and ICS must be hardened as best as possible.

Human error and sabotage

Problem description & causes

Personnel working in the ICS environment have a special position with regard to safety and security. This applies both to in-house staff and to all external personnel, e.g. for maintenance or construction - regardless of whether they have access to the systems or work remotely. Since, security can never be guaranteed by technical measures alone, organizational regulations are required.

Possible threat scenarios

1. Misconfiguration of security-relevant components (e.g. firewall) or network components, but also of ICS components.
2. Especially the uncoordinated installation of updates or patches can lead to problems in the functioning of individual components and their interaction.
3. Side effects of intentional acts must be taken into account (damage to equipment and installations, placement of listening devices, etc.).
4. Compromise of systems through unauthorized software and hardware. In the case of hardware, these include game consoles, digital cameras, smartphones, WLAN routers or other USB devices belonging to staff.
5. Create unapproved configurations for infrastructure and security components (e.g. add a firewall rule to allow unauthorized outside access from mobile devices).

In principle, the above scenarios can be triggered by espionage and sabotage as well as by negligence or other human error and misconduct. In particular, such incidents can lead to a significant impairment of availability due to organizational deficiencies. Many compromises are only possible due to such deficiencies.

Countermeasures

1. Establish the "need-to-know" principle: knowledge of system details, passwords, etc., and access to sensitive data should be restricted, when possible.
2. Creation of suitable conditions for committed, qualified and networked employees to ensure competence in the operation and administration of functional as well as safety-specific components. Qualification and training programs, as well as awareness-raising measures, must be designed for the long term and made mandatory.
3. Disabling of Internet access for control systems and production-related systems as well as provision of separate components for non-ICS tasks, which are available to the operators, e.g. for Office, e-mail, ERP, etc., are adequately secured and integrated in another network.
4. Establishment of standardized processes for new hires or employees leaving the company as well as for externally contracted persons (e. g. from manufacturers or service providers).
5. Suitable guidelines ("Policies & Procedures") for the handling of technical systems by employees (e.g. handling of removable data carriers, communication behaviour with e-mail and in social networks, password guidelines, installation of individual software, etc.).
6. Establish appropriate policies, especially for critical processes in the ICS network: For example, specifications regarding security and configuration management that regulate the involvement of security experts and other relevant roles so that changes or updates are only made after coordination with them. It is important to document all specifications and, if possible, to take accompanying precautions (e.g., dual control principle).
7. Automatic monitoring of system states and configurations.
8. Secure storage of projects and configurations.

Compromise of extranet and cloud components

Problem description & causes

The trend towards outsourcing IT components or application, which is widespread in conventional IT, can also be found in ICS. Often, these are not components that directly control real processes. However, there are more and more providers of externally operated software components in the area of data acquisition and processing on historians, for the calculation of complex models for the configuration of machines or the optimization of manufacturing processes (big data, digital twin). Security-specific components are also sometimes offered as cloud-based solutions. For example, providers of remote maintenance solutions place the client systems for remote access in the cloud, with which the maintenance technician can gain access to the respective components.

Currently, such solutions are of particular interest to small and medium-sized enterprises (SMEs), as in-house operation is often not economical, while the cloud enables cost-effective advantages such as scalability, redundancy and pay-per-use. However, such cloud solutions result in the system operator having very limited control over the security of these components and associated detection capabilities of a compromise. These components, however, may still be connected directly to local production.

Possible threat scenarios

1. Disruption or interruption of communication between local production and the outsourced (cloud) components, e.g. through denial of service attacks. Due to cascade effects, production can be impaired locally.
2. If there is too much and one-sided dependence on cloud-based services, the effects of a failure can endanger infrastructures and their production across locations.
3. Exploitation of implementation errors or inadequate security mechanisms to gain access to externally stored data (data theft, deletion).
4. If the clients of a cloud provider are insufficiently separated, attacks on third-party cloud services can lead to a compromise (collateral damage).

