SIEMENS

Ingenuity for life

Industrial Security

Cybersecurity for Telecontrol

Cybersecurity for Water and Wastewater Industry

White Paper

Version 06/2020

siemens.com/telecontrol

Contents

Introduction

The backbone of a reliable water supply are facilities and systems that, in addition to their actual functionality, are also protected from the inside and the outside with regard to cybersecurity. There are now legal requirements and guidelines in many countries that oblige operators of so-called critical infrastructures to protect and harden their systems accordingly, and to provide appropriate proof about that. The basis for a holistic view of cybersecurity is provided by the international standard IEC 62443.

Cybersecurity for Telecontrol

1. Water/Wastewater Requirements

The prerequisite for a functioning society is a reliable and secure public infrastructure, e.g., for water and energy supply. Due to the advancing digitalization and the associated trends in the use of standard IT services, the widespread availability of mobile communications and the Internet, the increasing convergence of networks, or the utilization of cloud services, the danger that the public infrastructures become a target of cyberattacks continues to increase. Threats range from pure espionage and manipulation of confidential data to sabotage of the entire production or process sequence.

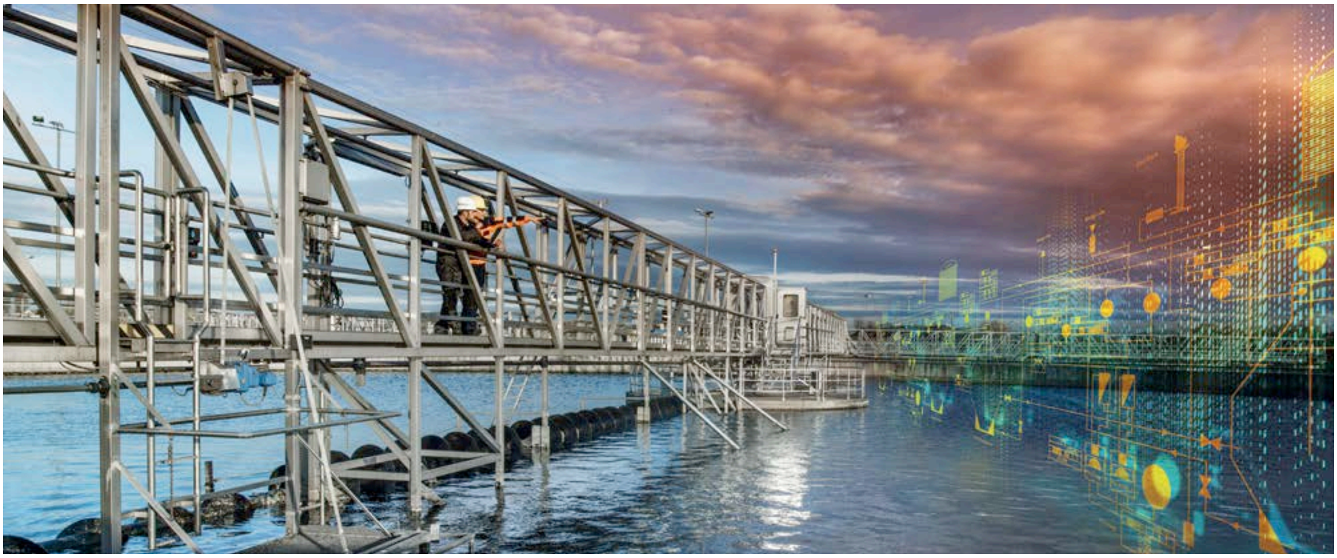
Activities in Germany

Against this background, the IT Security Act was enacted in Germany with the German Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik – BSI) being the central point of contact. The IT Security Act obliges operators of so-called critical infrastructures to adequately protect IT systems, components, and processes, and to provide proof of compliance with the requirements to the BSI at least every 2 years.

https://www.bsi.bund.de

According to the current regulations, those sectors and industries are considered critical infrastructures that are essential for the maintenance of important social functions, health, security, and economic or social well-being of the society. These include the areas of water, energy, nutrition, transport and traffic, health, IT and telecommunications, finance and insurance, government and administration, as well as media and culture. In turn, this applies to facilities that supply 500,000 people or more. For the water sector, this also gives rise to the parameter of 22 million m³ of water (pumped, distributed, discharged, or treated), starting which a facility falls within the critical infrastructure range.

