Technology Report

Cyber security and resilience guidelines for the smart energy operational environment

Executive summary

Cyber security has become an increasingly vital requirement for any business, particularly those dealing with critical infrastructure, such as power system operations responsible for managing the rapidly evolving electric system. These energy businesses must navigate their way through increasingly changing and risky business environments, while continuing to provide and improve their services to end users. Challenges include the transition to clean energy resources and society's increasing reliance on electrical energy.

At the same time, evolving regulations, breath-taking new technologies, and innovative market opportunities are impacting the existing business structures, including the interconnection of distributed energy resources owned and operated by third parties, the rapidly expanded use of electrical vehicles, the reorganization of the power system with microgrids, availability of cloud services, and increased utilization of the Internet of Things (IoT) technologies.

In parallel with the paradigm shifts in the energy business environment, the energy industry has accelerated its evolution toward digitization and is becoming increasingly reliant on cyber assets (systems, controllers, intelligent devices) to manage the delivery of electrical energy. These cyber assets are crucial to the safety, efficiency, and reliability of electrical energy.

However, these cyber assets present serious challenges: businesses must also determine how to cope with the reality of deliberate cyber attacks, such as the successful cyber attack against the Ukrainian SCADA system[1], as well as how to remain resilient to the more mundane but equally critical inadvertent cyber threats arising from personnel mistakes, the complexity of systems, the multitude of new participants in the energy market, equipment failures, and natural disasters. Energy businesses that used to address only the system engineering process (design, deployment, integration, procedures, and maintenance) must now include cyber security services and technologies into these engineering processes. As a result, the new systems could be significantly different in configurations, capabilities, and constraints.

In the energy operational environment, there are five critical concepts for cyber security that should be understood as these energy businesses struggle to implement the necessary cyber security policies, procedures, and technologies. These five critical concepts on cyber security and resilience for the smart energy are illustrated in Figure 1[2].

This IEC Technology Report provides guidelines based on these five cyber security concepts. They cover the cyber security issues that these businesses must address in order to mitigate the possible human safety, physical, functional, environmental, financial, societal, and reputational impacts of "successful" cyber attacks. The authors have focused on the electrical and gas operational environments[3], but almost all these cyber security issues apply also to other energy environments.

1 ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf

2 All diagrams not otherwise noted, were developed by the authors of this report.

Figure 1 | Five cyber security concepts

Concept #1 Resilience should be the overall strategy for ensuring business continuity. When focusing on resilience in general, organizations must consider safety, security, and reliability of the processes and the delivery of their services. Resilience includes security measures that can mitigate impacts, not only before incidents (identify and prevent), but also during such incidents (detect and respond) and after incidents have been resolved (recover). For resilience of cyber assets, organizations must similarly consider safety, security, and reliability for cyber assets. Resilience thus involves a continuous improvement process to support business continuity. Resilience is not just a technical issue but must involve an overall business approach that combines cyber security techniques with system engineering and operations to prepare for and adapt to changing conditions, and to withstand and recover rapidly from disruptions. Information sharing and interoperability within and across organizations is also becoming a crucial part of resilience.

Concept #2 Security by design is the most cost-effective approach to security. Security is vital for all critical infrastructure and should be designed into systems and operations from the beginning, rather than being applied after the systems have been implemented. This means that the products, the systems, the processes and the organization should be designed or set up from the beginning with security in mind. However, recognizing that security cannot easily be added to legacy

3 For this document, the electrical and gas operational environment covers transmission and distribution operations, field operations, electrical generation operations, and interactions with energy and ancillary markets. It is understood that there are "gray areas" as to which environment a particular system might belong to, and there are many interactions between operational systems and corporate systems which could affect operations. So the term "environment" is used as a general term to identify the differences between entities that can affect physical processes and systems and those that do not directly affect physical processes and systems. This includes any "IT" systems that could affect "OT" systems.

systems, particularly since system components may have different life cycles, it is crucial that even for these existing systems, transitions to security-based designs should be managed by including security controls in all system retrofits and upgrades. Security by design combines business organizational policies with security procedures and the supportive technologies. Organizational policies include security regulations, personnel training, and segregation of duties, while security procedures include CERT information sharing, backup and recovery plans, and secure operations. Security technologies include physical and logical techniques, such as physical site access locks, access control, authentication and authorization for all communications, and security logs.

Concept #3 IT and OT are similar but different. Technologies in operational environments (called OT in this document) have many differing security constraints and requirements from information technology (IT) environments. The primary reason is that power systems are cyber-physical systems and security incidents can cause physical safety and/or electrical incidents, while such physical consequences are not usually a problem in corporate environments. For IT environments, confidentiality of sensitive business and customer information is usually the most important, but in comparison for OT environments, the availability, authentication, authorization, and data integrity of power system information are usually the more critical requirements, since power data is typically not sensitive. At the same time, the OT environment is increasingly relying on cyber technologies and is inheriting more and more devices and platforms from the IT world, while both IT and OT environments are increasingly converging on the use of well-known and ever evolving IoT technologies. This interconnection of IT/OT and increased dependence on IoT technology is leading to additional vulnerabilities and challenges on ensuring adequate security in the energy environment. Therefore the selection of appropriate security measures have to be focused on the security requirements as determined by risk assessment.

Concept #4 Risk assessment, risk mitigation, and continuous update of processes are fundamental to improving security. Based on an organization's business requirements, its security risk exposure must be determined (human safety, physical, functional, environmental, financial, societal, and reputational) for all its business processes. Risk assessment identifies the vulnerabilities of systems and processes to deliberate or inadvertent threats, determines the potential impacts, and estimates the likelihood that the incident scenarios could actually occur. The strategy for risk mitigations must take into account operational constraints, as well as looking to engineering designs and operational procedures for improving resilience, while also evaluating the cost for implementing such a potential risk mitigation strategy and degree to which it mitigates the risk. Risk assessment also requires that mitigation processes are re-evaluated during regular periodic security reviews or triggered by actual security incidents.

Concept #5 Cyber security standards and best practice guidelines for energy OT environments should be used to support the risk management process and establish security programs and policies. Cyber security measures should not be re-invented. Key cyber security standards and best practice guidelines have already been developed for different areas and purposes of security. Cyber security planning should use these cyber security standards and guidelines to improve resilience, security, and interoperability throughout the energy OT environment, using the right standards, guidelines, and procedures for the right purposes at the right time.

This IEC Technology Report has been developed by the task force on cyber security in IEC Systems Committee on Smart energy Working Group 3.

Table of contents

Section 1

Resilience as the overall strategy for ensuring business continuity

Resilience must be the overall strategy for ensuring business continuity. Resilience covers measures that can mitigate impacts from safety, security, and reliability incidents, not only before such incidents (identify and prevent), but also during incidents (detect and respond) and after incidents have been resolved (recover). This report focuses on the cyber security aspects, while still taking into account safety and reliability as underlying requirements, since they can often mitigate security challenges. For example, the NIST Cyber Security Framework[4] and ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27019 provide descriptions of these resilience concepts for cyber security (see Figure 2).

Cyber security is far more than preventing attacks launched by malicious hackers. Cyber security for smart energy improves the resilience[5] of the power system by mitigating the threats from security

Figure 2 | NIST framework for resilience (Credit N. Hanacek/NIST)

4 www.nist.gov/cyberframework

5 Resilience is defined as the "ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents." [SOURCE: US Presidential Policy Directive – Critical Infrastructure Security and Resilience].

An supplementary definition states that resilience includes "the ability to reduce the magnitude and/or duration of disruptive events. The effectiveness of a resilient infrastructure or enterprise depends upon its ability to anticipate, absorb, adapt to, and/or rapidly recover from a potentially disruptive event."

"incidents" that affect cyber assets[6] that could disrupt operations.

Mitigation of threats to resilience combines cyber security techniques (such as access control, authentication, detection of anomalous behaviour, and incident logging) with organizational and engineering methods, which allow the organization to prepare for and adapt to changing conditions, as well as to withstand and recover rapidly from disruptions. These engineering methods would include traditional power system reliability measures, such as redundant equipment, contingency analysis, and backup systems, but would also include methods focused on addressing cyber asset vulnerabilities, such as planning for the loss of multiple cyber assets, isolation capability to limit cascading cyber attacks, and even training personnel in manual operations typically performed automatically.

Checks on data entry or control commands would be included in resilience support for the simple reason that mistakes are the most common "cyber incident". Since people with detailed knowledge of power system operations are the most dangerous attackers, additional cyber security and/or engineering methods may need to be deployed to mitigate this type of vulnerability, such as two-factor authentication, segregation of networks, and continuous monitoring for anomalous traffic. Backup generators, communication networks and spare cyber equipment should be located in secure sites, yet easily accessed when needed, because storms can affect not only the power system but also their cyber assets.

6 A cyber asset is any equipment with computer processing capability, including controllers of hardware assets, but not the hardware assets themselves (e.g. electromechanical breaker). Cyber assets can be affected by physical actions (cut a wire, damage a transformer) as well as cyber actions (introduce malware, inadvertently enter incorrect data).

Section 2

Security by design as most cost effective approach

Designing security into cyber systems from the beginning is the most cost-effective approach to cyber security, since it minimizes risk and financial expenditure. Effective security cannot just be "patched" on to existing power system operational processes but should be an intrinsic part of system designs and configurations, operational procedures, and information technologies. Inserting security procedures and technologies afterwards is costly because often they are *ad hoc* and require major modifications to system configurations, as well as significant retraining of personnel. If designed in from the beginning, security becomes a normal part of the life cycles of power system cyber assets and operational procedures.

The term "security by design" covers many aspects, such as component designs, software implementations, system configurations, network configurations, planning procedures, and data management. Many of the benefits of security by design can be realized even if systems are just being upgraded or slowly replaced, since having a well-thought through security plan is critical for including security at each upgrade or replacement step.

Some of the security design aspects include becoming aware of potential threats and vulnerabilities through a risk analysis that takes into account the environments in which the component may be deployed before finalizing system and network configurations. For example, if some critical systems are located within a well-defined electronic security zone, then access to these critical systems can use the access and monitoring controls provided by the zone perimeters for crossing between different security zones (see Figure 3). Such a design reduces "attack surfaces" that could be exploited by malicious entities or simply misused by accident.

Security by design also permits more consistency across all systems with well-defined configurations of networks and information flows. Users would have consistent procedures to follow, rather than *ad hoc* security approaches. This consistency would therefore be easier to implement and maintain, less likely to have security gaps, and less costly to manage globally.

Security by design concepts can apply to planning for the inevitable "successful" security incidents (failure scenarios) which should trigger the development of procedures for coping, such as designing in degradation modes.

In security by design, access control can be implemented down to the data levels, not just the system levels, which allows true end-to-end security between users and their access to data, thus limiting very precisely who can monitor and/or control what data. The same access control can also be applied to the data flows between software applications in the OT environment.

Flows of valid information to the right place within the right time are the most critical requirements for operational environments. Security by design, usually requiring new or updated applications, can ensure that this level of assurance can be provided by secure protocols which would be natively supported by systems and would be part of the core capabilities of the systems. For example, validating information can help mitigate the threat of people who have the knowledge to disrupt power system operations, by ensuring data verification is engineered within each system. At the same time,

access to data may be constrained due to security policy requirements

Security policies, established during the design of systems, can institute procedures for purchasing and updating systems. With such security policies, the configurations of communication networks can be carefully designed, and the security of the supply chain can be better known and managed.

Nonetheless, it is well recognized that security cannot easily be designed into legacy systems, particularly since power system components may have vastly different life cycles. It is therefore crucial that even for existing systems, transitions to security-based designs should be managed by including security controls in all system retrofits and upgrades.