Countermeasures

1. Contractual obligation of the operators of external components to a sufficient level of security, e.g. by means of a Service Level Agreement (SLA).
2. Use of trustworthy and, if possible, certified providers.
3. Operate a private cloud to maintain control and protect process know-how.
4. Use of sufficiently strong cryptographic mechanisms (encryption, integrity protection) to secure the data stored in the cloud.
5. Use of Virtual Private Networks (VPN) to secure the connection between local production and external components.

Social engineering and phishing

Problem description & causes

Social engineering is a method of gaining unauthorized access to information or IT systems through mostly non-technical actions. Social engineering exploits human characteristics such as curiosity, helpfulness, trust, fear or respect for authority. These characteristics often serve as a distraction strategy for an attacker to tempt employees into a thoughtless or negligent act. A classic example of this is fraudulent emails (phishing emails). These tempt employees to open attachments with malware or contain links to manipulated websites. This threat is closely related to malware Infection with malware via Internet and Intranet .

Possible threat scenarios

1. Phishing attacks, in which the attacker uses fake messages to obtain victims' access data or distributes malware.
2. Messages with seemingly harmless links or attachments that install malware such as Trojans or ransomware when opened.
3. Spear phishing attacks, in which an attacker usually attacks a small number of people, but in which emails are then precisely adapted to the respective target persons. Public information from company websites or social networks is used for this purpose, among other things.
4. The attacker can gain unauthorised access to a building by appearing confident and friendly or by pretending to be someone else (e.g. posing as a technician).

Countermeasures

1. Conduct regular security awareness training for specific target groups.
2. Organizational measures: Establish and enforce security policies.
   a. Identify and classify information that has value to the business.
   b. Establishment of a data backup concept
   c. Introduce confidentiality and/or data protection declarations not only for own employees but also for partners and service providers.
   d. Guidelines for destroying information printed on paper (e.g. shredding).
   e. Safe disposal of digital data carriers.
   f. Regulations for the handling of mobile devices (privacy film, storage in a safe, etc.).
3. Establish alerting channels in case of incidents and also already in case of suspicion. These should be defined and communicated and should not have any negative consequences for the reporting employees.
4. Use of technical security mechanisms to enforce applicable regulations and automatically detect misconduct or attacks (e.g. device control, network segmentation, or access control).
5. Regular backups to restore data and applications

(D)DoS attacks

Problem description & causes

In the case of denial-of-service attacks, the communication link is overloaded or disrupted, or the receiving server is overloaded with requests. As a result, no or delayed data exchange is possible. This risk exists especially with Internet-connected systems. In the case of remote access, this interface can be overloaded, which prevents further monitoring or control. Measurement and control data can then no longer be transmitted.

This is also possible with wireless interfaces by interfering with the radio spectrum.

The observed frequency and bandwidth of DoS attacks is increasing every year. The trend moves from simple variants with high bandwidths to ambitious and intelligent forms that are tailored to the application. Attackers here take the application and the infrastructure into account and also react to countermeasures.

Possible threat scenarios

1. (D)DoS attacks on the Internet connection of central or remote components: This can be done, among other things, through botnets that an attacker can rent, for example.
2. DoS attacks on the interfaces of individual components: In this case, the processing logic of a component is disturbed and crashed by certain messages. This can affect control devices or central components (e.g. databases or application servers).
3. Attacks on wireless connections (e.g. WLAN, LoRaWAN) or mobile networks (e.g. GSM, LTE, 5G). This can be done, for example, by:
   a. the use of jamming transmitters, which overlap the corresponding frequency ranges,
   b. the use of fake base stations, i.e. fake base stations that trick the attacked systems into connecting to a false radio network,
   c. the sending of special data packets that cause existing connections to be terminated.
4. DoS attacks using ransomware (e.g. Trickbot[2]).

Countermeasures

1. Strict configuration and hardening of network access and communication channels.
2. Use dedicated wired connections for critical functions.
3. If applicable: Establish intrusion detection systems (IDS) to detect attacks and alert through alternate channels.
4. Redundant connection of components using different protocols or communication paths.

