Securing the Power System Information Infrastructure

IEC 62351 Application Notes

Volume 1: General Security and Descriptions of the Parts of IEC 62351

Version 0.1

Date 2025-03-03

Contents

Table of Figures

Table of Tables

Document history

Any person intervening in the present document is invited to complete the table below before sending the document elsewhere. The purpose is to allow all actors to see all changes introduced and the intervening persons.

Any important message to IEC editors should also be included in the table below.

Name of intervening person	Date	Brief description of the changes introduced
S. Fries	03.02.2020	Initial version based on the split of the existing document into three volumes: 1. White Paper Update 2. From requirements (the what) to solutions (the how) 3. Application Examples of IEC 62351
F. Cleveland	20.12.2023	Editorial
F. Cleveland	6.11.2024	Editorial
S. Fries G. Pugni	9.1.2024	Updates
F. Cleveland	1.21.2025	Editorial

Executive Summary

IEC TC57 WG15, Data and communication security is tasked to build standards on data and communication security. In addition to developing those cybersecurity standards, the group has developed this set of Application Notes as overviews to our IEC 62351 series of cybersecurity standards (Volume 1) as well as general guides on cybersecurity (Volume 2) and use cases for implementing the IEC 62351 standards (Volume 3).

This Volume 1 document provides application notes for the cybersecurity standards (IEC 62351 [1]) to provide an overview of their scope, purposes, and how they may be combined as frameworks to meet specific scenarios and requirements. Examples are also included for utilizing specified IEC 62351 functionality to secure a power system communication infrastructure since this is their target domain. The goal is to show the contribution of different IEC 62351 parts in the setup and operation of power system automation.

Some of these cybersecurity standards focus on deployment environments which utilize IEC TC57 defined communication standards like the telecontrol protocols IEC 60870-5 [2] or the control protocol IEC 61850 [3] and the corresponding data models. However, these standards are not limited only to these deployment environments, and the IEC 62351 standards may be used in other similar environments.

As illustrated in Figure 1, IEC 62351 provides technical (how) security standards and does not address the organizational (what) requirements for security. It is expected that power systems as a critical infrastructure are operated in accordance with an information security management like ISO 27001 [4]. Specifically, for power systems, ISO 27019 [5] provides an augmentation of the cybersecurity controls defined in ISO 27002 [6] to address the needs for the power system domain. Other examples targeting a security framework are provided by the NIST Cyber Security Framework [7] or the NISTIR 7628 for Guidelines on Smart Grid Security Controls [9]. In addition to the operation, an integrator may leverage parts of the IEC 62443 series [10] to derive further security requirements for the overall system (by using the part 2-4 and part 3-3) in terms of technical security controls.

1 Introduction

1.1 Motivation for this document

This document provides application notes for the cybersecurity standards (IEC 62351 [1]) to provide an overview of their scope, purposes, and how they may be combined as frameworks to meet specific scenarios and requirements. Examples are also included for utilizing specified IEC 62351 functionality to secure a power system communication infrastructure since this is their target domain. The goal is to show the contribution of different IEC 62351 parts in the setup and operation of power system automation.

Some of these cybersecurity standards focus on deployment environments which utilize IEC TC57 defined communication standards like the telecontrol protocols IEC 60870-5 [2] or the control protocol IEC 61850 [3] and the corresponding data models. However, these standards are not limited only to these deployment environments, and the IEC 62351 standards may be used in other similar environments.

1.2 Security Impact for power systems as cyber-physical systems

Power systems are “cyber-physical” systems, since cyber actions can have physical impacts. This implies that security measures may have different levels of importance, depending upon these potential physical impacts. In particular in this Operational Technology (OT) environment, authentication, authorization, data integrity, and availability are usually seen as the more important security requirements. These are the technical security requirements that the IEC 62351 standards focus on.

Authentication: The term “secure power systems” relates to different aspects of operating a power system securely. One critical aspect is the protection and authentication of data as it is exchanged for the purpose of monitoring, control, and maintenance of power automation systems. Protection of data implies the use of cryptographic techniques, so a vital technical precondition is the secure distribution, secure storage, and secure application of cryptographic material by authorized entities. This cryptographic material, including cryptographic keys, secure storage, and cryptographic methodologies, can then be used to support bilateral and multilateral authentication.

Authorization: In addition to cryptographic techniques, authorization of access to data involves the secure establishment of which users and applications may access or issue controls to what equipment. This authorization, although protected by cryptographic means, must reflect security policies defined by organizations.

Data integrity: The integrity of data in power system automation is crucial to safe and secure operations. Confidentiality is usually of less importance except for sensitive or personal data, therefore cryptography in power system automation is usually focused more on detecting unauthorized modifications of data rather than protection of the information itself. Logging of security events, including unsuccessful attacks, is also crucial to future data integrity.

Availability: a particularly important security requirement for the power industry, typically must combine cryptography and engineering strategies. These strategies must be tightly intertwined to achieve the degree of availability desired, so events that may impact availability need to be made visible.

1.3 Role of IEC 62351 as technical (how) standards

Cybersecurity standards and guidelines can be categorized as “What” standards and “How” standards. “What” standards cover the overall cybersecurity requirements and include guides on potential security threats and the derivation of security requirements based on a risk-based approach for the power system domain.

The “How” standards, like the IEC 62351 series, focus on the detailed solutions for meeting the “What” requirements. As illustrated in Figure 1, IEC 62351 provides technical (how) security standards and does not address the organizational (what) requirements for security. It is expected that the reader is generally aware of security requirements and that the main interest lies in the application of IEC 62351 defined security features to address these security requirements.

It is expected that power systems as a critical infrastructure are operated in accordance with an information security management like ISO 27001 [4]. Specifically, for power systems, ISO 27019 [5] provides an augmentation of the cybersecurity controls defined in ISO 27002 [6] to address the needs for the power system domain. Other examples targeting a security framework are provided by the NIST Cyber Security Framework [7] or the NISTIR 7628 for Guidelines on Smart Grid Security Controls [9]. In addition to the operation, an integrator may leverage parts of the IEC 62443 series [10] to derive further security requirements for the overall system (by using the part 2-4 and part 3-3) in terms of technical security controls.

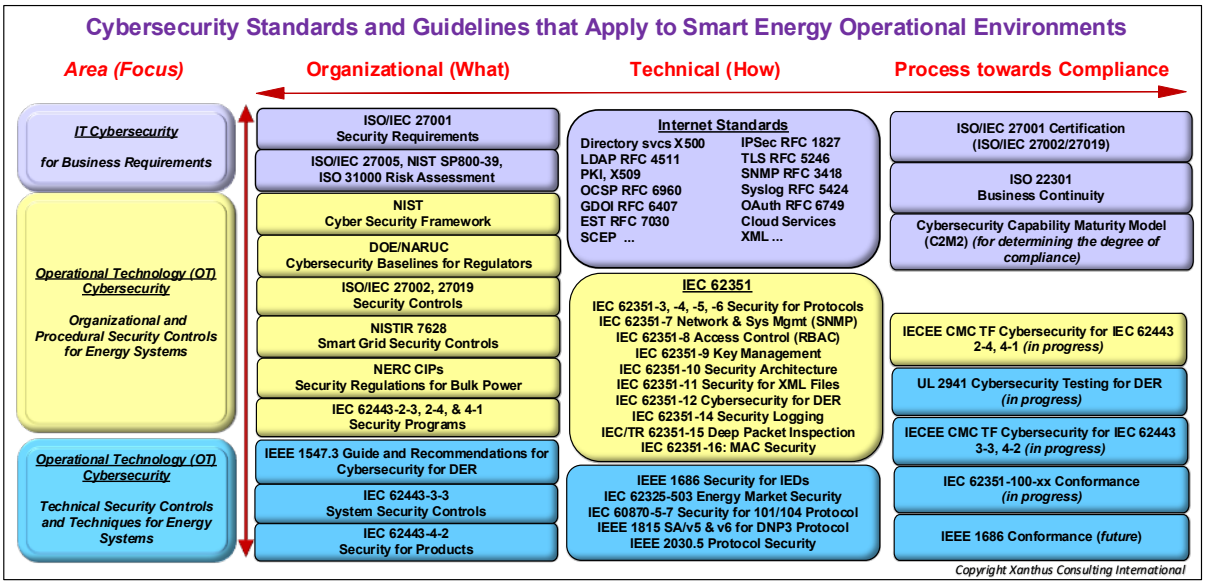

Figure 1: Cybersecurity standards and guidelines that apply to smart energy operational environments

IEC 62351 in this respect specifies the necessary technology to address the derived requirements and to realize dedicated security controls. Figure 2 shows the interplay of security requirements stemming from ISO/IEC 270xx series, the IEC 62443 frameworks and IEC 62351 as domain specific security standard.