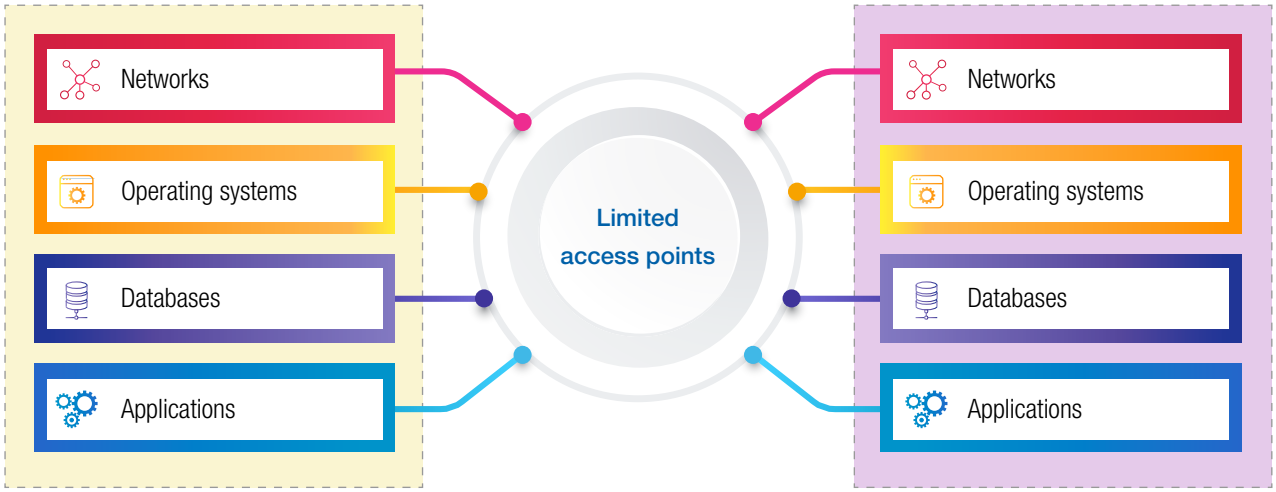

Figure 3 | Security by design example: electronic security perimeters with limited access points

Section 3

IT vs OT: different security requirements in the IT environment and technologies in OT environments

In traditional business environments, the IT department is considered the expert in all things termed “cyber security”. For most corporate cyber assets, this IT expertise is well placed to understand and address the threats, and to design methods to minimize vulnerabilities and respond to attacks. In general, corporate cyber assets are mostly concerned about the confidentiality of the information contained within computer systems, with the result that most IT security focuses on preventing access to this sensitive data.

However, technologies in the operational (OT) environment can affect the management of the cyber-physical power system and can thus affect safety and reliability. Therefore, technologies in the OT environment have different requirements and constraints when applying security measures to ensure that these systems can continue to support the same power system safety and reliability levels. For instance, security measures must take into account the time latency requirements of systems in the OT environment. For example, in substations the information flows can have latencies of less than a few milliseconds, while SCADA systems in control centres may need time latencies of seconds.

In the OT environment, deliberate cyber security incidents or inadvertent mistakes and failures of cyber assets can have physical repercussions since power systems are “cyber-physical systems”. The repercussion with the greatest consequence is safety: the deliberate or inadvertent mis-operation of a cyber asset could cause harm or even death. The second most important repercussion is the reliability of the power system to provide electrical energy or the gas system to provide gas energy to customers. Although these OT infrastructures have always been built with reliability of their physical assets (generators, breakers, transformers, power lines, gas lines) as the most critical design requirement, the reliability of the supporting cyber assets must nowadays also be designed to the same degree.

As illustrated in Figure 4, for IT environments, confidentiality of sensitive business and customer information is usually the most important, but in comparison for OT environments, the availability, authentication, authorization, and data integrity of power system information are usually the more critical requirements, since power data is typically not sensitive. With their experience in focusing on energy system reliability, it is often the experts in operations who best understand what responses to cyber asset incidents may or may not be appropriate, and, combined with IT cyber expertise, how best to utilize engineering methods and operations of the “physical” energy systems to minimize the impacts of such cyber asset incidents.

Operational environments have some very specific security challenges. For instance, high availability of both physical and cyber assets requires engineering designs with the focus on redundancy, high reliability, high performance requirements of these assets. The security requirements of the OT environment may necessitate changes in network configurations and information flows, such as use of security perimeters, demilitarized zones, and firewalls. In addition, very high speed, real-time processes, involving peer-to-peer interactions, autonomous actions, time sensitivity, and other

characteristics, require different security solutions to those typically used in IT, for instance, requiring only authentication and not encryption.

At the same time, operational constraints must be taken into account in these designs. For instance, constraints on equipment resources (timing, bandwidth, network access) can impact the cyber security procedures and technologies that could be used. In particular, heavy encryption techniques or online access to certificate authorities are generally not possible for operational assets. Additionally, the timing for system maintenance and equipment updates or upgrades is constrained by power system operational requirements, such as only having short windows during the spring or fall for taking equipment out of service for such updates.

Another constraining element for applying cyber security measures reflects the large numbers of legacy equipment with long life cycles that cannot be easily upgraded to include cyber security techniques. Therefore, other security measures must be found, such as virtual private networks or methods to isolate or segregate the devices. In addition, given the criticality of power system operations, security should not prevent operational actions, particularly emergency actions, meaning that “break the glass” scenarios must also be built into security procedures.

Another major change is the need to utilize Internet of Things (IoT) networks and technologies, in particular to interact with customer sites for monitoring and managing distributed energy resources (DERs) and communicating with smart meters. This use of IoT implies that utilities can no longer rely only on their own proprietary communication networks but must nonetheless still apply cyber security techniques to the interactions across public networks using well-known communication technologies.

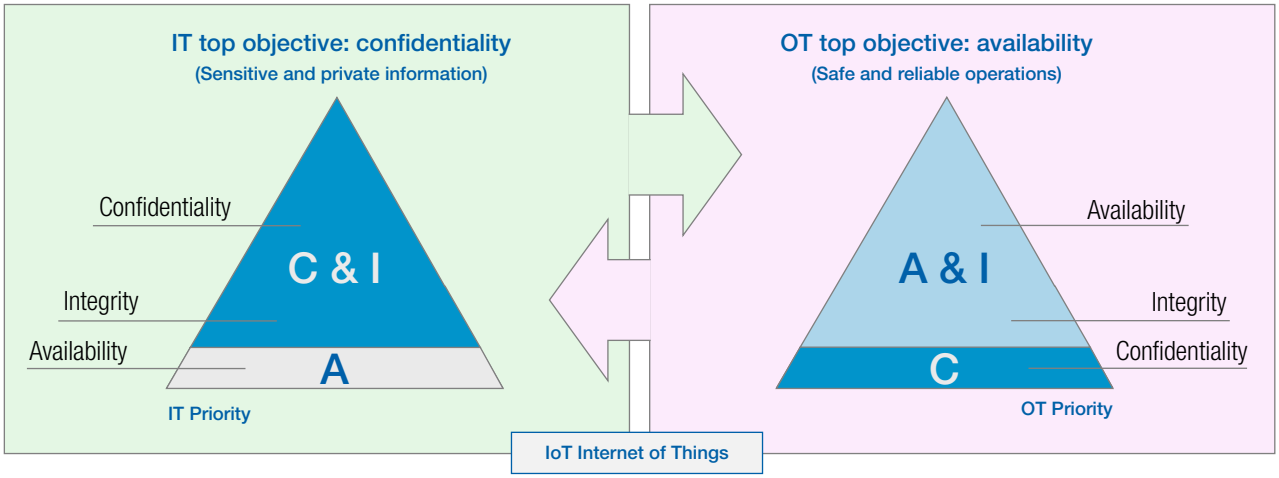

Figure 4 | Example of the different priorities of IT and OT primary security objectives

Section 4

Risk assessment, risk mitigation and risk life cycle processes

Risk assessment, risk mitigation, and life cycle continuous update of processes are fundamental methodologies for providing security. Using business requirements (financial, brand, operation, societal) as inputs, thanks to proven methodologies defined in international standards that are applicable for OT environments, organizations can determine security risk exposure, select and apply appropriate security measures, follow them closely and update them when needed, in a continuous improvement process.

Risk assessment involves both objective and subjective analyses. There are many risk assessment methods and guidelines that can be used to identify the risks in the OT environment. The choice of which risk assessment method to apply to different situations and environments could be quite challenging, depending on different constraints in different organizations, such as national regulations, time constraints, and executive directives.

There is no single or perfect way for mitigating risks. In the OT environment, the principles chosen for addressing risk mitigation must absolutely integrate the operational constraints of the systems in order to take into account personal safety, to provide protection of physical assets, and to ensure the required performance of these systems.

For the best risk assessment process, it is key to integrate the experts of each utility domain directly as part of the cyber security team, not only as contributors to risk mitigation methods, but also as contributors to risk assessment life cycle updates.

A risk can be described as a combination of the consequences that would follow from the occurrence of an unwanted event and the likelihood of the occurrence of the event.

- Consequences may include safety, financial, environmental, societal, etc. of an event (e.g. failed process, loss of information, personnel harm)
- Risks should be identified, quantified or qualitatively described, and prioritized against risk criteria and objectives relevant to the organization

Risk assessment should identify, quantify, and prioritize risks against criteria for risk acceptance and objectives relevant to the organization. The results should guide and determine the appropriate management action and priorities for managing information security risks and for implementing controls selected to protect against these risks. Risk assessment should include:

- The systematic approach of estimating the magnitude of risks (risk analysis); and
- The process of comparing the estimated risks against risk criteria to determine the significance of the risks (risk evaluation)

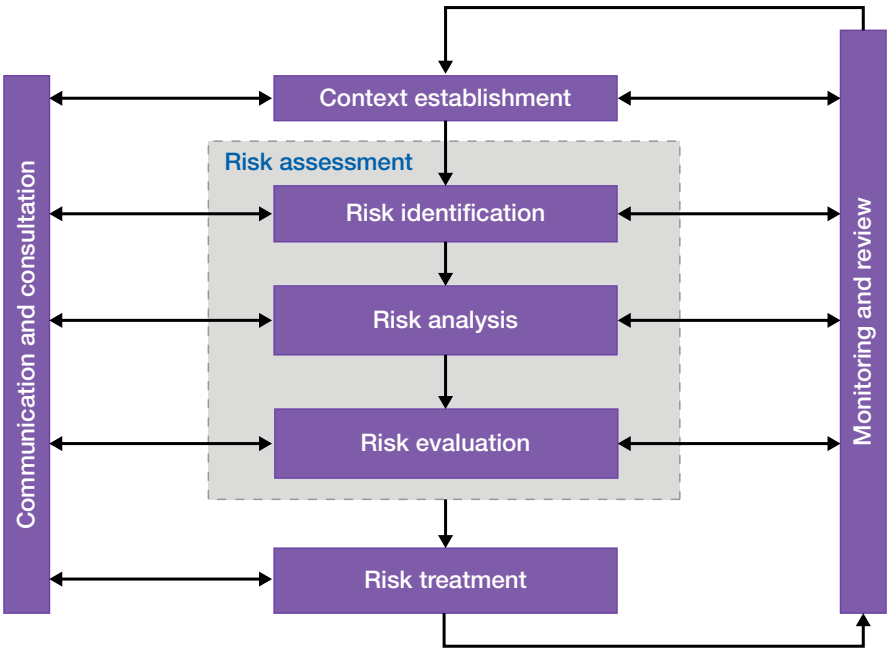

Figure 5 | Risk management process (ISO/IEC 27005:2018)

Figure 5 illustrates the general risk management process, while the key steps of any risk assessment method include:

- Collect the high-level business and regulatory requirements that apply to the OT environment, and identify the impacts (safety, economics, operational) if the requirements are not met
- Choose the risk assessment method, based on organizational requirements and constraints
- Choose the scope of the risk assessment to be performed, based on the boundaries of the targeted systems, including not only the systems internal to the boundaries, but also the interfaces with other OT and non-OT systems
- Threats can be associated with physical equipment, information, processes, interactions, configurations, and other assets
- Risk mitigation involves balancing the risk against the mitigation costs for reducing that risk to an acceptable level. Internal security policies must determine what are acceptable risks. Risk mitigation may involve an update to the risk assessment to ensure that the risks are indeed acceptable, particularly if many changes have been made as part of risk mitigation
- Apply security controls[7] to mitigate the risks that were identified:
  - Security control solutions may consist of organizational measures, processes, and/or technologies that are implemented in the systems
  - The efficacy of the security control solutions could be assessed to determine if they have actually mitigated the risk acceptably

7 Control (from ISO/IEC 27000:2018): measure that is modifying risk. Note 1 to entry: Controls include any process, policy device, practice, or other actions which modify risk. Note 2 to entry: It is possible that controls not always exert the intended or assumed modifying effect.