https://www.kritis.bund.de



Protection of critical water/wastewater infrastructures

Cybersecurity for Telecontrol

In order to support the operators of critical infrastructures in complying with the legal requirements, industry associations in Germany have defined corresponding guidelines and instructions in industry-specific security standards. For the water sector (drinking water supply and wastewater disposal), operators are supported with specific stipulations for setting up measures to protect the plant operation [1, 2]. Among other things, this also includes the setup and operation of a so-called "Information Security Management System" (ISMS), which is intended to enable compliance with the current state of the art in information security, which in turn is required by corresponding obligations to provide proof.

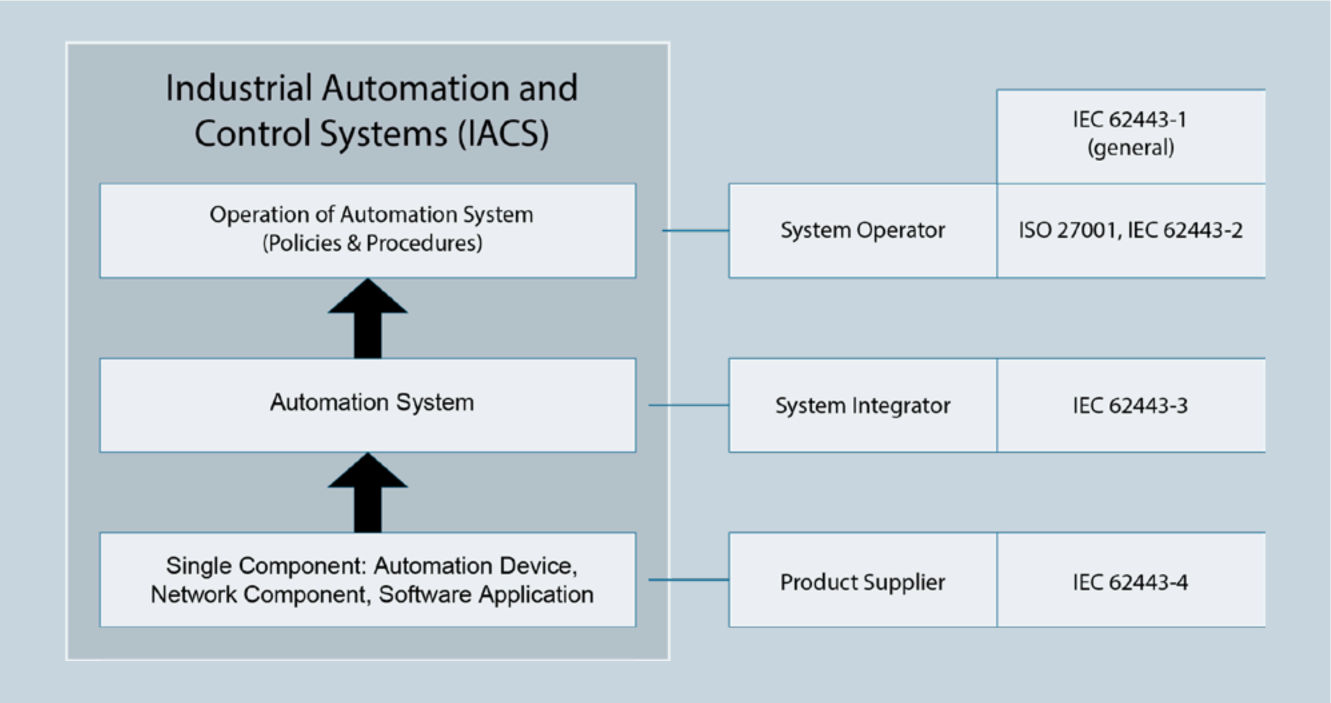
In orientation guides for the industry standards, the recommendation was made to introduce an ISMS based on ISO 27001. Furthermore, operators of critical infrastructures must set up a 24/7 contact point, which can be used to communicate with the authorities at any time and via which all IT incidents that have occurred must be reported to the authorities. In general, appropriate IT security measures must be taken to ensure "the availability of the systems and data, integrity of the processed information and systems, authenticity of the origin of the data and information, as well as confidentiality of the data and information."

