Federal Office
for Information Security

RECOMMENDATION: IT IN PRODUCTION

Industrial Control System Security

Top 10 Threats and Countermeasures 2019

Manufacturing systems and process automation systems – collectively termed Industrial Control Systems (ICS) – are used in almost all infrastructures handling physical processes. Applications range from energy production and distribution, gas and water supply to industrial automation, traffic control systems and state-of-the-art facility management. These ICS are increasingly exposed to the same cyber threats as conventional IT systems. In light of the increasing frequency of incidents and newly discovered vulnerabilities, asset owners need to address these issues urgently. 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 to infrastructures directly connected to the internet as well as to infrastructures that can be targeted by cyber attacks indirectly.

In the context of its analyses and cooperation with industrial partners on cyber security, the BSI has compiled a list of the current threats with the highest criticality for ICS. The identified threats are presented using the following structure:

1. Description of the problem and causes: Presentation of the cause and determining factors contributing to the presence of a vulnerability or threat situation.
2. Potential threat scenarios: Description of the specific potential to use the determining factors illustrated in the preceding paragraph to carry out an attack.
3. Countermeasures: Description of options currently deemed suitable to counter the threat and to minimize the residual risk.

The present summary document can not and should not be considered as a complete list of threat scenarios and countermeasures. Rather, the described scenarios are intended to illustrate the scope of the associated threat. The cited countermeasures represent starting points to counter the respective threats and allow a first assessment of the effort required for defence. In the end, it has to be tested for each individual use case and assessed in the context of a risk analysis if any specific countermeasures are suitable and which alternative countermeasures may be necessary. Among other factors, efficiency and cost-effectiveness have to be taken into account. In all cases, compatibility with running operations and the real-time and safety requirements in effect has to be ensured. In addition, the implementation of safeguards 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.

BSI Publications on Cyber-Security

Threats and their consequences

Risks to an ICS result by threats which can potentially cause damage to the ICS, and therefore to the associated enterprise, due to existing vulnerabilities. The following table offers an overview of the most critical and most common threats to ICSs.

Hereby, a distinction between primary attacks and subsequent attacks is introduced. The focus is on primary attacks used by the threat agent to penetrate an industrial facility, whereas subsequent attacks allow threatening of or access to additional internal systems.

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	

Starting from most primary attacks, an attacker can penetrate further into the organization with each subsequent attack. The following figure serves to illustrate the connection:

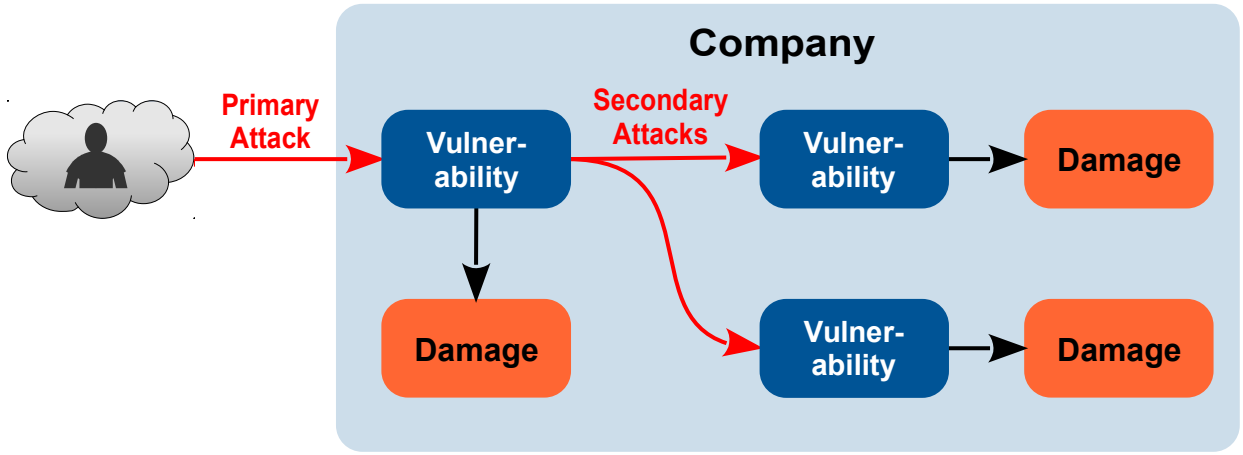

Figure 1: Sequence of primary attacks and follow up attack including associated damage