  - These security control solutions could include both cyber security measures as well as power engineering measures (procedures, technologies, and/or real-time operations)
- Once the risk assessment has been completed and the risk mitigation control solutions have been selected, these solutions are implemented on the systems
  - Verify over time that the applied controls have been applied correctly and really provide the expected mitigations
  - Include an assurance process, such as an audit, possibly by a different group
- Determine what actual control implementations (i.e. which specific procedures and/or technologies and/or commercial products) should be applied for each type of security control
  - Some security control solutions may not be able to be implemented in some systems, particularly for legacy systems (e.g. anti-virus applications or secure patching procedures)
  - Constraints on these control solutions should be identified, given the variety of issues associated with diverse OT environments, such as different constraints in a substation environment (long times between the ability to patch systems) or a DER environment (poor on-site security knowledge)
- Over time, all of these control solutions should be monitored to ensure that they are continuing to be effective or if possible attacks have potentially overcome the control solutions
  - In all cases, possible security events identified by this monitoring should be sent to a central CERT site
  - The CERT should be capable of filtering and assessing the importance of any security event or sequence of security events

Section 5

Cyber security standards and best practices

Given the complexity of business processes and the wide variety of cyber assets used in the smart energy environment, no existing single cyber security standard can address all security requirements, security controls, resilience strategies, and technologies. Some standards and guidelines are focused on the high level organizational security requirements and more detailed recommended controls (what), while other standards focus on the technologies that can be used to supply these cyber security controls through validated techniques and with a focus on interoperability (how).

While many additional documents and regulations are applicable to national and local regions, the key IEC, ISO, IEEE, NIST, and IETF cyber security standards and best practices are illustrated in Figure 6, organized by type (what, how, process towards compliance) and by level (high general level, high energy-specific level, detailed technical level).

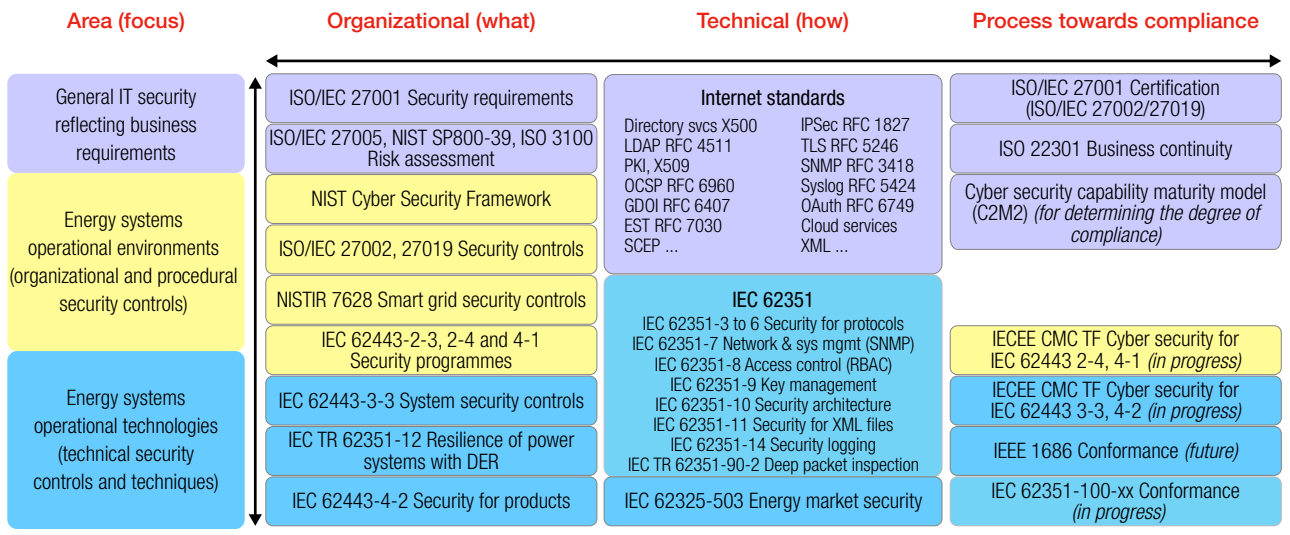

Figure 6 | Key cyber security standards and guidelines

Section 6

Conclusions

As cyber security has become an increasingly vital requirement for any business to survive in an increasingly automated environment, corporate executives must become cognizant of the key security and resilience characteristics of their business since the security culture must start from the top of an organization. Security policies, security procedures, and security technologies can only be effective if security and resilience is seen as critical by top management and is promulgated down to all levels. This requirement is particularly important for businesses that are deemed critical infrastructures, particularly those in the energy operational environment.

Five concepts for cyber security are critical for executives in the energy operational environment to understand as their businesses struggle to implement the necessary cyber security policies, procedures, and technologies.

Concept #1 Resilience should be the overall strategy for ensuring business continuity. When focusing on resilience in general, organizations must consider safety, security, and reliability of the processes and the delivery of their services. Resilience includes security measures that can mitigate impacts, not only before incidents (identify and prevent), but also during such incidents (detect and respond) and after incidents have been resolved (recover).

Concept #2 Security by design is the most cost-effective approach to security. Security is vital for all critical infrastructure and should be designed into systems and operations from the beginning, rather than being applied after the systems have been implemented. However, it is recognized that security cannot easily be added to legacy systems, so it is crucial that even for these existing systems, transitions to security-based designs should be managed by including security controls in all system retrofits and upgrades.

Concept #3 IT and OT are similar but different. Technologies in operational environments (called OT in this document) have many differing security constraints and requirements from information technologies (IT) environments. The primary reason is that energy systems are cyber-physical systems and security incidents can cause physical safety incidents and/or vital losses of energy. Therefore, availability, authentication, authorization, and data integrity of operational information are usually more critical requirements than confidentiality. Nonetheless, both IT and OT environments are increasingly relying on IoT technologies.

Concept #4 Risk assessment, risk mitigation, and continuous update of processes are fundamental to improving security. Based on an organization's business requirements, its security risk exposure must be determined (human safety, physical, functional, environmental, financial, societal, and reputational) for all its business processes. Risk assessment identifies the vulnerabilities of systems and processes to deliberate or inadvertent threats, determines the potential impacts of incidents, and estimates the likelihood that the incident scenarios could actually occur.

Concept #5 Cyber security standards and best practice guidelines for energy OT environments should be used to support the risk management process and establish security programmes and policies. Cyber security measures should not be re-invented: key cyber security standards and best practice guidelines have already been developed

for different areas and purposes of security. Cyber security planning should use these cyber security standards and guidelines to improve resilience, security, and interoperability throughout the energy OT environment, using the right standards, guidelines, and procedures for the right purposes at the right time.

Taking these 5 concepts into account, some key conclusions include:

- The executive level must take the lead on cyber security. Many cyber security issues must be addressed at the executive level, such as security policies, system architectures, personnel organization, security procedures, and types of security technologies:
  - In particular, security education and training programmes need to be developed, as well as policies on sharing security vulnerabilities, threats, and solution information with other corporations such as through CERTs
  - For example, just encrypting communications does not mean that the systems are secure: stolen or guessed passwords can still permit dangerous actions to be instigated in cyber-physical systems
- The existing cyber security standards and best practices related to security requirements and controls are quite mature and should be the start of any cyber security process. However, implementing the security procedures and technologies to meet the requirements of these existing standards may not be completely effective:
  - Cyber standards are regularly reviewed and updated to reflect new security issues and may not be available and/or complete
  - New technologies are always introducing new threats and/or vulnerabilities, for which new standards or guidelines need to be developed
  - Cyber hackers are always inventing new ways of exploiting vulnerabilities which can cause cyber incidents. Standards or guidelines may not have yet had time to address these new threats
  - Compliance with cyber security standards provide a large level of assurance, but this does not mean that the systems are necessarily completely secure, partly because the complexity of systems and their configurations may make it impossible to address all cyber issues, and partly because there will always be successful attacks
  - Cyber security standards can support the interoperability of these increasingly complex communicating systems, by defining validated and limited sets of security technologies and procedures
- Continuous monitoring and improvement of security measures is vital, given that technologies are always changing, new vulnerabilities are being found daily, and cyber hackers are always one step ahead of cyber security solutions

Annex A: Key Cyber Security Standards and Guidelines[8]

A.1 ISO/IEC 27000 Cyber Security Standards

A.1.1 ISO/IEC 27001 ISMS Family

The ISO/IEC 27000 series covers a wide range of cyber security requirements and guidelines, including those supporting the setting up of the ISO/IEC 27001 ISMS (*Information Security Management System*) which is covered in this Annex. This ISO/IEC 27001 family of standards has grown quickly over the last years as depicted in Figure 7 and Table 1.

ISO/IEC 27001 (with other standards in the family 27XXX) also provides the framework for 3rd party audits and certification of an organisation's ISMS. Organisations can have their information security management system certified against ISO/IEC 27001 by independent certification bodies that have to be accredited by a national accreditation body.

The ISMS family of standards consists of inter-related standards, already published or under development, and contains a number of significant structural components. These components are focused on:

- Standards describing ISMS requirements (ISO/IEC 27001);
- Certification body requirements (ISO/IEC 27006) for those certifying conformity with ISO/IEC 27001; and
- Additional requirement framework for sector-specific implementations of the ISMS (ISO/IEC 27009).

Other documents provide guidance for various aspects of an ISMS implementation, addressing a generic process as well as sector-specific guidance.

Relationships between the ISMS family of standards are illustrated in the following figure:

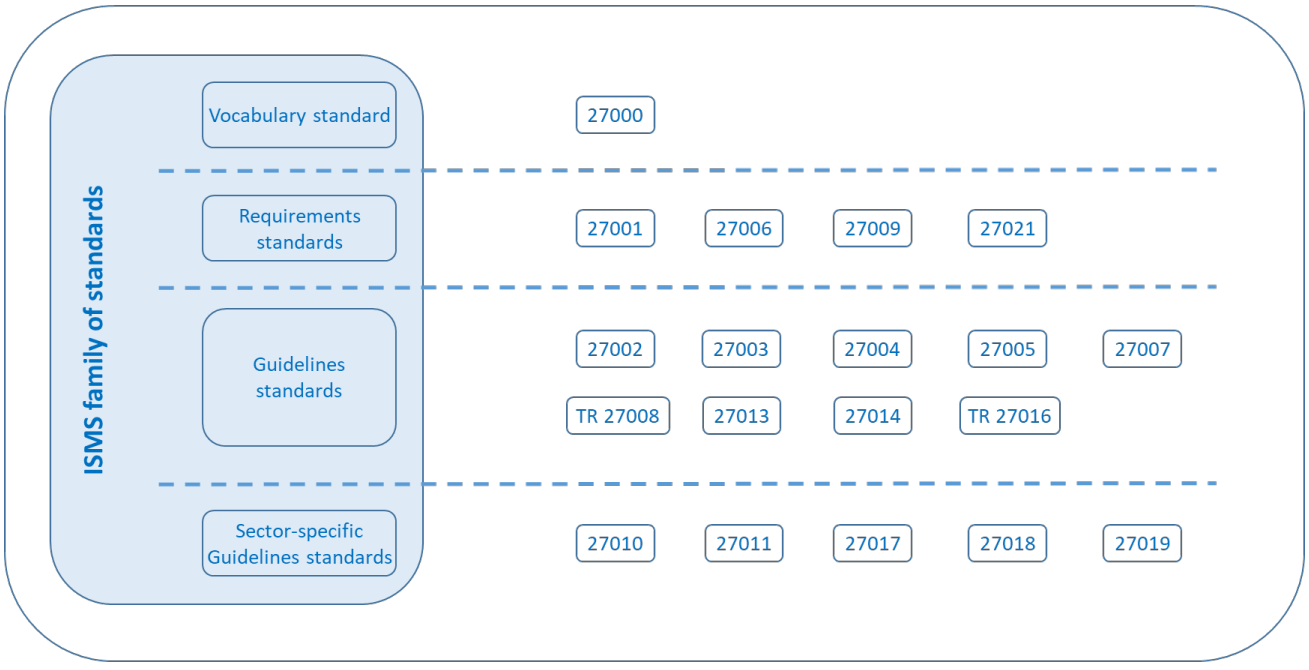

Figure 7: ISMS family of standards relationships

[8] This document references each standard only by its number, while understanding that some requirements in a standard may change over time as it is revised and republished. Actual revision dates may be found by going to the source organization.