In addition, the BSI has made a document on DDoS mitigation available on the websites of the Alliance for Cyber Security to support those affected in emergency planning and defence against DDoS attacks[3] A comparison of one's own countermeasures should be made.

2 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2020.pdf
3 https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_002.html

Internet-connected control components

Problem description & causes

Despite the recommendations of product vendors, ICS components such as programmable logic controllers are often connected directly to the Internet. As a consequence, those are easily detected by search engines. Furthermore, these components often do not provide a sufficient security level like in standard IT. In addition, (timely) installation of patches is not possible for these components if a vulnerability is discovered. Therefore, implementing additional security mechanisms is required urgently.

Possible threat scenarios

1. Finding control components through general search engines ("google dorks"), special search engines like Shodan[4]or own internet scans.
2. Direct access to unprotected components or use of publicly available standard passwords to perform unauthorized operation and manipulation.
3. Exploitation of vulnerabilities in the accessible services such as web interface (WWW), FTP, SNMP or TELNET to gain access to the components or to impair their availability. Often ICS protocols (e.g. Modbus or Bacnet) are also directly accessible. Since they usually have no or only weak authentication functions, attackers can send control commands directly to the downstream components.

Countermeasures

1. No direct connection of control components to the Internet.
2. Hardening the configuration of control components such as disabling unneeded services, changing default passwords.
3. Use of additional controls such as firewalls and VPN solutions.
4. Timely updating vulnerable products by updates or patches if possible.

4 https://www.shodan.io/

Intrusion via remote maintenance access

Problem description & causes

External access for maintenance purposes is widespread in ICS installations. Often there are default accesses with standard passwords or sometimes hard-coded passwords. External accesses via Virtual Private Networks (VPN) are sometimes not limited in terms of the systems that can be accessed, i.e., additional systems can be accessed via a maintenance access for a specific system. Inadequate or lacking authentication and authorization as well as flat network hierarchies facilitate the intrusion.

The respective manufacturers and external service providers are often used for the maintenance and programming of components. This poses additional challenges for security management, as the security concepts of multiple parties must be reconciled.

Possible threat scenarios

1. Direct attack on a maintenance access, e.g. by means of
   a. Brute force attack on password protected access,
   b. Reuse of a previously recorded token,
   c. Web-specific attacks (e.g., injection or CSRF) on access points used for maintenance purposes.
2. Indirect attack via the IT systems of the service provider for which the external access was created, e.g.
   a. Trojan that exploits access directly on the external maintenance computer,
   b. Theft of a password, certificate or other token or other procurement of required access data, e.g. through bribery / blackmail of an employee with such authorization or an internal perpetrator,
   c. Using stolen notebooks that have software configured for external access.

Countermeasures

1. Standard users/passwords of a manufacturer (delivery state) are to be blocked/deleted (acceptance protocol).
2. Use of sufficiently secure authentication methods such as pre-shared keys, certificates, hardware tokens, one-time passwords, and multi-factor authentication through possession and knowledge.
3. Protection of the transmission path by encryption, e.g. with TLS[5].
4. Sufficiently granular segmentation of networks to minimize the "reach" of remote access.
5. Set up access points for remote maintenance in a demilitarized zone (DMZ) so that service providers connect to a DMZ first instead of to the ICS network, and from there they only have the access they need to the target system.
6. Remote access must always be routed through a firewall that grants and monitors access to the target system. Only the IP addresses, ports and systems required for maintenance are released.
7. Activation of remote access by internal personnel only for the duration and purpose of remote maintenance.
8. Logging of remote accesses to ensure traceability. Supplementary processes must ensure that this log data is evaluated and archived.
9. All accesses are to be personalised, i.e. refrain from functional accounts being used by more than one person. Only one login per user is allowed at the same time.
10. Conduct audits for such systems / accesses.

