SIEMENS
Ingenuity for life

Cybersecurity in the dairy and soft drink industry

Risk minimization according to CRITIS

The increasing digitalization of companies and the associated networking of nearly all sectors are generating tremendous economic potential. Today over 20 billion devices and machines are already connected via the Internet. By 2030 this number will grow to about half a trillion. Digitalization and connectivity can be drivers for growth and prosperity, but increasing connectivity also creates new vulnerabilities that need to be responded to quickly and consistently.

This also applies to companies in the food and beverage industry

In 2017 one of the world's largest food and beverage corporations fell victim to Trojan ransomware. The "Petya" malware attacked computer systems around the world and locking their users out in order to extort ransom money. According to the company's own estimates, the cyberattack resulted in a loss of revenues amounting to roughly $140 million. It was several days before the most important systems were up and running and several weeks before the remaining systems were usable.

This and similar incidents over the past few years have prompted legislators in numerous countries to adopt rules and regulations pertaining to cybersecurity. These standards are intended to protect critical infrastructures so as to guarantee supply reliability for the countries' citizens and stability for the countries themselves.

In Germany, for example, the "Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme" (Act to Enhance the Security of Information Technology Systems = IT Security Act) came into force in July 2015. This act requires that operators of critical infrastructures (CRITIS) implement certain measures. "Operators of critical infrastructures" also include companies in the food and beverage sector, because cyberattacks against this industry don't just disrupt production and cause financial damage, they can also pose health risks.

The main priority is to prevent manufacturing errors and the manipulation of production and avert a loss of reputation. Appropriate security measures aren't a luxury, they're a necessity.

Contents

Legislators regulate IT security worldwide

Since July 2015, Germany's IT Security Act has required the reporting of security incidents that affect certain critical infrastructures. Over time, CRITIS operators will also be required to comply with minimum cybersecurity standards. The implementation of these standards is based in particular on IEC 27001 and IEC 62443. Manufacturers of automation and network components and plant operators must implement state-of-the-art cybersecurity measures. The legal term "state of the art" is used because experience has shown that technological development progresses faster than legislation. The state of the art at any given point in time can be determined on the basis of existing national or international standards like DIN and IEC or based on best practices for the specific industry.

State of the art according to IEC 62443

The IEC 62443 documents are organized as follows:

- IEC 62443-1 includes terminology, concepts, use cases, and models.
- IEC 62443-2 is aimed at plant operators and describes activities like the implementation of a security management system and patch management.
- IEC 62443-3 describes security technologies for controllers and network components.
- IEC 62443-4 is aimed at manufacturers and formulates procedures for protecting the development process and other activities.

This division of information shows that cybersecurity is seen as a comprehensive process and that security standards must be complied with while components are under development.

The FDA Food Safety Modernization Act (FSMA) in the U.S. includes similar standards that comprise a combination of monitoring, intervention options, and verification of cybersecurity measures, among other things. In Great Britain, PAS 96:2017 regulates security and preventive measures against attacks on the food and beverage industry.

Basically, what all the laws and standards have in common is that they're composed of a mixture of technical standards, obligations to report incidents, and monitoring of compliance with standards.