Table 1: ISMS family of standards

Standard	Title	Type
ISO/IEC 27000:2018	Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary	Terminology
ISO/IEC 27001:2013	Information technology -- Security techniques -- Information security management systems -- Requirements	Requirements
ISO/IEC 27006:2015	Information technology -- Security techniques -- Requirements for bodies providing audit and certification of information security management systems	
ISO/IEC 27009: 2016	Information technology -- Security techniques -- Sector-specific application of ISO/IEC 27001 -- Requirements	
ISO/IEC 27021:2017	Information technology -- Security techniques -- Sector-specific application of ISO/IEC 27001 -- Requirements	
ISO/IEC 27002:2013	Information technology -- Security techniques -- Code of practice for information security controls	Guidelines
ISO/IEC 27003:2017	Information technology -- Security techniques -- Information security management systems -- Guidance	
ISO/IEC 27004:2016	Information technology -- Security techniques -- Information security management -- Monitoring, measurement, analysis and evaluation	
ISO/IEC 27005:2018	Information technology -- Security techniques -- Information security risk management	
ISO/IEC 27007:2017	Information technology -- Security techniques -- Guidelines for information security management systems auditing	
ISO/IEC TS 27008:2019	Information technology -- Security techniques -- Guidelines for the assessment of information security controls	
ISO/IEC 27013:2015	Information technology -- Security techniques -- Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1	
ISO/IEC 27014:2013	Information technology -- Security techniques -- Governance of information security	
ISO/IEC TR 27016:2014	Information technology -- Security techniques -- Information security management -- Organizational economics	
ISO/IEC 27010:2015	Information technology -- Security techniques -- Information security management for inter-sector and inter-organizational communications	Sector-specific guidelines
ISO/IEC 27011:2016	Information technology -- Security techniques -- Code of practice for Information security controls based on ISO/IEC 27002 for telecommunications organizations	
ISO/IEC 27017: 2015	Information technology -- Security techniques -- Code of practice for information security controls based on ISO/IEC 27002 for cloud services	
ISO/IEC 27018:2019	Information technology -- Security techniques -- Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors	
ISO/IEC 27019:2017	Information technology -- Security techniques -- Information security controls for the energy utility industry	

For the Smart Grid, the most relevant standards for the implementation of an ISMS are ISO/IEC 27001, ISO/IEC 27002, and ISO/IEC 27019. These standards are presented in the following sections.

A.1.2 ISO/IEC 27001

ISO/IEC 27001 is a worldwide recognized standard providing requirements for the setting up of an information security management system (ISMS). An ISMS is described as "*a systematic approach for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an organization's information security to achieve business objectives. It is based on a risk assessment and the organization's risk acceptance levels designed to effectively treat and manage risks*"[9].

The following steps needs to be applied and continually repeated to establish, monitor, maintain and improve an ISMS:

a) identify information assets and their associated information security requirements, while considering legal, regulatory, and contractual requirements;

b) assess information security risks and treat information security risks including:
   - a risk analysis and risks evaluation ;
   - the application of appropriate controls and risks acceptance;

c) Select and implement relevant controls to manage unacceptable risks.
   - Controls can be selected from ISO/IEC 27002 and all ISO/IEC 27002 sector-specific standards, e.g. ISO/IEC 27019 for the energy sector;

d) Monitor, maintain and improve the effectiveness of controls associated with the organization's information assets.

A.1.3 ISO/IEC 27002:2013

ISO/IEC 27002 is a code of practice - a generic set of controls addressing information security control objectives to mitigate security risks impacting for example the confidentiality, integrity and availability of information.

ISO/IEC 27002 security controls are organized within the following main clauses:

- Organization of information security
- Human resource security
- Asset management
- Access control
- Cryptography
- Physical and environmental security
- Operations security
- Communications security
- System acquisition, development and maintenance
- Supplier relationships
- Information security incident management

[9] ISO/IEC 27000:2018 " Information technology — Security techniques — Information security management systems — Overview and vocabulary"

- Compliance

A.1.4 ISO/IEC 27019:2017

ISO/IEC 27019 provides guiding principles based on ISO/IEC 27002 for information security management applied to process control systems as used in the energy utility industry. The aim of ISO/IEC 27019 is to extend the ISO/IEC 27000 set of standards to the domain of process control systems and automation technology. This allows the energy utility industry to implement a standardised information security management system (ISMS) in accordance with ISO/IEC 27001 that extends from the business to the process control level.

The scope of ISO/IEC 27019 covers process control systems used by the energy utility industry for controlling and monitoring the generation, transmission, storage and distribution of electric power, gas and heat in combination with the control of supporting processes. This includes in particular the following systems, applications and components:

- The overall IT-supported central and distributed process control, monitoring and automation technology as well as it systems used for their operation, such as programming and parameterisation devices;
- Digital controllers and automation components such as control and field devices or PLCs, including digital sensor and actuator elements;
- All further supporting it systems used in the process control domain, e.g. for supplementary data visualisation tasks and for controlling, monitoring, data archiving and documentation purposes;
- The overall communications technology used in the process control domain, e.g. networks, telemetry, telecontrol applications and remote control technology;
- Digital metering and measurement devices, e.g. For measuring energy consumption, generation or emission values;
- Digital protection and safety systems, e.g. protection relays or safety PLCs;
- Distributed components of future smart grid environments;
- All software, firmware and applications installed on above mentioned systems.

A.2 NIST Cybersecurity Framework

The NIST Cybersecurity Framework provides a policy framework of computer security guidance for how organizations can assess and improve their ability to identify their cyber assets, prevent security events where possible, detect security events as they inevitably occur, respond to and cope with security events even while they are impacting system functions, and ultimately recover from such security events. Figure 8 provides a useful diagram of the framework, while the following paragraphs identify the key framework aspects.

Identify: "Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities."

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
PR	Protect	PR.AC	Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

Figure 8: NIST Framework for Improving Critical Infrastructure Cyber security (2017)

- Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.
- Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.
- Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.
- Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.
- Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.

Protect: "Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services."

- Access Control (PR.AC): Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.
- Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.
- Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.
- Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.
- Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components is performed consistent with policies and procedures.
- Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.

Detect: "Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event."

- Anomalies and Events (DE.AE): Anomalous activity is detected in a timely manner and the potential impact of events is understood.
- Security Continuous Monitoring (DE.CM): The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.
- Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events.

Respond: "Develop and implement the appropriate activities to take action regarding a detected cybersecurity event."

- Response Planning (RS.RP): Response processes and procedures are executed and maintained, to ensure timely response to detected cybersecurity events.
- Communications (RS.CO): Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies.
- Analysis (RS.AN): Analysis is conducted to ensure adequate response and support recovery activities.
- Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident.
- Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.

Recover: "Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event."

- Recovery Planning (RC.RP): Recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity events.
- Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.
- Communications (RC.CO): Restoration activities are coordinated with internal and external parties, such as coordinating centres, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors.

The benefit of using the NIST Framework allows for an organization to have a common language and systematic methodology for managing cyber security risk. The Core includes activities to be incorporated in a cyber security program that can be tailored to meet any organization's needs. The Framework is designed to complement, not replace, an organization's cyber security program and risk management processes. The Framework helps guide key decision points about risk management activities through the various levels of an organization from senior executives, to business and process level, and implementation and operations as well.

A.3 ISO 31000 and ISO 22301

A.3.1 ISO 31000 Risk Management – Principles and Guidelines

ISO 31000:2009 covers the principles and generic guidelines on risk management. ISO 31000 seeks to provide a universally recognized paradigm for practitioners and companies employing risk management processes to

replace the myriad of existing standards, methodologies and paradigms that differed between industries, subject matters and regions. Figure 9 illustrates this generic risk management process.

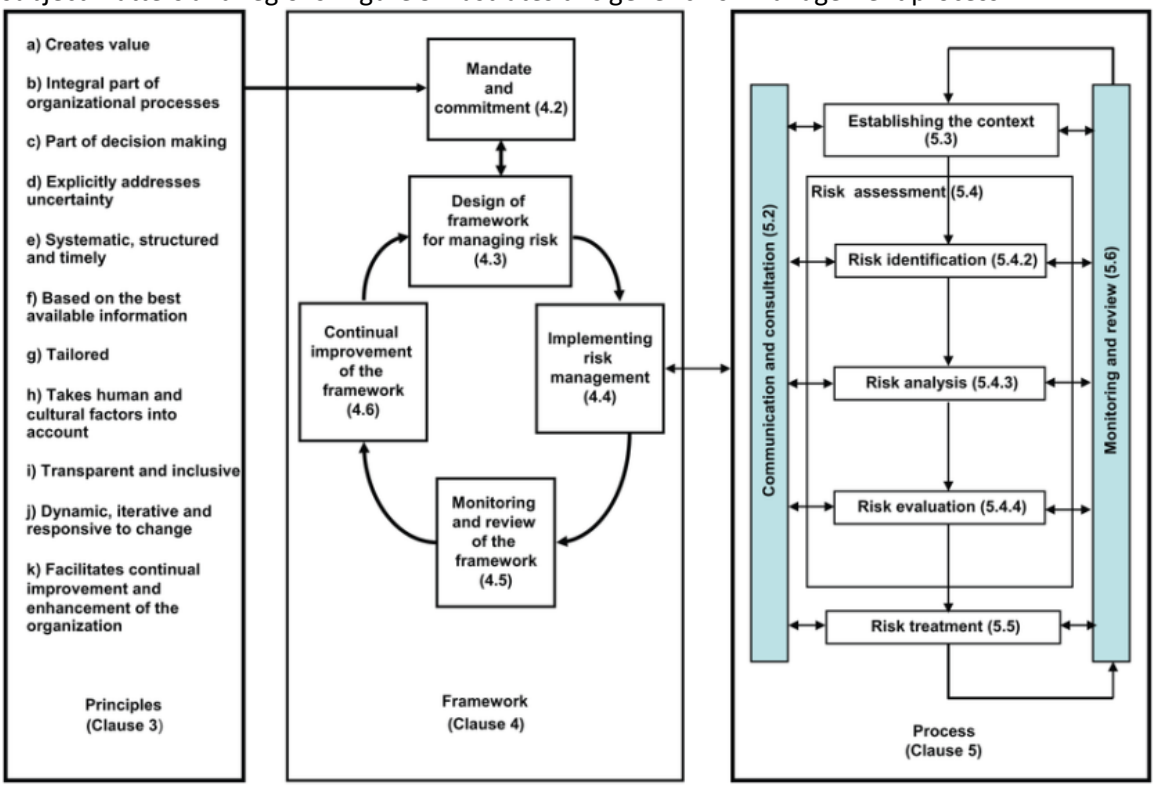

Figure 9: Risk management process (ISO 31000)

ISO 31000 is divided in:

- Scope
- Terms and definitions
- Principles
- Reference framework
- Process

ISO 31000 benefits:

- Improvement of operational efficiency and governance
- Increased credibility thanks to the application of international reference standards for efficient risk management
- Demonstration of the use of advanced risk management techniques and greater trust of customers and stakeholders
- Analysis and management of risks to minimize losses
- Better performance and flexibility of the management system
- Effective reaction to change in relation to business growth to achieve greater solidity

The 2018 version is more short and clear; following the changes:

- Review of the principles of risk management, considered key criteria for the effectiveness of the standard
- Greater attention to the leadership role of top management to ensure that risk management is integrated throughout the company
- More emphasis on the nature of risk management, based on new experiences, prior knowledge and analysis processes

- Streamlining content, paying more attention to maintaining an open model that regularly exchanges feedback with the external environment, to adapt to multiple needs and contexts

A.3.2 ISO 22301 - Business continuity management systems – Requirements

ISO 22301 is the normative standard to manage the business continuity of a company. It defines the security requirements to develop a documented management system to "Plan, Do, Check, and Act". Business continuity requires that this management system should be continuously monitored, maintained, and improved, with the focus on protecting the business from security incidents, reducing the possibility of their occurrence, providing answers when incidents do occur, and restoring the company's business to normal after such an incident. Figure 10 illustrates this business continuity model.