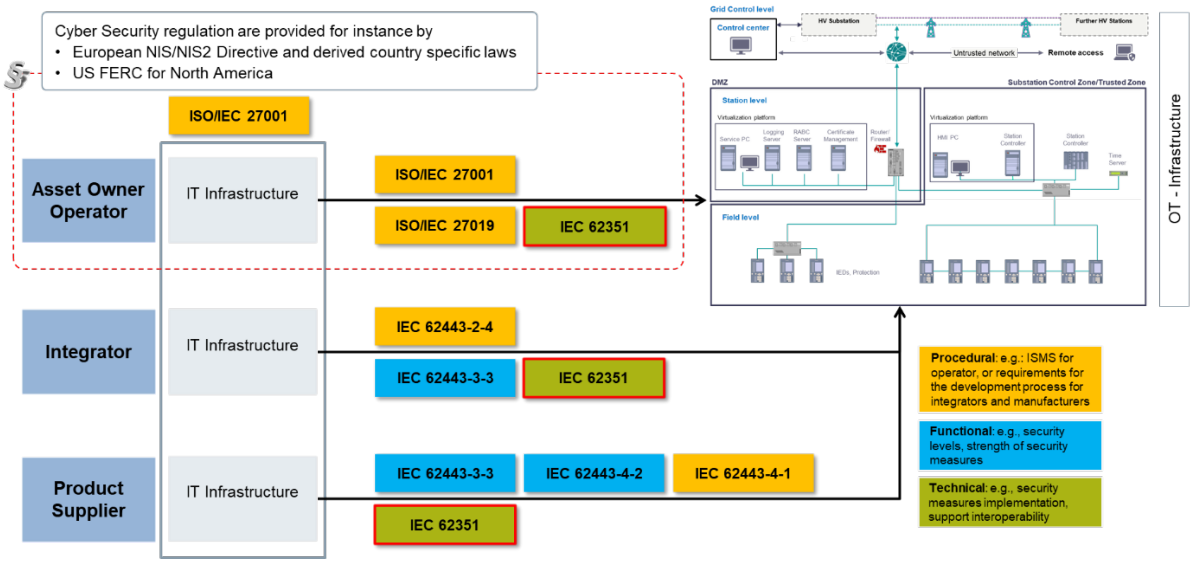

Figure 2: Interplay of Cybersecurity Standards

1.4 Document structure

The structure of this Volume 1 of the IEC 62351 Application Notes is as follows:

1. Clause 1 is an introduction to cybersecurity concepts and to the role of IEC 62351 standards.
2. Clause 2 covers some key security concepts.
3. Clause 3 provides an overview of the structure and current state of IEC 62351.
4. Clause 4 describes the IEC 62351 standards in more detail.

1.5 Target audience of this document

Target audience for this document are system architects, operators, integrators, and manufacturers of power automation system components, who are in charge of planning and operating components of the digital grid. Note that this document only provides an overview about the functionalities, but not sufficient technical detail necessary for an implementation. Moreover, the application examples in this document are only example use cases to show IEC 62351 security measure applicability in differing scenarios.

1.6 Terminology

For the purposes of this document, the terms and definitions of the following sources apply. ISO and IEC maintain terminological databases for use in standardization at the following addresses:

- IEC 62351-2: Glossary of terms
- IEC Electropedia: available at http://www.electropedia.org/
- ISO Online browsing platform: available at http://www.iso.org/obp

In addition, the following terms and definitions are used, which are:

- Bootstrapping of security credentials: provisioning of operational security parameters (e.g., operational security key material, access control information) in the target deployment environment. This is typically secured by procedural and/or technical means.
- Imprinting of security credentials refers to the provisioning of security parameters (e.g., identity information, security key material) during manufacturing. These credentials can be used to support a secure bootstrapping.

2 Security Concepts

2.1 Key security concepts for cyber-physical systems

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 concepts are illustrated in Figure 3[1] and captured in the box below.

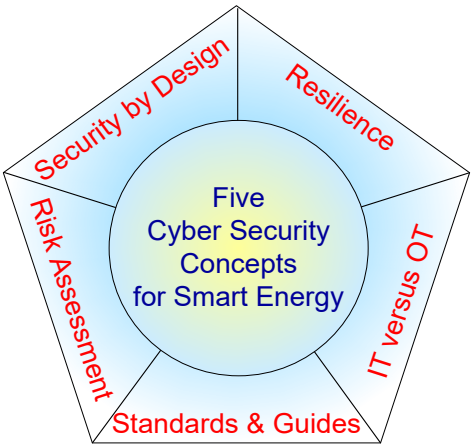

Figure 3: Five Cyber Security Concepts

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 & prevent), but also during such incidents (detect & 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 crucial as a part of resilience.

Concept #2. Security by Design is the most cost-effective approach to security: Security is vital for all critical infrastructures 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 setup from the beginning with security in mind. However, recognizing that security cannot easily be added to legacy 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

[1] All diagrams not otherwise noted, were developed by the CSTF members.

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 Informational Technologies (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. See Figure 4.

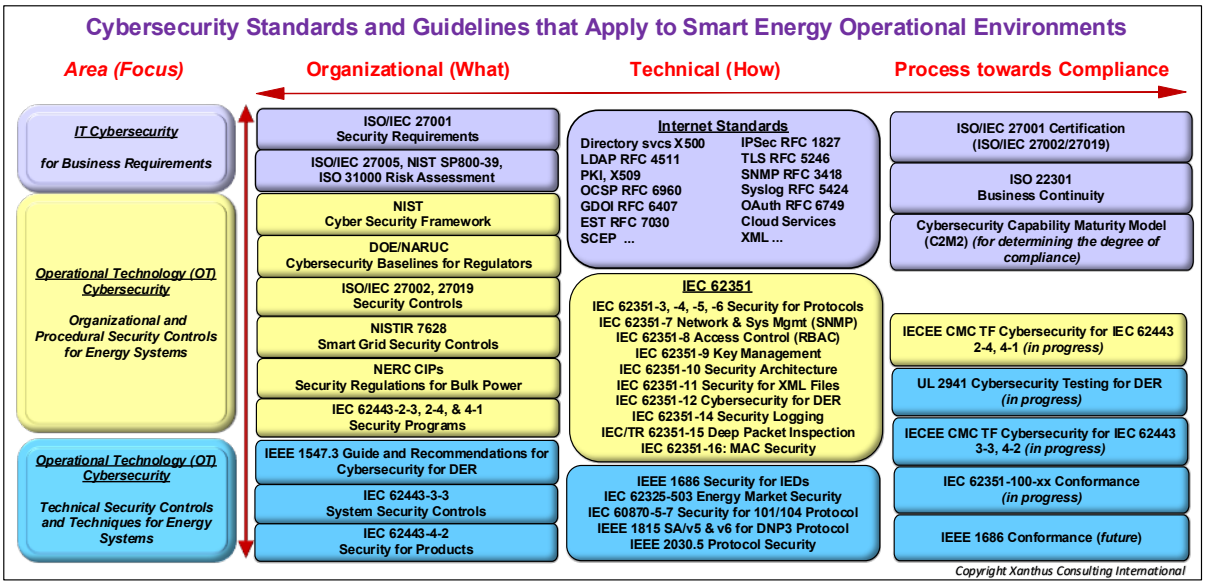

Figure 4: Concept #5: Use cybersecurity standards and guidelines

2.2 Security threats

Security entails a much larger scope than just the authentication of users and the encryption of communication protocols. End-to-end security involves security policies, access control mechanisms, key management, audit logs, and other critical infrastructure protection issues. It also entails securing the information infrastructure itself.

Security threats include:

- Inadvertent Threats
  - Safety Failures
  - Equipment Failures
  - Carelessness
  - Natural Disasters
- Deliberate Threats
  - Disgruntled Employee
  - Industrial Espionage
  - Vandalism
  - Cyber Hackers
  - Viruses and Worms
  - Theft
  - Terrorism

The key point is that the overall security of power system operations is threatened not only by deliberate acts of espionage or terrorism but by many other, sometimes deliberate, sometimes inadvertent threats that can ultimately have more devastating consequences than direct espionage.

