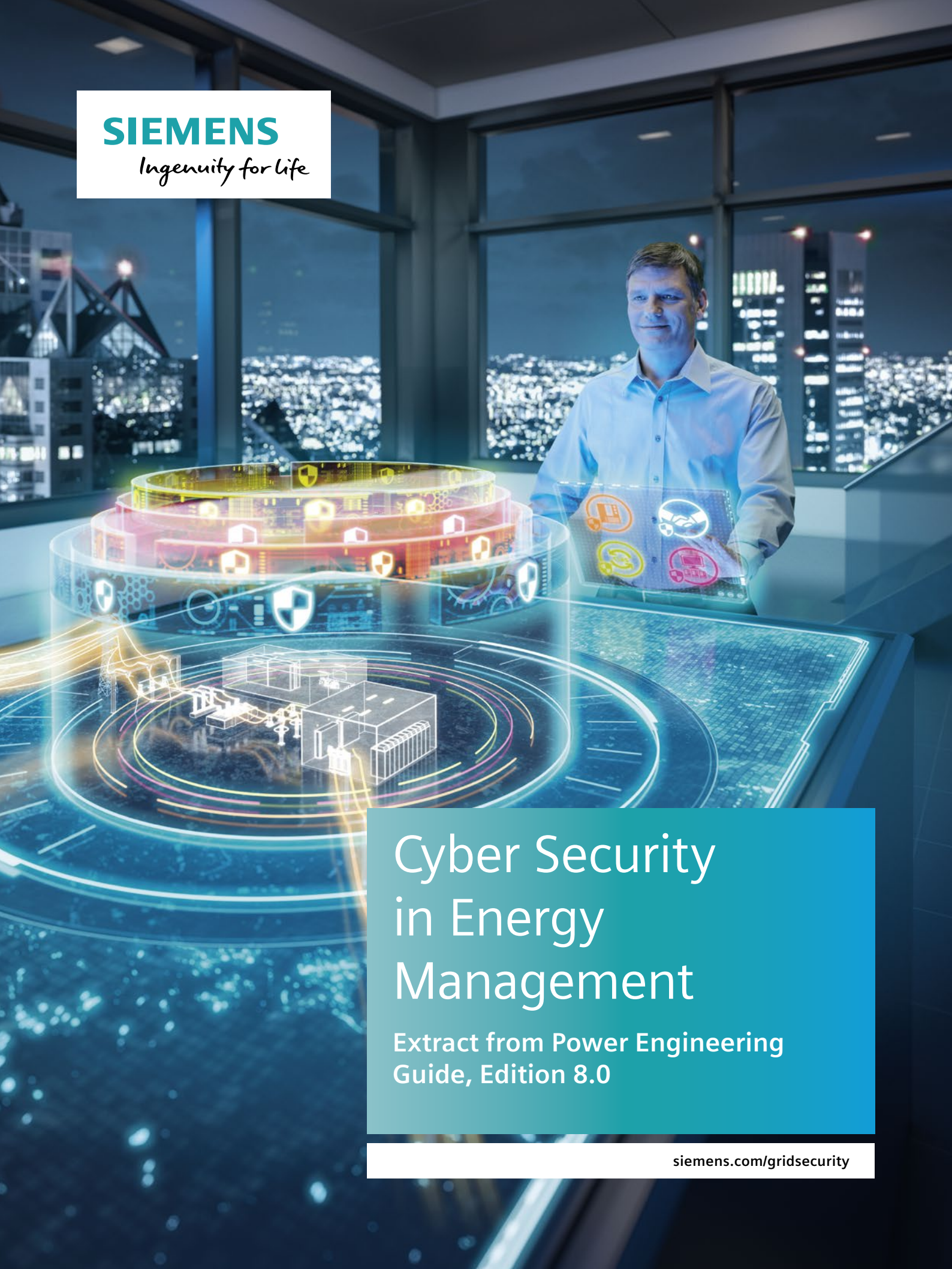

SIEMENS
Ingenuity for life

Cyber Security in Energy Management

Extract from Power Engineering Guide, Edition 8.0

siemens.com/gridsecurity

When it comes to grid security, you shouldn't trust just anyone

Cyber security is a highly sensitive area that demands a trustworthy partner. A technology partner who understands how products, systems, and solutions integrate with the processes and people behind them.

We combine an industry-leading smart grid portfolio with extensive experience and expertise in delivering cyber security solutions. As a multinational company with a global reach, we have the size and competence to provide reliable and sustainable support that you can rely on.

Our domain knowledge and integration capabilities make our portfolio the most comprehensive in the industry. We offer product, solution, and service security that includes unique life-cycle support.

We actively work with international standards organizations to develop and improve security standards for smart grids, and we advise regulatory authorities on technical and process-related topics.

We facilitate a Siemens wide Cyber Emergency Response Team (CERT), and our oversight of CERT gives us increased visibility into global cyber security threats.

The following chapter comprises an extract of the Power Engineering Guide on cyber security. It illustrates a 360° view on cyber security in energy management environments. The extract includes vendor, integrator and operator roles and a holistic approach that addresses people, processes, products and systems.

1 Cyber security

1.1 Cyber security in energy management

Providing a cost-efficient, secure and reliable energy supply is the core business of electric utilities that operate critical infrastructure. The way grids are operated and managed has changed dramatically due to the integration of renewable and decentralized energy resources, the need for network optimization, the interaction with prosumers and consumers, and the participation of new market entrants. With information and communication technology penetrating down to the distribution network and even households, the growing interconnections create more points for potential attacks to critical infrastructure. Consequently, cyber security is top of mind for power system operators today.

As shown in fig. 1, one key target of a power system operator is security of supply, i.e. to ensure a stable supply of power at any time, at competitive costs and while considering regulations. From that perspective cyber threats are perceived as risks jeopardizing the security of supply. Cyber security encompasses all the measures dealing with mitigating such risks, following industry standards, and where relevant, meeting local regulation related to cyber security. To achieve this target, the power system operator:

- Must comply to related cyber regulations which describe 'What must be done'
- Should conform to related cyber standards that describe 'How it needs to be done'
- Shall mitigate cyber risks.

Cyber security controls can be implemented in the area of people and organization, processes, and products and systems. This reflects the so called '3'P's' relevant for a holistic cyber security approach.

Siemens products and solutions enable operators to be compliant with cyber regulations. Furthermore, the products adhere to international standards in order to support interoperability with third-party components. Siemens provides cyber security consultancy services that cover assessments for regulatory compliance and establishment of protection concepts for mitigating cyber risks in energy automation.