Whereas the above-mentioned series of ISO standards is generally aimed at operators of IT systems, the IEC 62443 standard is consulted in addition when considering industrial systems. It has become a trendsetting series of standards for industrial cybersecurity in recent years, and is compatible with ISO 27001.

In other countries of the European Union as well as globally, activities by governments and authorities are underway to define the framework for appropriate protective measures in important areas. Laws are passed and guidelines are created to protect critical infrastructures and thus the population – ensuring the social functioning. Beside physical protection, the primary concern is again the protection against cyberattacks. The basis for a holistic view of cybersecurity for systems and facilities is therefore provided by the international standard IEC 62443 as well.

2. IEC 62443: Targeted Cybersecurity Measures

The IEC 62443 standard, which consists of several parts, deals with the cybersecurity of "Industrial Automation and Control Systems" (IACS). It was developed explicitly for industrial environments and their specific requirements and covers all areas of industry from discrete manufacturing to process industries to distributed supply systems. In its various parts, the series of standards addresses not only the system operators, but also the system integrators / system builders as well as the product suppliers / component manufacturers and service providers. On this broad foundation, Siemens has established a comprehensive cybersecurity strategy that helps to meet the requirements of the BSI and the water/wastewater industry standard – effectively protecting the entire facility or system against attacks.