5 https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Mindeststandards/TLS-Protokoll/TLS-Protokoll_node.html

Technical failure and force majeure

Problem description & causes

Software errors in safety-specific components and ICS components that can lead to unforeseen misbehavior cannot be ruled out, nor can possible hardware defects and network failures. Hardware defects in particular are more likely to occur in some application scenarios in view of the operating environments to be found there (dirt, temperature, etc.).

Possible threat scenarios

1. Defect of components, e.g. failure of hard disks or switches, cable break, etc. at runtime, which lead to an immediate failure.
2. Both hardware defects and errors in software components can go unnoticed for a long time and only become a problem when, for example, systems are restarted or a certain boundary condition occurs.
3. Software errors can lead to the failure of a system. For example, an update of the operating system for a central security component can lead to the system no longer functioning correctly after a necessary restart.
4. In the event of climate change or extreme weather events, such as heat waves or floods, previous protective measures or planning (e.g. with regard to cooling) may not be adequate and lead to outages.

In particular, such incidents can lead to a significant impairment of availability due to organizational deficiencies.

Countermeasures

1. Establish an emergency management system that includes aspects such as possible countermeasures, system recovery procedures, alternative communication options, and conducting drills.
2. Keeping replacement or spare equipment on hand.
3. Maintaining and using test and staging systems on which patches, updates and new software components are thoroughly tested before they are installed on production systems.
4. Use of standardized, disclosed interfaces that are not a single vendor's own development. This reduces the risk of undetected gaps.
5. Redundant design of important components.
6. When selecting the systems and components used, sufficient minimum requirements must be set and enforced - in accordance with the identified need for protection. Important aspects in this context are:
    a. Trustworthiness and reliability of manufacturers,
    b. Robustness of the products,
    c. Existence of appropriate security mechanisms (e.g. secure authentication),
    d. Long-term availability of spare parts, updates and maintenance,
    e. timely availability of patches,
    f. open migration paths,
    g. Abandonment of unneeded product functions.
7. Regular review of the measures with regard to suitability and framework conditions

A solid basis for these and other aspects is provided, for example, by a white paper published by BDEW[6].

6 https://www.bdew.de/service/anwendungshilfen/whitepaper-anforderungen-sichere-steuerungs-telekommunikationssysteme/

Soft- and hardware vulnerabilities in the supply chain

Problem description & causes

Supply chains are sometimes very complex structures with a high degree of interconnectedness, within which manufacturers are often also customers. Vulnerabilities can therefore have an impact on all parts of the supply chain. Vulnerabilities in hardware and software, along with misconfigurations, are the starting point of many security problems (including those mentioned in this document). The integration of libraries or external source code (from third-party vendors) increases the dependencies between different vendors.

Updates to address vulnerabilities must be incorporated into their products by all parties involved in the supply chain. Depending on the length of this supply chain, it takes time for all parties to be informed of the vulnerability, take action, and notify customers.

Possible threat scenarios

1. A threat can originate from any part of the supply chain. The earlier in the chain vulnerable code is present, the more products are affected and the more difficult it is to determine one's own vulnerability. There are also examples where malicious functions or vulnerabilities have been deliberately built in by attackers.
2. The resulting errors can have various effects. These range from incorrect calculations to access rights that are too far-reaching to the possibility of executing arbitrary code. This not only affects primary attacks, but is "often essential" for follow-up attacks.
3. Not all vendors respond to vulnerability notifications. This also applies to the manufacturer's information channels for notifying its customers about vulnerabilities, updates or workarounds. Attackers use phishing mails with supposed information about patches to distribute malicious code.
4. There are chess points in an external library that no longer receives updates or the manufacturer is no longer active on the market.

Countermeasures

1. Asset management should be available. Information sources should also be stored that provide information on security advisories and updates. This also includes contact information for manufacturers, integrators and other service providers involved.
2. Trusted sources should be used when obtaining updates and libraries. The integrity should be validated before use.
3. A vulnerability management process should be established.[7] This process coordinates and evaluates incoming security reports and plans and implements the integration of updates in components and systems.