Subsequent attacks include in particular:

- Extraction of credentials to increase privileges: Standard IT components used in industrial environments such as operating systems, application servers or databases usually contain bugs and vulnerabilities. Threat agents can take advantage of these.
- Unauthorised access to further internal systems: Insiders or subsequent attacks in particular have an easy job if services and components in an enterprise or control network do not use adequate methods for authentication and authorization. For instance, a subsequent attack of this kind can be applied by using a brute force or dictionary attack on authentication mechanisms.
- Manipulation of fieldbus communication: Most control components currently communicating via plaintext protocols. As a result, little effort is usually required to read, manipulate or issue control commands.
- Manipulation of network components: Threat agents can manipulate routers or firewalls overriding security mechanisms or reroute data traffic.

The implementation of measures to counter such subsequent attacks should be carried out after establishing basic protection against primary attacks, in the context of so-called defence-in-depth concepts [1].

Insufficient organisational policies and lack of knowledge or human error favour attacks and facilitate subsequent attacks. In addition, they impede the detection of attacks as well as sanitizing and restoring systems after a successful attack. The potential associated damage can take many forms and has to be assessed as rather critical:

- Loss of availability of the ICS / loss of production
- Data leakage / loss of know-how (intellectual property)
- Physical damage to facilities
- Triggering of safety procedures or interfering with safety systems
- Deterioration of product quality

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

Assesment Criteria

The basis for evaluating threats are the expertise from security-specific incidents, threat intelligence reports as well as reports from the industrial sector. As a result, the order of the threats just illustrate the recent development. Even if the trends is static or decreasing, the corresponding threat has to be taken seriously.

The recent assessment criteria deviate from those of previous years [2], [3] since the criterion of prevalence for evaluating the risk is essential. This is the case because the criteria exposure, exploitability, and detection remaining more or less unchanged. Contrary, the prevalence relies significantly on the activity of criminal groups.

Estimating the threat and risk for your own enterprise, you should evaluate the individual countermeasures regarding their technical or organisational feasibility. This assessment should go hand in hand with a cost estimation of the respective countermeasure. On the other hand, it is particularly important to assess the business impact, i.e. the economic consequences for the enterprise, for each case individually. Usually this can only be done by the asset owner taking the general conditions and potential subsequence attacks into account.

Infiltration of Malware via Removable Media and External Hardware

Description of problem & causes

Removable media such as USB flash drives are widely used. Company employees often use them both in the office and ICS networks. Also, they take them home frequently to continue working there or copy the latest music on it for work. In addition, external personnel often carry their own notebook computers with external data and maintenance software, which is used likely at different companies.

Regarding the history of ICS, security awareness is mainly limited to the aspects of availability and physical security such as safety, access restrictions and protection from external influences. As a result, employees are often unaware of the effects caused by malware.

Potential threat scenarios

1. USB flash drives may have been infected in the office network or private environment. In that way, malware can find its way directly into ICS networks.
2. Notebook computers used for maintenance may have been infected when accessing the Internet, office networks, or in the infrastructure of the respective service provider. As soon as they are operated in the ICS network, systems and components become infected with malicious code.
3. Project files or executable applications can contain malicious code leading to an infection or data leakage.

Countermeasures

1. Introduction of strict organisational policies and technical controls with regard to removable media:
   a. Taking inventory and whitelisting of approved removable media.
   b. Security perimeter for removable media (virus protection and file whitelisting, provided on a computer using a different operating system than the maintenance computers).
   c. Exclusive use of in-house, possibly personalised removable media.
   d. Exclusive use in the ICS network.
   e. Physical barriers preventing (unauthorised) connection of USB devices using resin, USB locks or desoldering from circuit boards.
   f. Full encryption of data media.
2. Introduction of strict organisational policies and technical controls with regard to external notebook computers used for maintenance :
   a. Exchange of data only via removable media subject to the controls stated above.
   b. Introduction of quarantine networks for access of external service providers.
   c. Virus Scan of external notebooks before accessing the actual system.
   d. Full encryption of maintenance notebook computers are kept by the asset owner.