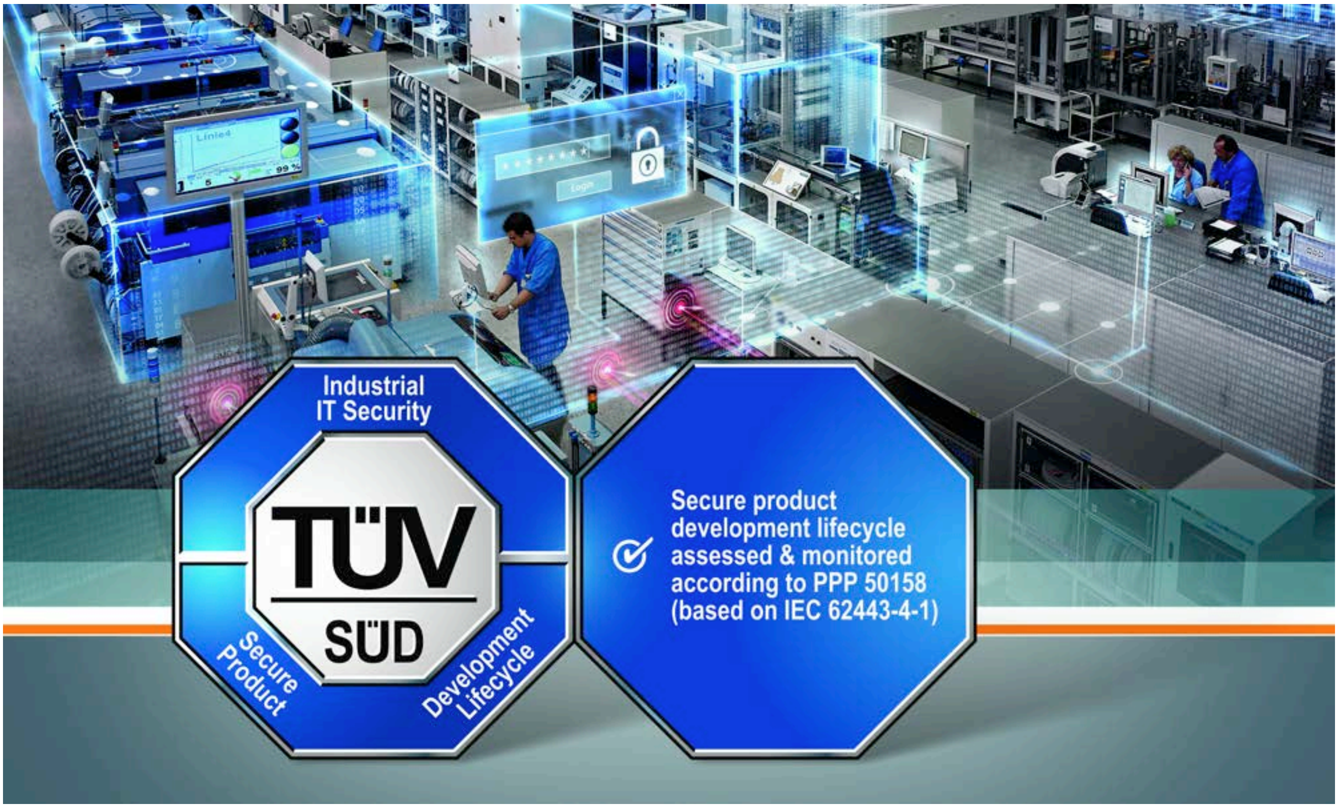

Industrial Automation and Control Systems (IACS)
Operation of Automation System (Policies & Procedures)
Automation System
Single Component: Automation Device, Network Component, Software Application
IEC 62443-1 (general)
System Operator
ISO 27001, IEC 62443-2
System Integrator
IEC 62443-3
Product Supplier
IEC 62443-4

Overview of IEC 62443

2.1 Certified Product Life Cycle according to IEC 62443-4-1

Part 4-1 of IEC 62443 defines the way in which the used components are manufactured by the product supplier. It does not matter whether it is a component with dedicated security functions like a firewall, a switch, or a complex automation component. Only if the combination of all components, i.e., the entire system, stands on a reliable and secure foundation, an effective protection concept can be built upon it. Thus, in August 2016, Siemens was the first company to receive certification based on IEC 62443-4-1 from TÜV SÜD (Germany) for the overarching development process for products in automation and drive technology, including industrial software.

The standard takes into account the following security-relevant aspects of the product life cycle, among other things: skills and expertise, process and quality assurance, security aspects of third-party components, secure architecture and secure design, handling of security vulnerabilities, provision of security updates, as well as patch and change management. By taking these aspects into account, specific attention is already paid during the development phase of a product to avoid vulnerabilities and to rule out or minimize security risks by choosing an appropriate system architecture. Should vulnerabilities nevertheless arise in firmware or software, users will be proactively informed and appropriate countermeasures or security updates be provided.


Industrial IT Security
TÜV SÜD
Secure Product
Development Lifecycle
Secure product development lifecycle assessed & monitored according to PPP 50158 (based on IEC 62443-4-1)
Linie4
Login

TÜV SÜD IEC 62443-4-1 for Siemens

2.2 Product Requirements according to IEC 62443-4-2

Although the water/wastewater industry standard primarily relates to the operation of an ISMS and thus mandates compliance with the processes and work instructions, the components used must support fundamental technical functions to give operators of critical infrastructures the ability to meet the requirements of the industry standards.

The IRC portfolio (IRC: Industrial Remote Communication) in the field of telecontrol from Siemens supports the necessary security functions either directly with the respective automation component or in combination with additional security components from Siemens (in accordance with part 3 of IEC 62443). The following are examples of important functions that support the secure operation of the facility or system to meet the necessary security requirements. A complete analysis and design of the facility or system should be determined as part of a security assessment, see Chapter 4 "Security Assessment according to IEC 62443 / ISO 27001 from Siemens" in this document.

1. **Signed firmware to protect against manipulated firmware updates**
2. **Secure email transmission via secure connections**
3. **Secure end-to-end encryption with OpenVPN/IPsec**
4. **Security events for the traceability of security-relevant system events**
5. **Reduced attack surface by deactivating unused services**
6. **Protection of components as part of a defense in depth concept**

Cybersecurity for Telecontrol

1. **Signed firmware to protect against manipulated firmware updates**
   To protect automation components from both dangerous malware and from fake or manipulated firmware updates, updates are digitally signed. Thanks to the automatically initiated verification of this signature during an update process, both the authenticity and the integrity of the corresponding files are ensured. If an irregularity is found during this process, the update process is automatically terminated, whereby the integrity of the component itself is ensured. Manipulated firmware versions, malware, or other data packets not signed by Siemens can thus not be executed on the component.
   Siemens also supports this functionality with the following telecontrol modules:
   SIMATIC CP 1243-1, CP 1243-8 IRC, CP 1243-7 LTE, CP 1542SP-1 IRC, TIM 1531 IRC and RTU3000C.