2.3 Security purposes

The purposes for security protection are often described as 5 layers, with security measures addressing one or more of these layers:

- **Deterrence and delay**, to try to avoid attacks or at least delay them long enough for counter actions to be undertaken. This is the primary defense, but should not be viewed as the only defense.
- **Detection of attacks**, primarily those that were not deterred, but could include attempts at attacks. Detection is crucial to any other security measures since if an attack is not recognized, little can be done to prevent it. Intrusion detection capabilities can play a large role in this effort.
- **Assessment of attacks**, to determine the nature and severity of the attack. For instance, is the entry of a number of wrong passwords just someone forgetting or is it a deliberate attempt by an attacker to guess some likely passwords.
- **Communication and notification**, so that the appropriate authorities and/or computer systems can be made aware of the security attack in a timely manner. Network and system management can play a large role in this effort.
- **Response to attacks**, which includes actions by the appropriate authorities and computer systems to mitigate the effect of the attack in a timely manner. This response can then deter or delay a subsequent attack.

2.4 Security processes

Large and small utilities face substantial cybersecurity challenges that are both institutional and technical due to the following major changing business and technical environments:

- **Interactions with more stakeholders:** Utilities must exchange information with many other stakeholders, including other utilities, retail energy service providers, smart meters at customer sites, widely distributed small generation and storage systems, and many other businesses.
- **Network configurations:** Although sensitive operational systems are never supposed to be "directly connected with the Internet" or other unauthorized networks, sometimes they are indirectly connected through mis-configurations, handheld devices, and even thumb-drives.
- **Internet-based technologies:** Utilities increasingly use "open systems", Internet-based technologies, and general consumer products rather than their legacy, one-of-a-kind products. These modern technologies are less expensive and generally more interoperable, but are also more familiar to malicious threat agents who are able to access them and find the inevitable vulnerabilities.
- **Integration of legacy systems:** At the same time, the existing or "legacy" systems have to be integrated with these more modern systems, often through "gateways" and "wrapping" which lead to their own cybersecurity vulnerabilities.
- **Increased attraction of the power industry to cyber attackers:** The power industry, as a Critical Infrastructure that is vital to national security, is subject to the growing sophistication of cyber attackers and to the increasing desire of these cyber attackers to cause financial and/or physical harm the power industry.

2.5 Security planning

Security must be planned and designed into systems from the start. Security functions are integral to the designs of systems. Planning for security, in advance of deployment, will provide a more complete and cost-effective solution. Additionally, advanced planning will ensure that security services are supportable (may be cost prohibitive to retrofit into non-planned environments). This means that security needs to be addressed at all levels of the architecture.

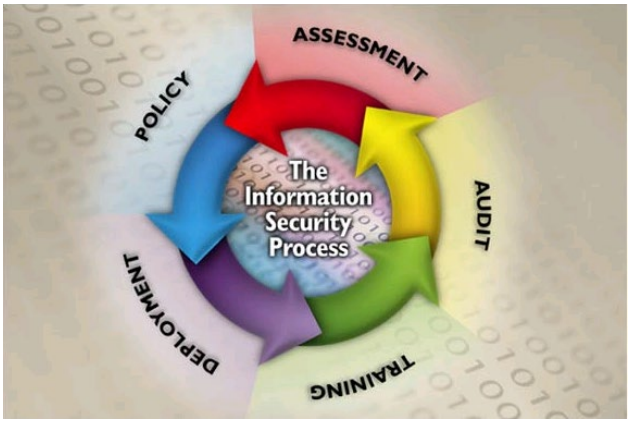

Figure 5: General Security Process – Continuous Cycle

As shown in Figure 5, security is an ever evolving process and is not static. It takes continual work and education to help the security processes keep up with the demands that will be placed on the systems. Security will continue to be a race between corporate security policies/security infrastructure and hostile entities. The security processes and systems will continue to evolve in the future. By definition there are no communication connected systems that are 100% secure. There will always be residual risks that must be taken into account and managed. Thus, in order to maintain security, constant vigilance and monitoring are needed as well as adaptation to changes in the overall environment.

The process depicts five high level processes that are needed as part of a robust security strategy. Although circular in nature, there is a definite order to the process:

- **Security Assessment** – Security assessment is the process of assessing assets for their security requirements, based on probable risks of attack, liability related to successful attacks, and costs for ameliorating the risks and liabilities. The recommendations stemming from the security requirements analysis leads to the creation of security policies, the procurement of security-related products and services, and the implementation of security procedures.
  - The implication of the circular process is that a security re-assessment is required periodically. The re-evaluation period needs to be prescribed for periodic review via policy. However, the policy needs to continuously evaluate the technological and political changes that may require immediate re-assessment.
- **Security Policy** – Security policy generation is the process of creating policies on managing, implementing, and deploying security within a Security Domain. The recommendations produced by security assessment are reviewed, and policies are developed to ensure that the security recommendations are implemented and maintained over time.
- **Security Deployment** – Security deployment is a combination of purchasing and installing security products and services as well as the implementation of the security policies and procedures developed during the security policy process. As part of the deployment aspect of the Security Policies, management procedures need to be implemented that allow intrusion detection and audit capabilities, to name a few.
- **Security Training** – Continuous training on security threats, security technologies, corporate and legal policies that impact security, Security measures analysis is a periodic, and best practices is needed. It is this training in the security process that will allow the security infrastructure to evolve.

- **Security Audit (Monitoring) –** Security audit is the process responsible for the detection of security attacks, detection of security breaches, and the performance assessment of the installed security infrastructure. However, the concept of an audit is typically applied to post-event/incursion. The Security Domain model, as with active security infrastructures, requires constant monitoring. Thus the audit process needs to be enhanced.

When attempting to evaluate the security process on an enterprise basis, it is impossible to account for all of the business entities, politics, and technological choices that could be chosen by the various entities that aggregate into the enterprise. Thus to discuss security on an enterprise level is often a daunting task that may never come to closure. In order to simplify the discussion, allow for various entities to control their own resources, and to enable the discussion to focus on the important aspects, security will be discussed with regards to Security Domains.

2.6 Security requirements

Users, whether they are people or software applications, have zero or more of four basic security requirements, which protect them from four basic threats:

- Confidentiality – preventing the unauthorized access to information
- Integrity – preventing the unauthorized modification or theft of information
- Availability – preventing the denial of service and ensuring authorized access to information
- Non-Repudiation/Accountability – preventing the denial of an action that took place or the claim of an action that did not take place.

2.7 Security attacks

The threats can be realized by many different types of attacks, some of which are illustrated in Figure 6. As can be seen, the same type of attack can often be involved in different security threats. This web of potential attacks means that there is not just one method of meeting a particular security requirement: each of the types of attacks that present a specific threat needs to be countered.

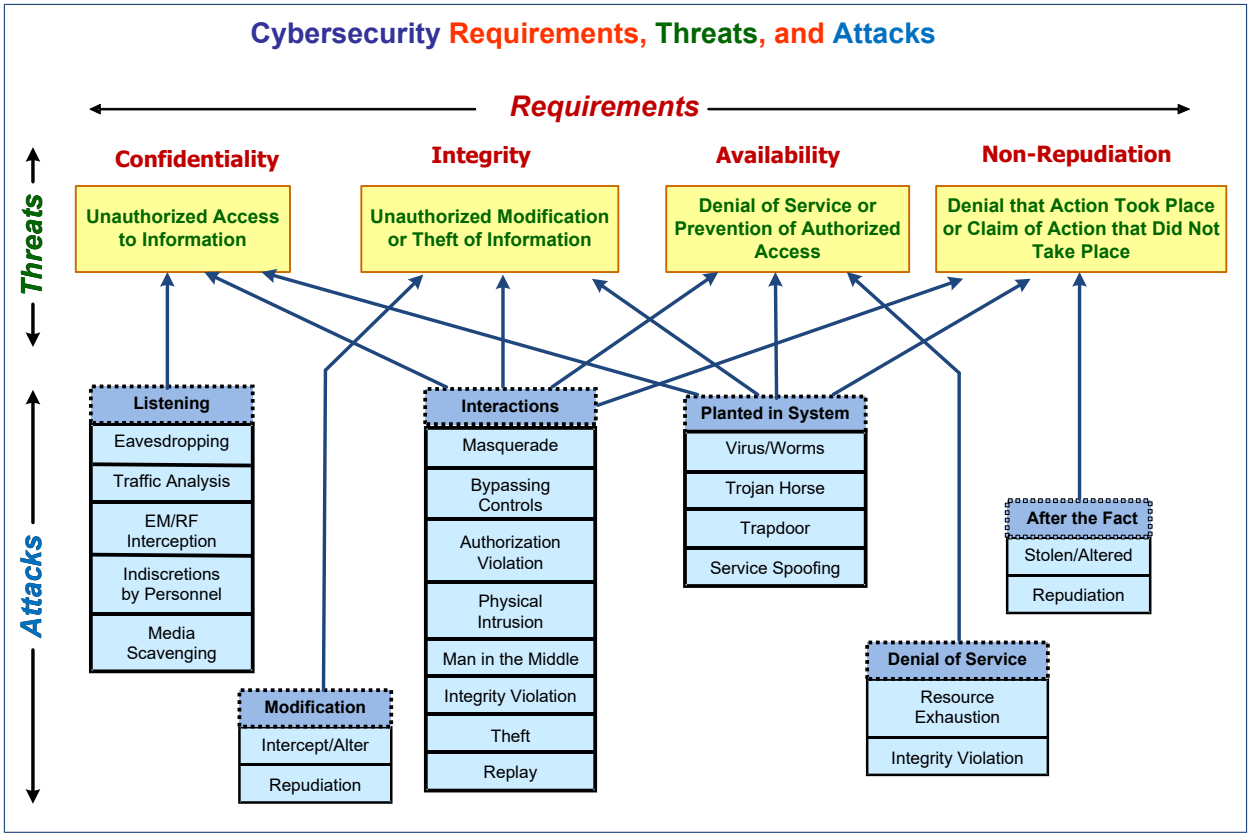

Figure 6: Security Requirements, Threats, and Possible Attacks, indicating those being addressed by WG15

