Cyber Security Standards and Regulations in Energy Automation Systems

F. Buchi, S. Fries, D. Kroeselberg

Siemens AG

Germany

KEYWORDS

Smart energy grid, substation automation, cyber security, integrity protection, centralized security management.

1 INTRODUCTION

Background

Increased networking of energy automation systems, standardization of communication protocols and software components ensure efficient operation but increase the process network's exposure and attack surface. Cyber security threats for energy automation systems are real and the consequences of a successful attack are far-reaching. Governments react with the introduction of regulatory requirements for critical infrastructure. Prominent examples are the United States with the NERC CIP (North American Electric Reliability Corporation, Critical Infrastructure Protection) requirements, Germany with an IT Security law or France with a new regulation on cyber security defined by ANSSI (Agence nationale de la sécurité des systèmes d'information). Several international standards cover technical and organization aspects of cyber security. These standards like IEC 62443, IEC 62351 or the ISO/IEC 27000 series either directly address cyber security with focus on operational technology and automation control, or define domain-specific profiles of general security mechanisms. At the same time, it is important to understand the different target audiences and different depths of requirements per standard, and combine them in a way to achieve appropriate protection of a target deployment.

Purpose of this paper

This paper introduces and structures the most relevant cyber security standards and regulatory frameworks for the energy automation domain according to their specific target audiences. Security requirements are analyzed, and the benefits and consequences for product vendors, system integrators and operators are investigated. Implementation examples for selected security requirements are given. These are used to demonstrate required security activities along the complete lifecycle of a substation automation system.

Siemens AG – Energy Management
Humboldtstrasse 59,
90459 Nuremberg,
Germany

2 BODY

2.1 Overview

Over the recent years there have been substantial changes in what is commonly referred to as energy automation, or in other words the automated processes associated with the generation, transmission and distribution of electrical power. While in the past the power infrastructure was vertical and managed by single entity, structural changes such as the deregulation and further the increase of distributed energy resources (DER) have resulted in a larger number of distinct actors being involved in the availability of electric power networks both on operational technology (OT) and information technology (IT) . Business and operational processes communicate across the boundaries of the actors OT and IT assets, increasingly using standard IT components, standardized IP based protocols and public communication infrastructure.

As a consequence the power infrastructure is considerably more vulnerable to cyber attacks than in a world of isolated systems connected over a dedicated infrastructure. Examples of such exposure are remote access for maintenance tunneled over the Internet, or the potential software vulnerabilities and resulting exposure to malware and manual attacks associated with the increased amount of software components in substations. A further aspect leading de facto to an increased exposure is the more common availability of standard diagnostics tools, e.g. for standardized communication protocols. Also, the increasing use of standard operating systems and middleware increase the necessity to deal with known vulnerabilities, as security patches appear with higher frequency for widely used standard IT software, compared to embedded systems focused on a specific industry domain and use case.

While the exposure of OT systems has increased progressively over the last years, it has increasingly become the focus of attackers and security researchers. In this context, the fact that there are few instances of known successful cyber attacks on power infrastructure should not mislead: cyber attacks are mostly reported in a restricted manner to selected authorities. Reports from authorities such as the ICS CERT in USA do in turn show that there is a sustained amount of cyber incidents affecting the energy sector[1]. Recent successful attacks such as the blackout perpetrated on several Ukrainian DSOs in December 2015[2] do show how real the risk is and lead to improvements in protecting Energy generation and distribution against cyber security risks.

The topics to be jointly addressed by power utilities, vendors, and integrators, have several dimensions. One dimension is about the levers to be activated:

- Technology (security capabilities of products and systems)
- Processes addressing secure and security operations
- Organizational aspects (e.g. people, policies, tools)

Another dimension is supply-chain oriented and consists of defining responsibilities and requirements associated with the actors involved in the lifecycle of the assets under consideration:

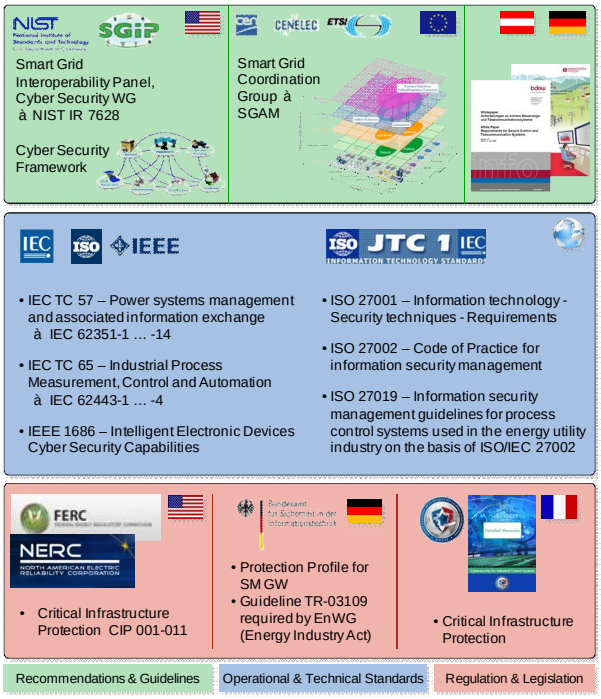
- The hardware and software vendors, providing products with appropriate security functionalities
- The integrator delivering systems configured and tested as to meet the required security level
- The operator, in charge of maintaining the systems and ensuring secure operations

We expect that, driven by the challenges of vulnerability and patch management, there will be an increasing need for collaboration between the operator and vendors over the lifetime of the system to address these challenges.

2.2 Cyber Security Standard, Guidelines, and Regulation in Energy Automation

Cyber Security Standards are a prerequisite for interoperability of different vendors' products to ensure seamless interconnection and information exchange between the various actors and roles in energy automation systems. There exist different types of standards describing organizational and technical security requirements on one hand and on the other technical security standards providing specific technological solutions as well as procedures for organizational and management aspects for the operating environment. Besides standardization there exist regulations, which are typically country specific and address the secure operation of an infrastructure. This in turn is supported by a technical security solution. The picture is completed by guidelines, which describe best practices for secure deployment and operation

of energy automation systems. Ideally, there is interplay between the standardization, regulation, and the guideline activities.



Note: the stated organizations and standards are just examples and are not complete

Figure 1: Energy Automation relevant Security Standards, Guidelines, and Regulation

Figure 1 shows prominent examples for dedicated bodies providing regulative documents, technical standards, and also guidelines and recommendations. The listed documents are seen as relevant, when planning energy automation systems and deployments. The following subsections provide more details on some of the mentioned examples, focusing on the international standardization.

2.2.1 Examples for Cyber Security Standards

2.2.1.1 IEC 62443

The standardization of IEC 62443 targets the harmonization of industrial automation cyber security requirements. The scope includes products and systems as well as organizational, operational and process-related security aspects. IEC 62443 is a framework of different specifications targeting security requirements and side conditions of industrial and energy automation systems. It focuses on the design of secure solutions considering high availability, configuration (engineering information), long life cycles, unattended operation, real-time operation, and communication, as well as safety requirements. The individual parts cover common definitions, and metrics, requirements on setup of a security organization (ISMS related), and processes, defining technical requirements on a secure system, and to secure system components as shown in Figure 2. As shown, the parts are in different state of completeness.

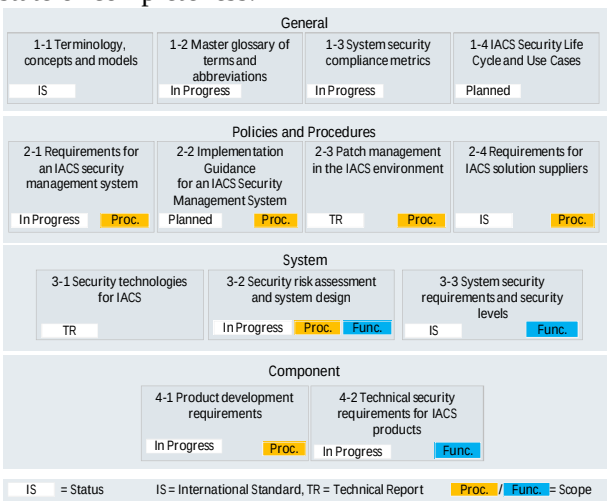


Figure 2: Overview IEC 62443 Parts and Status

As shown in Figure 2, specific parts of IEC 62443 are developed as basis for security certification programs, where the initial focus is on part 2-4 with reference systems based on part 3-3 (both parts approved as international standard). Efforts for aligned criteria for certifiers have been started in the IEC EE to utilize IEC 62443 as the base for a certification scheme. The parts currently in focus of certification are IEC 62443-2-4 and IEC 62443-3-3.