7 https://www.bsi.bund.de/csaf

Supplementary security measures

Basic measures

At this point, it should be emphasized that the best practices described are only intended to provide an introduction to an orderly IT security process within an ICS or an entire company. The goal should be to establish a functioning information security management system on the basis of established standards that contain both general IT security and specific ICS security requirements. Examples of such standards are:

- BSI IT-Grundschutz[8],
- ISO/IEC 27000-Reihe[9],
- VDI/VDE 2182[10],
- IEC 62443[11].

Building on those standards, an information security management system (ISMS) for ICS operation should be understood as a part of the super ordinate management system of an enterprise. Also, tt takes into account the specific risks of ICS and aims to permanently control, check, maintain and continually improve information security.

Most importantly, the following elementary controls should be considered introducing an ISMS. They serve to provide an overview of the present systems and their infrastructure to define responsibilities and to gain awareness of existing risks. For this purpose, it is useful to implement controls as early as possible to allow further planning to be as comprehensive and cost-efficient as possible.

- Setting up a security organization: This comprehensive task serves to define roles relevant for security and the associated responsibilities for the security of ICS components. This responsibility for security does not only concern to the individuals fulfilling these roles. The entire staff of an enterprise has to become aware of this responsibility and live it. In the end, the security of ICS should be a natural part of the organizational concept.
- Creation and maintenance of documentation: Documentation and information concerning the security of ICS components such as risk and vulnerability analysis, network plans, network management, configuration or security program and organization should be created, maintained and sufficiently protected against unauthorized access. If applicable, standard procedures for service providers and product suppliers should be included. This documentation enables to avoid incompatibilities and inconsistencies of software in specific versions and configurations. Furthermore it allows identify parts ofthe installation affected by vulnerabilities. In addition, physical and logical network-plans in particular enable consistent management of the infrastructure and the contained components.
- Risk management: One of the most important tasks is risk management. In this context, all functional as well as security specific resources of an ICS should be considered. These should be systematically analyzed and evaluated. The goal is to identify and prioritize threats and to derive suitable technical as well as organisational countermeasures. In fact, this is the only way for an enterprise to substantially assess its security level and the residual risks.
- Business continuity management (BCM): The aim of BCM is to ensure that business operations are not interrupted even in the event of massive damage events (prevention) or

8 https://www.bsi.bund.de/grundschutz
9 https://www.iso.org
10 https://www.vdi.de/uploads/tx_vdirili/pdf/9875774.pdf
11 https://webstore.iec.ch/preview/info_iec62443-1-1{ed1.0}en.pdf

can be continued within a reasonable time after a failure (response). BCM comprises organizational, technical, structural and personnel measures. To this end, institutions can partly draw on existing security measures of other management systems, such as the ISMS, or expand them if necessary.

- Reduction of vulnerabilities: As the threats continually change and develop, regular countermeasures are required in order to fend off potential attacks. In addition to staff training and subscription to security notifications such as by component vendors or the "Allianz für Cybersicherheit", this includes actively searching for vulnerabilities. These countermeasures must be carried out regularly.
- Detection of attacks and adequate responses: To detect and understand attacks, IT- and ICS-specific procedures as well as internal and external notification channels have to be defined.[12]

The role of corporate management

It is the duty of the management of a company to define the rules governing cyber security and to communicate them to everyone concerned in a qualified way. Sustaining the fulfillment of these expectations, suitable control mechanisms have to be introduced. Therefore, it is important not to consider cyber security as a secondary goal implied by the implementation of functional requirements. In fact, cyber security is one of the critical aspects for attaining the corporate objectives. Aside from economic considerations, the management may be personally liable to grant sufficient security levels. All in all, cyber security is in the management's own interest.

To enable corporate management to achieve the general conditions for a sufficient level of cyber security, adequate support must be provided by the technical personnel. This includes awareness of the effects of potential security incidents and providing target group specific information about the current state of implementation of cyber security. As part of strategic planning, corporate management has to be involved in all important decisions at an early stage. In this context, the remaining residual risks as well as instances of urgent need for action have to be emphasized. Also, the technical personnel should be aware that security is in the interest of corporate management. Furthermore the relevant foundations for decision-making should be made transparent to enable the corporate management to act accordingly.