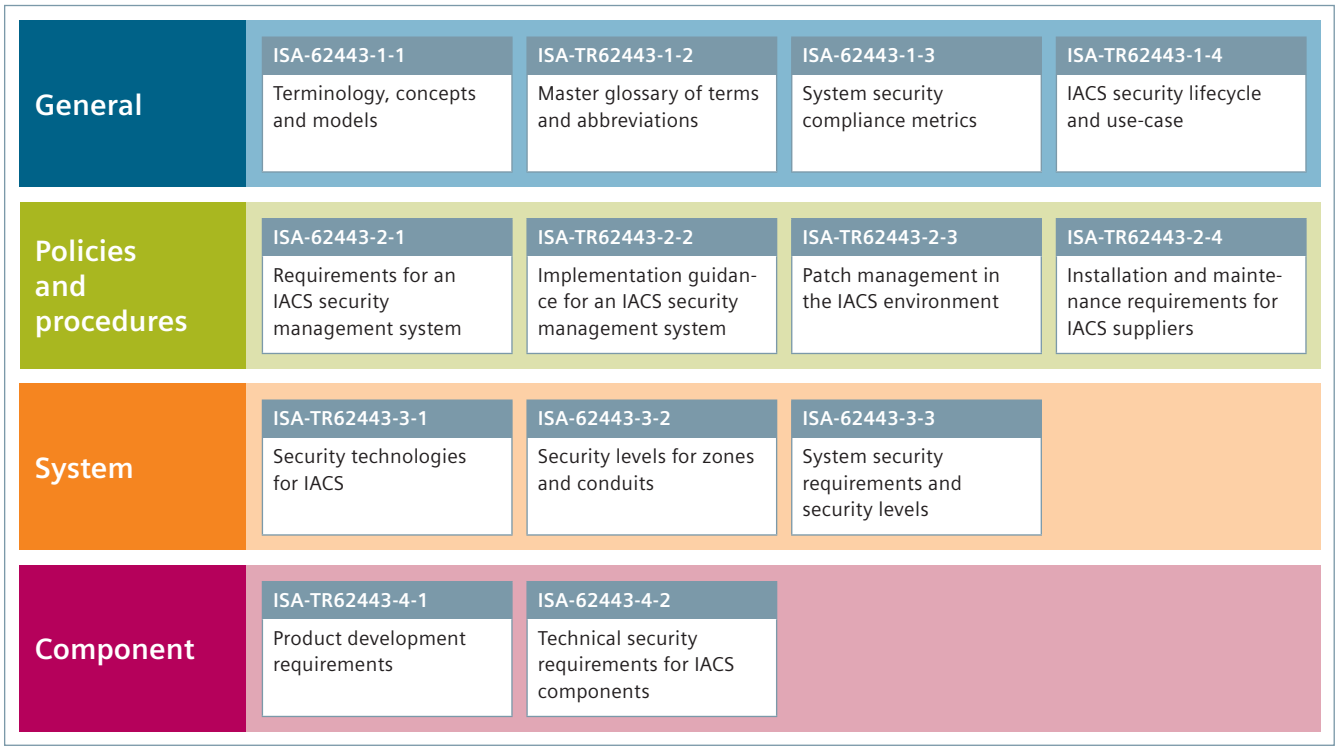

Fig. 1: Documents of the IEC 62443 standard

Cybersecurity: An ongoing process

Effective protection from cyberattacks isn't achieved by a one-time implementation of security measures: It's an ongoing process.

Following a risk analysis (assessment) of an automated process, measures need to be implemented to minimize risks (implementation). These measures must be monitored and there must be continuous verification of whether the measures need to be revised due to a change in the threat scenario (management). The required measures are as varied as the risks assessed. Based on the level of automation, the technology used, and OT (operational technologies) and IT (information technologies) connectivity, security experts develop appropriate security mechanisms that are tailored to each company and its processes.

The plant operator is always responsible for IT security. Even if plant operations are partially or completely unsupported by the company's own personnel due to outsourcing, the plant operator is still responsible. Threats due to outsourcing also need to be assessed. It's generally recommended that personnel undergo trainings that increase their awareness of cyberattacks and that enable them to respond quickly and purposefully in the event of an emergency.

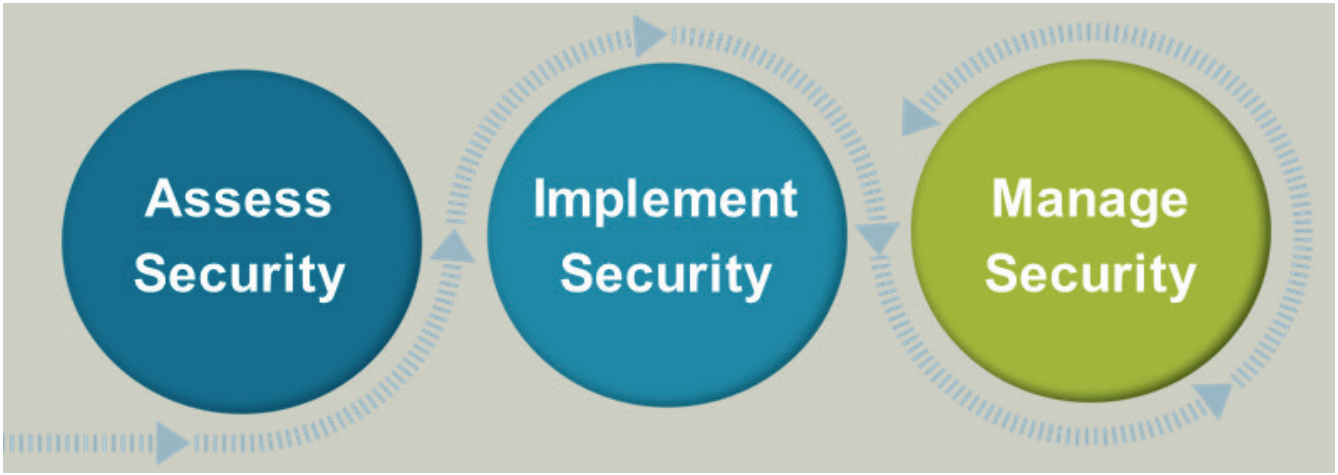

Fig. 2: The three phases of IT/OT security or industrial security

Threats:
Targets of attack and types of attackers

What are the objectives of attackers who try to overcome security measures? Attackers generally fall into four categories.

Untrained attackers ("script kiddies") use finished scripts from the Internet as a simple means to attack known vulnerabilities "just because they can".

Trained attackers ("hackers") launch more complex attacks for the purpose of gain and, for example, to extort ransom money for encrypted data.

Industrial espionage is usually practiced by insiders who use their specialized knowledge to steal data or harm the company. In this case, (former) employees target a specific company.

Technically, **state-driven attacks** are the most dangerous. These attacks generally take advantage of previously unknown vulnerabilities with various goals in mind: access to sensitive data, data manipulation, disruption of manufacturing processes, or even the destruction of entire plant sections. In addition to financial gain, the motivation can also be to destabilize a country – for example, by attacking the food supply.