2.2.1.2 IEC 62351

IEC 62351 targets the specification of security mechanisms applicable to the power systems domain. This standard provides currently 14 parts addressing security measures for authentication, integrity, confidentiality and role based access control for dedicated use case involving protocols like IEC 61850, IEC 60870-5, IEC 60870-6, and IEEE 1815 as shown in Figure 3.

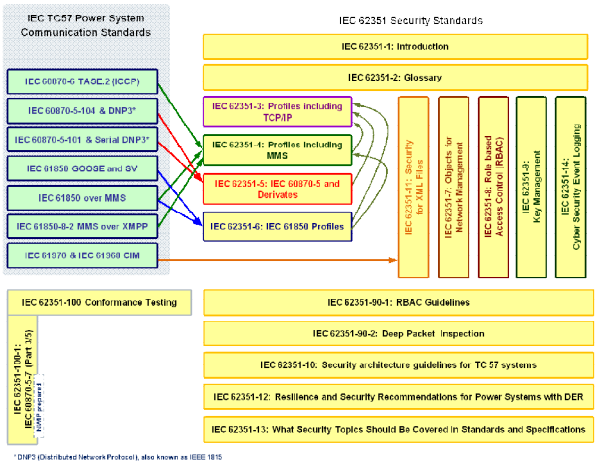


Figure 3: Overview IEC 62351 Parts and Relation to other Energy Automation Protocols

The technical security measures defined in IEC 62351 can be directly used to address security requirements from other technical standards like IEC 62443 (see section 2.2.1.1) or from recommendations like the BDEW Whitepaper (see below). One of the main goals of IEC 62351 is the provisioning of end-to-end security, which is achieved on either transport or on application layer. Note that end-to-end security here refers to mutual authentication and integrity and confidentiality protection of communicated data. This is the scope of multiple parts as there are IEC 62351-3, -4, -5, -6. Besides the provisioning of security services to protect communicated data, there is also a definition of the interactions with a security infrastructure. This is done by providing a specification for the key management (IEC 62351-9) specifying the management of security credentials and IEC 62351-8 for supporting authorization with a role based model. A further specification targets security specific event (IEC 62351-14) and monitoring information (IEC 62351-7) to enhance the today's network monitoring and logging solutions with energy domain specific information. Also the overall security architecture and connected security means has been developed (IEC 62351-10) also in cooperation with Cigré.

The security measures in IEC 62351 are defined in a way to utilize existing technology as much as possible and to profile the existing means to meet the energy automation specifics. One prominent example is the application of Transport Layer Security protocol TLS [6] to protect TCP based communication. A further example is provided by the selected security credential targeted for authentication and access control. For this the ITU-T standard X.509 is heavily used.

Within substation automation the IEC 62351 parts 3, 4 and 5 regarding the security means in conjunction with IEC 62351-9 providing the key management are mostly in focus of integrators. These parts focus on securing the telecontrol communication (IEC 60870-5 and IEC 61850), which is used to connect to substation external peers.

2.2.1.3 ISO/IEC 270xx

The ISO/IEC 270xx framework establishes guidelines und general principles for initiating, implementing, maintaining, and improving information security management in an organization. Specifically, ISO/IEC 27001 specifies information security management system (ISMS) requirements, while ISO/IEC 27002 provides a code of practice for information security controls. Figure 4 below shows the interworking between the different ISO 270xx parts for a Smart Energy System.

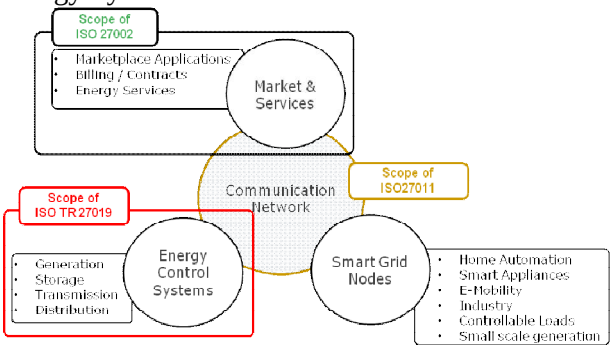


Figure 4: Interworking of different ISO 270xx standards to provide energy system wide ISMS

In ISO/IEC TR 27019, energy utility industry specific implementation guidance based on the code of practice in ISO/IEC 27002:2013 is given. The additional requirements, or clarifications based on ISO/IEC 27002 extend the ISMS scope to process control (OT) environments. The specific target domain includes systems and networks for controlling and supervising the generation, transmission and distribution of electric power, gas and heat in combination with the control of facilitating processes. To complete the picture, ISO 27011 provides the domain specific mapping for the telecommunication domain used for network services.