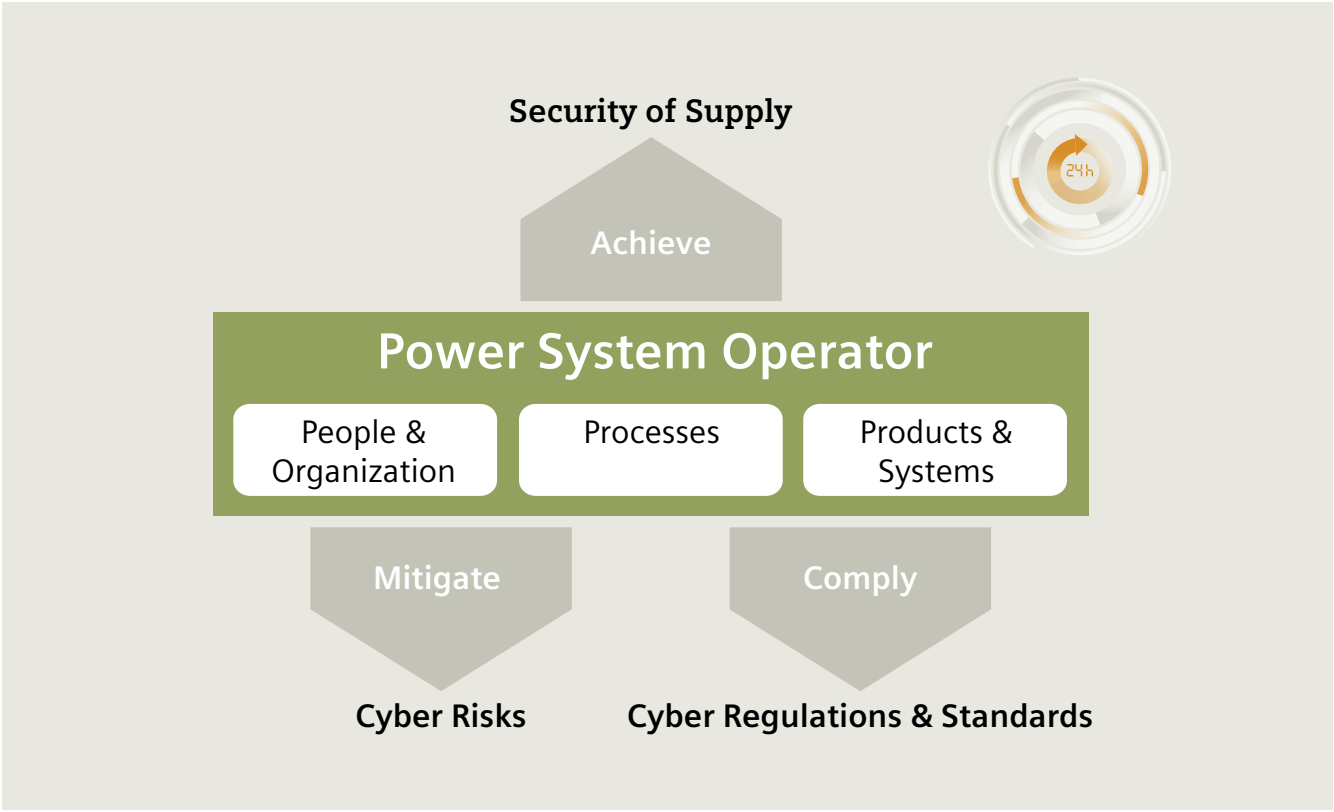

Fig. 1: Cyber security targets for a power system operator

1.2 Cyber security framework

The cyber security framework defines the way how cyber security has to be addressed by the various actors in the energy value chain. It is based on the following:

1. Cyber security regulation
   Cyber security regulations must be supported by all actors within the energy value chain.
2. Cyber security standards
   Existing international standards describe cyber security ranging from governance to specific realization options in products. The three key standards in energy automation are ISO/IEC 27001, IEC 62443 and IEC 62351.
3. Cyber security guidelines
   Guidelines give recommendations on cyber security implementation. The most common and recognized guidelines are: NERC CIP, BDEW whitepaper.

As part of the guidelines, Siemens defines 14 categories of security measures, see fig. 2. Reflecting a holistic approach to cyber security, these categories encompass the so called '3 P's':

- People and organizations: those who are running the company
- Processes: those used by the people and organizations to fulfill the business needs
- Products and systems: the underlying infrastructure to support the business needs.

Categories of security measures related to organization and processes are indicated in the gray boxes in fig. 2.

Security measures related to products and systems are categorized over the green boxes in fig. 2.

The categories of security measures are described here:

1. Organizational preparedness

Establish security measures to develop, integrate and maintain secure products and solutions. This impacts the whole organization in the form of defined roles, clear responsibilities, adequate qualification, policies, processes, tools, and communication. The information security policies at Siemens are in accordance with ISO/IEC 27001.

2. Secure development

Secure development is a systematic approach to integrate cyber security into the product and solution development lifecycle. It is part of the complete process chain, from cyber security requirements to cyber security validation. It also covers the securing of the IT infrastructure that is needed for the development organization.

3. Secure integration and service

Cyber security is an integral part of Siemens' processes to deliver solutions to the customer, who receives solutions with design, integration and commissioning executed according to cyber security best practices, ensuring optimal support for secure operations.

4. Vulnerability and incident handling

Vulnerability and incident handling is the process defining how an organization reacts to and handles security vulnerabilities and incidents, including the related internal and external communication. The process also interfaces as required with the regular vulnerability monitoring and patch development process of the product or solution development.

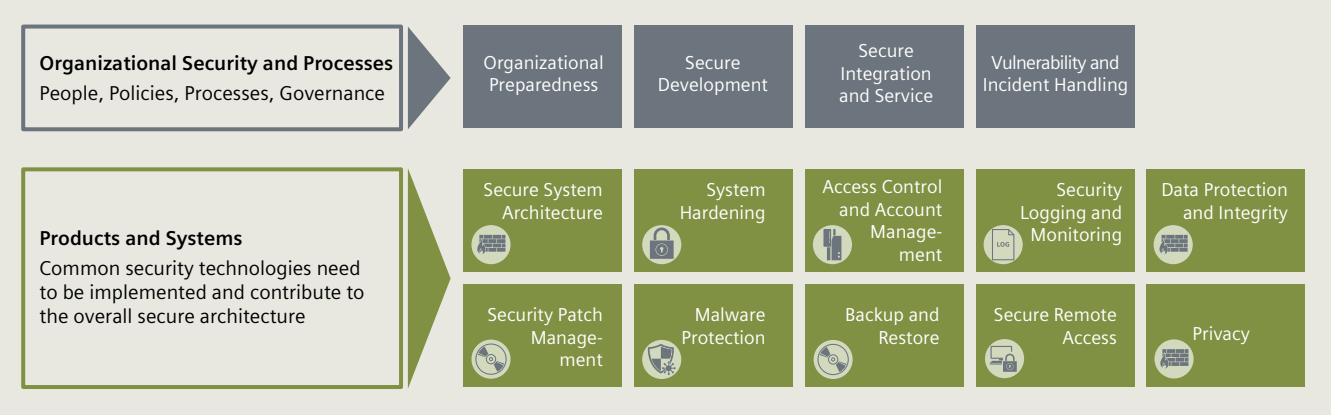

Fig. 2: Siemens categories of cyber security measures

Siemens has its own in-house Computer Emergency Response Team (CERT). The Siemens ProductCERT team is mandated with monitoring and analyzing security issues and publishes product related advisories on vulnerabilities and associated mitigation recommendations in conjunction with the respective Siemens organizational units. Additionally, with its recognized expertise in penetration testing Siemens ProductCERT checks Siemens products and third-party components used within the Siemens portfolio for weak points by means of selective hacker attacks, resulting in recommendations on implementation guidances to the respective Siemens organizational units.