Malware Infection via Internet and Intranet

Description of problem & causes

Enterprise networks use standard components such as operating systems, webservers and databases. Browsers or e-mail clients are typically connected to the Internet. New vulnerabilities of these components are discovered almost every day. A perpetrator may use those getting into the intranet deploying malware. Alternatively, malware may be placed in the intranet by infected removable media. In both cases, critical or sensitive information can be obtained by the threat agent. Furthermore, maintaining an proper IT-Security is hampered by the increasing prevalence of ethernet-based networks and protocols in ICS environments and their connection to enterprise computing (fileservers, ERP and MES systems). If a threat agent manages to get into the office network or is already present in the intranet, he may infiltrate the ICS network directly or via a subsequent attack. Those relationships are often not obvious immediately.

Access from the ICS network or a network close to ICS to other networks – especially the Internet – can result in targeted as well as untargeted attacks.

Potential threat scenarios

1. Exploitation of known vulnerabilities or so-called zero-day exploits. The latter are previously unknown attacks that cannot yet be detected by antivirus products and the like.
2. Manipulation of external web pages, e.g. in order to carry out a drive-by download. In doing so, the victims can get infected by simply accessing the website. One example would be browsing the internet using systems that are part of the control room or other operating controls.
3. Conducting attacks on enterprise web pages (e.g. SQL injection, cross-site scripting etc.).
4. Components are infected by untargeted malware (e.g. worms), limiting their functionality or availability.
5. Installation of private hardware such as WLAN-router for using smartphones, gaming PC or consoles. This hardware might be already infected or can be used as attack vectors (see capture Human Error and Sabotage)

Countermeasures

1. Maximal isolation of the different networks (segmentation) by firewalls and VPN solutions to largely eliminate attack paths leading to the ICS network. Isolation of unprotected / unpatchable systems (“secure islands“).
2. Use of conventional safeguards at the perimeter (e.g. firewalls, antivirus software) or on the ICS (e.g. application whitelisting, firewalls if applicable).
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 operating systems and applications in the office and back-end networks and, if applicable, in ICS networks.
5. Monitoring log files for unusual connections or connection attempts.
6. Optimal hardening of all IT components (services, computers) used in office and ICS environments.

Human Error and Sabotage

Description of problem & causes

Staff working in an ICS environment are in a special position regarding security. This applies to in-house staff as well as to all external personnel such as for maintenance or construction. It does not matter if they have access to facilities or work from a remote location. Since, security can never be guaranteed by technical controls alone, organisational regulations are required.

Potential threat scenarios

1. Incorrect configuration of network components, components related to security such as firewalls, or ICS components in general.
2. In particular, the uncoordinated installation of updates or patches can lead to problems of the functionality of individual components and their interaction.
3. Side-effects of intentional actions such as damaging devices and installations or placing of covert listening devices need to be considered .
4. Compromising systems by unauthorised software or hardware. This includes games, digital cameras, smartphones, or other USB devices owned by operators.
5. Creation of unreleased configurations for infrastructure and security components. An example would be adding a firewall rule to allow unauthorised access from outside via mobile endpoints.

The scenarios described above can generally be triggered by espionage and sabotage, but also by carelessness and human error. In particular, incidents of these kinds can lead to a significant limitation of availability due to organisational shortcomings. Many compromising situations are only possible because of such shortcomings.