Threats

The German Federal Office for Information Technology (Bundesamt für Sicherheit in der Informationstechnik = BSI) has identified the following as the ten most frequent attacks on industrial plants (Status: BSI-CS 029 | Version 2.0 dated July 11, 2018):

1. Unauthorized use of remote maintenance access that enables external access to industrial control systems (ICSs) that are often insufficiently protected.
2. Online attacks via office IT, which is generally connected to the Internet and can also establish a connection to the IC network.
3. Attacks on standard components like operating systems, application servers, or databases that typically contain errors and vulnerabilities that attackers can exploit. These components can also be deployed in ICS systems, which increases the risk.
4. (D)DoS attacks on network connections can overload systems and disrupt the functionality of the ICS network or the ICS itself.
5. Human error and sabotage by internal or external perpetrators are a tremendous threat. Negligence and human error also threaten confidentiality and availability.
6. Malware is often introduced via removable storage devices or the mobile IT components of external employees (example: Stuxnet).
7. Control commands can be easily read and imported because most control components communicate via plain-text protocols, which means that their communication is unprotected.
8. Unauthorized access to network components is possible if insiders – or outsiders who've penetrated the security measures – access components using unsecure authentication and authorization methods.
9. Attackers can manipulate network components in order to conduct man-in-the-middle attacks or facilitate sniffing.
10. The potential of failures resulting from extreme environmental influences or technical defects can never be completely eliminated, but the risk and consequential damage can be minimized using appropriate components and security measures.

Cybersecurity: Step-by-step procedure

The list of threats shows that very different methods can be used to launch attacks, and the process needs to be protected from this wide range of threats. The German industry standard and IEC 62443 define a multistep process for implementing cybersecurity.

1. Object selection serves to record and document all the systems in the plant, including subsystems and a network plan.
2. The threats are derived from a selection of use cases: for example, the fact that a system can be attacked via a remote maintenance access.
3. The threat assessment identifies the threats for each use case: for example, remote maintenance access can be used by an unauthorized person.
4. The risk analysis involves identifying potential threats based on a risk matrix.

   A threat with a high probability of occurrence and high potential damage appears in the red area in the upper right-hand corner of the matrix (high risk). A low extent of damage and probability of occurrence means a low risk and appears in the green area in the lower left-hand corner. BSI Standard 200-3 provides an exact breakdown of the extent of damage (degree to which plant operation is limited), probability of occurrence, and risk.
5. A process to determine necessary measures defines concrete options that are described in detail in the next section.
6. Measure implementation includes the scheduling and organizational planning of implementation. It also includes defining responsibility and clearly allocating the budget for measure implementation.
7. For the audit, the measures must be verified, plant documentation must be complete, and checklists must be filled out. The effectiveness of the measures needs to be verified at regular intervals. If faults are detected – for example, from changed risks or new types of malware – the entire process must be restarted, beginning with the threat assessment.

Security concept

Because threats differ in terms of their nature, they can originate internally or externally, and different attackers have different levels of expertise, it's important to create a multilayer security concept in order to provide a process delivering the best possible protection. For example, even if the firewall has been breached because the attacker has physically entered the plant, additional security mechanisms need to protect the terminal devices.

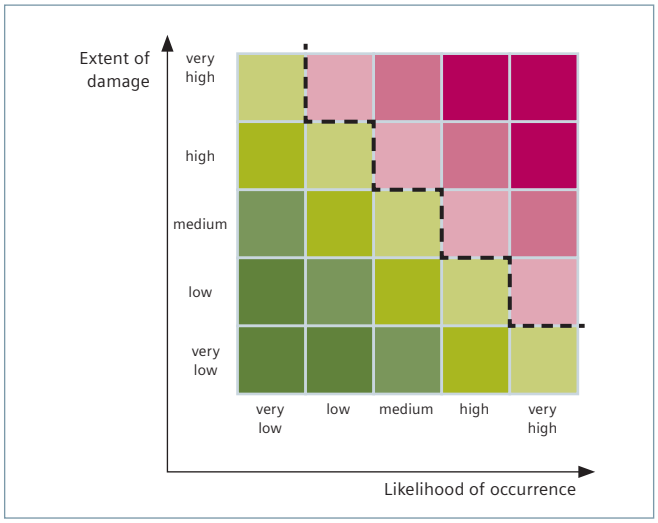

Fig. 3: Risk matrix based on BSI Standard 200-3

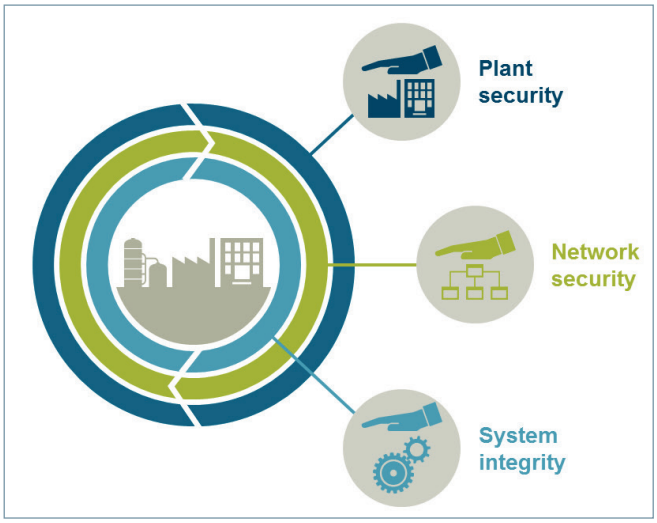

Fig. 4: "Defense in Depth" security concept

The figure shows a multilayer security concept that defines plant security, network security, and system integrity as the three essential layers of effective security.