2. **Secure email transmission via secure connections**
   To transmit information from an automation component, e.g., a SIMATIC RTU3000C telecontrol module, to a defined recipient while maintaining confidentiality, email sending via an encrypted connection is advisable. With a previously imported digital certificate, it is possible to encrypt emails to be sent via STARTTLS. In this way, critical system events and diagnostic messages as well as process data can be securely transmitted to the desired recipient. In addition to the encrypted transmission, zipped attachments can be protected with a predefined password. The access to the transmitted data can thus be purposefully limited depending on the application and area of responsibility.
   Siemens also supports this functionality with the following telecontrol modules:
   SIMATIC CP 1243-1, CP 1243-8 IRC, CP 1243-7 LTE, CP 1542SP-1 IRC, TIM 1531 IRC, and RTU3000C.

3. **Secure end-to-end encryption with OpenVPN/IPsec**
   To be able to communicate securely with a remote component, the transmission via virtual private networks (VPNs) lends itself. Thanks to the certificate-based authentication of the participants and an end-to-end encryption, information and configurations can also be securely transmitted across public networks. Through the OpenVPN implementation, secure tunnel connections can be set up between a SIMATIC RTU3000C and any OpenVPN server. With these tunnels not only telecontrol protocols but also any configuration, firmware update, time synchronization, or log information can be transmitted. In combination with the SINEMA Remote Connect solution from Siemens, OpenVPN can be used to set up a comprehensive remote access solution with granular access rights.
   Siemens also supports this functionality with the following telecontrol modules:
   SIMATIC CP 1243-1, CP 1243-8 IRC, CP 1243-7 LTE, CP 1542SP-1 IRC, TIM 1531 IRC in combination with Siemens security components, and RTU3000C

4. **Security events for the traceability of security-relevant system events**
   To maintain transparency about security-relevant activities throughout the entire network and on individual end devices, the system components, such as the CP 1243-8 IRC, support the recording of so-called security events. Thanks to these logged system events, unauthorized configuration changes, system accesses, or integrity violations can be tracked. Taking current data protection regulations into account, the recorded events can be sent to higher-level security applications and analysis/archiving systems using Syslog. In connection with a secure end-to-end encryption, the events can be transmitted encrypted to the desired recipients.
   Siemens also supports this functionality with the following telecontrol modules:
   SIMATIC CP 1243-1, CP 1243-8 IRC, CP 1243-7 LTE, CP 1542SP-1 IRC, TIM 1531 IRC in combination with Siemens security components for network cells and RTU3000C.

5. **Reduced attack surface by deactivating unused services**
   To keep the attack surface of the automation environment as small as possible, unused and unnecessary network services can be permanently deactivated via appropriate configuration interfaces. For instance, access to the web-based management of a component can be restricted to the secure HTTPS protocol. Requests over the insecure HTTP variant are forwarded to HTTPS or rejected.
   Siemens generally follows this approach for all SIMATIC products for telecontrol.

6. **Protection of components as part of a "Defense in Depth" concept**
   To protect an automation system comprehensively and holistically against cyberattacks, it should be set up according to the recommendations of IEC 62443 and as part of a defense in depth concept. For the essential network security required, Siemens offers an extensive portfolio with which the systems can be protected in a modular and needs-based manner. With SCALANCE S, for example, Industrial Security Appliances are available with which the data traffic to and from the protected network cell can be controlled and monitored. With this concept, different security measures are combined and protection is possible not only in width, but also in depth.

   Further information on the "Defense in Depth" protection concept from Siemens can be found at: www.siemens.com/industrialsecurity