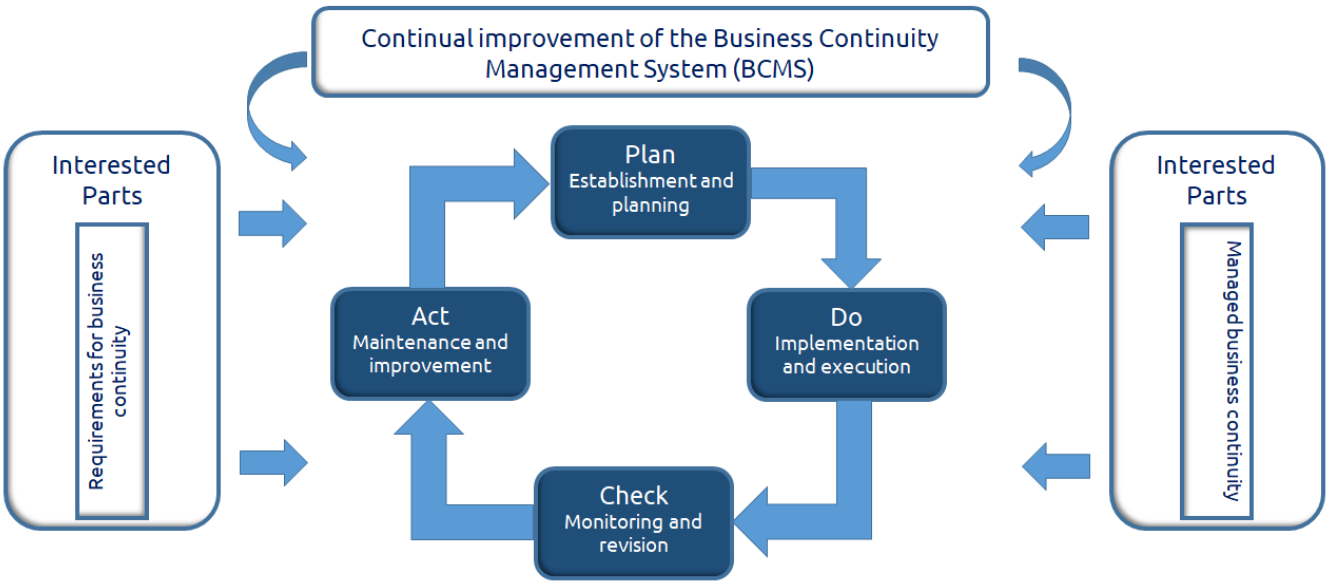

Figure 10: ISO 22301 PDCA (Plan-Do-Check-Act) model

ISO 22301 uses the 'ISO High Structure Level' schema and is divided in 10 chapters:

1. Scope
2. Normative references
3. Terms and definitions
4. Context
5. Leadership
6. Planning
7. Support
8. Operation
9. Performance evaluation
10. Improvement

For the company is recommended to execute some best practice and control action:

- Plan ordinary exchange from principal and disaster recovery SCADA system
- Plan an unexpected exchange from principal and disaster recovery SCADA system
- Plan a 'not plan' physical inspection to the various business continuity plan

A.4 NISTIR 7628 Guidelines for Smart Grid Cyber security (What)

A.4.1 NISTIR 7628 Cyber Security Controls

The NISTIR 7628 consists of guidelines intended primarily for addressing cyber security of Smart Grid systems and the constituent subsystems of hardware and software components. The NISTIR 7628 guidelines are very similar in scope to the ISO/IEC 27019 standard, except these guidelines focus exclusively on the Smart Grid sector. It defines approximately 300 high-level security controls, based on similar security controls in other NIST documents, including the NIST Framework (see Figure 11).

Ref.	NIST Smart Grid security requirements families
SG.AC	Access Control
SG.AT	Awareness and Training
SG.AU	Audit and Accountability
SG.CA	Security Assessment and Authorization
SG.CM	Configuration Management
SG.CP	Continuity of Operations
SG.IA	Identification and Authentication
SG.ID	Information and Document Management
SG.IR	Incident Response
SG.MA	Smart Grid Information System Development and Maintenance
SG.MP	Media Protection
SG.PE	Physical and Environmental Security
SG.PL	Planning
SG.PM	Security Program Management
SG.PS	Personnel Security
SG.RA	Risk Management and Assessment
SG.SA	Smart Grid Information System and Services Acquisition
SG.SC	Smart Grid Information System and Communication Protection
SG.SI	Smart Grid Information System and Information Integrity

Figure 11: NIST Smart Grid Security Requirements Families

A.4.2 NISTIR 7628 Cyber Security Logical Reference Model

These NISTIR 7628 guidelines also extend these cyber security controls beyond the general requirements. They describe a high-level logical interface reference model which defines 22 logical interface categories. These logical interface categories are characterized by the communication requirements and constraints between systems within and across Smart Grid domains, covering: operations, market operations, back office systems, substations, customer sites, DER, and other field equipment. For each of these logical interface categories, the appropriate high-level security requirements are also identified and annotated. Figure 12 shows the Logical Reference Model (sometimes referred to as “the Spaghetti Diagram” that illustrates the types of communication requirements and constraints associated with the Smart Grid.

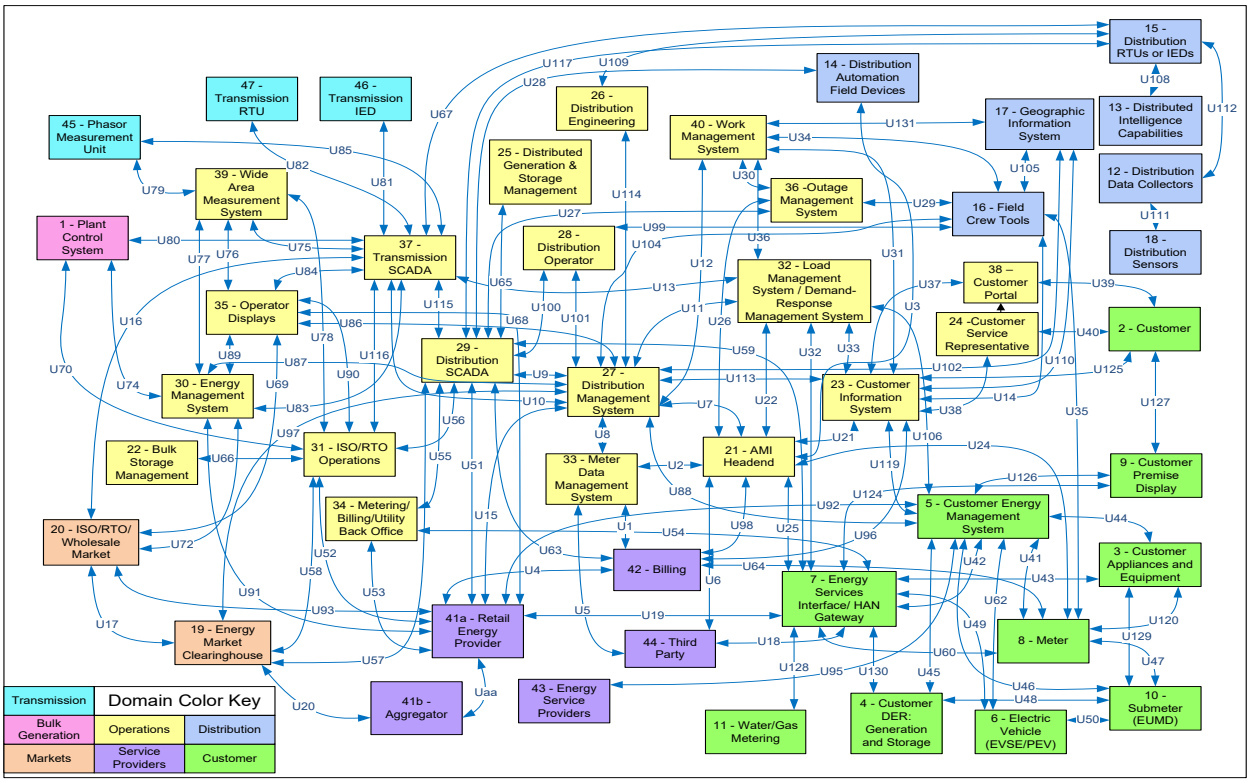

Figure 12: NISTIR 7628 “Spaghetti Diagram” High Level Logical Reference Model

A.5 IEC 62443 Series for Industrial Automation

A.5.1 IEC 62443 Background

The international series of standards IEC 62443 are being developed jointly by the International Electrotechnical Commission (IEC) and the ISA99 to address the need to design cybersecurity robustness and resilience into industrial automation and control systems (IACS), covering both organizational and technical aspects of security over the life cycle of systems. Although initially focused on industrial automation, this cyber security set of standards has also been adopted by the energy sector, since it provides a methodology for applying security in operational and field environments for cyber-physical systems. It can be used in conjunction with the ISO/IEC 27000 series (in particular with ISO/IEC 27019 for the energy domain) and with IEC 62351 which provides some security solutions.

A.5.2 IEC 62443 Organization

As shown in Figure 13, different parts of the standard are grouped into four clusters covering:

- General concepts, definitions and topics that are common to the series;
- Policies and procedures associated with IACS security including security program requirements for asset owners, and service and solution providers along with a methodology to evaluate the level of protection provided by an operational IACS;
- Technical requirements and risk assessment methodology for cybersecurity on system-wide level, and
- Requirements on the secure development lifecycle of system components, and the security requirements of such components at a technical level.

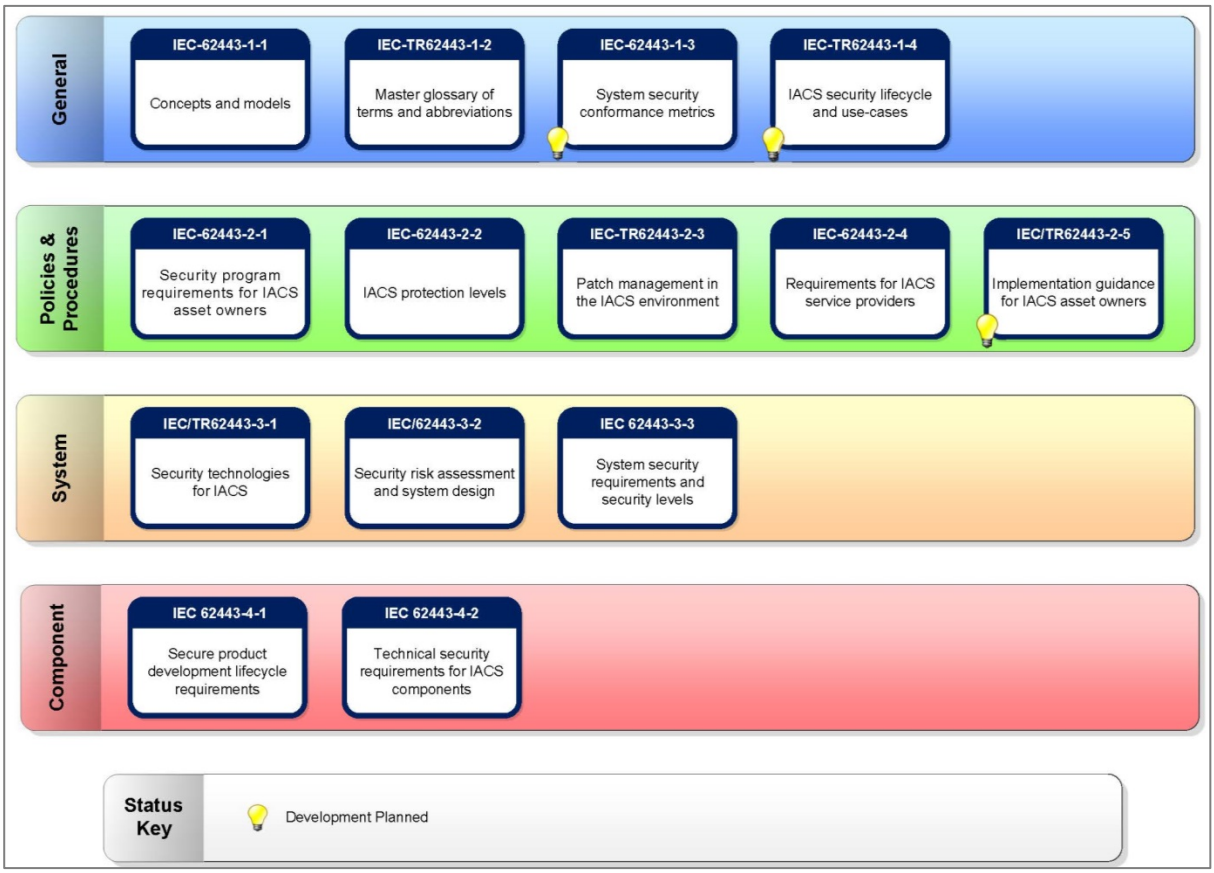

Figure 13: IEC 62443 Series of Industrial Security Standard – Overview (ISA99.org)

The different parts shown in Figure 13 are described briefly below.

- General parts:
  - IEC/TS 62443-1-1 defines the terminology, concepts and models for Industrial Automation and Control Systems (IACS) security, which are used throughout the series. In particular, seven foundation requirements (FRs) are defined: Identification and authentication control (FR1), Use control (FR2), System integrity (FR3), Data confidentiality (FR4), Restricted data flow (FR5), Timely response to events (FR6), and Resource availability (FR7).
  - IEC/TS 62443-1-2 includes the definition of terms and acronyms used in the IEC 62443 standards.
- Policies and Procedures related parts:
  - IEC 62443-2-1 specifies asset owner security program requirements for an industrial automation and control systems (IACS) and provides guidance on how to develop and evolve the security program. The elements of an IACS security program described in this standard define required security capabilities that apply to the secure operation of an IACS, and are mostly policy, procedure, practice and personnel related.
  - IEC/IS 62443-2-2 Ed.2 specifies a framework and methodology for evaluation of the protection of an IACS based on the notion of (technical) security level and the maturity of the connected processes. The concept of protection level is a security rating of the combination of technical and organizational measures and defines an indicator of the comprehensiveness of the security program.
  - IEC/TR 62443-2-3 defines the patch management in the IACS environment. Specifically, it provides a defined format for the exchange of information about security patches from asset owners to product suppliers, and a definition of some of the activities associated with the development of the

patch information by product suppliers and deployment of the patches by asset owners. The exchange format and activities are defined for use in security related patches; however it may also be applicable for non-security related patches or updates.