5. Secure system architecture

A cyber security architecture must not only support the regulatory requirements, but should provide security by design, too. Protecting the power system requires a defence-in-depth approach, addressing cyber risks and supporting secure operations through people, processes and technologies.

Fig. 3 outlines a typical network architecture. The basis is a clear segmentation of the network into manageable zones equipped with appropriate cyber security measures in order to enable a secure and cost-efficient operation.

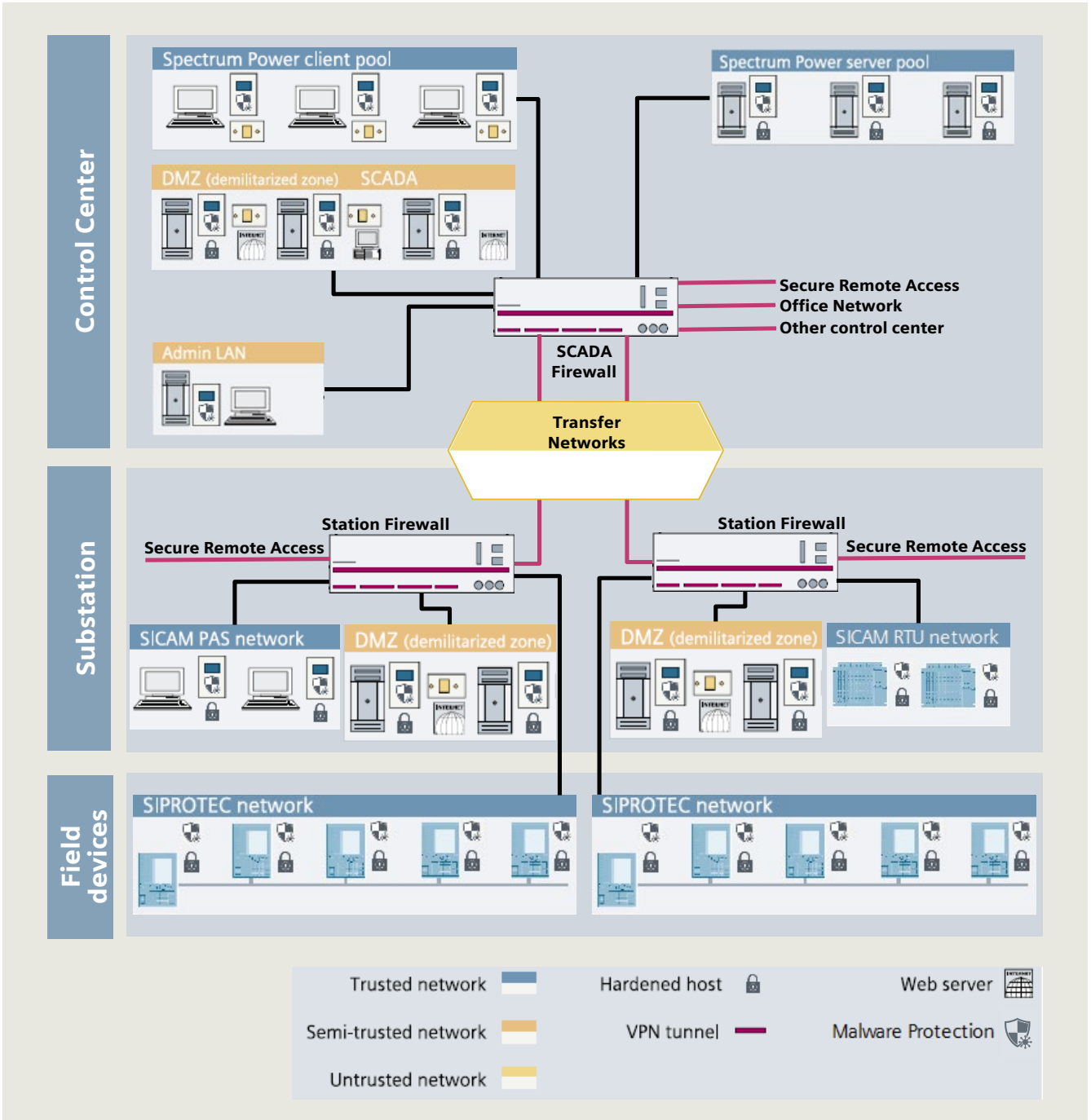

Fig. 3: Cyber security architecture

The architecture is the most visible part of a comprehensive cyber security approach. It forms the basis for applying further measures in people, processes and products as defined covering this cyber security framework.

6. System hardening

Hardening reduces the attack surface of the products and solutions by means of secure configuration. This is reached, e.g., by removal of unnecessary software, unnecessary usernames or logins, disabling of unused ports, or OS hardening. Siemens provides guidelines for products and systems on hardening and can support operators in hardening of their infrastructure.

7. Access control and account management

Access control is the selective restriction of access to products, solutions, or infrastructure, by authenticating users (and systems) and authorizing them by granting appropriate permissions. Account management is the definition of different user accounts with suitable privileges that is best performed in a centralized way with unified security policies. Siemens can support system operators in design and implementation of an access control and account management system. Power system operators can integrate Siemens energy management products seamlessly into their central user management solutions alongside products from other vendors.

8. Security logging / monitoring

Security logging / monitoring means to capture and monitor all security related activities performed across the system, including user account activities such as login/logout, or failed login attempts. Alarms are reported for further follow-up accordingly. Siemens products and solutions support centralized logging of security events and alarms by means of the syslog messaging standard, thereby providing the basis for sophisticated Security Information and Event Management (SIEM) solutions.

9. Security patching

Security patch management includes vulnerability monitoring for all software components (own and third-party) used in a product or solution, classification of the vulnerabilities and available patches, security patch compatibility tests and, if needed, the development of additional security patches to address incompatibilities. For a solution, this includes the delivery and maintenance of a system with up-to-date security patch level installed. Siemens offers comprehensive patch management services to energy automation operators.