2.8 Security Countermeasures

Security countermeasures, as illustrated in Figure 7, are also a mesh of interrelated technologies and policies. Not all security countermeasures are needed or desired all of the time for all systems: this would be vast overkill and would tend to make the entire system unusable or very slow. Therefore, the first step is to identify which countermeasures are beneficial to meet which needs.

In these figures, the four security requirements (confidentiality, integrity, availability, and non-repudiation) are shown in red words. The security threats are shown with a yellow background. The key security services and technologies used to counter the threats are shown in purple and tan, while security management items are shown in blue. Security policy is shown in green.

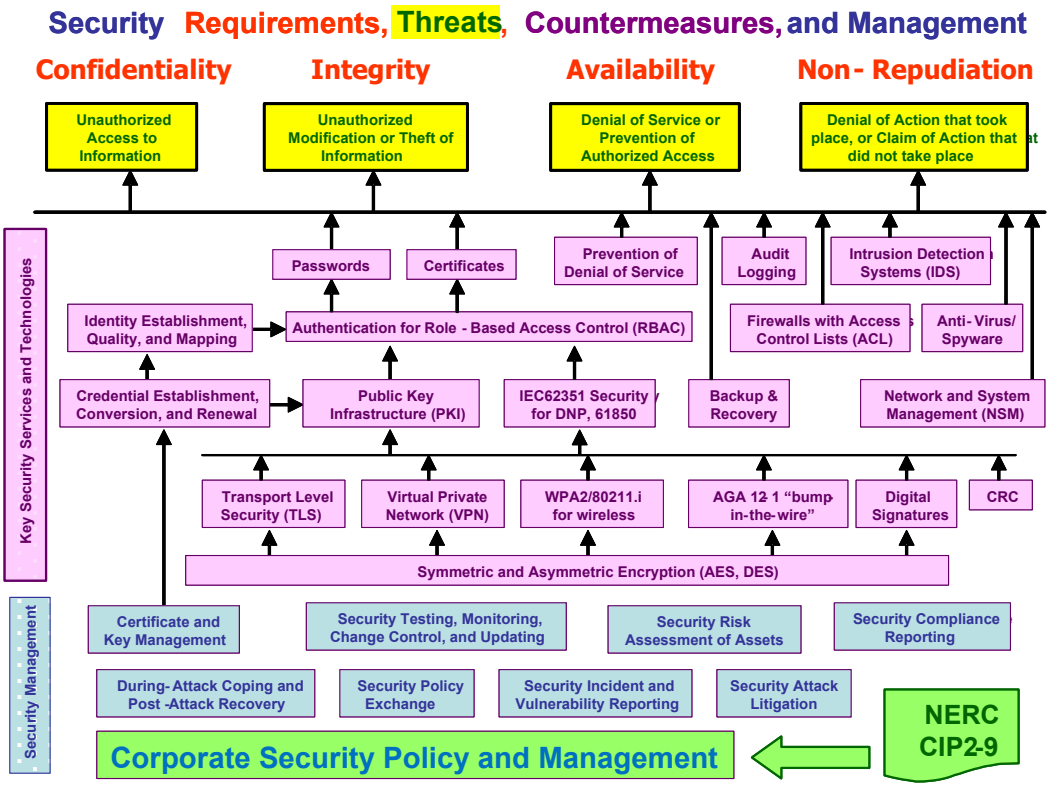

Figure 7: Overall Security: Security Requirements, Threats, Countermeasures, and Management

3 IEC TC57 WG15: Security for Power System Communications

3.1 Scope of IEC TC57 WG15

IEC TC57 WG15 was formed to develop cybersecurity standards for the power system application domain. Its scope and purpose are to:

> *"Undertake the development of standards for security of the communication protocols defined by the IEC TC 57, specifically the IEC 60870-5 series, the IEC 60870-6 series, the IEC 61850 series, the IEC 61970 series, and the IEC 61968 series.*
>
> *Undertake the development of standards and/or technical reports on end-to-end security issues."*

The initial scope of these standards were communication protocols utilized in power system automation defined by the IEC TC 57 (see Figure 8), specifically the IEC 60870-5 series, the IEC 60870-6 series, the IEC 61850 series, the IEC 61970 series, and the IEC 61968 series. Besides standards defined in IEC, also IEEE defined standards like IEEE 1815 (DNP3) are considered. The result is the standards framework IEC 62351.

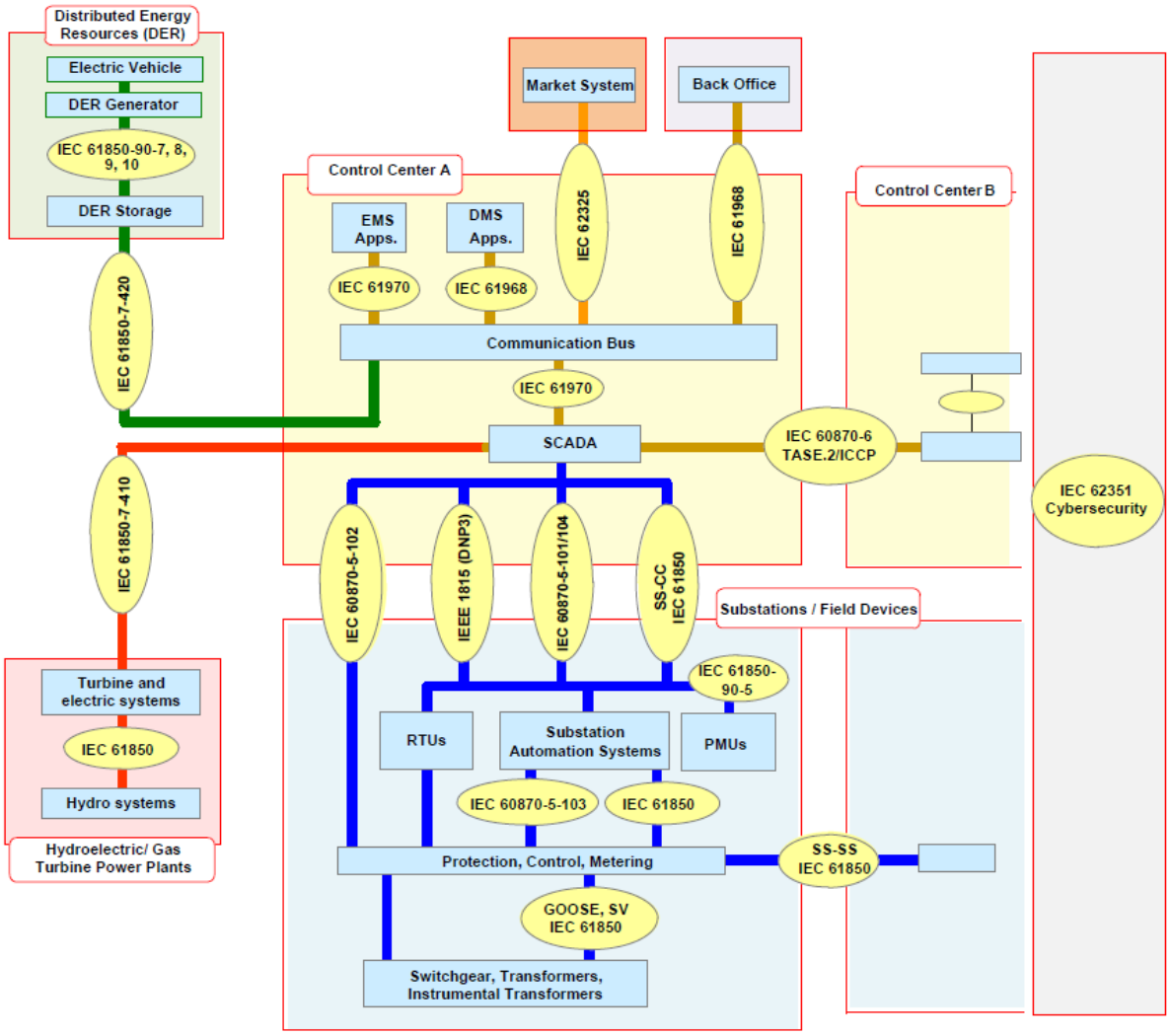

Figure 8: Standards domain in a power system (see [19])

3.2 Overview of IEC 62351 Standards and Guidelines

The IEC 62351 standards and guidelines (some under development or update) are briefly described in Table 1.