2.2.1.4 IEEE 1686

IEEE 1686 defines the functions and features to be provided in intelligent electronic devices (IEDs) to accommodate critical

infrastructure protection (CIP) programs. The standard addresses security regarding the access, operation, configuration, firmware revision and data retrieval from an IED. Also addressed is the encryption of communications with the IED. It serves as a procurement specification for new IEDs or analysis of existing IEDs. Outside the scope of this specific standard is the determination of the system security architecture, as is only addresses embedded security features of the IED and the associated IED configuration software.

2.2.2 Examples for Cyber Security Regulation

Cyber Security Regulation provides requirements targeting to support the resilience of critical infrastructures like a regional, national or pan-national bulk power grid. These regulations are typically country specific and rely on existing standards. The following examples directly apply to Smart Energy:

- NERC-CIP: In the U.S., the North-American Electric Reliability Corporation (NERC) defines cyber security standards for critical infrastructure protection (CIP) in the energy sector [13]. The set of standards provide a security requirement framework for security control perimeters and access management with incident reporting and recovery for critical cyber assets and cover functional as well as non-functional requirements. They apply to asset owners and consist of a mixture of organizational, process, and technical requirements. NERC CIP is formally controlled and enforced in the U.S. and in Canada.
- ANSSI: In France, the Agence nationale de la sécurité des systèmes d'information defines binding measures for critical infrastructure systems.
- German BSI: defines the IT Security Law [17] finalized in 2015. This requires appropriate protection and monitoring, as well as the implementation and further certification of an Information Security Management System (ISMS) based on ISO27001.

2.2.3 Examples for Cyber Security Guidelines

As shown in Figure 1, the picture is completed by guidelines and recommendations, which may be used for instance in tenders to require specific security measures and procedures. The following list provides several examples of such guidelines:

- NIST IR7628: defined in the Cyber Security Working Group (CSWG), which is part of the Smart Grid Interoperability Panel (SGIP). The document develops a comprehensive set of cyber security requirements and consists of three parts targeting strategy, security architecture and requirements, and supportive analyses and references. Especially the second part provides a detailed analysis of the interfaces and communication relations and their security implications.
- SGIS Report: The security subgroup of the European Smart Grid Coordination Group (SG-CG) addressing the European Commission mandate M/490 [15] addressed cyber security in the (European) smart grid. Smart Grid services shall be enabled through a Smart Grid information and communication system that is inherently secure by design within the critical infrastructure of transmission and distribution networks, down to connected properties. The report describes an analysis framework applied to different use cases and mapped to standards work to address identified security requirements. The investigation into security was closely connected to Smart Grid Architectural Model (SGAM) developed by a different working group. The final report of the security subgroup (see [16]) provides recommendations of security means, to be applied in the different zones and domains of SGAM. Moreover, a gap analysis mapping the collected security requirements to existing standards has been concluded.
- BDEW Whitepaper: The German Association of Energy and Water Industries (Bundesverband der Energie- und Wasserwirtschaft – BDEW) introduced a white paper (cf. [4]) defining basic security measures and requirements for IT-based control, automation and telecommunication systems, taking into account general technical and operational conditions. It can be seen as a further national approach targeting similar goals as NERC-CIP. The white paper addresses requirements for vendors and manufacturers of power system management systems and is used as an amendment to tender specification. Meanwhile, there is also a country specific regulation enhancement available for Austria. The white paper was also one base for the development of the international standard ISO/IEC 27019.

2.2.4 Conclusion regarding Cyber Security Standard, Guidelines, and Regulation in Energy Automation

As shown in the previous subsections, there exists a variety of cyber security related requirements and guidelines applicable in Energy Automation targeting technical and organizational security means. Although there is not a single comprehensive standard or norm covering comprehensively the cyber security measures the industry is converging to a limited set of standards who are now gaining increased acceptance worldwide, as shown in Figure 5.