10. Malware protection

Protection of a product or solution against malware is ensured through the support of appropriate malware protection solutions (e.g., classical antivirus, application whitelisting, or software signing) and appropriate procedures to ensure that all systems are protected against latest malware. Siemens has malware protection available for key components used in the energy automation, offers technical solutions for malware protection and supports customer to establish a secure update process for antivirus patterns.

11. Backup and restore

Backup is the process of copying and archiving of software, configuration data, and operational data, such that a product or solution can be restored, e.g., after a data loss event. This includes appropriate measures and procedures for disaster recovery. Siemens has backup and restore concepts available, and supports system operators to assess and establish respective process.

12. Secure remote access

Secure remote access in context of substation automation systems is the encrypted, authenticated and authorized access to substation assets from remote sites through potentially untrusted networks. Siemens offers a certified secure remote access solution optimized to the needs of power system operators.

13. Data protection and integrity

Data protection ensures the protection of all sensitive data across the system both in rest and in transit. Such data must be accessible only to authorized persons or processes. In addition, also the integrity of data and communication across the system, and the availability of the data needs to be ensured through appropriate methods. Siemens components support the required functionality to meet data protection and integrity needs, while processes implemented within Siemens ensure that customer data are managed with due care at all phases of customer projects.

14. Privacy

This ensures the users' ability to control when, how, and to what extent information about themselves will be collected, used, and shared with others. Information privacy is a particularly sensitive matter where personally identifiable information is collected, e.g. such as in Smart Metering application. The Siemens portfolio helps operators to comply with the associated regulatory requirements.

1.3 Operational security

In operational security, the interplay of the '3 P's' becomes obvious: products and systems, people and organizations need to work together according to the defined processes. In operational security, key functionalities include measures such as security patch management, access control and account management, security logging and monitoring, and malware protection. These measures are necessary to establish a protective and detective environment, where accountability and traceability of all actions involved in operation of an energy grid become relevant and support the possibility to take corrective control within the operational environment. Siemens has the target to support operational security by relying on international standards.

1. Vulnerability and incident handling

Handling vulnerabilities and incidents is one of the mandatory requirements to protect the energy network.

Vulnerability handling includes the definition of counter-measures, if required, and the communication towards the operator in order to inform appropriately about critical vulnerabilities, work-arounds, and available patches, see fig. 4.

On the other hand, power system operators need to be able to analyze provided security advisories, and to define and apply counter-measures effectively.

Just as vulnerability handling supports to protect the business, incident handling addresses the needs to respond to, and recover from, cyber incidents in an effective manner. The security measures needed for incident handling are the same as for vulnerability handling, but require additional measures in organizational preparedness to be covered, particular in the area of process handling.

2. Security patch management

One of the most crucial activities in cyber security is patch management. Due to the increased interconnectivity, the threat that attackers utilize known vulnerabilities has increased tremendously.

Standards such ISO / IEC 27002 and IEC 62443-2-3 give guidance to operators about how to implement adequate measures for a patch management process. A summary of the recommended process steps for operators are:

- Taking a complete asset inventory
- Checking available patches
- Checking compatibility
- Testing in an environment that reflects the production environment
- Scheduling the patch installation
- Installing patches or mitigation measures
- Updating the asset database.

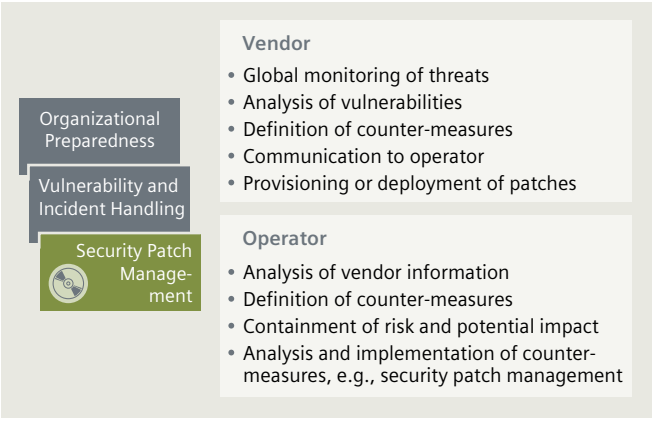

Fig. 4: Tasks and security measures needed in vulnerability handling

Equally, defined requirements for system vendor on patch management are defined in standards such as IEC 62443-2-3 and IEC 62443-2-4:

- Providing documentation concerning patch management policies for components and systems
- Verification of patches concerning compatibility and applicability for own and third-party components
- Providing the patch information and patches to the operator
- Providing lifecycle information for products and systems including end-of-life information.

Siemens meets these requirements with a comprehensive patch management process for products and systems. This includes a regular patch test for own and third-party components, and the provision of the test results to customers. Hereby, Siemens in-house CERT is used for a comprehensive vulnerability scanning and communication of vulnerabilities and advisories for all Siemens products, see section 1.2 item 4. Additionally, as a prerequisite for a patch management process, Siemens provides 'back-up and restore' documentation on product and system level.

A simplified process is shown in fig. 5, with the initial activities and the cyclic activities of a complete patch management process from the operator's point of view.

The initial activities includes the migration to a secure system (step 0 in fig. 5), the definition of the assets to be taken into scope, and prepare the asset data as required in order to be able to perform patch management (steps 1 and 2).

The recurring activities start with the collection of patch information based on the asset inventory (step 3) and a decision, what, whether and when patches have to be installed (step 4); the patch validation (step 5) and the patch installation (step 6) follows accordingly. Finally, the asset data needs to be updated (step 7).

Siemens offers comprehensive patch management services for products and systems to meet the regulatory requirements derived from ISO/IEC 27001 based on all process steps.

3. User management and access control

The basic principle of access control is shown in fig. 6. Access control ensures that users (and systems) can only interact with resources as intended. This is only possible if the user is authenticated, i.e., if it is verified that the user is who he claims to be, and also authorized, i.e. it is verified that the user is permitted to perform the operation he intends to perform with/on the resources. Identity management is the trust base in this pyramid, as it manages the users and credentials to be controlled. For completeness, access control does not only consider the users, but also any resources such as devices or applications.

Access control is relevant in all lifecycle phases (from commissioning, operation and renovation to decommissioning) of systems and networks. The most crucial phase for cyber security is during the daily operations. Typical access control scenarios include physical access, HMI access, IED access, remote access, etc. Additionally, due to safety reasons, emergency access routes are defined in order to bypass the regular access control mechanism.