Table 1: IEC 62351 standards and guidelines

IEC 62351 Document	Description	Status
Introductory documents		
IEC/TS 62351-1: Introduction	Covers the background on security for power system operations, and introductory information on the series of IEC 62351 security standards	TS 2007
IEC/TS 62351-2: Glossary of terms	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.	TS 2008

IEC 62351 Document	Description	Status
IEC 62351 Application Notes	Introduction into IEC 62351 and its application: ▪ Vol 1 provides an overview on general security requirements and gives an overview on the IEC 62351 series ▪ Vol 2 targets addressing common security requirements from IEC 62443 and also the NIST CSFW using IEC 62351 ▪ Vol 3 provides application examples for how best to use the IEC 62351 series	Volume 1 (this document) Volume 2 and 3 published in 2024
IEC 62351 Crypto Agility Roadmap	Addresses the roadmap to ensure crypto agility in IEC 62351 security means. This also addresses Post-quantum cryptographic algorithms	*pending*
Protocol security standards		
IEC/IS 62351-3: Security for profiles including TCP/IP	Profiling of the existing security protocol Transport Layer Security (TLS) to protect TCP based communication. This part is self-contained since Ed. 2 and can be used in conjunction with other parts of IEC 62351 and thus enables a re-use of existing solutions. As it applies to communication utilizing TCP/IP based communication it addresses: ▪ IEC 60870-6 (TASE.2 / ICCP) ▪ IEC 60870-5 Part 104 ▪ IEC 61850 over TCP/IP ▪ IEEE 1815 (DNP 3) over TCP/IP	TS 01/2007 IS Ed 1.0 12/2015 IS Ed 1.1 03/2018 IS Ed 1.2 02/2020 IS Ed. 2 06/2023
IEC/IS 62351-4: Security for profiles including MMS and derivatives	Utilizes IEC 62351-3 to protect the TCP based IEC 61850 communication (T-profile) and defines additional security mechanisms on application layer (A-profile, End-to-end security profile) to protect end-to-end security in scenarios with classical communication (e.g., control center to substation) or web-based approaches (e.g., for the introduction of DER using publish-subscribe mechanisms). covers 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	IS 11/2018 IS Ed 1.1 07/2020
IEC/IS 62351-5: Security for IEC 60870-5 and derivatives	Defines security mechanisms to protect serial communication (IEC 60870-5-101) and DNP3 (IEEE 1518). Additionally, this part utilizes IEC 62351-3 to protect the TCP based IEC 60870-5-104 communication (T-profile). Note that the actual security parameter definition for the TLS profile is done in IEC 60870-5-7. It addresses both serial and networked profiles used by: ▪ IEC 60870-5-7 (security details for IEC 60870-5-101 and 104) ▪ IEEE 1815 (DNP 3)	TS Ed 1.0 08/2009 TS Ed 2.0 04/2013 IS Ed 1 01/2023

IEC 62351 Document	Description	Status
IEC/IS 62351-6: Security for IEC 61850 profiles	Utilizes part 3 to protect the TCP based IEC 61850 communication (T-profile in conjunction with Part 4). Additionally, security mechanisms are defined to protect GOOSE and SV supporting multicast communication. This part specifies the combination of security profiles for IEC 61850 services, which run over TCP/IP like MMS and also GOOSE and SV, which can be used within substations based on a layer 2 communication or in the wide area case based on UDP/IP communication. The necessary group based key management is defined in IEC 62351-9 and enhances an already IETF-standardized approach. Part 6 has cross relations to: ▪ IEC 62351-9 for the key management of group of certificates and also group based symmetric keys. ▪ IEC 61850-8-1 incorporates protocol enhancements for GOOSE ▪ IEC 61850-9-2 incorporates protocol enhancements for SV	TS 01/2007 IS Ed 1 10/2020
IEC/IS 62351-11: Security for XML Files	Protection of XML based data, which can be enhanced with RBAC elements. 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.	IS 09/2016
IEC/IS 62351-16 Profiles for Layer 2 Security, MACsec	This standard is a work-in-progress and specifies Media Access Control Security (MACsec) as a method for the security of OSI Layer 2 IEC 61850 protocols. This document is self-contained and meant to complement existing methods found in IEC 62351-6. Part 16 identifies how to implement MACsec with a focus on interoperability between devices both inside and outside substations in such a way as to provide low-latency encryption optimized for embedded devices to enable confidentiality for Layer 2 GOOSE and Sampled Values. Part 16 is intended to define a profile for MACSEC security in a similar way as IEC 62351-3 profiles TLS. In addition different key management approaches (MACSEC, GDOI) are considered to provide the relevant security parameters.	WD
Supporting security standards		
IEC/IS 62351-7: Network and System Management (NSM) data object models	Addresses the Network and System Management (NSM) of the information infrastructure, which defines abstract NSM data objects for the power system operational environment and reflect 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 are available as code components.	IS Ed 1.0 2017 IS Ed 2.0 *ongoing*

IEC 62351 Document	Description	Status
IEC/IS 62351-8: Role-Based Access Control	Defines profiles for role-based access control to convey the role information in different formats as access tokens. They enable the dynamic assignment of roles to authorize users or applications. The assignment of permissions to a role has a more static character and depends on the associated data model (e.g., IEC 61850). Besides the definition of standard roles, the exchange of information for custom defined roles is defined. The role information is provided depending on the utilized profile, either directly to the user/application or may be fetched by the accessed entity, e.g., via LDAP or RADIUS.	TS in 2011 IS Ed 1.0 04/2020 IS Ed 2.0 *pending*
IEC/PAS 62351-8-1: RBAC – Definition of roles and permissions for engineering	Enhances IEC 62351-8 with the definition of permissions as rights on engineering specific objects, as well as the assignment of these permissions to the defined mandatory roles.	NP in 01/2025 pending
IEC/IS 62351-9: Key Management	Provides the base for the management of credentials and keys to be used in the security mechanisms of the different IEC 62351 parts. It specifies how to generate, distribute, revoke, and handle digital certificates and cryptographic keys to protect digital data and its communication. Specifically, this part addresses the management of certificates and corresponding private keys, which are utilized in almost every part of IEC 62351. Additionally, it defines the group-based communication security in the context of multicast communication scenarios by profiling and enhancing GDOI as established standard. Enhancements are provided to allow use of GDOI also for distributing security parameters for GOOSE, SV, and PTP.	IS Ed 1.0 05/2017 IS Ed 2 06/2023
IEC/IS 62351-14 Cyber Security Event Logging	Specifies technical details for the implementation of security logs: communication, content and semantics. The events are defined in a general format, while the transport mapping is done to syslog specifically.	IS Ed 1 *pending*
IEC/IS 62351-15 Deep Packet Inspection of encrypted communication	Deep Packet Inspection (DPI) includes a variety of techniques that allow authorized network owners to assess encrypted data with the goals of visibility, anomaly and intrusion detection for a given network in scope. In the security landscape, DPI is becoming a core security control used for overall visibility, threat management, and ultimately risk mitigation. This is complementary to other network and system monitoring types as described in IEC 62351-7 and IEC 62351-14.	WD
Supporting security guidelines		
IEC/TR 62351-10: Security Architecture	Overview and typical requirements to security architectures in power automation. 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.	TR 10/2012