Countermeasures against subsequent attacks

Various suitable countermeasures exist protecting against potential subsequent attacks. These include physical safeguarding of the infrastructure against unauthorized local access, recording and evaluating of log data, and hardening of IT and ICS components. These controls, as well as additional countermeasures are explained in detail in the BSI's ICS Security Compendium. It is strongly recommended to implement these kinds of controls. On the contrary, the widespread opinion that singular safeguards or security products are enough to achieve a sufficient security level can have disastrous consequences. Instead, implementation of the so-called defense-in-depth approach, i.e. a multi-layered security concept in which the chosen security mechanisms form suitable redundancies and offer mutual support, will yield the desired results.

12 https://www.allianz-fuer-cybersicherheit.de/Webs/ACS/DE/Service/Meldungen/meldungen_node.html

Self Check

The following list of questions assist in self-assessment of the security level in your enterprise. Small and medium sized enterprises (SMEs) can answer the questions with the entire enterprise in mind. For larger enterprises, it is appropriate to limit this to individual parts such as an single production line. Also, it is recommended and might even be necessary not to answer the questions on your own, but discuss them with the people in charge of IT and production.

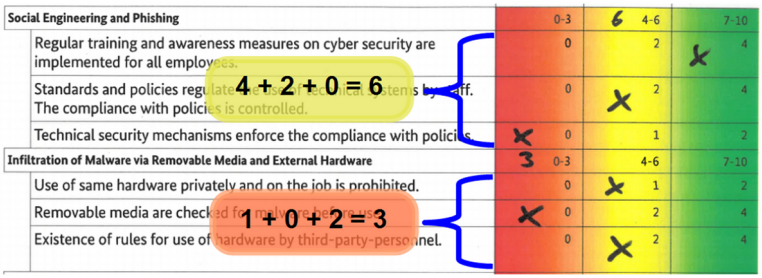

Figure 2: Example of filled-in self-check sheet

Please assess for each of the individual countermeasures whether they have been implemented completely, in part, or not at all for the enterprise or the analysed segment. A score is given for each field. Add the scores obtained for each section and enter the sum in the line with the corresponding headline. The following figure shows an example. In case a safeguard is not required, please write down the full score. For example, this would be the case for item 'Intrusion via Remote Access', if no access points for remote maintenance in the entire enterprise are required and applied. Finally, add up all obtained scores and enter them into the scale in the last line.

The result provides a preliminary self-assessment of your protection against the most critical threats in the area of industrial control systems and/or industrial IT. This self-check may be considered as a first orientation for the security assessment of an installation or an enterprise. It cannot and must not replace a comprehensive cyber-security analysis. For this reason, the obtained total score should be treated with caution. The following recommendations apply depending on the obtained score:

- 0-25: The current situation on www.allianz-fuer-cybersicherheit.de and the Top 10 Threats and Countermeasures for ICS illustrate why you should act now.
- 26-50: Some security mechanisms have already been implemented. However, there is need for action regarding elementary countermeasures cited in the present Top 10.
- 51-75: Perform a risk analysis in order to analyse which security mechanisms you need to improve most urgently to be protected against certain threats.
- 76-100: Your enterprise already handles cyber security responsibly. That does not mean, however, that you are reliably protected against cyber attacks. You should pursue the path to a systematic and comprehensive approach such as IT-Grundschutz or IEC 62443. The BSI's ICS Security Compendium guides you in that direction.

In the context of addressing these questions, you may already have begun to discuss with your co-workers which measures would be necessary and useful in order to improve security. This is a great opportunity to set a starting point for further steps. Also, the results obtained from the self-check can be used to discuss the issue of enterprise security in general and in production in particular with the management.