There are several options to realize access control in the power grid with different levels of depth and security. A typical for a centralized approach is the usage of LDAP or RADIUS servers in order to manage identities. Authentication and authorization can be established by means of password verification or by using a public key infrastructure (PKI) based handling of X.509 certificates. The access rights are defined by the system or device, as these are specific to those devices based on the operational function provided.

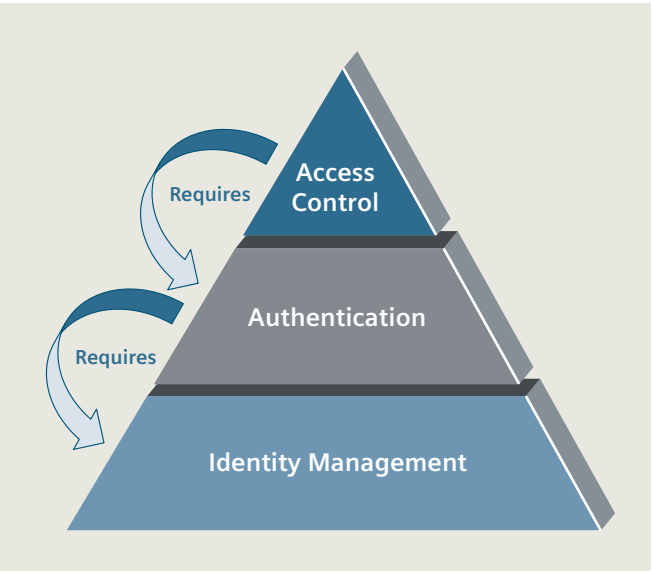

Fig. 6: Identity and access management – the basic principle

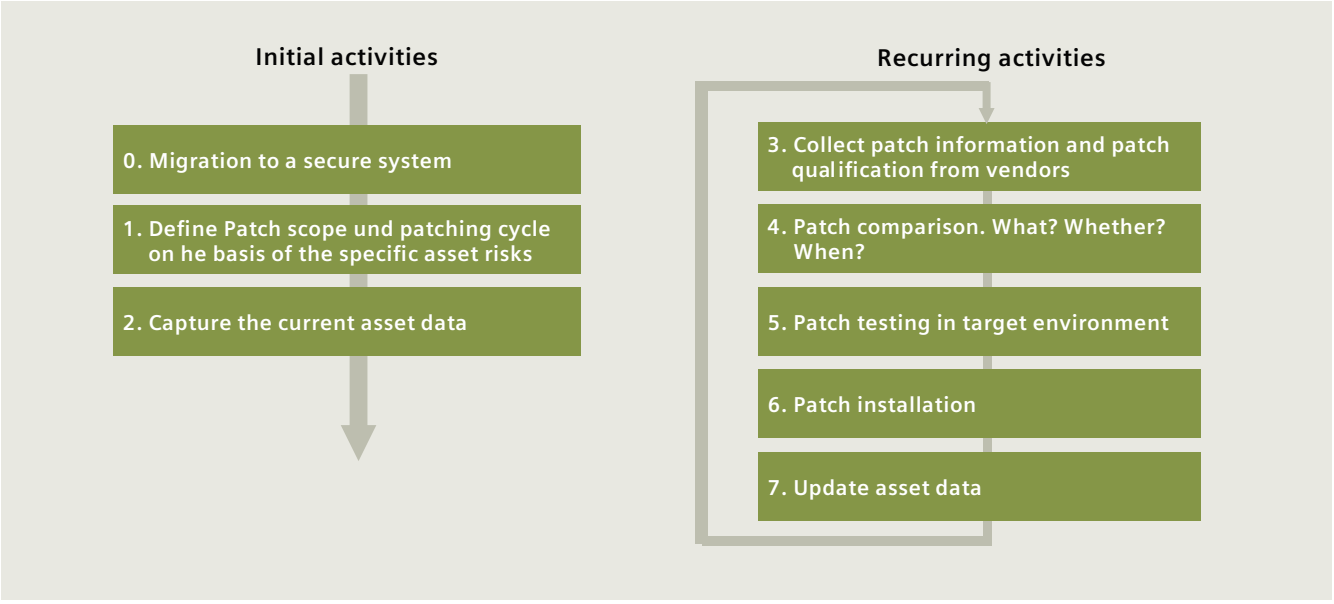

Fig. 5: Simplified patch management process

Fig. 7 shows a role based access control (RBAC) example. A user is requesting access to an IED via a device management tool (1). The IED is sending this request to an Active Directory (AD) domain controller for authentication of the user (2). AD replies with the result of the authentication. If the user has been successfully authenticated by the IED, it retrieves the role information of the user by AD, which indicates the authorization level of the user (3). The IED then initiates the role-based user session (4).

Due to the multi-vendor environment of power grids, a standardized approach based on IEC 62351 is most crucial for an effective access control implementation in order to support interoperability.

It is important to consider transitionary technologies and tools that address the restrictions of the generation-old secondary equipment that will continue to represent the majority installed base along the years to come. Centralized access management solutions like the Siemens CrossBow can close the gap by managing the users and rights for both, old- and newer generation secondary equipment.

4. Centralized logging

In order to get visibility of activities and events in the power grid, monitoring is essential. A basic functionality of monitoring is the centralized logging. Centralized logging means to collect information about events and activities in the energy grid on a central spot for further analysis. The base of centralized logging is the syslog functionality.

Centralized logging is defined in standards such as RFC 5424/5/6 (syslog), and the applications thereof in the energy-sector-covering standards such as IEEE 1686 and IEC 62351. Furthermore, guidelines like BDEW whitepaper or NERC CIP give guidance on what needs to be monitored. Siemens supports centralized logging and offers system operators centralized logging solutions.

5. Malware protection

Malware protection emphasizes measures and concepts implemented in order to protect systems against malware iinfection, which is required for all system components. In other words, systems used in process networks and control systems shall feature protection concepts against malware infection. The potential sources of malware infection could be infected portable media ((e.g., USB flash drive, CD, etc), network shares or infected PCs (e.g., service PC).

Different technical solutions against malware are possible. Classical antivirus and application whitelisting for PC-based systems, and software signing for embedded devices. Antivirus patterns shall be regularly updated without using a direct connection to update-servers located in external networks, e.g., Internet. Possible approaches are realized with an internal update server or with a documented secure manual process (e.g., through external secure devices). In order to ensure compatibility with new anti-virus patterns, Siemens regularly tests the compatibility of new antivirus patterns against the Siemens application.

In this context, Siemens provides technical solutions for malware protection and supports customer to establish a secure update process for antivirus patterns.