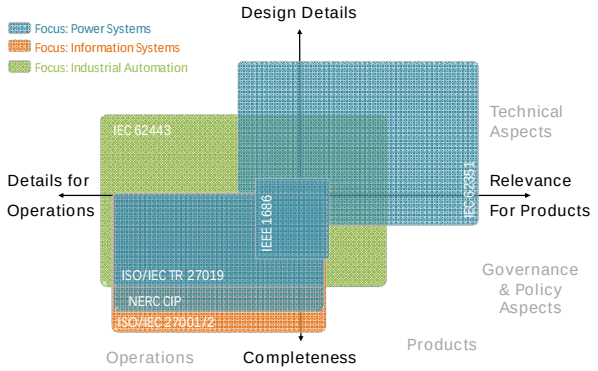


Figure 5: Coverage of the Cyber Security Documents

2.2.5 Recommendations to utilities in GCC regarding Cyber Security Standards and Guidelines

The previous sections have shown how the standardization activities around cyber security have gained in maturity and converged to a reduced set of standards which are now recognized industry wide.
Of specific interest for utilities is IEC62433, from which requirements to System Integrators, that is to Suppliers of Utilities can be directly derived.
The authors therefore formulate the following recommendations to utilties:

- Require System Integrators to have their scope of supply comply with IEC62443-3-3 and their project delivery processes comply with IEC62433-2-4.
- Aligning the organization of the Utility with ISO27001 further complements this approach

Utilities may find it challenging to assess to which extent the claims of their suppliers to be compliant to their requirements are genuine. Such concern can be addressed by requiring Suppliers such as System Integrators to achieve certification from an external party.

2.3 Towards patch management: Required building blocks and realization approaches

2.3.1 Motivation and typical challenges in industrial environments

To ensure secure operation of energy automation systems, the security standards discussed in the scope of this paper cover a broad range of technical aspects related to the protection of critical components. Besides a secure system design for the automation solution, strong focus is put on the secure configuration and hardening of the system's components and network configuration. Resulting measures focus on applying recommended component security measures and integrating supporting security controls like firewalls, network monitoring systems, or application whitelisting solutions. The overall target is to reduce the system's attack surface as much as possible.

As part of the system hardening, it is important to ensure that known vulnerabilities in the system's software components are recognized, evaluated, and appropriate measures taken to address them. This largely comes down to the management of security patches for diverse software parts used in the automation solution. It relies on appropriate procedures and on established interfaces between the solution and software component suppliers, and the party performing security patch management.

	Energy Control Systems	Office IT
Anti-virus / mobile code	Uncommon / hard to deploy	Common / widely used
Component Lifetime	Up to 30 years	3-5 years
Application of patches	Use case specific	Regular / scheduled
Outsourcing	Rarely used	Common
Real time requirement	Critical due to safety	Delays accepted
Security testing / audit	Rarely (operational networks)	Scheduled and mandated
Physical Security	Very much varying	High
Security Awareness	Increasing	High
Confidentiality (Data)	Low – Medium	High
Integrity (Data)	High	Medium
Availability / Reliability	24 x 365 x ...	Medium, delays accepted
Non-Repudiation	High	Medium

Figure 6: Comparison of Security Requirements in OT and IT

In critical infrastructure environments security patch management is recognized as one of the more challenging areas, where security requirements need to be addressed. Major differences to regular corporate IT environments exist, as shown in Figure 6. Specifically for patch

management the marked differences are crucial. Recognized challenges for addressing security vulnerabilities through security patch management include:

- High-availability and real-time requirements to systems in operation. This especially holds for components close to the controlled energy distribution process like IEDs, or station controllers.
- Long component lifetimes in deployments, leading to software components being in continued operation after their end-of-life has been reached. This results in the lack of security patch support from the original software component supplier and motivates different approaches for reducing the attack surface. Migration strategies are necessary, which may include solutions for "freezing" the system such that only well-known software processes are allowed to run, known as "application whitelisting". The latter approaches apply best to stable configurations that do not need to change over time, whereas they tend to become complex for components that receive dynamic configuration or software changes.
- Complexity in deployments that typically include a wide range of different component types (e.g. embedded controllers with specialized OS and software, standard-OS based systems with a range of middleware and energy specific applications, network devices like switches, firewalls, or NTP servers).