	Not implemented	Partially implemented	Implemented
Social engineering and phishing	0-3	4-6	7-10
Regular training and awareness measures on cyber security are implemented for all employees.	0	2	4
Standards and policies regulate the use of technical systems by staff. The compliance with policies is controlled.	0	2	4
Technical security mechanisms enforce the compliance with policies.	0	1	2
Infiltration of malware via removable media and mobile systems	0-3	4-6	7-10
Use of same hardware privately and on the job is prohibited.	0	1	2
Removable media are checked for malware before use.	0	2	4
Existence of rules for use of hardware by third-party-personnel.	0	2	4
Infection with malware via Internet and Intranet	0-3	4-6	7-10
The enterprise network is segmented separating office- and ICS-networks in particular.	0	2	4
Virus protection has been introduced for e-mail, file servers, PCs as well as on network boundaries between ICS and other networks.	0	2	4
It is impossible to access the Internet from the ICS network.	0	1	2
Intrusion via remote maintenance access	0-3	4-6	7-10
Remote access always requires authentication and is encrypted.	0	2	4
Remote access is fine-grained, i.e. access only to the required component instead of the entire subnet.	0	1	3
There are security policies in place for computers performing remote maintenance (e.g. up-to-date virus protection)	0	1	3
Human error and sabotage	0-3	4-6	7-10
The “need-to-know“ principle has been introduced to prevent sensitive information from being distributed more widely than necessary.	0	2	4
There are sufficient standards in place regarding security and configuration management.	0	1	3
Technical controls monitor the current system configurations and states.	0	1	3

	Not implemented	Partially implemented	Implemented
Internet-connected control components	0-3	4-6	7-10
There is no direct connection of control components with the Internet.	0	2	4
Configuration of control components has been hardened such as disabling unneeded services or changing default passwords.	0	1	3
Additional controls such as firewalls and VPN solutions are used.	0	1	3
Technical failure and force majeure	0-3	4-6	7-10
Security aspects are considered during selection of components based on ISA 99, BDEW White paper or other appropriate standards.	0	2	4
Important IT systems feature a redundant design and a distributed structure.	0	1	3
Procedures have been defined to respond to system failure.	0	1	3
Compromise of extranet and cloud components	0-3	4-6	7-10
Users of external components are obliged to comply with a sufficient security level, e.g. through a Service Level Agreement.	0	2	4
Only trusted and, if possible, certified service providers are used.	0	1	3
Operations are conducted in the form of a private cloud or with guaranteed strict separation of clients.	0	1	3
(D)DoS attacks	0-3	4-6	7-10
Mechanisms for detection and alerting in case of significant changes to network traffic have been introduced.	0	2	4
External connections of critical systems are designed with redundancy via different communication technologies.	0	1	3
Contingency planning documents how to proceed in case of a DDoS attack as well as the relevant external contacts.	0	1	3
Soft- and hardware vulnerabilities in the supply chain	0-3	4-6	7-10
There is a central asset/device management?	0	2	4
Information on vulnerabilities is obtained from manufacturers or integrators and evaluated in regular basis.	0	1	3
Provided updates are scheduled and imported into maintenance processes.	0	1	3
GESAMTPUNKTZAHL			(0-100 Punkte)

Many risks and threats cannot be minimised by the implementation of technical controls alone, but rather by a combination of organizational regulations and technical controls.

The countermeasures proposed in the present document are generally suitable to limit the identified threats with regard to their probability of occurrence as well as their impact. However, it is important for the understanding of security for all persons involved that certain residual risks will always remain.

For further information on security in factory automation and process control see the BSI's ICS Security Compendium, which is available free of charge. Among other things, it describes controls intended to be used in addition to the primary attacks described here for protection against subsequent attacks in the context of a defense-in-depth approach. The ICS Security Compendium, as well as additional publications and tools, are available on the BSI website:

https://www.bsi.bund.de/ICS

Here you can also obtain additional information on issues such as raising employee awareness, security management, or technical requirements as well as more topics related to Industrial Control Systems.

If you have any further questions regarding security in industrial control systems, you can contact the BSI under

ics-sec@bsi.bund.de