Plant security measures

Organizational measures include all the measures for physically protecting the plant. In addition to protection from break-ins, this must also include procedures to protect the plant from environmental influences.

Threats

- Break-in/vandalism
- Unauthorized access
- Flooding
- Fire
- Smoke/dust/corrosive gases
- Lightning/overvoltage/EMC

Organizational measures

Depending on the specific threats, appropriate measures have to be taken to protect the plant. Particular attention is required for outstations (for example, warehouses) that are usually unoccupied and monitored remotely from the control center. Outstations must be secured against break-ins and doors and windows must be suitably protected.

Door/window contacts can notify the controller if doors or windows are opened, and the controller can notify the control center. An IP camera can help detect attackers and monitor the building from the control center.

Different production areas must also be physically separated by means of differentiated access control. For example, critical components need to be secured in a locked control cabinet (also see page 13).

The guidelines for physical access protection measures also determine the cybersecurity measures that are required and the strength of these measures. For example, in areas that are only accessed by select authorized persons, the network access interfaces and automation systems don't have to be as securely protected as they would in publicly accessible areas.

With certification according to IEC 27001, companies can reduce information security risks, comply more fully with relevant security regulations and requirements, and foster an internal security culture.

Network security measures

The network must be structured to withstand potential attacks to the greatest possible degree while also taking into account access options, availability, and protection.

Access options

As a rule, networks are open systems with a connection to the Internet. For most plant operators, outside access for the purpose of maintenance, diagnostics, optimization, patches, updates, and other activities has become essential.

Availability

The automated process – which is controlled, for example, via the network using PROFINET communication – must be executed independent of individual line interruptions. The monitoring systems in the control center need to be able to continue monitoring the process even when individual routers fail.

Protection

The process has to be protected from all potential risks that might threaten the network, including unauthorized access, malware, and (D)DoS attacks. All types of communication other than authorized and permitted access must be blocked using appropriate measures.

IEC 62443 requires the following elements for network protection:

- Segmentation of the network architecture
- Isolation or segmentation of high-risk components
- Blocking of unnecessary communication
- Access via firewalls

Network segmentation

Network segmentation using firewalls provides protection from attacks from the network. The network is divided into functional groups – for example, production networks, plant network, and office network – and access is precisely controlled by firewalls.

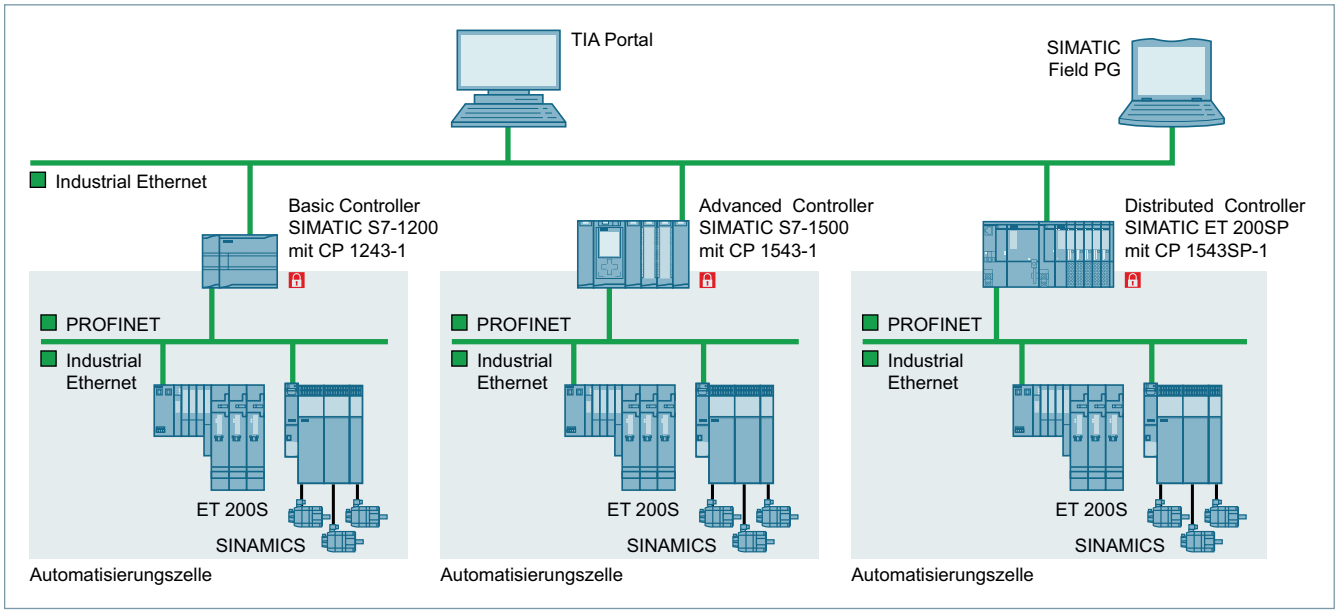

Fig. 5: Network segmentation according to IEC 62443-2-1

Demilitarized Zone (DMZ)

Figure 5 shows a network configuration recommended in IEC 62443-2. The automation cells at the bottom are combined as functional units and are each separated from the plant-wide network by a firewall. The plant network at the top contains all the higher-level devices that are important for operating the plant, like the control center and servers. The interface between the plant network and the office network is again separated by a firewall. One or more demilitarized zones (DMZs) can be set up here. In a DMZ, the devices from the higher- and lower-level networks don't communicate with one another directly. Instead, they communicate via a server that, for example, retrieves the plant's status from the automation cells and makes this information available to the higher-level network. The office network is also protected from the Internet by one or more firewalls.