IEC 62351 Document	Description	Status
IEC/TR 62351-12: Resilience and Security Recommendations for Power Systems with DER	Recommendations for the incorporation of decentralized energy resources DER in the power grid. 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.	TR 04/2016
IEC/TR 62351-13: Guidelines on What Security Topics Should Be Covered in Standards and Specifications	Recommendations for editors of standards and specifications regarding the handling of security specific requirements in power systems. 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".	TR 08/2016
IEC/TR 62351-90-1: Guidelines for Using Part 8 Roles	Guidance for using role-based access control (RBAC) specifically the handling of custom based roles.	TR 01/2018
IEC/TR 62351-90-2: Deep Packet Inspection	Guidance for supporting deep packet inspection (DPI) when using encrypted communication links.	TR 09/2018
IEC/TR 62351-90-3: Guidelines for Network Management	Guidance on applying monitoring and logging in power systems (using SNMP and syslog).	TR 03/2021
IEC/TR 62351-90-4: Migration support to stronger cryptographic algorithms	Guidance on migrating to stronger cryptographic algorithms, e.g., to address upcoming requirements to support post-quantum cryptographic algorithms.	TR *pending*
Conformance testing		
IEC/TS 62351-100-1: Conformance test cases for IEC 62351-5 and IEC 60870-5-7	Conformance test cases associated with IEC 62351-5 and companion standards. Focus is on secure telecontrol over TCP and serial protocols in the context of IEC 60870-5-7.	TS 11/2018
IEC/TS 62351-100-3: Conformance test cases for IEC 62351-3	Conformance test cases associated with IEC 62351-3 as general base to be used by other test specifications	TS 01/2020
IEC/TS 62351-100-4: Conformance testing for 62351-4 with IEC 61850	Conformance test cases associated with IEC 62351-4 (End-to-end security profile)	TS 11/2023
IEC/TS 62351-100-4.1: Conformance testing for 62351-4 with IEC 61850 using the A-profile	Conformance test cases associated with IEC 62351-4 (A-profile)	TS *pending*
IEC/TS 62351-100-6: Conformance testing for 62351-6 with IEC 61850-8-1 and 61850-9-2	Conformance test cases associated with IEC 62351-6	TS 08/2022

IEC 62351 Document	Description	Status
IEC/TS 62351-100-8: Conformance testing for 62351-8 Role-based Access control	Conformance test cases associated with IEC 62351-8	NWIP *pending*
IEC/TS 62351-100-9: Conformance testing for 62351-9	Conformance test cases associated with IEC 62351-9 focusing on group-based key management	NWIP *pending*
Documents applying IEC 62351		
IEC/PAS 61850-90-19: Using Role Based Access Control (RBAC) and IEC 61850 (joint with WG10)	Defines the application of RBAC in the context of IEC 61850. It utilizes IEC 62351-8 to provide the mapping of roles to permissions and additionally specifies the binding to objects of the underlying data model. IEC/PAS 61850-90-19 has cross relations to: ▪ IEC 62351-8 for the general RBAC approach ▪ IEC 61850-8-1 for the definition of unique identifiers for objects in SCL files	PAS *pending*
IEC/TS 60870-5-7 Ed.2: Security for IEC 60870-5-101/104 (joint with WG3)	Defines the application of security measures for the 101 (serial) and 104 (TCP/IP-based) protocols using security means defined in related IEC 62351 parts. Moreover, it defines the mapping of permissions to enable RBAC and also defines security means for the broadcast serial communication. IEC/TS 60870-5-7 has cross relations to: ▪ IEC 62351-3 for the TLS profile to secure TCP/IP based communication (104) ▪ IEC 62351-5 for providing application layer security when using serial protocols (101) ▪ IEC 62351-8 for the general RBAC approach	CDV *pending*

3.3 Correlation of communication standards

There is not a one-to-one correlation between the IEC TC57 communication standards and the IEC 62351 security standards. This is because many of the communication standards rely on the same underlying standards at different layers. In addition, some security documents cover broader concepts rather than specific cryptography. The scopes and interrelationships between the IEC TC57 standards and the IEC 62351 security standards are illustrated in Figure 9.

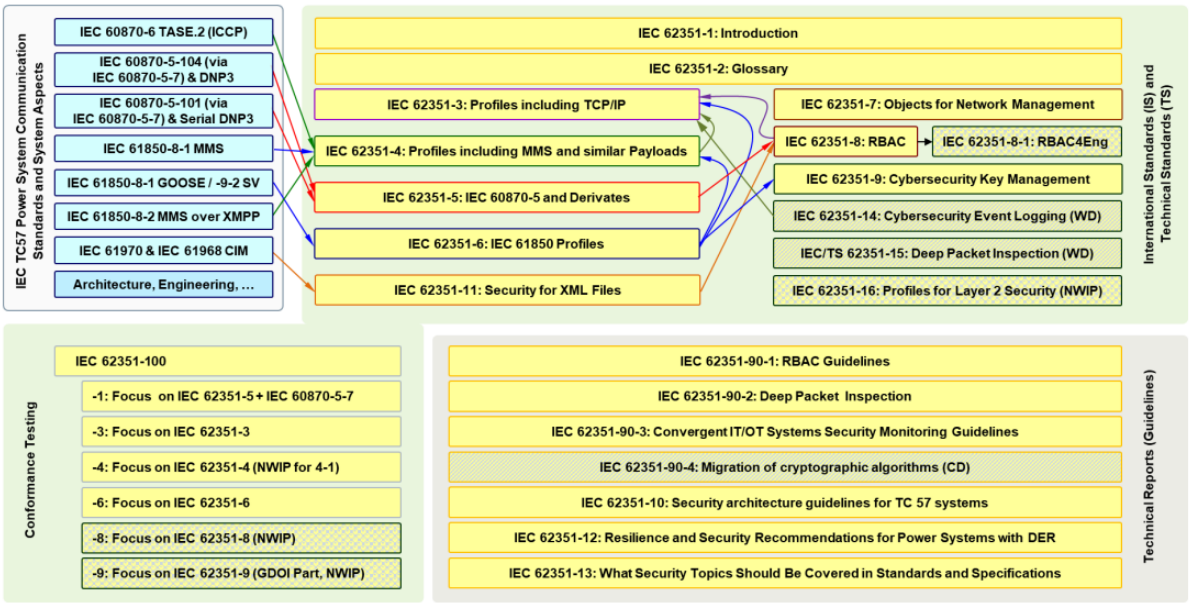

Figure 9: Interrelationships between the IEC TC57 Standards and the IEC 62351 Security Standards

4 Discussion of IEC 62351 Standards and Guidelines

4.1 IEC 62351 Parts 1-2 – Introduction and Glossary

4.1.1 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. It covers many of the same issues as this document, although needs updating.

4.1.2 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

4.2 IEC 62351 Parts 3-6, 11 – Security Standards for IEC TC57 Communication Standards

4.2.1 Overview

Since it was formed, WG15 has undertaken the development of security standards for the four communication standards listed above: IEC 60870-5, its derivative DNP, IEC 60870-6 (ICCP), and IEC

61850. These security standards must meet different security objectives for the different protocols, which vary depending upon how they are used.

Some of the security standards can be used across a few of the protocols, while others are very specific to a particular profile. The different security objectives include authentication of entities through digital signatures, ensuring only authorized access, prevention of eavesdropping, prevention of playback and spoofing, and some degree of intrusion detection. For some profiles, all of these objectives are important; for others, only some are feasible given the computation constraints of certain field devices, the media speed constraints, the rapid response requirements for protective relaying, and the need to allow both secure and non-secured devices on the same network.

This work was published by the IEC as IEC 62351, Parts 3-6. Initially, these documents were all Technical Specifications, but are now being converted to International Standards. They include:

- **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[2] ().**
  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 Sample Values

The interrelationship of these security standards and the protocols are illustrated in Figure 9.

4.2.2 IEC 62351-3: Security for Profiles That Include TCP/IP

IEC 62351-3 provides security for communication profiles that build on TCP/IP, including IEC 60870-6 TASE.2, IEC 61850 ACSI over TCP/IP, and IEC 60870-5-104.

Rather than re-inventing the wheel, it profiles the use of TLS for both versions (1.2 and 1.3), which is commonly used in for secure interactions, covering authentication, confidentiality, and integrity.

This part specifically describes parameters and settings for TLS that should be used for application in the power system domain. This specifically relates to

- Mutual authentication of communication peers based on X.509 certificates. This also involves the verification of the certificates including their revocation state. For revocation, IEC 62351-3

[2] Note: and possibly similar payloads such as XML XSDs – under discussion

considers different approaches like the CRLs, which are distributed in dedicated time frames, providing bulk revocation information from issuing CAs. Also considered is OCSP allowing to query the revocation state of a single certificate. In addition, TLS specific means to provide inband revocation information (i.e., OCSP stapling) are taken into account. Mutual authentication is intended to thwart masquerading or also man-in-the-middle attacks.