Countermeasures

1. Introduction of the “need to know“ principle: Knowledge of system details or passwords as well as access to sensitive data is provided only if necessary.
2. Creation of a general framework for motivated, qualified and connected staff to ensure operator and administrator competence for functional as well as security-specific components. Qualification and training programmes, as well as awareness-raising measures, are to be designed sustainably and compulsory.
3. Disabling internet access for control systems and those close proximity to the production environment. Furthermore, components for operational tasks separate from the ICS such as e-mail and further office applications shall be sufficiently secured and integrated into a different network.
4. Introduction of standardised processes for just hired or leaving staff as well as external contractors such as product suppliers, vendors, or service providers.
5. Suitable standards such as policies and procedures regarding technical systems. Examples are handling of removable media, communication behaviour in e-mail and social networks, password policies or installation of individual software.
6. Introduction of suitable policies for critical processes in the ICS network. For example, standards concerning security and configuration management regulating the involvement of security experts and other relevant roles. This should ensure that changes or updates are implemented only after they have been consulted. In this context, it is important documenting all agreements backed up by additional arrangements such as using the four-eyes principle.
7. Automatic monitoring of system status and configurations.
8. Secure storage of projects and configurations.

Compromising of Extranet and Cloud Components

Description of problem & causes

The common trend in conventional IT to outsource IT components is also gaining traction in the ICS sector. This usually does not concern components directly controlling actual processes, as latency will usually prevent real-time requirements from being fulfilled. However, the number of providers of externally operated software components in the area of data capture and processing on historians, for the calculation of complex models for the configuration of machines or the optimisation of manufacturing processes (Big Data), has been continually increasing. Also, security specific components are occasionally offered as a cloud-based solution. For example, providers of remote maintenance solutions place the client systems for remote access in the cloud, which the maintenance technicians can use to access the different components.

Solutions of this kind are currently of particular interest for small and medium sized enterprises (SMBs) since independent operations are often uneconomical. On the contrary, cloud-based systems are affordable and offer advantages such as scalability, redundancy, and pay-per-use. These cloud solutions, however, lead to the asset owner having only very limited control over the security of these components. These components, however, may still be connected directly to local production.

Potential threat scenarios

1. Interference with or disruption of communication between local production and the outsourced (cloud) components caused by, for example, denial-of-service attacks. Also, cascade effects can impair local production.
2. Exploitation of implementation errors or insufficient security mechanisms in order to gain access to data stored externally (data theft, deletion).
3. If a cloud provider's clients are insufficiently separated, attacks on other cloud services may lead to interferences (collateral damage).

Countermeasures

1. Contractual obligation for operators of external components to provide a sufficient level, e.g. through a service-level-agreement (SLA).
2. Use of trusted and, if possible, certified service providers.
3. Operation of a private cloud to retain control and protect process know-how.
4. Use of sufficiently strong crytographic mechanisms such as encryption or integrity protection to protect 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

Description of the problem & causes

Social Engineering is a method to gain unauthorised access to information or IT systems by usually non-technical means. Social engineering exploits human traits such as curiosity, helpfulness, belief, fear or respect for authority. These characteristics are often used by threat agents as a diversion strategy to entice employees to act thoughtlessly or carelessly. Typical examples are fraudulent e-mails (phishing mails). These try to tempt employees to open attachments containing malware or lead them to malicious websites.

Potential threat scenarios

1. Phishing attacks are used by a threat actor to obtain victim's login credentials or to distribute malware through fraudulent messages.
2. E-mails with seemingly unoffending harmless links or attachments which install malware like trojans or ransomware in case of a execution.
3. Spear phishing are used to attack a usually small number of targets with e-mails tailored precisely to the targeted persons. Among other sources, public information taken from company websites or social networks is used for this purpose.
4. A threat agent may also gain unauthorized access to a building or site by confident and friendly demeanour or by providing false information such as pretending to be a service technician.

Countermeasures

1. Conducting target audience specific security awareness training.
2. Organisational precautions: Compilation and enforcement security policies.
   a. Identification and classification of information valuable to the enterprise.
   b. Establishing data backup policies.
   c. Introduce confidentiality and/or privacy agreements not only for in-house staff, but also for partners and service providers.
   d. Established policies for destruction of information printed on paper such as shredding.
   e. Secure disposal of digital storage media.
   f. Regulations for handling of mobile devices such as privacy film or secure storage.
3. Introduce alarm channels for incidents and already for suspicious behaviour. Those reports should be defined and communicated clearly and without any negative consequences for reporting staff.
4. Use of technical security mechanisms to enforce the applicable regulations and for automatic detection of misconduct or attacks such as device control or access control.
5. Periodical backups to restore data and applications in case of an incident.