In this example, the configuration creates three defensive walls for the automation cells that control the process. The office network, which is potentially affected by the more frequent introduction of malware (for example, USB sticks), is separated from the automation cell by two firewalls. The closer an employee works to the automation cell, the more important it is that they constantly be made aware of cybersecurity issues.

Remote access and distributed outstations

The connection of external distributed stations poses a special challenge. While these stations must be able to function autonomously, it must also be possible to monitor them from the control center. An outstation's network must be protected and access to the outstation has to be secure, even if it's connected via a separate network or the company's own connection. The outstation can be connected via cable (like ADSL or SHDSL) or radio link (for example, LTE, UMTS). The modem must contain a firewall and be VPN-compatible.

To increase security, the VPN connection can be configured for remote access according to IEC 62443 so that the tunnel is established only when an on-site technician activates the VPN at the module.

Wireless connections via WLAN

Special attention must be paid to wireless transmission via WLAN or other technologies. In the case of wired communication, an attacker must have physical access to the cables or network components in order to read data or tamper with data traffic. With wireless communication, the radio waves are spread over a larger area, making an attack easier.

If a WLAN is required in the automation cell, a separate WLAN must be set up for automation. The office WLAN must be operated through different WLAN access points in order to maintain network segmentation.

Organizational measures for a WLAN

The access point must be installed so that it's inaccessible or secured in a closed control cabinet, and the WLAN antennas have to be installed remotely. This will prevent attackers from physically accessing the access point. The WLAN frequency also needs to be carefully selected, because other applications that use the same frequency can interfere with transmission in a way similar to jammers, or can even disrupt it completely.

Technical security mechanisms for a WLAN

WPA2 encryption is the current state of the art.
Older encryption methods (WEP and WPA) must no longer be used because they're not secure and are easy to decrypt.
The default password and SSID need to be changed,
and the SSID must be hidden.

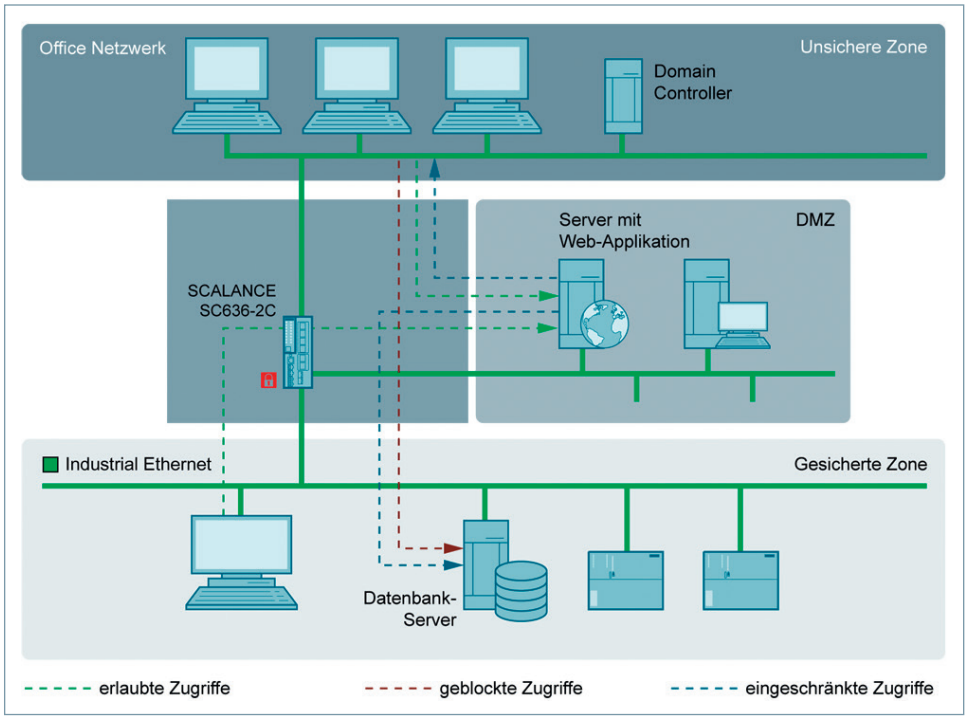

Fig. 6: Connection of a local service PC via a DMZ port on the SCALANCE S615

General requirements for network elements

The international standard for the secure configuration and management of network components according to the IEC 62443 standard recommends the following features and security mechanisms for configuring and protecting devices.

Access protection and account management

To protect network components from unauthorized access, it must be possible to manage and, if necessary, block accounts for which access has been enabled. The following features need to be supported:

- Configure access options
- Identify users/make users identifiable via accounts
- Set up/change/terminate accounts via a central manager
- Document accounts and account users
- Delete or lock unused accounts
- Verify access rights on a regular basis
- Change default passwords

Access protection requirements can be implemented by means of user management components (UMCs). With UMCs, different user accounts are created on a central server known as the UMC ring server. TIA Portal projects can use these users and these users can be granted access rights to network components and participants.