- TLS session parameters like the selection of supported cipher suites, the refresh of session key material, but also the re-authentication of communication peers. These settings are intended to provide an integrity and confidentiality protected communication in addition to the mutual authentication achieved during the TLS handshake. Note that also integrity-only cipher suites are considered, to enable monitoring also in case of secured communication.

- Security eventing is used to ease the handling of failure situations according to IEC 6251-14.

However, TLS does not protect against denial of service. This security attack should be guarded against through implementation-specific measures or infrastructure related security measures.

4.2.3 IEC 62351-4: Security for Profiles That Include MMS and Similar Payloads

IEC 62351-4 provides security for profiles that include the Manufacturing Message Specification (MMS) (ISO 9506) and similar payloads, such as IEC 60870-6 (TASE.2 (ICCP)), IEC 61850-8-1 (MMS-based), and IEC 61850-8-2 (XML/XSDs over XMPP).

The communication security provided by this standard include:

- Transport profile (layers 1-4 of the OSI Reference Model): this document specifies how to use Transport Layer Security (TLS) and the securing of IETF RFC 1006, requiring compliance with IEC 62351-3.
- Application profiles: An application profile defines the sets of protocols and requirements for layers 5-7 of the OSI Reference Model.

There are two T-profiles and four application profiles identified within the TC 57 context. This specification shall specify security extensions for all of the identified profiles except for the OSI T-profile.

4.2.4 IEC 62351-5: Security for IEC 60870-5 and Derivatives (i.e. DNP 3)

IEC 62351-5 provides different solutions for the serial version (primarily IEC 60870-5-101, as well as parts 102 and 103) and for the networked versions (IEC 60870-5-104 and DNP 3).

Specifically, the networked versions that run over TCP/IP can utilize the security measures described in IEC 62351-3, which includes confidentiality and integrity provided by TLS encryption. Therefore, the only additional requirement is authentication.

The serial version is usually used with communications media that can only support low bit rates or with field equipment that is compute-constrained. Therefore, TLS would be too compute-intense and/or communications-intense to use in these environments. Therefore, the only security measures provided for the serial version include some authentication mechanisms which address spoofing, replay, modification, and some denial of service attacks, but do not attempt to address eavesdropping, traffic analysis, or repudiation that require encryption. These encryption-based security measures could be provided by alternate methods, such as VPNs or “bump-in-the-wire” technologies, depending upon the capabilities of the communications and equipment involved.

The general consensus is that all three of these key management issues should be available. However, the exact mechanisms for key management is still under discussion, since there are no easy answers or existing standards (e.g. from NIST or ISO/IEC) for key management under the conditions of widespread, low bandwidth configurations, where “rolling out trucks” just to handle key updates is not an economic option.

IEC 60870-5-7 provides the details on how to implement IEC 62351-5 for the 101 and 104 protocols. DNP3 has incorporated the IEC 62351 security requirements into the IEEE 1815 DNP3 standard. This standard is currently (January 2024) being updated.

4.2.5 IEC 62351-6: Security for IEC 61850 Peer-to-Peer Profiles (e.g. GOOSE)

The IEC 61850 profile that includes the MMS protocol running over TCP/IP uses IEC 62351-3 and IEC 62351-4. Additional IEC 61850 profiles that run over TCP/IP (web services or other future profiles) will use IEC 62351-3 plus possible additional security measures developed by the communications industry for application-layer security (out-of-scope for this set of standards).

IEC 61850 contains three protocols that are peer-to-peer multicast datagrams on a substation LAN and are not routable. The main protocol, GOOSE, is designed for protective relaying where the messages need to be transmitted within 4 milliseconds peer-to-peer between intelligent controllers. Given these stringent performance requirements, encryption or other security measures which may significantly affect transmission rates are not acceptable. Therefore, authentication is the only security measure included as a requirement, so IEC 62351-6 provides a mechanism that involves minimal compute requirements for these profiles to digitally sign the messages.

4.2.6 IEC 62351-11: Security for XML Files

Within the industry and the IEC, the use of XML to exchange information is becoming more prevalent. Within the scope of the IEC, exchanges of XML-based documents are used for IEC 61970 as well as for some types of information exchanges in IEC 61850. XML-based information exchanges are also utilized within other standards, such as IEEE 1815 (DNP3) and IEEE C37.111 (COMTRADE). For these standards and other XML-based documents, the information contained in the document may:

- Be sensitive to inadvertant or malicious modifications of its contents that could result in mis-operation/misinterpretation if the exchanged information is used (e.g. a tamper security vulnerability).
- Contain confidential or private data.
- Contain subsets of information that may be considered sensitive by the document creation entity.

This part of IEC 62351 proposes to standardize mechanisms to protect the document contents from tampering/disclosure when the document is being exchanged (e.g. in transit). Additionally, this part proposes to standardize a mechanism to aid in the protection of the information when in transit across multiple parties with different trust relationships (e.g. entity A trusts entity B; B trusts A and C, and A needs to exchange information with C. but A does not know of or trust C). As an example, a utility (A) may trust an aggregator (B). The aggregator trusts the utility and a DER facility (C). The utility therefore sends an XML-based document with both sensitive and general information to the aggregator and “trusts” that the aggregator will only send the non-sensitive information on to the DER facility. This part provides a mechanism to identify the sensitive information so that the middle entity (B) can determine not to send it on.

Although this document is intended to secure XML documents used within the scope of the IEC, the mechanism/methodologies specified within this document can be applied to any XML document.

4.3 IEC 62351 Parts 7-9, 14-16: End-to-End Security Requirements

WG15 undertook broader efforts when it was urged by TC57 to work toward end-to-end security, which entails a much larger scope than protecting communication protocols. End-to-end security involves security policies, access control mechanisms, key management, audit logs, and other critical infrastructure protection issues. The first effort in this expanded scope was to develop network and system management data objects to help manage the information infrastructure.

4.3.1 IEC 62351-7: Security through Network and System Management

4.3.1.1 Scope and Objectives of IEC 62351-7

The scope of IEC 62351-7 focuses on Network and System Management (NSM) of the information infrastructure. Power systems operations are increasingly reliant on information infrastructures, including communication networks, intelligent electronic devices (IEDs), and self-defining communication protocols. Therefore, management of the information infrastructure is crucial to providing the necessary high levels of security and reliability in power system operations. WG15 has therefore developed abstract Network and System Management (NSM) data objects for the power system operational environment (currently a Working Group draft). These NSM data objects reflect what information is needed to manage the information infrastructure as reliably as the power system infrastructure is managed.

The ISO CMIP and the IETF SNMP standards for Network Management can provide some of this management. In SNMP, Management Information Base (MIB) data is used to monitor the health of networks and systems, but each vendor must develop their own set of MIBs for their equipment. For power system operations, SNMP MIBs are only available for common networking devices, such as routers. No standard MIBs have been developed for IEDs, so vendors use “ad hoc” or proprietary methods for monitoring some types of equipment health. This standard thus provides MIB-like data objects (termed NSM data objects) for the power industry.

The abstract SNMP client/agent model is assumed within the standard, but SNMP itself is not presumed to be the protocol of choice. Instead, the NSM data objects defined in this document represent the set of information that is deemed mandatory, recommended, or optional in order to support network and system management and security problem detection. These abstract NSM data objects are currently represented in tables, but may possibly be represented in UML classes.

The NSM data objects can then be mapped to any appropriate protocol, including IEC 61850, IEC 60870-5, IEC 60870-6, SNMP, Web Services, or any other appropriate protocol. An initial mapping to SNMP will be developed before the document is submitted to the IEC.

The general philosophy of this document is to document the type and definition of the information required to perform End-to-End security detection within a TC57 environment. The use/non-use of the recommended MIBs outside of the TC57 environment is out-of-scope for this document.

4.3.1.2 Purpose of Network Management: Information Infrastructure Security

The Information Infrastructure in power operations is not typically treated as a coherent infrastructure, but is viewed as a collection of individual communication channels, separate databases, multiple systems, and different protocols. Often SCADA systems perform some minimal communications monitoring, such as whether communications are available to their RTUs, and then

they flag data as “unavailable” if communications are lost. However, it is up to the maintenance personnel to track down what the problem is, what equipment is affected, where the equipment is located, and what should be done to fix the problem. All of this is a lengthy and ad hoc process. In the meantime, the power system is not being adequately monitored, and some control actions may be impossible. As the analysis of the August 14, 2003 blackout showed, the primary reason behind the blackout itself was the lack of critical information made available to the right user at the right time.