2.3.2 Patch management requirement

The security requirements standards discussed in this paper typically formulate requirements that focus on aspects supporting the security patch management process of utilities, whereas utilities experience growing requirements from regulatory bodies in this area. It is important to understand the specific role of each standard and its requirements to vulnerability and patch management. Taking the IEC 62443 framework as example,

- IEC 62443 part 4-1 focuses on requirements to the management of security patches for 3rd party software components and on the development and testing of security patches for own developed software. Both need to be integrated into the regular product development process.
- IEC 62443 part 2-4 focuses on all aspects of security patch management that are important during integration and commissioning of a secure solution. It can also be applied to subsequent service and maintenance efforts to keep the security patch level up-to-date.
- IEC 62443 part 2-1 (based on ISO-IEC 27002) focuses on requirements to asset- and change management as well as the technical vulnerability management procedures as part of operating the system in a secure way.

Table 1 provides an overview about vulnerability and patch management related security requirements that can be found in the discussed standards.

Table 1: Vulnerability and patch management requirements overview

Specification	Content	Relevant sections
IEC 62443-2-4	Process and procedures for handling vulnerabilities and patches during system integration, maintenance, service.	• Detailed requirements in SP11.1 to SP11.6
IEC 62443-4-1 work-in-progress	Process and procedures for handling vulnerabilities and patches as part of secure development.	• Practice 6 – security defect management • Practice 7 – security update management
IEC 62443-2-1 work-in-progress	Based on ISO27002, profiling for industrial automation control	• 12.6 Technical Vulnerability Management • Annex B5 (Extended Control) • (work-in-progress)
IEC 62443-2-3	General patch management considerations and recommendations (all stakeholders). Draft patch information exchange format (XML based).	• Full document
NERC CIP-007	Requires security patch management procedures, time frames and configuration change management procedures for the asset owner	• CIP-007 R2 • CIP-010 R1
ISO/IEC TR 27019 work-in-progress	Profiling for process control systems of Energy utilities. Specifically covers up-to-date software inventory (installation, upgrade, change)	• 12.6 Technical Vulnerability Management
BDEW Whitepaper	Requirements to suppliers covering security patches and 3rd party support, security update and maintenance process, configuration and change management.	• 2.1.1.3/4/5 (Patch Management, 3rd party support) • 2.5.4/5 (Secure Update and Maintenance Processes, Configuration and Change Management)

It is noteworthy that the standards requirements rather focus on high-level aspects regarding required procedures, timelines, and coverage of the vulnerability and patch management process that needs to be in place. Further discussion regarding implementation, realization approaches, and data exchange formats can be found in the technical report IEC62443-2-3.

2.3.3 Aspects of a security patch management process

The security requirements related to security patch management that are summarized in Table 1 can be addressed by a set of procedures, activities, and tools. Ensuring an overall approach to effective security patch management requires that both technical and procedural aspects are addressed. The following aspects should therefore be covered:

- Asset management including actual software configuration and installed patch level of the system.
- A strategy for patching the system's software components.
- Documentation of all patch management related procedures and activities.
- Security vulnerability monitoring that continuously identifies known vulnerabilities and corresponding security patches (or other mitigations).
- A procedure to classify vulnerabilities in the specific system context and decide required measures.
- Deployment procedures and tooling to apply required security patches.
- Interfaces between parties performing patch management and software component vendors for exchanging patch management related information and trusted software updates.
- Interfaces between patch management and incident handling procedure and people in the involved stakeholder's organizations to ensure that measures can be triggered as needed in case of critical vulnerabilities.
-

2.3.4 Recommendations to utilities

For the proper handling of patch management procedures as part of secure operation and in line with the requirements of ISO/IEC 27001/2 and the profiling of 27019, utilities need an appropriate level of support of their procedures from suppliers. It is therefore recommended to utilities to define their approach to patch management and further express requirements to their suppliers based on IEC 62443-2-4 requirements, especially those provided in SP11 of the standard. These are considered the most accurate set of patch management related security requirements that state what suppliers need to provide to allow secure operation in alignment with ISO/IEC 27019.

The following are key capabilities to be met by suppliers:

- To perform state-of-the-art security vulnerability monitoring,
- to provide recommendations and documentation of patch management procedures and tooling support,
- to offer information and interfaces to support the operational patch management process,
- and to offer timely support for the proper handling of critical vulnerabilities that may impact secure operation.