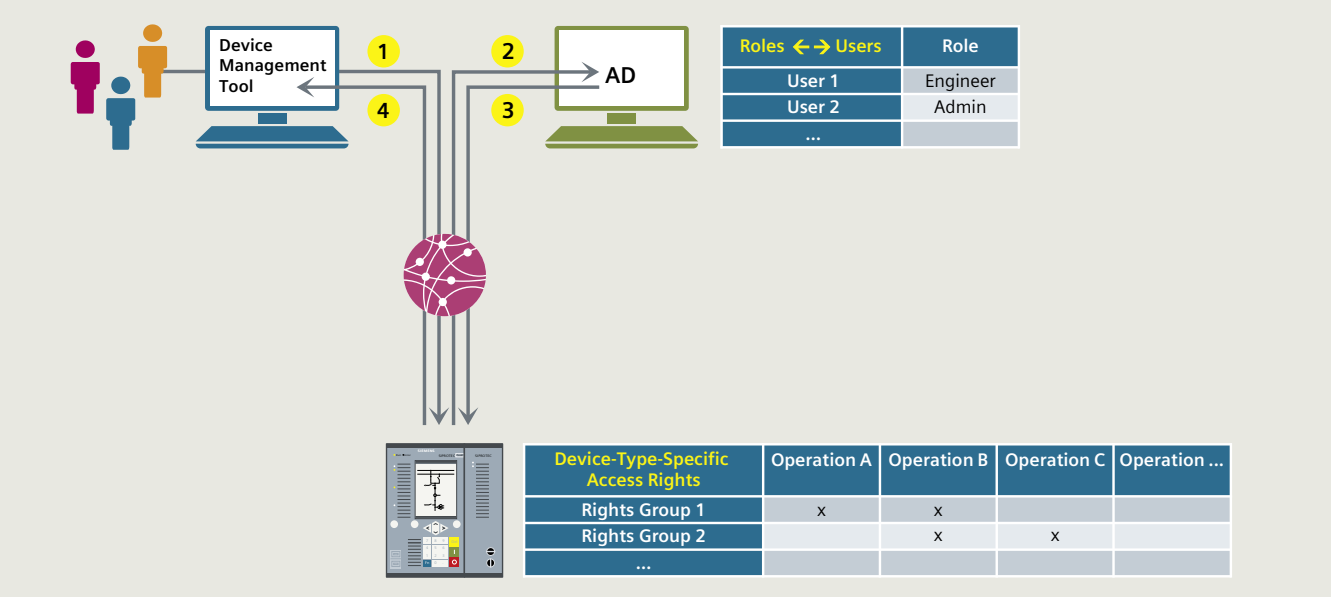

Fig. 7: Example for role-based access control

1.4 Applied cyber security

An effective cyber security requires addressing cyber security on various levels. This section will provide best-practice examples in which the methodology and security measures described above have been applied in order to protect products and systems.

The implementation of cyber security requires to consider the requirements as defined in the cyber security framework (section 1.2), and to support operational cyber security requirements (section 1.3).

1. Product security

Siemens has taken a holistic approach for the energy automation portfolio including processes, communication, employees and technologies. First, cyber security is established in the organization by defined roles, rules and processes; a governance structure has been implemented according to ISO/IEC 27001. Second, secure product development is part of the product lifecycle management that satisfies the stringent demands on cyber security and incorporates a secure product architecture.

Product development includes the secure design starting with security requirements, the implementation of software, and the execution of systematic cyber security tests. Cyber security of Siemens' own infrastructure also plays a major role. Internal design documentation and the source code have to be protected against unauthorized access and tampering in order to secure the integrity needs.

Security-enabled energy automation products are the foundation of a secure energy automation system. Cyber security requirements for the products depend on various factors, including the intended function (protection, control, operation or monitoring) and the spatial layout of the products. Security functions in modern energy automation products follow the general goals of cyber security: availability, integrity and confidentiality, and meet the industry specific standards. State-of-the-art protection devices are capable of satisfying these needs, see fig. 8. Secure communication between the engineering software and the device is crucial for secure operation. The encrypted connection is only established after mutual authentication. A connection password is used and managed in this process that complies with the BDEW whitepaper and NERC CIP recommendations. All security-relevant events are logged in a non-erasable security log. The protection device is equipped with a crypto chip that assures the cryptographic functions, including an integrity check of the device firmware in a protected environment.

For more information on vulnerabilities and updates of products and solutions:

Siemens Internet:

siemens.com/cert/advisories

ICS-CERT:

https://ics-cert.us-cert.gov/advisories

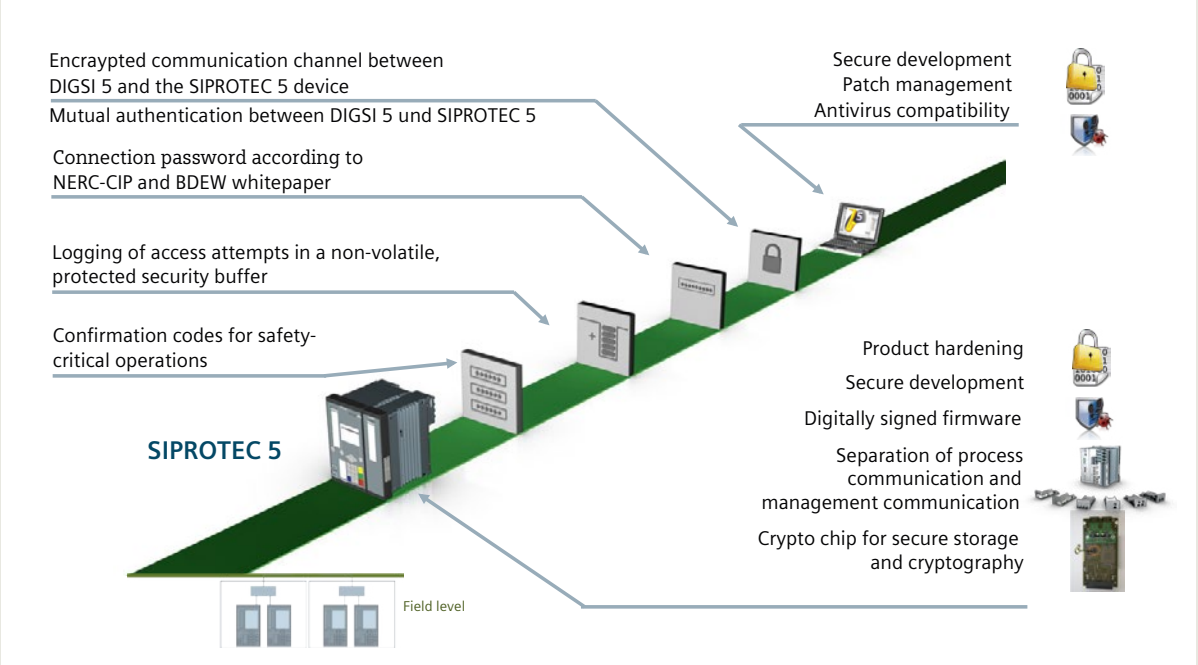

Fig. 8: Security features of a state-of-the-art protection device

During software production, the firmware is provided with a digital signature which the device can authenticate in order to ascertain that the firmware has not been tampered on its transit from the production facilities to the device itself. Furthermore, the device enables a physical separation of process and management communication. Devices communicating outside of a physically protected zone have to satisfy higher communication security requirements than devices communicating within a physically protected area.