Access control: authentication

When a component is accessed, it must be possible to identify the user who's accessing it. Authentication needs to provide the following mechanisms:

- Access possible only if the user has been authenticated (or there is sufficient access control)
- Strong security mechanisms for administrative access
- Recording of all accesses to critical systems
- Identification of all remote access users
- Guidelines for remote access, automatic logout after a period of inactivity
- Remote access locked after repeated failed logins
- Reauthentication during remote access after a period of inactivity
- An authentication mechanism must also be set up for task-to-task communication

These requirements relate to different systems and must therefore be taken into account for the entire plant. For remote access, for example, the requirements can be met by SINEMA Remote Connect because, among other things, automatic logout after inactivity and the locking of an IP after several failed login attempts are already implemented and remote accesses are always logged. In the TIA Portal, users can be granted access to the project and separate access to the security configuration. Because the security configuration requires its own access rights, the requirement for additional security for administrative access is also met.

Access control: Authorization

Authorization means granting specific rights to previously authenticated users: for example, access to a component. IEC 62443 mentions the following points with regard to authorization:

- Logical or physical method for access permission
- Role-based access to system or information
- Right to access safety features must be a separate right
- Multiple access levels must be configured for critical systems

Network management

SNMP, which is now supported by all network interfaces, can be used for network management. In conjunction with the SINEMA server, SNMP can be used to monitor the network and plant sections connected via a VPN. This enables all network sections to be managed and failures to be detected more quickly.

Network plan

A physical network plan – a topological view – is required for documenting the plant and showing how the participants are interconnected. This network plan had to indicate addresses (IP and MAC), port connections, and installation locations. It could be printed out from the TIA Portal, or the SINETPLAN network planning tool could be used.

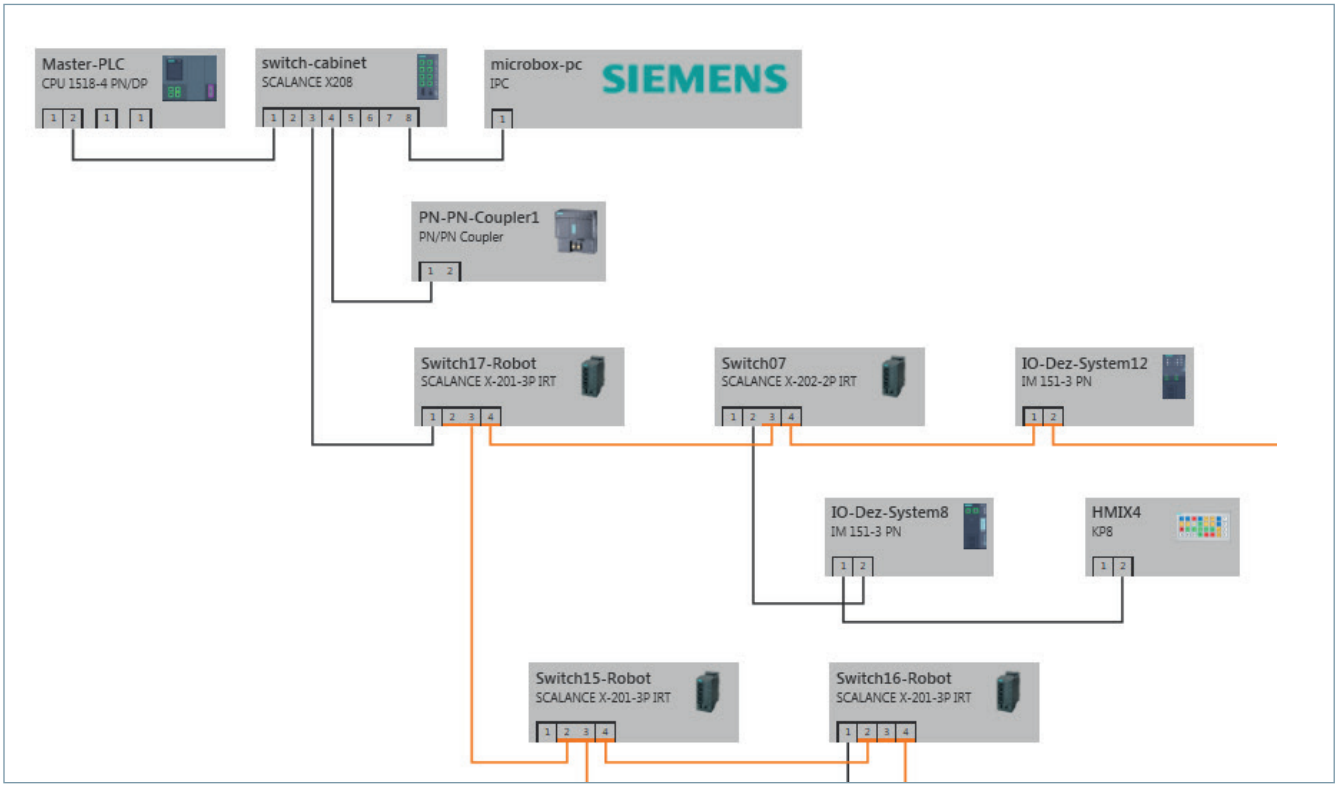

Fig. 7: Topological network in SINETPLAN

System integrity measures

System integrity means that the authenticity and genuineness of data and programs within a system are guaranteed. No one is allowed to change the program or tamper with data (either in the communication channel or in the system) or copy the program or data without authorization. Process control expertise must also be protected.