2.3.5 Integrity throughout the security patch management procedures

Security patches address vulnerabilities in software components and therefore reduce the overall attack surface of an energy automation system. For deciding, which security patches are critical for a given system within its operational environment and the need to be installed, appropriate classification procedures need to be established. These take into account aspects like applicability, criticality of a vulnerability (e.g. based on the CVSS score), or exposure of the affected software components.

However, as soon as it has been decided to install a specific security patch, it is essential to ensure the integrity of the finally installed piece of software along the whole distribution chain. This includes patch retrieval from trusted sources, secure distribution and transfer to the target deployment, and secure rollout procedures. One example underlining the importance of ensuring the integrity of patches along their distribution chain is the dragonfly case [20] that focused on the energy sector. Attack vectors included the distribution chains for OT device software updates.

An effective way to ensure such software integrity is to digitally sign software update

packages (whether security related or regular functional updates) based on X.509 certificates, and enable cryptographically secured verification of the signature at the final target where the package is installed. As example for energy automation, firmware updates for IED devices that can be verified at the target IEDs, help to ensure that any integrity violation in the firmware can be detected prior to installation, leading to rejection of corrupt or manipulated updates.

Related security requirements can be found for example in IEC 62443-2-4, where SP 11.06 requires that software update processes ensure the authenticity and integrity of the software running on the affected device where updates are applied.

2.3.6 Supporting security measures through an appropriate infrastructure

Ensuring the authenticicty and integrity of security patches is typically achieved by utilizing digital signatures. They involve cryptographic key material in form of certificates and corresponding private keys. The de-facto standard for certificates is the ITU-T recommendation X.509 which is commonly referred to as X.509.

The necessary technical and organizational means for utilizing X.509 key material is provided as Public Key Infrastructure (PKI). In general, a PKI provides a secure, reliable, and scalable environment for the complete lifecycle of key material, i.e., generating, distributing, and querying public keys for secrecy, correctness, and sender verification. The specifics of X.509 certificate management in power systems are specified in IEC 62351-9 as shown in Figure 7. The standard IEC62351-9 is versatile and enables a variety of security services:

- Firmware and patch signatures to ensure integrity and thus to be able to detect manipulations of the packages (see use case 1 in Figure 7).
- Identification and authentication of the communication peers (user or IEDs) for substation automation communication, telecontrol, engineering of, and remote access to field devices. This functionality can be enhanced with role-based access control as specified in IEC 62351-8 (see use case 2 in Figure 7).
- Protection of the session key negotiation as part of the utilized security protocols. One example is TLS, which is used to protect the TCP based communication of IEC 60870-5-104 for telecontrol or IEC 61850 for substation automation. Here, the X.509 key material is utilized to setup an authenticated and integrity and confidentiality protected communication channel, to be used for substation communication (see use case 3 in Figure 7).

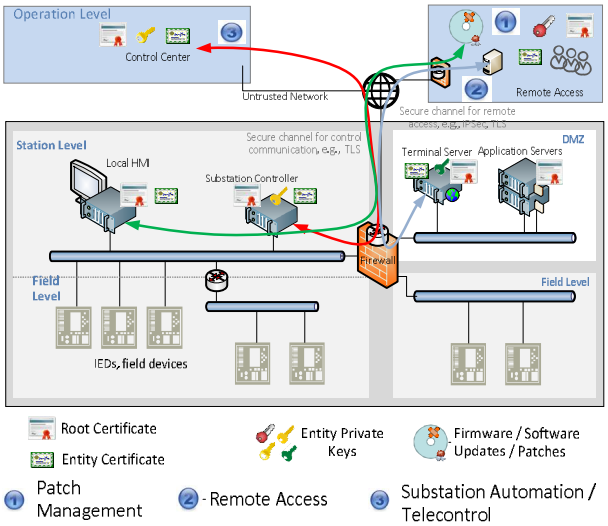


Figure 7: Application of X.509 key material to support security services in substation automation

As stated above, the foundation for these security services is the existence of a PKI with technical interfaces to the different components and the established processes for operating a PKI. In the context of smart grid, a PKI may be owned and operated by a utility company as a purely internal PKI, or it may be a public PKI, provided as a security service by an external supplier based on a contractual relationship. The application and operation strongly depend on the target use case and thus have to be tailored accordingly. Interoperability of different vendors products and thus to the interoperation between different parties is granted with the use of the standard X.509.