(D)Dos Attacks

Description of problem & causes

Wired as well as wireless connections are used for communication between ICS components. If these connections are interrupted, measuring and control data for example cannot be transmitted anymore. Another option is to overload a component with a very high number of queries making it impossible to deliver a timely answer. This is called a (distributed) denial-of-service ((D)DoS), i.e. deliberately causing a malfunction. In some cases this attacks are distributed over several threat agents.

Current threat situations

“The reported high occurrence of further IoT botnets with botnet capacities in the six-figure range further increases the probability of occurrence and the potential impact of DDoS attacks [4].“ Therefore, the ICS environment has to be protected against these attacks regarding the continues increasing interconnectivity between IT and OT.

Potential threat scenarios

1. (D)DoS attacks on the internet connection of central or remote components. For example, this can be done by a rentable botnets. In addition, “hacktivism“ groups such as Anonymous are becoming increasingly relevant in this context.
2. DoS attacks on the interfaces of individual components: This type of attack interrupts the processing logic of a component using specific messages and causes it to crash. This can affect control devices or central components (e.g. databases or application servers), among others.
3. Attacks on wireless connections such as WLAN or mobile communications networks (GSM, UMTS, LTE). This can be done, for example, by:
   a. the use of disrupting or jamming transmitters with corresponding frequency ranges,
   b. the use of fake base stations leading the attacked systems to connect with an incorrect wireless network,
   c. sending especially crafted data packages causing existing connections to be aborted.
4. DoS attacks with the help of ransomware such as Trickbot[1]

Countermeasures

1. Strict configuration and hardening of network access points and communication channels.
2. Use of dedicated, cabled connections for critical applications.
3. Where applicable: Installation of intrusion detection systems (IDS) to detect attacks and trigger alarms via alternative channels.
4. Redundant connection of components using different protocols and/or communication channels.

In addition to the countermeasures, the BSI provides a document on DDoS mitigation on the web pages of the Allianz für Cyber-Sicherheit [5] (Alliance for Cyber Security). A comparison with own countermeasures should be performed.

1 https://www.tz.de/muenchen/region/fuerstenfeldbruck-computervirus-legt-kreisklinik-lahm-betrieb-mit-starken-einschraenkungen-10563771.html

Control Components Connected to the Internet

Description of problem & 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.

Potential threat scenarios

1. Retrieval of control components by common search engines ("Google dorks") or specialised search engines such as Shodan[2], Censys, or custom internet scans.
2. Direct access to unprotected components or use of publicly available default passwords to perform unauthorised operation and manipulation.
3. Exploitation of vulnerabilities in available services such as web interface (WWW), FTP, SNMP, or TELNET to gain access to components or to limit their availability.

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.

2 https://www.shodan.io/

Intrusion via Remote Access

Description of problem & causes

External access for maintenance purposes is very common for ICS. Also common are poorly secured access codes such as default or even hardcoded passwords is a widespread issue. Furthermore, external access via Virtual Private Networks (VPN) is sometimes not limited with regard to specific system. As a consequence, further systems are accessible. In sum, the main causes are lack of authentication and authorisation as well as flat network structures.

The respective product suppliers and external service providers are often contracted for maintenance and programming of components. This creates additional challenges for security management as it requires harmonisation of the security concepts from several parties.

Potential threat scenarios

1. Direct attack on an maintenance access point, e.g. by
   a. a brute-force attack on password-protected access points,
   b. re-use of a previously recorded token,
   c. web-specific attacks, e.g. injection or CSRF, on access points used for maintenance.
2. Indirect attack via the IT systems of the service provider the external access was created for, e.g.
   a. trojans exploiting the access directly on the external maintenance computer,
   b. theft of passwords, certificates or other tokens or other ways of aquiring login details, e.g. by bribing / blackmailing staff possessing such privileges,
   c. use of stolen notebook computers with software configured for external access.