  - IEC 62443-2-4 specifies requirements for security capabilities for IACS service providers that they can offer to the asset owner during integration and maintenance activities of an Automation Solution. Some of these capabilities reference security measures defined in IEC 62443-3-3 that the service provider must ensure are supported in the Automation Solution.

- System related parts:
  - IEC/TR 62443-3-1 provides a current assessment of various cybersecurity tools, mitigation counter-measures, and technologies that may effectively apply to the modern electronically based IACSs regulating and monitoring numerous industries and critical infrastructures. It describes several categories of control system-centric cybersecurity technologies, the types of products available in those categories, the pros and cons of using those products in the automated IACS environments, relative to the expected threats and known cyber vulnerabilities, and, most important, the preliminary recommendations and guidance for using these cybersecurity technology products and/or countermeasures.
  - IEC 62443-3-2 establishes requirements for risk assessment in order to partition an IACS (as a system under consideration) into zones and conduits. A zone is a grouping of assets based on risk, while communications between zones is through so called “conduits”. Conduits may then be mapped to the logical network protocol communication between two zones. This document also establishes requirements for detailed risk assessments of each zone and conduit, and for assigning Security Level targets (SL-Ts) on threat and risk.
  - IEC 62443-3-3 provides detailed technical control system requirements (SRs) associated with the seven foundational requirements (FRs), including defining the requirements for control system capability security levels. These requirements are intended to be used, along with the defined zones and conduits for the system under consideration, for the definition of the appropriate security capabilities at the control system level.
- Component related parts
  - IEC 62443-4-1 specifies process requirements for the secure development of products used in industrial automation and control systems. It defines a secure development life-cycle for the purpose of developing and maintaining secure products.
  - IEC 62443-4-2 specifies the cyber security technical requirements for components, such as embedded devices, network components, host components and software applications. The requirements are derived from the system level requirements defined in IEC 62443-3-3.

Different types of roles are involved in the secure development, operation and support of an IACS. Figure 14 below gives an overview about these various roles and their interactions with the industrial automation and control systems.

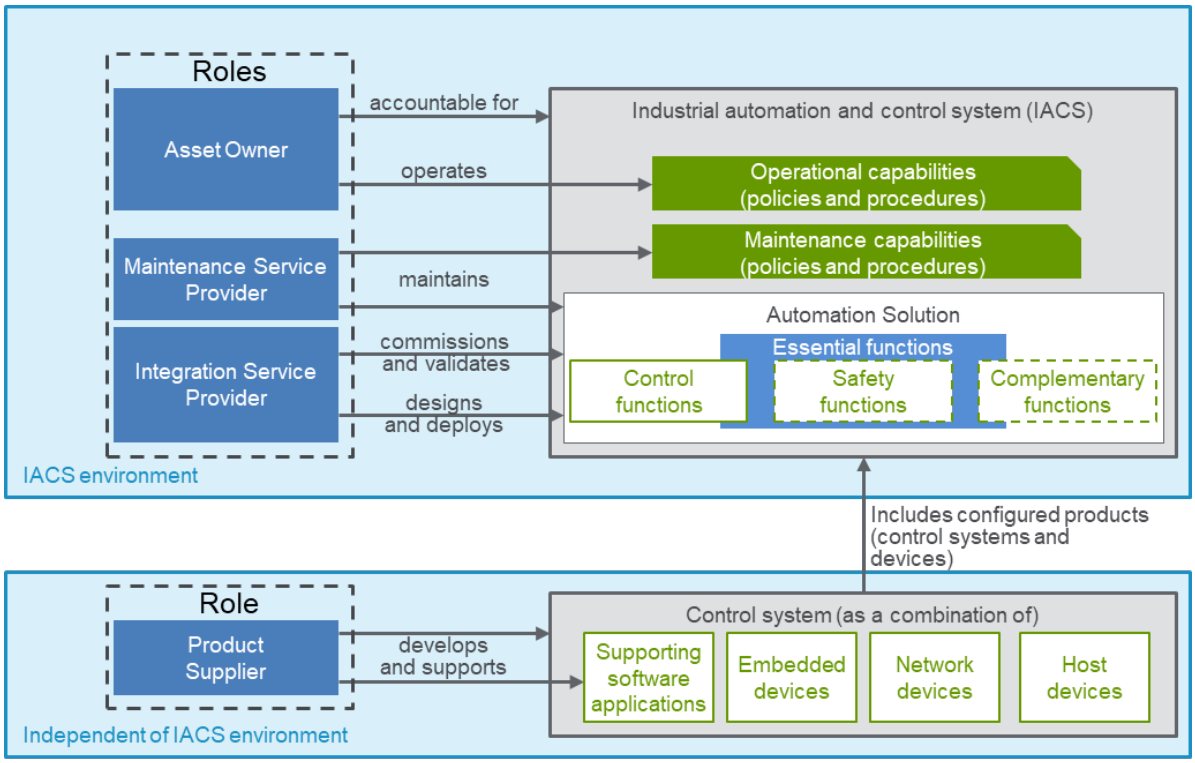

Figure 14: Application of IEC 62443 parts by different roles (ISA99.org[10])

A.5.3 IEC 62443-3-3 System Security Requirements and Assurance Levels

Although each part of IEC 62443 is important, IEC 62443-3-3 has become one of the most visible and utilized parts. It defines four security levels (SL1, SL2, SL3, SL4) (see Figure 15). These security levels correlate the required set of countermeasures with the strength of a potential adversary, in order to counter different levels of risk. To meet a specific SL, the defined requirements must be fulfilled. It does help to focus only on certain facets of security. The security requirements defined by IEC 62443-3-3 help to ensure that all relevant aspects are addressed.

4 Security Level (SL)	
SL 1	Protection against **casual or coincidental** violation
SL 2	Protection against **intentional violation** using **simple means** with low resources, generic skills and low motivation
SL 3	Protection against intentional violation using **sophisticated means** with **moderate resources**, IACS specific skills and moderate motivation
SL 4	Protection against intentional violation using sophisticated means with **extended resources**, IACS specific skills and high motivation

Figure 15: IEC 62443 Defined Security Levels

IEC 62443-3-3 also covers security requirements and is aligned with the concept of seven foundational requirements (FR) as defined in IEC 62443-1-1. The technical security requirements are grouped according to the FRs Identification and authentication control (FR1), Use control (FR2), System integrity (FR3), Data confidentiality (FR4), Restricted data flow (FR5), Timely response to events (FR6), and Resource availability (FR7). For each of the foundational requirements, there exist several concrete technical security requirements (SR) and requirement enhancements (RE) and these are assigned to the 4 security levels according to the level of threat mitigation provided. In the context of communication security, these security levels are specifically interesting for the “conduits” connecting different zones.

To reach a dedicated security level, the requirements (SR) and potential requirement enhancements (RE) defined for that security level have to be fulfilled. The standard foresees that a security requirement can be addressed either directly or by a compensating countermeasure. The concept of compensating

[10] Derived by ISA99 from IEC 62443-2-4 Ed1.1: 2017

countermeasures allows a certain security level to be reached even if some requirements cannot be implemented directly. For example, some components, particularly legacy equipment, cannot support the required technical features. This approach is in particular important for existing systems, so called “brown-field installations”, as existing equipment can be continued to be used for many years.

The security level of a zone or a conduit (a conduit connects zones) is more precisely a security level vector with seven elements (see also annex A of IEC 62443-3-3). The elements of the vector designate the security level for each foundational requirement. This allows defining the security level specific for each foundational requirement. If, e.g., confidentiality is not a security objective within a zone, the security level element corresponding to FR4 “Data confidentiality” can be defined to be SL1 or even none, although SL3 may be required for other foundational requirements (e.g., for FR1, FR2, and FR3). Hence, the resulting security level vector for a zone could be SL=(3,3,3,1,2,1,3) or SL=(2,2,2,0,1,1,0).

The recently approved IEC 62443-4-2 provides cyber security technical requirements for components types embedded devices, network components, host components and software applications. The requirements are derived from the system level requirements in IEC 62443-3-3.

The IECEE offers a conformance assessment program that intends to provide a framework for assessments in accordance with the IEC 62443 standards to result in IECEE Certificates of Conformity. The certificates provided by IECEE include capability certifications of IEC 62443-2-4 Process, Products and Solutions, and IEC 62443-4-1 for organization capabilities. The scheme also supports product certificates of conformity for control systems (IEC 62443-3-3) and components (IEC 62443-4-2), in each case, these certifications can optionally be provided in conjunction with IEC 62443-4-2, but also for products (see IEC 62443-4-1 and 62443-4-2).

A.6 IEC 62351 Cyber Security Series for the Smart Grid

A.6.1 IEC 62351 Overview

The IEC 62351 series of standards[11] include cyber security technologies for the communication protocols defined by the IEC TC 57, specifically the IEC 60870-5 series (including IEEE 1815 (DNP3) as a derivative standard), the IEC 60870-6 series, the IEC 61850 series, the IEC 61970 series, and the IEC 61968 series. As shown in Figure 16 there is not a one-to-one correlation between the IEC TC57 communication protocol standards and the IEC 62351 security standards. This is because many of the communication protocols rely on the same underlying standards at different layers.

The IEC 62351 series also defines the cyber security requirements for implementing security technologies in the operational environment, including objects for network and system management (e.g. with SNMP), role-based access control (RBAC), cryptographic key management, and security event logging.

Technical specifications for conformance testing, applicable for these standards, are also being developed as part of this series as IEC/TS 62351-100-xx.

IEC 62351 standards profile the use of existing Internet standards whenever possible to meet domain-specific needs. Reusing the same security standards across different communication protocols supports the interoperability of these protocols.

[11] More detailed information can be found on the public web site: http://iectc57.ucaiug.org/wg15public/default.aspx

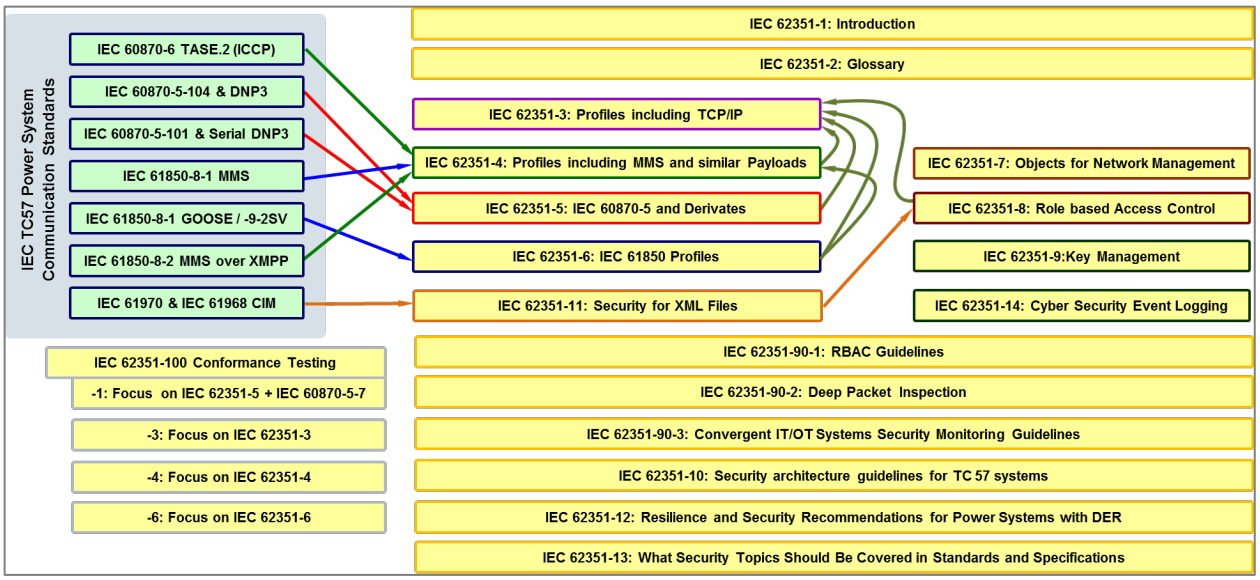

Figure 16: IEC 62351 series of cyber security standards

A.6.2 IEC 62351 Cyber Security Standards for Communication Standards

The following parts of the IEC 62351 cyber security standards series provide security for different communication protocol standards:

- IEC/TS 62351-1: Introduction: This first part of the standard covers the background on security for power system operations, and introductory information on the series of IEC 62351 security standards.
- IEC/TS 62351-2: Glossary of Terms: This part includes the definition of terms and acronyms used in the IEC 62351 standards. These definitions are based on existing security and communications industry standard definitions as much as possible, given that security terms are widely used in other industries as well as in the power system industry. The terms in this glossary are provided for free access on the IEC web site at http://std.iec.ch/terms/terms.nsf/ByPub?OpenView&Count=-1&RestrictToCategory=IEC%2062351-2
- IEC 62351-3: Data and Communication Security – Profiles Including TCP/IP. These security standards cover those profiles used by:
  - IEC 60870-6 (TASE.2 / ICCP)
  - IEC 60870-5 Part 104
  - IEEE 1815 (DNP 3) over TCP/IP
  - IEC 61850 over TCP/IP
- IEC 62351-4: Data and Communication Security – Profiles Including MMS and Similar Payloads. These security standards cover those profiles used by:
  - IEC 60870-6 (TASE.2 / ICCP) using MMS
  - IEC 61850-8-1 using the MMS profile of data objects
  - IEC 61850-8-2 using XML XSDs mapped from MMS data objects
- IEC 62351-5: Data and Communication Security – Security for IEC 60870-5 and Derivatives (i.e. DNP 3.0). These security standards cover both serial and networked profiles used by:
  - IEC 60870-5-7 (security details for IEC 60870-5-101 and 104)
  - IEEE 1815 (DNP 3)
- IEC 62351-6: Data and Communication Security – Security for IEC 61850 Peer-to-Peer Profiles. These security standards cover profiles in:
  - IEC 61850 that do not run over TCP/IP – GOOSE and SV

A.6.3 IEC 62351 Additional Cyber Security Standards and Technical Reports

Additional IEC 62351 cyber security standards provide requirements while technical reports (TR) provide guidelines for implementing security technologies:

- IEC 62351-7: Network and System Management (NSM) of the information infrastructure, which defines abstract NSM data objects for the power system operational environment and reflects what information is needed to manage the information infrastructure as reliably as the power system infrastructure is managed. A mapping to SNMP MIBs was also developed and is available as code components.
- IEC 62351-8: Role-Based Access Control for Power System Management. The purpose of this standard is to:
  - Introduce "subjects-roles-rights" as authorization concept (in ANSI INCITS 359-2004, referred to as "users-roles-permissions")
  - Promote role-based access control for the entire pyramid in power system management
  - Enable interoperability in the multi-vendor environment of the power industry
  - IEC 61850-90-19 is developing the RBAC requirements for IEC 61850.
- IEC 62351-9: Key Management. This standard specifies how to generate, distribute, revoke, and handle digital certificates and cryptographic keys to protect digital data and its communication. Included in the scope is the handling of asymmetric keys (e.g. private keys and X.509 certificates), as well as symmetric keys (e.g. session keys).
- IEC/TR 62351-10: Security Architecture. This technical report targets the description of security architecture guidelines for power systems based on essential security controls, i.e., on security-related components and functions and their interaction.
- IEC 62351-11: Security for XML Files. This standard defines the security requirements for exchanges of XML-based documents which are used for IEC 61970 as well as for some types of information exchanges in IEC 61850.
- IEC/TR 62351-12: Resilience for Power Systems with DER Systems. This technical report provides resiliency recommendations for engineering/operational strategies and cyber security techniques that are applied to Distributed Energy Resources (DER) systems. It covers the resilience requirements for the many different stakeholders of these dispersed cyber-physical generation and storage devices, with the goal of enhancing the safety, reliability, power quality, and other operational aspects of power systems, particularly those with high penetrations of DER systems.
- IEC/TR 62351-13: What Security Topics Should Be Covered in Standards and Specifications. This technical report provides guidelines whose purpose is to support the developers of standards with addressing cyber security at the appropriate level for their standard. This document provides suggestions on what security topics should be covered in standards and specifications that are to be used in the power industry, and was a major source of information for IEC Guide 120, "*Security Aspects - Guidelines for their Inclusion into Publications*".
- IEC 62351-14: Cyber Security Event Logging. This part of the IEC 62351 series specifies technical details for the implementation of security logs: communication, content and semantics.

A.6.4 IEC 62351 Technical Specifications for Conformance Testing

The IEC 62351 cyber security technical specifications for conformance testing are being developed and planned. They consist of the following:

- Part 100-1: Conformance Testing for Part 5
- Part 100-3: Conformance Testing for Part 3

- Part 100-4: MMS Conformance Testing for Part 4
- Part 100-6-1: 61850-8-1/9-2; 100-6-2: ICCP; 100-6-3: 61850-8-2 Conformance Testing for IEC 61850
- Part 100-7: Conformance testing for network management
- Part 100-8-1: RBAC; Part 100-8-2: RBAC for 61850 in 90-19
- Part 100-9: Conformance testing for key management
- Part 100-14: Conformance testing for Event Logging

A.7 IEC 62325-503 Cybersecurity for the Energy Market

The IEC 62325-503 is part of the IEC 62325 series dedicated to the energy market communications. This standard is called “MADES” (MArket Data Exchange Standard), and among its objectives: "The purpose of MADES is to create a secured message exchange standard based on standard communication protocols and utilising IT best practices for exchanging data over any TCP/IP communication network, in order to facilitate business-to-business (B2B) information exchanges as described in IEC 62325-351 and the IEC 62325-451 series."

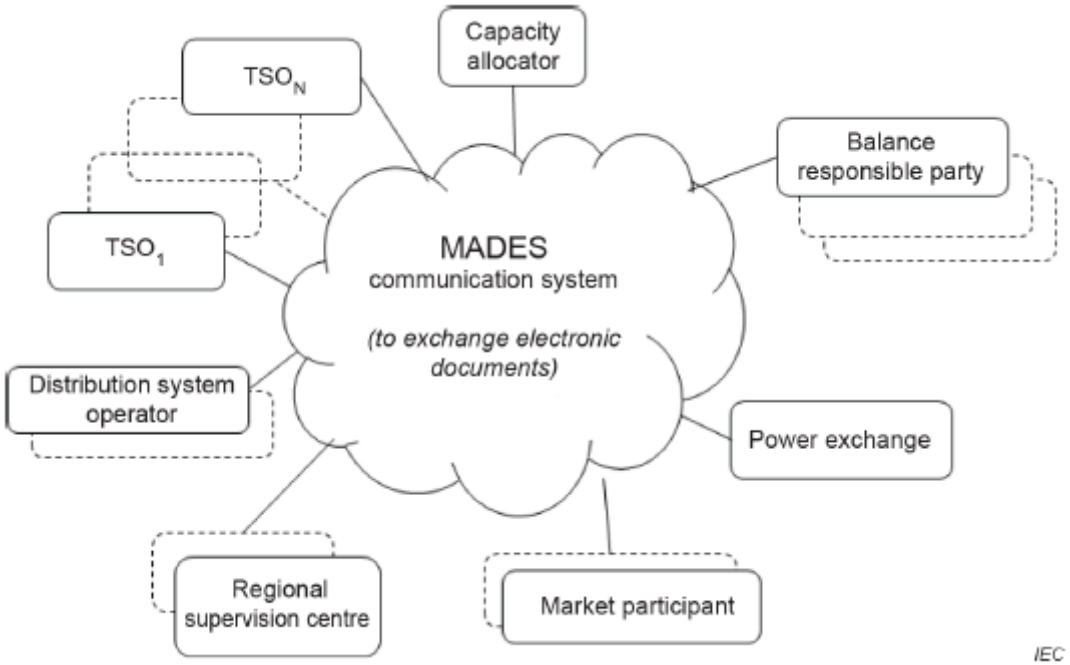

Figure 17: MADES overview (source: IEC 62325-503:2018)

As mentioned in IEC 62325-503, the goals of MADES security are:

- The security solution is transparent to applications – no specific implementation is required for an application to communicate securely.
- All communication channels are encrypted.
- Only the intended recipient can read a message.
- The recipient of a message can unambiguously identify the sender.
- Non-repudiation – A message together and its acknowledgement form an unambiguous proof that the sender sent the message and that the recipient received it.
- Rely on non-proprietary IT standards, including the Internet cyber security standards as applicable

A.8 Internet Cyber Security Standards

A.8.1 General

Many standards and de facto standards have been developed for the Internet over the last years. These Internet standards are often referenced by other standards or are used directly to provide security solutions. Although not immune from the need to upgrade over time, these Internet standards provide well-known and well-established techniques that improve the interoperability of systems and information flows.

These Internet standards can apply to many domains, including the Smart Grid. Examples of some of the Internet technologies are identified below and where they are used in some Smart Grid cyber security standards.

A.8.2 IETF standards

The Internet Engineering Task Force (IETF) is an open standards organization that develops "Request for Comments (RFC)" standards. In particular, the IETF is responsible for the Internet TCP/IP standards and the IP suite, and has defined the associated security standards. These security RFCs form the basis of many other standards, such as the IEC 62351 standards.

- **Transport Layer Security (TLS) (RFC 5246)** is a cryptographic protocol designed to provide communications security over a computer network. The TLS protocol aims primarily to provide privacy and data integrity between two or more communicating computer applications. Several versions of the protocol are currently in use in applications. It is referenced in a number of IEC 62443 and IEC 62351 standards, and is specifically the basis of IEC 62351-3.
- **Hypertext Transfer Protocol Secure (HTTPS) (RFC 2818)** is an extension of the Hypertext Transfer Protocol (HTTP). It is used for secure communication over a computer network, and is widely used on the Internet. In HTTPS, the communication protocol is encrypted using Transport Layer Security (TLS), or, formerly, its predecessor, Secure Sockets Layer (SSL). The protocol is therefore also often referred to as HTTP over TLS, or HTTP over SSL.
- **Simple Network Management Protocol (SNMP) (RFC 3418)** is a protocol for collecting and organizing information about managed devices on IP networks and for modifying that information to change device behaviour. Devices that typically support SNMP include cable modems, routers, switches, servers, workstations, printers, and other network devices. SNMP exposes this data in the form of variables on the managed systems organized in a management information base (MIB) which describe the system status and configuration. It provides the first mapping of utility-focused network devices in IEC 62351-7.
- **LDAP** (**Lightweight Directory Access Protocol) (RFC 4511)** is an open, vendor-neutral, industry standard application protocol for accessing and maintaining distributed directory information services over an Internet Protocol (IP) network. RFC 4513 includes the different authentication methods available to LDAP over TLS. It is based on a subset of the ITU's X-500 directory services, making it simpler to implement and use.
- **Online Certificate Status Protocol (OCSP) (RFC 6960)** is used for obtaining the revocation status of an X.509 digital certificate. It was created as an alternative to certificate revocation lists (CRL), specifically addressing certain problems associated with using CRLs in a public key infrastructure (PKI). It is referenced in a number of IEC 62443 and IEC 62351 standards.
- **Enrollment over Secure Transport (EST) (RFC 7030)** describes a simple, yet functional, certificate management protocol targeting Public Key Infrastructure (PKI) clients that need to acquire client certificates and associated Certification Authority (CA) certificates. It is referenced in IEC 62351-9.

- **Simple Certificate Enrollment Protocol (SCEP)** is an IETF draft. This protocol is used by numerous manufacturers of network equipment and software who are developing simplified means of handling certificates for large-scale implementation to everyday users, as well as being referenced in other industry standards. It is referenced in IEC 62351-9.
- **OAuth (RFC 6749)** is an open standard for access delegation, commonly used as a way for Internet users to grant websites or applications access to their information on other websites but without giving them the passwords. This mechanism is used by companies to permit the users to share information about their accounts with third party applications or websites. It is referenced in IEC 62351-8.
- **OAuth 2.0 (6750)** is the specification for Authorization Framework: Bearer Token Usage, which describes how to use bearer tokens in HTTP requests to access OAuth 2.0 protected resources. Any party in possession of a bearer token (a "bearer") can use it to get access to the associated resources (without demonstrating possession of a cryptographic key). To prevent misuse, bearer tokens need to be protected from disclosure in storage and in transport.
- **Group Domain of Interpretation (GDOI) (RFC 6407)** is a cryptographic protocol for group key management, as opposed to pairwise key management. The GDOI protocol is run between a group member and a "group controller/key server" (controller) and establishes a security association among two or more group members. It is referenced in IEC 62351-9.
- **Kerberos (RFC1510)** is a centralized server system designed for small, single-authority networks to provide “challenge/response” services based on a simple, secure “ticket” concept. Challenge/response authentication requires that the service requester, the IACS operator, and service provider know a “secret” code in advance. When service is requested, the service provider sends a random number or string as a challenge to the service requester. The service requester uses the secret code to generate a unique response for the service provider. If the response is as expected, it proves that the service requester has access to the “secret” without ever exposing the secret on the network. Since Kerberos tokens can become very large if the user is a member of a lot of groups, the devices will have to be able to support such large tokens. It is referenced as optional in some IEC 62443 and IEC 62351 standards.
- **Syslog (RFC 5424)** is a standard for message logging. It allows separation of the software that generates messages, the system that stores them, and the software that reports and analyses them. Each message is labelled with a facility code, indicating the software type generating the message, and assigned a severity level. It serves as the basis for IEC 62351-14.
- **Internet Protocol Security** (**IPsec) (RFC 1827)** is a secure network protocol suite that authenticates and encrypts the packets of data sent over an internet protocol network, including in virtual private networks (VPNs). IPsec includes protocols for establishing mutual authentication between agents at the beginning of a session and negotiation of cryptographic keys to use during the session. It is referenced in a few IEC 62443 and IEC 62351 standards.