A promising aspect of PKI in the context of energy automation is that it supports “off-line” use cases, such as providing the possibility to perform authentication of a user or of a component towards an asset even in the absence or unavailability of communication to a central server. A concrete example is provided by the authentication of a maintenance engineer connecting to an IED located in an isolated substation. The authors estimate that as of today there is no scalable alternative to PKI for such use cases.

While the approach described in this solution may seem complex to the reader, it shall be noted that PKI is a technology, which has been

deployed for years on very large scale and is already utilized in the IT world. Examples are provided by securing web communication through the well known HTTPS protocol or email encryption.

3 CONCLUSION & OUTLOOK

We have described a subset of standards, guidelines and regulative requirements, which are gaining increased acceptance within the industry and which can be used by power utilities, vendors and integrators as guidelines for improving the cyber security of their systems. Is important to note that each standard has a specific scope and that therefore should be applied according to its specific focus.

Among the various technical, procedural, and organizational aspects to be considered when implementing security controls, the implementation of patch management remains challenging. We have identified the key tasks to be addressed by the ecosystem of vendor-integrator-operator. From a technological point of view the introduction of PKI based services in power systems has been discussed and motivated. Especially for the secure deployment of patches of software a PKI enabling the application of digitally signed software components can provide the necessary security infrastructure. Moreover, as PKI services are also required for other applications like secure communication or role based access control, these are expected to become a standard functionality in power system deployments over time.

REFERENCES

[1] US NCCIC/ICS CERT – Year in Review, https://ics-cert.us-cert.gov/sites/default/files/Annual_Reports/Year_in_Review_FY2015_Final_S508C.pdf

[2] US ICS-CERT – Attacks against the Ukrainian infrastructure, https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01

[3] NERC, North American Reliability Corporation, http://www.nerc.com/page.php?cid=2|20

[4] BDEW – Bundesverband Energie- und Wasserwirtschaft, Datensicherheit, http://www.bdew.de/bdew.nsf/id/DE_Datensicherheit

[5] ISO/IEC 62351, Part 1-14, http://www.iec.ch/smartgrid/standards/

[6] RFC5246: The Transport Layer Security (TLS) Protocol Version 1.2, T.Dierks, E.Rescorla, August 2008, http://tools.ietf.org/html/rfc5246

[7] ISO TR 27019: Information security management guidelines for process control systems used in the energy utility industry on the basis of ISO/IEC 27002, March 2013

[8] ISO/IEC 27002:2005 Information technology – Security techniques – Code of practice for information security management, June 2005 http://www.iso27001security.com/html/27002.html

[9] ISO 61850: Communication networks and systems for power utility automation

[10] IEC 60870-5-104: Telecontrol equipment and systems – Part 5-104:Transmission protocols – Network access for IEC 60870-5-101 using standard transport profiles, http://webstore.iec.ch/webstore/webstore.nsf/Artnum_PK/36194

[11] IEC 60870-5-7: Telecontrol Equipment and Systems Part 5-7: Security Extensions to IEC 60870-5-101 and IEC 60870-5-104 protocols

[12] RFC 5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley, W. Polk, May 2008, https://tools.ietf.org/html/rfc5280

[13] NERC-CIP, North American Electric Reliability Corporation, “CIP Critical Infrastructure Protection Standards”, Version 5 – Subject to future enforcement, see http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx

[14] NERC, Compliance Committee, “Progress Report on Implementation of Risk based Compliance Monitoring and Enforcement Program”, November 2015.

[15] Mandate M490, http://ec.europa.eu/energy/gas_electricity/smartgrids/doc/2011_03_01_mandate_m490_en.pdf

[16] CEN/CENELEC/ETSI Smart Grid Reports: www.cencenelec.eu/go/SmartGrids/

[17] German IT Security Law, July 2015, http://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl115s1324.pdf (German)

[18] German Energy Act, EnWG, July 2012, http://www.gesetze-im-internet.de/bundesrecht/enwg_2005/gesamt.pdf (German)

[19] Technical Guideline TR 03109, Technische Vorgaben für intelligente Messsysteme, 2015, https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03109/index_htm.html (German)

[20] Symantec Official Blog, "Dragonfly: Western Energy Companies under sabotage threat", June 2014. http://www.symantec.com/connect/blogs/dragonfly-western-energy-companies-under-sabotage-threat