For distribution automation scenarios, where it is not always possible to establish adequate physical security measures to protect automation equipment from process communication manipulation, Siemens RTU products support end-to-site encryption of the process communication to the control centers, see fig. 9.

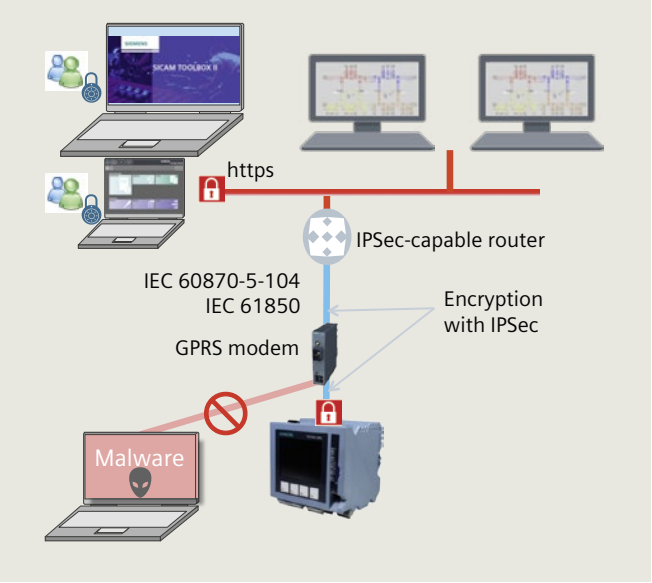

Fig. 9: Example for a secure telecommunication

Siemens test security patches and virus patterns on reference system in order to verify that regular installations of operating system do not affect the availability of energy automation functions.

2. System security – digital substation example

As a system integrator, Siemens is responsible for integrating products in a secure way. This task, too, requires dedicated process descriptions, guidelines, and technical descriptions to ensure secure integration. The system configuration is subsequently carried out according to the technical descriptions. Security measures are validated during the Factory Acceptance Test (FAT) and Site Acceptance Test (SAT) based on defined test cases.

For substation automation systems, the realization of security functions is subject to a number of constraints like the requirement of availability, expected 24/7 operation without interruption. A substation is typically a mixture of PC-based and embedded systems from various vendors with life spans of up to 40 years. Hence, an energy automation system is frequently made up of various components from different vendors, different technologies, and different technological generations. Many of the established office IT measures prioritize protection goals differently, or inadequately account for the special boundary conditions. This calls for the implementation of strategies tailored to the needs of energy automation.

In fig. 10, the security measures applied to a digital substation are shown. All cyber security measures basically follow at least the security design principles “Defense in depth principle”, “Least privilege principle”, and “Network Segmentation”.

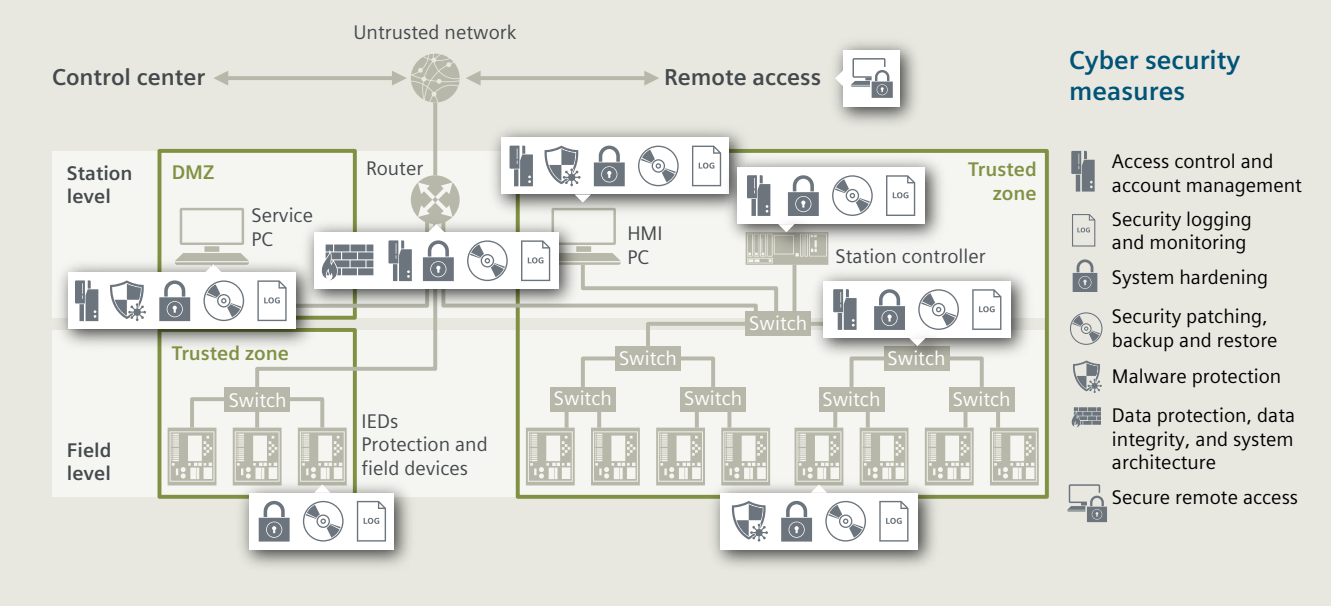

Fig. 10: Digital substation

Network segmentation is a powerful protection mechanism. The fundamental idea is to group network elements with sensitive communication needs and similar level of protection into the same subnet. Firewalls filter inbound and outbound traffic. These zones also called "trusted zones". It is not allowed to bypass the firewalls. The trusted zone is not accessible from outside, from untrusted networks. To get access to the trusted zone from outside, Siemens uses a "buffer" zone, the Demilitarized Zone (DMZ). With this approach, the security requirements for "trusted zone" internal communication can be often reduced to a feasible level for typical industrial components, compared to a larger network that does not rely on security zones.

The principle of least privilege is the practice of limiting access to the minimal level that will allow desired functionality. Applied to human users, the principle of least privilege means that the user has the lowest level of user rights to be able to execute the desired tasks. The principle is also applied to all other "members" of a system like devices, software applications, services, and processes. The principle is designed to limit the potential damage of any security breach, whether intended or unintended.