A.8.3 ITU Standards

- **Directory Services X-500** is a series of computer networking standards covering electronic directory services, which was first developed in 1988. The primary concept of X.500 is that there is a single Directory Information Tree (DIT), a hierarchical organization of entries which are distributed across one or more servers, called Directory System Agents (DSA). Each entry in the directory has a unique “Distinguished Name” which is combined with associated parameters, including a unique IP address, which supports the lookup of a name to resolve it to an actual Internet location. LDAP (RFC 4511) is a simplified version of X-500 directory services, and most commonly used today. ISO/IEC 9594 is the corresponding ISO identification, which is referenced in IEC 62351-9.

- **X.509** is a standard defining the format of public key certificates. X.509 certificates are used in many Internet protocols, including TLS/SSL, which is the basis for HTTPS, the secure protocol for browsing the web. They are also used in offline applications, like electronic signatures. An X.509 certificate contains a public key and an identity (a hostname, or an organization, or an individual), and is either signed by a certificate authority or self-signed. When a certificate is signed by a trusted certificate authority, or validated by other means, someone holding that certificate can rely on the public key it contains to establish secure communications with another party, or validate documents digitally signed by the corresponding private key. It is referenced in some IEC 62443 and IEC 62351 standards.

A.8.4 W3C Standards

W3C defines standards for application in environments utilizing web technologies, including security related standards. Three standards are referenced here with direct relation to security and which are being utilized in power system automation. Note that there exist more security related specifications.

- XML Signature: specifies the syntax and handling rules for different forms of digitals signatures of XML documents. Signatures are used to provide integrity, message authentication, and/or signer authentication services. The document also defines if the signature is located within the XML structure or just represented as a reference. In power system security specifications this part is currently applied in the secure file exchange between different operators (IEC 62351-11). (https://www.w3.org/TR/xmldsig-core1/)
- XML Encryption: specifies the process for encrypting data and representing the result in XML. The data as such may have different formats such as octet streams and other unstructured data, or structured data formats. The result is an XML Encryption element that contains or references the cipher data. In power system security specifications this part is currently applied in the secure file exchange between different operators (IEC 62351-11). (https://www.w3.org/TR/xmlenc-core1/)
- XACML: eXtended Access Control Markup Language specifies an attribute-based security policy framework. It also covers the description of the underlying architecture and the processing description on the evaluation of access requests based on defined rules. In power system security specifications it is currently used in the context of describing roles as exchange format between different vendors' products. (http://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-cos01-en.html)

A.8.5 Combinations of Security Technologies

Some security technologies are a combination of policies, procedures, and technologies that are not standards themselves but are widely implemented, using various security standards.

- **Public Key Infrastructure (PKI)** is a set of roles, policies, and procedures needed to create, manage, distribute, use, store & revoke digital certificates and manage public-key encryption. The purpose of a PKI is to facilitate the secure electronic transfer of information for a range of network activities such as e-commerce, internet banking and confidential email. It is widely used while a number of standards and applications exist that implement its concepts, but PKI itself is not defined in a standard.
- **Cloud Services Security** refers to a broad set of policies, technologies, applications, and controls utilized to protect virtualized IP, data, applications, services, and the associated infrastructure of cloud computing. The cloud service providers typically provide their own security methods and technologies, although ISO/IEC 27017 and other guidelines address the primary security requirements.

A.8.6 Cryptographic Methods

The following cryptography methods are commonly specified. Normative references should be used in most cases to point to specific cryptographic requirements. More information on NIST cryptographic toolkit can be found at http://csrc.nist.gov/groups/ST/toolkit/index.html, while NIST SP 800-131A Rev 2 (March 2019) *Transitioning the Use of Cryptographic Algorithms and Key Lengths*".

- Cryptographic key pairs are secure because it is generally very difficult to derive one from the other, even though they are mathematically linked so that if one key encrypts a message, the other key can decrypt it.
  - RSA (Ron Rivest, Adi Shamir and Leonard Adleman) uses the fact that it is difficult to factor a large integer composed of two or more large prime factors.
  - ECC (elliptic curve cryptography) uses the fact that finding the discrete logarithm of a random elliptic curve element with respect to a publicly known base point is infeasible. ECC keys are becoming more popular because they can be smaller in length while still providing the same level of security as RSA keys.
- Encryption consists in combining a cryptographic key with a block of plain text using a well-designed algorithm. The most common block cipher algorithm is the Advanced Encryption Standard (AES), usually either AES-128 or AES-256 (the number being the block length in bytes). NIST has identified AES as the preferred block cipher. Neither DES nor Triple DES (3DES) should be specified anymore.
- Confidentiality (but not authentication) is provided by block cipher modes. Block ciphers only encrypt one block, so block cipher modes are used to string together the encryption of messages that are longer than one block while still using the same cryptographic key. The most common block cipher modes are cipher-block chaining (CBC) mode and counter (CTR) mode.
- Authentication and integrity may be provided by digital signatures and/or by "hashing" messages with cryptographic keys. These methods do not provide confidentiality – the messages can be read by anyone – but they do provide authentication of the sender and the ability to determine if the message has be tampered with. They require less "compute" processing than the block cipher modes.
  - Digital signatures algorithms include RSA-based signature schemes, such as RSA-PSS or RSA ANS x9.31, and DSA and its elliptic curve variant ECDSA, e.g. ECDSA ANS X9.62
  - The cryptographic hashing methods or "codes" are called Message Authentication Codes (MAC). To avoid some confusion with the term "Media Access Control (MAC)", they are sometimes called Message Integrity Codes (MIC). The most common MAC algorithms include the Keyed-Hash Message Authentication Code (HMAC), CBC-MAC (CMAC), and Galois/Counter Mode (GCM) and GMAC. These can be further specified as to which hashing ciphers and block sizes to use, such as HMAC-SHA256 or AES-GMAC-128.
  - Combinations of confidentiality and authentication modes are called authenticated encryption (AE). Examples of AE modes are CCM (NIST SP800-38C), GCM (NIST SP800-38D), CWC, EAX, IAPM, and OCB.
  - Certificates are issued by Certificate Authorities (CA) as a method for certifying the validated identity of a device or software application – the equivalent to a birth certificate or passport for a human. Most certificates use the ITU X.509 format for public key certificates, which bind a public key to the certified device or application, which contains (and guards) the corresponding secret key. Public Key Infrastructure (PKI) is the most commonly used method.

Annex B: Bibliography

- Transport Layer Security (TLS) (RFC 5246)
- Hypertext Transfer Protocol Secure (HTTPS) (RFC 2818)
- Simple Network Management Protocol (SNMP) (RFC 3418)
- LDAP (Lightweight Directory Access Protocol) (RFC 4511, 4513)
- Online Certificate Status Protocol (OCSP) (RFC 6960)
- Enrollment over Secure Transport (EST) (RFC 7030)
- Simple Certificate Enrollment Protocol (SCEP)
- OAuth (RFC 6749, 6750)
- Group Domain of Interpretation (GDOI) (RFC 6407)
- Kerberos (RFC1510)
- Syslog (RFC 5424)
- Internet Protocol Security (IPsec) (RFC 1827)
- Directory Services X-500
- X.509 format of public key certificates.
- IEC TS 62351-1, *Power systems management and associated information exchange – Data and communications security – Part 1: Communication network and system security – Introduction to security issues*
- IEC TS 62351-2, *Power systems management and associated information exchange – Data and communications security – Part 2: Glossary of terms*
- IEC 62351-3, *Power systems management and associated information exchange – Data and communications security – Part 3: Communication network and system security – Profiles including TCP/IP*
- IEC 62351-4, *Power systems management and associated information exchange – Data and communications security – Part 4: Profiles including MMS*
- IEC 62351-5, *Power systems management and associated information exchange – Data and communications security – Part 5: Security for IEC 60870-5 and derivatives*
- IEC 62351-6, *Power systems management and associated information exchange – Data and communications security – Part 6: Security for IEC 61850*
- IEC 62351-7, *Power systems management and associated information exchange – Data and communications security – Part 7: Network and system management (NSM) data object models*
- IEC 62351-8, *Power systems management and associated information exchange – Data and communications security – Part 8: Role-based access control*
- IEC 62351-9, *Power systems management and associated information exchange – Data and communications security – Part 9: Cyber security key management for power system equipment*
- IEC TR 62351-10, *Power systems management and associated information exchange – Data and communications security – Part 10: Security architecture guidelines*
- IEC 62351-11, *Power systems management and associated information exchange – Data and communications security – Part 11: Security for XML files*

- IEC TR 62351-12, *Power systems management and associated information exchange – Data and communications security – Part 12: Resilience and security recommendations for power systems with distributed energy resources (DER) cyber-physical systems*
- IEC/TS 62443-1-1
- IEC 62443-2-1
- IEC/IS 62443-2-2
- IEC/TR 62443-2-3
- IEC 62443-2-4
- IEC/TR 62443-3-1
- IEC 62443-3-2, Security for industrial automation and control systems – Part 3-2: Security risk assessment and system design
- IEC 62443-3-3, *Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels*
- IEC 62443-4-1, Security for industrial automation and control systems – Part 4-1: Secure product development life-cycle requirements
- IEC 62443-4-2
- NISTIR 7628, *Guidelines for Smart Grid Cybersecurity*
- ISO 31000, Risk Management
- ISO 22301, Business continuity management systems
- CEN-CENELEC-ETSI Smart Grid Coordination Group, "SG-CG/M490/H_Smart Grid Information Security", 2014-12

About the IEC

The IEC, headquartered in Geneva, Switzerland, is the world's leading publisher of international standards for electrical and electronic technologies. It is a global, independent, not-for-profit, membership organization (funded by membership fees and sales). The IEC includes 173 countries that represent 99% of world population and energy generation.

The IEC provides a worldwide, neutral and independent platform where 20 000 experts from the private and public sectors cooperate to develop state-of-the-art, globally relevant IEC International Standards. These form the basis for testing and certification, and support economic development, protecting people and the environment.

IEC work impacts around 20% of global trade (in value) and looks at aspects such as safety, interoperability, performance and other essential requirements for a vast range of technology areas, including energy, manufacturing, transportation, healthcare, homes, buildings or cities.

The IEC administers four conformity assessment systems and provides a standardized approach to the testing and certification of components, products, systems, as well as the competence of persons.

IEC work is essential for safety, quality and risk management. It helps make cities smarter, supports universal energy access and improves energy efficiency of devices and systems. It allows industry to consistently build better products, helps governments ensure long-term viability of infrastructure investments and reassures investors and insurers.

A global network of 173 countries that covers 99% of world population and electricity generation

Offers an affiliate country programme to encourage developing countries to get involved in the IEC free of charge

Develops international standards and runs four conformity assessment systems to verify that electronic and electrical products work safely and as they are intended to

IEC International Standards represent a global consensus of state-of-the-art know-how and expertise

A not-for-profit organization enabling global trade and universal electricity access

Key figures

173
members and affiliates

>200
technical committees

20 000
experts from industry, test and research labs, government, academia and consumer groups

10 000
international standards published

4
global conformity assessment systems

>1 million
conformity assessment certificates issued

>100
years of expertise

ISBN 978-2-8322-7544-3

CHF 50.-

International Electrotechnical Commission

3 rue de Varembé
PO Box 131
CH-1211 Geneva 20
Switzerland

T +41 22 919 0211
info@iec.ch
www.iec.ch

IEC TEC Cyber security:2019-10(en)