Countermeasures

1. Default users / passwords of a product supplier (delivery condition) shall be deactivated, blocked or deleted (acceptance protocol).
2. Using sufficiently secure authentication procedures, e.g. pre-shared keys, certificates, hardware tokens, one-time passwords and multi-factor authentication through possession and knowledge.
3. Protection of the transmission route by encryption such as SSL/TLS.
4. Sufficiently granular segmentation of networks to minimise the “reach“ of remote access.
5. Setup of access points for remote maintenance in a demilitarised zone (DMZ). In that way, service providers first connect to a DMZ instead to the ICS network. There, they obtain the required access on the target system only.
6. Remote access should always be routed through a firewall permitting and monitoring access to the target system. This is limited to exposing only those IP addresses, ports and systems required for maintenance.
7. Enabling of remote access by internal personnel only for duration and the purpose of remote maintenance.
8. Logging of remote accesses to ensure traceability. Additional processes shall be used to ensure that the logged data is evaluated and archived.
9. All means of access must be personalised, i.e. no use of functional accounts used by more than one person. Only one login per user is allowed at any time.
10. Auditing of these systems / means of access.

Technical Malfunctions and Force Majeure

Description of problem & causes

It is impossible to exclude software errors in security-specific components and ICS components that may lead to unexpected malfunction as well as potential hardware defects and network failures. Hardware defects, in particular, are more likely in certain application scenarios caused by the existing environmental conditions such as dirt or temperature if the necessary precautions have not been taken.

Potential threat scenarios

1. Component defects such as failure of hard disks or switches or cable breakage during the runtime leading to immediate failure.
2. Both hardware defects and errors in software components can remain undiscovered for a long time and may not become problematic until systems are restarted or a certain constraint applies.
3. Software errors can cause a system to fail. For example, an update of the operating system of a central security component can lead to a system malfunction after a required restart.

In particular, incidents of this kind can lead to a significant limitation of availability due to organisational shortcomings.

Countermeasures

1. Establishing a business continuity management including aspects such as potential countermeasures, procedures for system recovery, alternative communication options, and conducting drills.
2. Provision of exchange or replacement devices.
3. Providing and applying test and staging systems used to test patches, updates, and new software components thoroughly before they are installed on production systems.
4. Using standardised interfaces that are not developed by the product supplier. This minimises the risk of undiscovered vulnerabilities.
5. Redundant design of important components.
6. For the selection of used systems and components, sufficient minimum requirements have to be defined and enforced according to the indentified need for protection. Some important aspects in this context are:
    a. trustworthiness and reliability of the product vendors,
    b. robustness of products,
    c. existence of suitable 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. no use of unneeded product features.

A sound foundation for these and other aspects can be found in a white paper by the BDEW [6].

Compromising of Smartphones in the Production Environment

Description of problem & causes

Displaying and modifying operations or production on a smartphone or tablet computer is increasingly promoted and used as an additional product feature for ICS components. This constitutes a special case of remote maintenance access adding additional attack vectors.

Potential threat scenarios

1. Theft or loss of smartphones.
2. Attack on the smartphone by additional programs collecting insufficiently protected information on the device.
3. Attack on the communication channel of the smartphone with the ICS component:
   a. logging of communication with the ICS,
   b. replay attacks through sending of previously recorded communication,
   c. reverse engineering of the used applications or the used protocol,
   d. man-in-the-middle attacks (MITM)

Countermeasures

1. Restriction of access to ICS systems via smartphones to read access. As a consequence, it should be impossible to modify operation or production parameters.
2. Use of products or included features of the operating system for access protection, protection against malware and remote deletion function (mobile device management).
3. No modification that are forbidden or critical to security such as jailbreaking or rooting may be carried out on smartphones.
4. Smartphone applications (apps) must be obtained from a certified source (App Store). Ideally, apps are audited and distributed centrally by the IT department.
5. Use of encrypted connections (VPN).
6. Assessment whether the benefits of using smartphone outweighs the risks.
7. No use of apps for direct access to ICS. However, indirect encrypted access by a secured terminal server, providing only the required programs, can be allowed.