Program access

The programming of controllers (PLCs) is also part of cybersecurity, which is why access to the project and to offices must be protected. The project can generally be protected using the Windows log. Beginning with TIA Portal V15, the entire project can be encrypted. This means that the project can only be opened using an additional user name and an additional password, which guarantees security when several people work on the same project simultaneously.

CPU access protection

Different passwords can be set up based on the different CPU access levels so that only qualified personnel have full access.

Web servers

More and more control solutions are using access via Web servers, which are often used for remote access as well. In this case, the Web servers must also be fully protected. HTTPS is the secure version of HTTP and is the preferred choice. Authentication and authorization as required by the industry standard can be achieved by configuring different users and access levels.

Secure communication

If the controller communicates outside its secure cell, this communication must be encrypted. The current state of the art is TLS encryption, which can be used in the S7-1500 via OPC UA or a TCP connection.

Another option for encryption is to use built-in firewalls to set up a VPN connection. The VPN tunnel is established between the firewalls, and communication between the automation cells is transmitted via the higher-level network in an encrypted form and decrypted by the target network.

Security measures on industrial PCs

PCs used in the industrial environment (IPCs) require special measures because they're directly exposed to several threats – including infected storage devices – whereas USB sticks can't be directly connected to a controller. The following measures serve to harden an IPC against cybersecurity attacks.

User accounts

It's advisable to set up administrator and user accounts. Only the administrator is authorized to make changes to security settings or to (un)install software.

The standard user is unable to perform these functions, which prevents the installation of malware during normal operations.

Configuration of guidelines

With the aid of the Microsoft Management Console, guidelines can be established for the use of storage devices, system control, among others. A document describing these guidelines and how they can be established is available online at:
https://support.industry.siemens.com/cs/ww/en/view/109475014

Enhanced Write Filter (EWF)

This feature is available on SIMATIC IPCs: It protects a portion of the file system from data modification by redirecting write access to the RAM. When the IPC is restarted, the file system is returned to its original state. Malware that was introduced is no longer present after a restart.

Firewall

Standard firewalls (Windows firewalls) already provide important basic protection. They absolutely must remain activated. Using appropriate rules, firewalls need to be configured in such a way that only user data can be communicated and all other communication is blocked.

Virus protection

Antivirus software can detect viruses and malware. At Siemens, we use a McAfee installation for our automation. A management server handles the antivirus clients on the PC systems and supplies the latest virus signatures. The management server can also notify service personnel via e-mail alarms.

IEC 62443-certified products

The controllers, PCs, and other systems selected for use have to contain security mechanisms, and they must have been tested for vulnerabilities. These tests are standardized: for example, an Achilles Certificate indicates that the system has undergone load and vulnerability tests. Manufacturers can also perform secure product development to ensure a high level of quality for their products. Siemens' development process has been tested and passed the IEC 62443-4 test:
https://www.siemens.com/press/PR2016080373DFEN

Personnel measures

The best technical and organizational security measures are useless if a company's employees are negligent. That's why training courses and clear definitions of areas of responsibility are an integral part of cybersecurity. IEC 62443 recommends that new personnel be screened to determine their reliability and to evaluate whether they can meet their responsibilities. The reliability of existing personnel must also be determined. Outside personnel can also attend trainings, but they should always be accompanied and supervised by the company's own trained personnel.

Responsibility

The industry standard requires that operators of critical infrastructures (CRITIS) designate the UP KRITIS organization as their cybersecurity contact. It's generally recommended that an individual or group be placed in charge of cybersecurity within the company.

Training

Regular training courses must be offered that cover the correct handling of installed systems, removable storage devices, and software; there should also be a training course on responding to incidents and all other potential threats. The industry standard explicitly requires that administrators be trained in the correct handling of network components to ensure that configurations are correctly performed.

Emergency plan and recovery

The industry standard requires a concept for handling an emergency when a threat has emerged and the process has been interrupted. This concept is also known as business continuity management. The following questions need to be answered:

- What's the maximum acceptable downtime?
- How can the process continue to function independent of the control system/office?
- How well can other plant sections compensate for the supply?
- How will the affected system be revised?
  - Through redundancies
  - Through a backup
- How will a recurrence of this failure be prevented?
  - Reporting
  - Optimization

Siemens ProductCERT

Siemens has a team of security experts that serves as a contact point for customers and their security experts when they detect a security vulnerability. This team – known as the Product Computer Emergency Response Team (ProductCERT) – immediately assesses and analyzes reported security vulnerabilities.