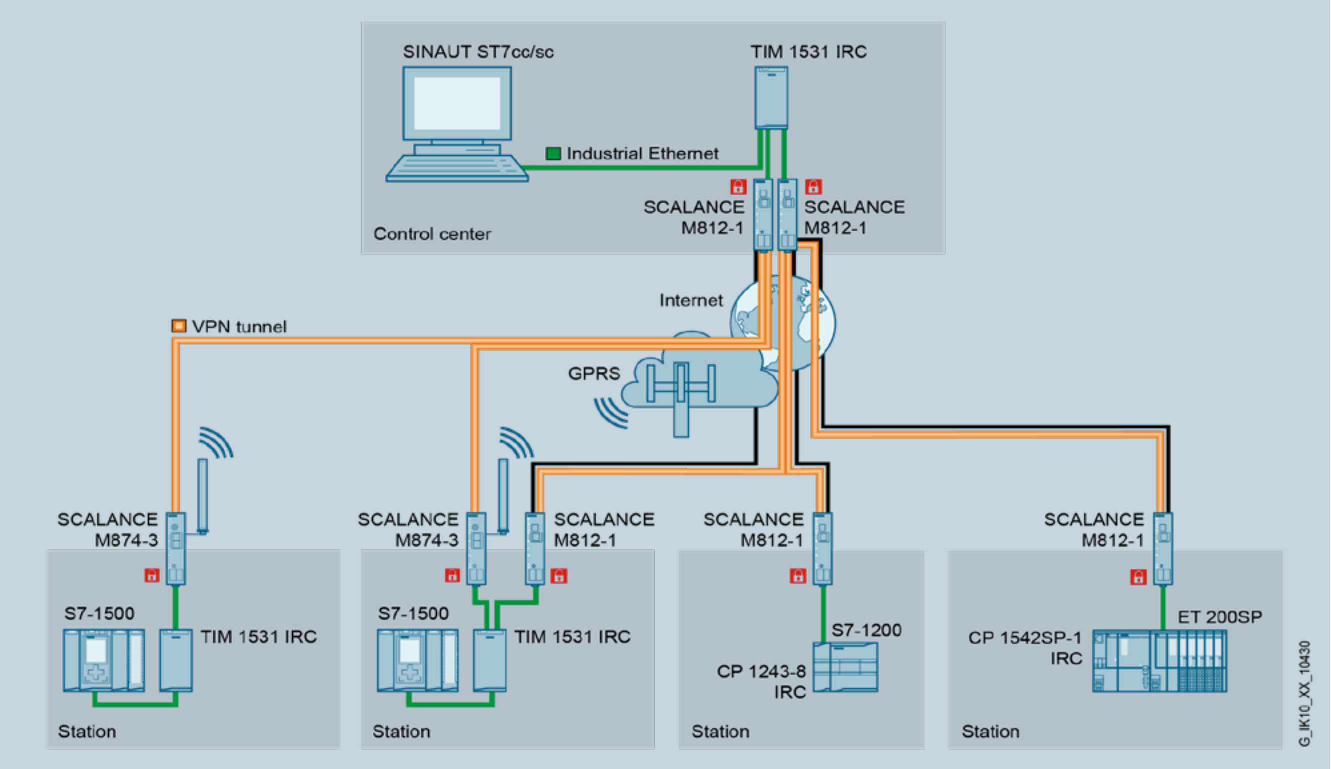
2.3 System Analysis according to IEC 62443-3

Based on the concept of modular and needs-based cyber protection, the overall system or facility solution can compensate for certain missing technical properties of the individual components. If, for example, an automation component has no integrated firewall functionality, this can be accomplished using upstream Industrial Security Appliances, such as a SCALANCE S upstream of a SIMATIC TIM 1531 IRC, so that the combination of these components meets the stipulated Industrial Security requirements. Within a network of an automation system, there is a great variety of device combinations and networking options.

To support the conception and creation of secure automation solutions, Siemens provides documented sample configurations (Blueprints) that are designed in accordance with IEC 62443 and thus represent a secure solution from an IT/OT perspective. Documentation based on the Siemens SCADA systems SIMATIC WinCC PROFESSIONAL/TIA, WinCC V7, and WinCC Open Architecture as well as based on the Siemens control system SIMATIC PCS 7 will be available.

As part of such a sample configuration, the illustration below shows an example of a secure telecontrol configuration based on the SIMATIC portfolio from Siemens. The remote terminal units (RTUs) as well as the master station in the control center consist of controllers from the SIMATIC family S7-1200 (Basic Controller), ET 200SP (Distributed Controller), and S7-1500 (Advanced Controller). The connection to the control center is made via public network with SIMATIC Telecontrol modules and SCALANCE Industrial Routers (DSL and mobile communications). The secure connections from the stations to the control center are implemented via VPN tunnels (OpenVPN). The security functions are performed either directly by the telecontrol module or in combination with the SCALANCE devices.

https://www.siemens.de/telecontro
l



Secure telecontrol solution with SIMATIC controllers from Siemens

Cybersecurity for Telecontrol

3. Always active: Industrial Security Alerts and Updates

The topic of Industrial Security moves in a very dynamic and complex environment. Products, systems, and also technologies that are considered secure today can already be outdated and insecure tomorrow. It is therefore necessary to continuously monitor and adapt the security measures so that the products used are always up to date when it comes to security updates. For this to succeed, “Siemens ProductCERT” analyzes all discovered and reported security problems related to Siemens products, solutions, and services – and pub-lishes security advisories on validated security vulnerabilities. The security advisories contain information on how to deal with the vulnerability and provide the necessary steps for the protected operation of Siemens products and solutions. A software or firmware update is commonly offered or certain actions are recommended. Security advisories can be sub-scribed to and displayed via an RSS feed so that the Siemens products used can always be kept up to date.