Additional Safeguards

Basic measures

It is important to emphasise at this point that the best practices described here are merely intended to enable a structured security process within an ICS or the enterprise as a whole. Instead, the goal should be to introduce a suitable information security management on the basis of established standards for both cyber security in general and ICS security in particular. As examples may serve:

- IT-Grundschutz ("IT baseline protection") based on ISO 27001[3],
- ISO/IEC 27000 series[4],
- VDI/VDE 2182[5],
- IEC 62443[6].

Building on those standards, an information security management system (ISMS) for ICS operation should be understood as a part of the superordinate management system of an enterprise. Also, it 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 organisation: 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 organisational 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 organisation should be created, maintained and sufficiently protected against unauthorised 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 of the installation affected by vulnerabilities. In addition, physical and logical network plans in particular enable stringent 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 analysed and evaluated. The goal is to identify and prioritise 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.

3 https://www.bsi.bund.de/EN/Topics/ITGrundschutz/itgrundschutz_node.html
4 https://www.iso.org
5 http://www.vdi.de/uploads/tx_vdirili/pdf/9875774.pdf
6 https://webstore.iec.ch/preview/info_iec62443-1-1{ed1.0}en.pdf

- Contingency plan management and restart procedures: After an incident, the processes for continued operations have to be defined to enable structured recommissioning. For secure and uninterrupted operation it is necessary that service and maintenance personnel as well as administrators know all ICS features and are able to operate them. This requires that all documents for operation and commissioning in the form of administrator and user guides are available and accessible for responsible and authorised staff.
- 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.[7]

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 emphasised. 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 unauthorised 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 defence-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.

7 https://www.allianz-fuer-cybersicherheit.de/ACS/DE/Meldestelle/meldestelle.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.

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 Removable 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.

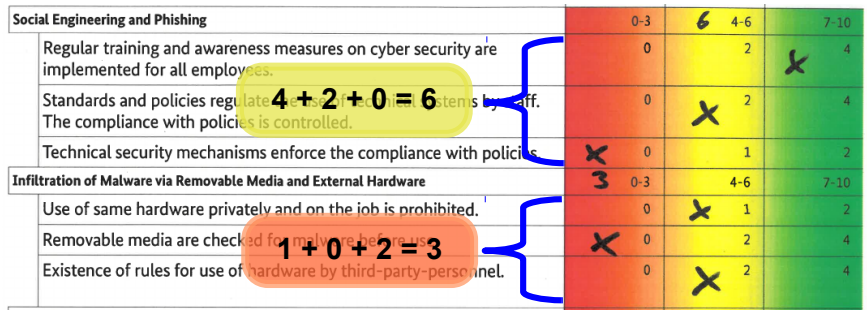

Figure 2: Example of filled-in self-check sheet

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	Partly implemented	Completely 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 External Hardware	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
Malware Infection 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 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	Partly implemented	Completely implemented
Control Components Connected to the Internet	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 Malfunctions 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
Compromising 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
Compromising of Smartphones in the Production Environment	0-3	4-6	7-10
Read access only is permitted on ICS systems, but no modification of operating or production parameters.	0	2	4
Smartphones use a strict basic configuration without jailbreaking or rooting.	0	1	3
Smartphone applications must be obtained from a certified source like an App-Store.	0	1	3
TOTAL SCORE			(0-100 points)

Many risks and threats cannot be minimised by the implementation of technical controls alone, but rather by a combination of organisational 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 defence-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

By means of the BSI publications, the Federal Office for Information Security (BSI) publishes documents about current topics in the field of cyber security. Please notice, that most of the referenced documents are available only in german. Comments and advices from readers are welcome and can be sent to info@cyber-allianz.de .

Literature

1: ICS-CERT, Recommended Practices, https://ics-cert.us-cert.gov/Recommended-Practices, Zugriff im Januar 2019
2: BSI, Industrial Control System Security: Top 10 Threats and Countermeasures, 2014
3: BSI, Industrial Control System Security: Top 10 Threats and Countermeasures, 2016
4: BSI, The State of IT Security in Germany 2018, 2018
5: BSI, Abwehr von DDoS - Angriffen v2.0, https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_002.pdf, 2018
6: BDEW, Requirements for Secure Control and Telecommunication Systems, 2018