Siemens Security Advisories

Siemens ProductCERT investigates all reported security issues and publishes Security Advisories on validated security vulnerabilities that directly involve Siemens products and require a software update, software upgrade, or another action on the part of the plant operator. Take advantage of this source of information for assessing the effects of a security vulnerability. Siemens deals openly with its own vulnerabilities so that you can respond before these vulnerabilities affect you. Stay up to date by subscribing to our RSS feeds:
https://new.siemens.com/global/en/products/services/cert.html

Overall picture

Comprehensive industrial security requires that all protection levels be taken into account. Security measures must be as varied as the potential risks. An end-to-end approach and multiple lines of defense can reliably protect industrial plants. To simplify this complicated issue for industry, Siemens offers a customized solution portfolio specifically aimed at the security of industrial plants and operational technologies.

The figure below represents a typical network architecture for a soft-drink plant. It shows the levels on which the security measures described in this document have been implemented according to the recommendations of the IEC-62443 standard.

Why Siemens?

Siemens offers a reliable foundation for secure and innovative automation solutions.

At Siemens we:

- Understand digitalization,
- Understand the food and beverage industry,
- Understand industrial communication,
- Understand industrial security, and
- Offer proven and certified security processes and products

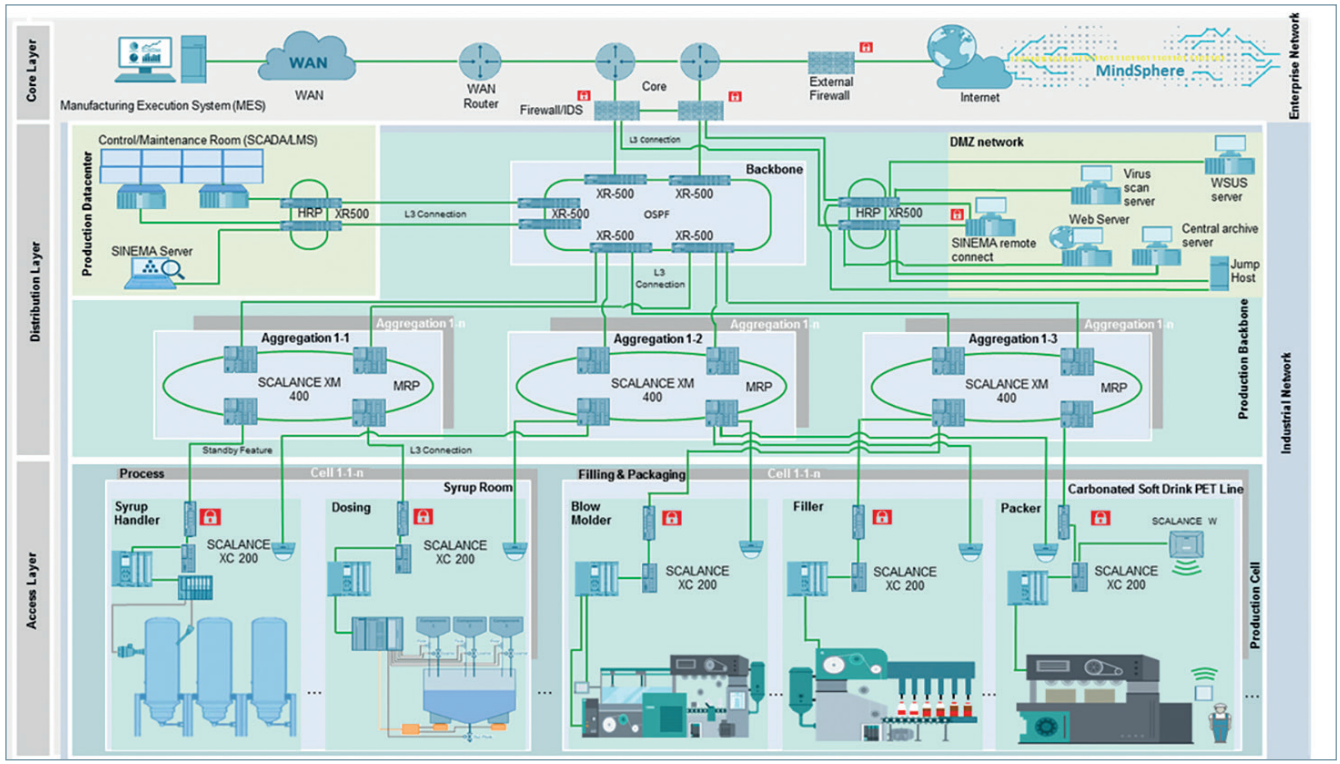

Fig. 8: Network architecture of a soft-drink plant

Terms and abbreviations

Authentication
The detection and identification of a user or (in the case of networked plants) another system.

Authorization
The right to access a system or a (software) section of a system or program.

Cybersecurity
All the technical measures for protecting a plant, including network protection, system hardening, and incident monitoring.

Process
The actual production process – for example, cheese production or bottling – regardless of whether it's a discrete or continuous process.

Virtual private network (VPN)
A VPN provides an encrypted connection between VPN subscribers. It's also referred to as a VPN group. A VPN resembles a tunnel where data traffic can be sent from either direction. In the tunnel, data traffic is transmitted in an encrypted form and at the end of the tunnel – meaning at the other VPN device – is delivered in a decrypted form. The terminal devices don't have to support encryption because encryption is performed by the VPN devices.

Siemens AG
Siemens Deutschland
Vertical Sales Food & Beverage
Lindenplatz 2
20099 Hamburg