Defense in depth is the coordinated use of multiple security controls to protect a system. The goal is to provide redundancy in case one security control fails or vulnerability in one security control is exploited. Components of defense in depth include, for example, the security controls such as firewalls, account management, malware protection, and secure hardening.

All security measures are implemented under considerations of the general limitations of substation automation systems and the security design guidelines. The cyber security measures are (cf. fig. 2 and section 1.2 on security categories):

- Access control and account management
- Security logging and monitoring
- System hardening
- Security patching, backup and restore
- Malware protection
- Data protection, data integrity, and system architecture
- Secure remote access.

Looking into malware protection as one cyber security measure example, the implementation offers different options (see also section 1.3 part 5).

Blacklisting / antivirus
Classical antivirus solutions that compare the content of the PC file system with patterns of known viruses. In case of a positive match, the antivirus software alerts the user.

Application whitelisting
An application whitelisting solution works according to a whitelisting mechanism. This is a protection mechanism that allows only trusted programs and applications to run on a system. After installation of the system software and applications, additional whitelisting software is installed on the virus-free system. After installation is complete, a whitelist of programs, applications and services will be generated by the whitelisting solution. All applications/programs/services on the list will be signed or secured by a checksum. This ensures that only approved software will be executed. Downloaded software or viruses that might potentially have infected the system after activation of the whitelisting protection will be prevented from executing.

All Windows-based PC systems are equipped with appropriate malware protection. The advantage of the application whitelisting is that it is not necessary to install regular pattern updates for newly developed malware immediately.

The decision on which solution fits best to the system operator's requirements and operational management has to be taken on a project- or system-specific basis.

Siemens offers comprehensive services and technology to support operators in defining protection concepts for digital substation and migration towards a modern architecture and defense-in-depth approach.

1.5 Cyber security consultancy

Cyber security in the energy sector is a broad topic where a lot of domain-specific knowledge and expertise is required in order to define appropriate measures. Siemens supports operators regarding the verification, definition and implementation of cyber security in systems, services and processes.

Siemens' cyber security consulting approach is based on the well-proven Smart Grid Compass® model, which has been developed by leading experts at Siemens and has since then been used to successfully transform a wide variety of system operators worldwide into an 'utility of the future'.

As shown in fig. 11, cyber security consultancy offered by Siemens is structured into 4 phases:

- **Orientation:** Comprehensive and objective analysis of the current cyber security status in the technology, process and organizational environments.
- **Destination:** Definition of the aspired security levels also with regard to the relevant regulatory requirements and standards, and derivation of concrete security measures
- **Routing:** Development of holistic cyber security. implementation roadmap based on derived measures, and including recommendations for implementation.
- **Navigation:** Continuous customer support during the implementation of security measures.

Systems with a high degree of protection against cyber security attacks are feasible when cyber security methods and functionality are implemented consequently. Siemens can support power system operators during assessment, definition and implementation of cyber security.

Siemens recommends and provides consultation while carrying out a risk assessment of an organization or infrastructure in order to obtain a comprehensive sight into existing risks, derive appropriate measures, and thus mitigate the risks identified.

1.6 Final remarks

An effective cyber security requires addressing cyber security holistically. Cyber security requires a continues effort to protect against existing and upcoming threats and risks. This is valid concerning processes, technologies and people such as ongoing competence management to keep the knowledge up-to-date, process improvements following international standards like ISO/IEC 27001 and maintenance for the technology to keep the security level up-to-date. This is valid for all stakeholders in the energy value chain, the operators, the vendors, system integrators and consultants.

Therefore, Siemens is addressing cyber security systematically in the complete lifecycle of his products & solutions based on international standards. Furthermore, Siemens has the policy to work according ISO/IEC 27001.

With our portfolio and services, and together with the Siemens CERT, Siemens is uniquely positioned as a strong and trusted partner for his customer.

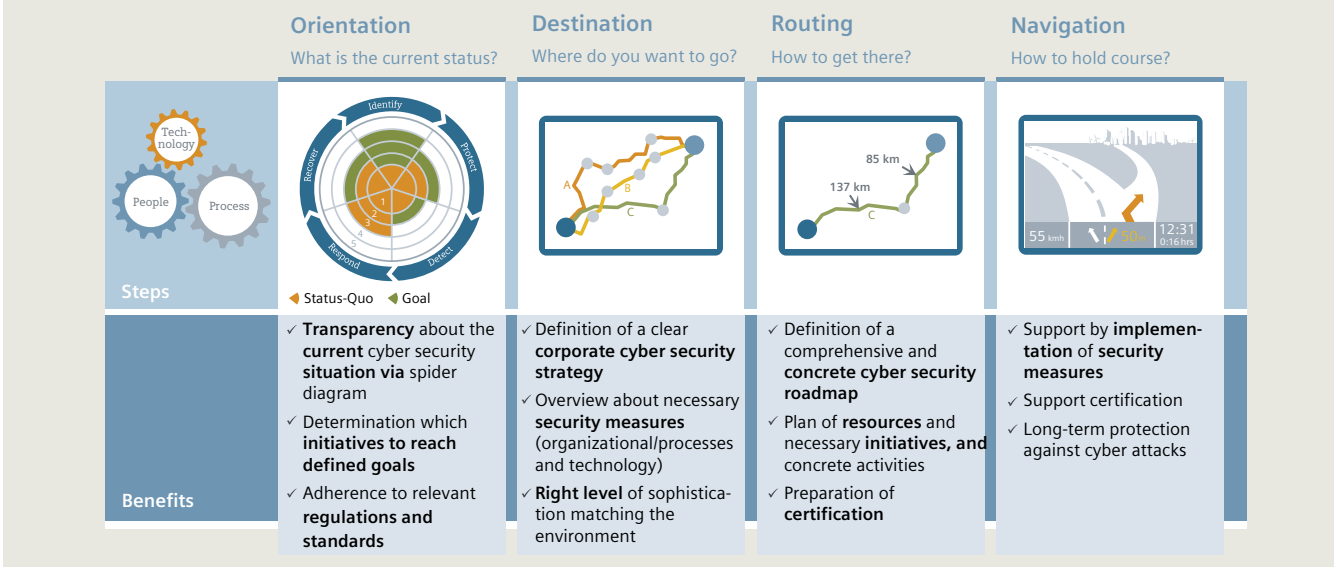

Fig. 11: Cyber security consultancy phases

Published by

Energy Management Division
Freyeslebenstrasse 1
91058 Erlangen, Germany

For further information please contact the
Customer Support for Power & Energy
Phone: +49 180 524 70 00
(Charges depending on provider)
E-mail: support.energy@siemens.com
siemens.com/csc

Article No. EMDG-T10100-00-7600
Printed in Germany
Dispo 06200
BG184-000595-00 | 08170.5