Further information:
https://new.siemens.com/global/de/produkte/services/cert.html#Benachrichtigungen

4. Security Assessment according to IEC 62443 / ISO 27001 from Siemens

To observe and implement all relevant points and measures for IT security and safe operation of a facility, a comprehensive security analysis is recommended. The security assessments from Siemens examine and analyze all aspects of security in production facilities. The assessments provide transparency and determine a comprehensive overview of the actual security state of the automation system. This is the prerequisite to recognize the need for action with regard to Industrial Security, and to take the right measures for closing any security gaps.

The assessments are based on the IEC 62443 or ISO 27001 standards. Aspects such as the network architecture of the facility, data flows, production systems and processes, as well as the employees themselves are analyzed:

- Industrial Security check:
  The result is a report with recommendations for measures to reduce the risk.
- IEC 62443 / ISO 27001 assessment:
  The result is a report with recommendations for closing the identified security gaps.
- Risk & vulnerability assessment:
  In this step, risks are identified, analyzed, classified, and assessed. This is the foundation for a risk-based, facility-specific security roadmap that is tailored to the customer and the customer’s facility – ensuring a comprehensive and uniform level of security.

The final report contains specific proposals and concepts for the step-by-step improvement of Industrial Security that are precisely tailored to the business areas examined. The assessments are available for Siemens and third-party systems.

Contact:
www.siemens.de/industrial-security-services

5. Conclusion

A holistic system approach is necessary for IT security and protection against attacks on machines and facilities in public infrastructures, in particular when it comes to the protection of critical infrastructures, e.g., the water and wastewater industry. Here, the IEC 62443 standard has become a trend-setting.

Besides security-relevant product properties including the certified product manufacturing process, system integrators as well as operators of facilities are especially obliged to meet the security requirements demanded e.g. by the BSI. Siemens offers a complete range of products, blueprints, and services to identify vulnerabilities and harden a facility accordingly that – in addition to the actual functionality – continue to meet all security requirements in the future.

www.siemens.de/industrial-security

6. Sources

[1] DWA set of rules: Leaflet DWA-M 1060, IT security – industry standard water/wastewater (Deutsche Vereinigung für Wasserwirtschaft, Abwasser und Abfall e.V. [German Association for Water, Wastewater and Waste – Registered Association]: DWA), 08/2017. [https://www.dwa.de]

[2] DVGW set of rules: Technical note – leaflet, DVGW W 1060 (M), IT security – industry standard water/wastewater (Deutscher Verein des Gas- und Wasserfaches e.V. [German Association for Gas and Water Applications – Registered Association]), 08/2017. [https://www.dvgw-regelwerk.de]

Further information

Published by
Siemens AG

Digital Industries
P.O. Box 48 48
90026 Nuremberg
Germany

Article No. DIFA-B10092-00-7600

Subject to changes and errors. The information given in this document only contains general descriptions and/or performance features which may not always specifically reflect those described, or which may undergo modification in the course of further development of the products. The requested performance features are binding only when they are expressly agreed upon in the concluded contract.

Security note

Siemens provides products and solutions with Industrial Security functions that support the secure operation of plants, solutions, machines, equipment and/or networks. They are important components in a holistic Industrial Security concept. With this in mind, Siemens' products and solutions undergo continuous development. Siemens recommends that you regularly check for product updates.

For the secure operation of Siemens products and solutions, it is necessary to take suitable preventive action (e.g. cell protection concept) and integrate each component into a holistic, state of the art Industrial Security concept. Third-party products that may be in use should also be considered. For more information on Industrial Security, visit:

www.siemens.com/industrial-security

To stay informed about product updates as they occur, sign up for a product-specific newsletter. For more information, visit

http://support.automation.siemens.com

siemens.com/telecontrol