Every utility is different in what information is available to its maintenance staff. Telecommunication technicians are generally responsible for tracking down any microwave or fiber cable problems; telecommunication service providers must track their networks; database administrators must determine if data is being retrieved correctly from substation automation systems or from GIS databases; protocol engineers must correct protocol errors; application engineers must determine if applications have crashed, have not converged, or are in an endless loop; and operators must filter through large amounts of data to determine if a possible “power system problem” is really an “information system problem”.

In the future, the problem of information management will become increasingly complex. SCADA systems will no longer have exclusive control over the communications to the field, which may be provided by telecommunication providers, or by the corporate networks, or by other utilities. Intelligent Electronic Devices (IEDs) will have applications executing within them whose proper functioning is critical to power system reliability. Field devices will be communicating with other field devices, using channels not monitored by any SCADA system. Information networks in substations will rely on local “self-healing” procedures which will also not be explicitly monitored or controlled by today’s SCADA systems.

4.3.1.3 NSM UML database and translation to SNMP MIBs

The telecommunication infrastructure that is in use for the transport of the telecontrol and automation protocols is already subject of health and monitoring control, using the concepts developed in the IETF simple network management protocol (SNMP) standards for network management; the power system specific devices (like teleprotection, synchrophasors, telecontrol and protections) need instead a specific solution for their monitoring.

These objects will provide monitoring data on TC57 protocols running inside power systems (IEC 61850, IEC 60870-5-104) and device specific environmental and security status. Also IEEE 1815 DNP3 is included in the list of monitored protocols. The NSM data objects use the naming conventions developed for IEC 61850, expanded to address NSM issues. These data objects, and the data types of which they are comprised, are defined as abstract models of data objects.

In order to allow the integration of the monitoring of power system devices within the NSM environment in this standard a mapping towards the simple network management protocol (SNMP) protocol of objects is provided.

SNMP was developed by the IETF as the protocol for transmitting MIBs over the Internet. Many systems use SNMP internally as well. MIBs do not need to be transmitted by SNMP – any protocol can be used, but due to SNMP popularity, SNMP is the preferred protocol. Eventually, other protocols, such as IEC 61850 protocols may be updated to also transmit the MIBs.

IEC 62351-7 was published as International Standard (IS) on 2017. In this version of IEC 62351-7 document, abstract NSM data objects are being defined in a Unified Modeling Language (UML) database. From this NSM database, SNMP MIBs can be automatically extracted.

Currently IEC 62351-7 is under revision for Ed.2 release. This new edition will align the monitoring objects with those required by the other IEC 62351 standard release. Furthermore a subset of

monitoring object will be stated as mandatory for the implementors. This is also due to the results published on 2021 in IEC TR 62351-90-3 “Power systems management and associated information exchange - Data and communications security - Part 90-3: Guidelines for network and system management”.

4.3.2 IEC 62351-8: Role-Based Access Control for Power System Management

The scope of this specification is the access control of users and automated agents to data object in power systems by means of role-based access control (RBAC).

The purpose of an access control mechanism is to protect system resources. For a system that implements RBAC, system resources can represent information containers (e.g. files, directories in an operating system and/or columns, rows, tables, and views within a database management system) or exhaustible device resources, such as printers, disk space and CPU cycles.

Under RBAC, security administration is simplified through the use of roles and constraints to organize subject access levels. RBAC thus can reduces costs within an organization primarily because it accepts that employees change roles and responsibilities more frequently than the rights within roles and responsibilities have to be changed.

RBAC is not a new concept; in fact, it is used by many operating systems (e.g., Solaris, Windows 2000 and above) to control access to system resources. RBAC is an alternative to the all-or-nothing super-user model. RBAC is in keeping with the security principle of least permission, which states that no user should be given more permission than necessary for performing that person’s job. RBAC enables an organization to separate super-user capabilities and package them into special user accounts termed *roles* for assignment to specific individuals according to their job needs. This enables a variety of security policies, networking, firewall, back-ups, and system operation. A site that prefers a single strong administrator but wants to let more sophisticated users fix portions of their own system can set up an advanced-user role. RBAC is not confined to users though, it applies equally well to automated computer agents, i.e., software parts operating independent of user interactions.

As in many aspects of security, RBAC is not just a technology; it is a way of running a business. RBAC provides a means of reallocating system controls, but it is the organization that decides the implementation.

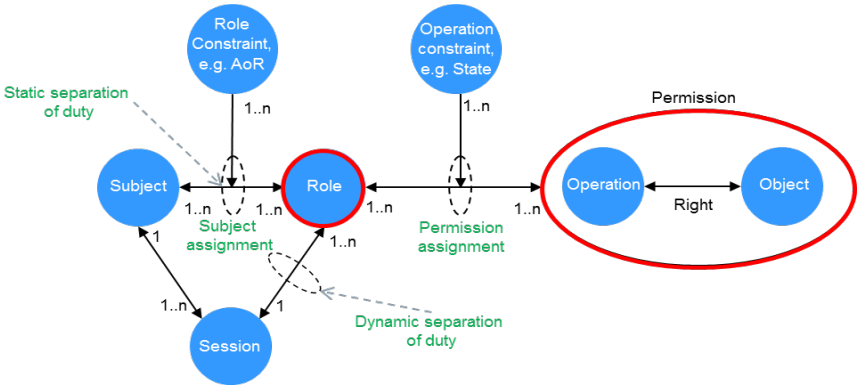

Figure 10: Role-based access control, permissions, and constraints

The scope of this specification is depicted in Figure 10 and comprises:

- Definition of pre-defined roles expected to be supported by different implementations.

- Definition of ways to defined custom roles in an interoperable way, based on XACML as common approach for describing roles and permission.

- Delegation the permission mapping to roles to referencing documents, which allows to map the permissions based on the underlying data model. This approach allows clear utilization of the for different data models, not just for the power system domain with IEC 61850, IEC 60870, or IEEE 1815, but also to data models applicable, e.g., web-based engineering. For this the specification also provides examples for the role to permission mapping as well as the consideration of constraints.

- Definition of access tokens, used to convey the role information including their definition (relation to the data model) and constraints (like the area of responsibility.

- Definition of different formats and distribution options of this access token information as profiles. These profiles consider transporting the access token information in public key certificates, attribute certificates, OAUTH tokens, RADIUS, and LDAP. Also specified is the verification of the access token information by the relying party.

Based on the scope, IEC 62351-8 requires the mapping of the defined mandatory-to-support roles to specific permissions and further to the application or data model specific objects by referencing standards. This is done for IEC 61850 in IEC 61850-90-19 and for IEC 60870-5 protocols in IEC 60870-5-7 as outlined in Figure 11 below.

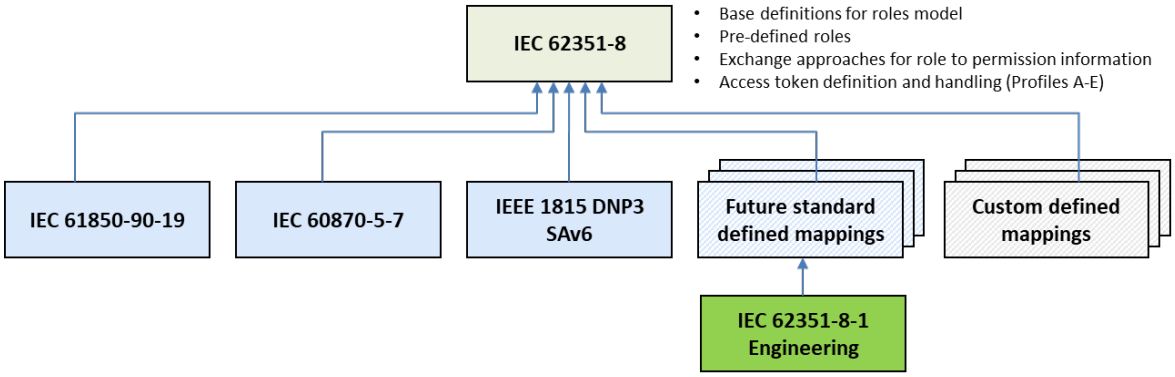

Figure 11: Documents defining role-to-permission mappings

4.3.3 IEC 62351-8-1 RBAC – Definition of roles and permissions for engineering

This part of IEC 62351 enhances the RBAC base specification in IEC 62351-8 for (web-based) engineering use cases as shown in Figure 11and targets the specification of role-to-permission assignment and the definition of permission and objects.

Engineering in the context of this part is understood as summary of activities related to configuration, parametrization, and monitoring. Different engineering use cases covering devices with single or multiple application support, web-based and local engineering are addressed.

Moreover, different approaches for engineering interaction are described (pull and push) for different connectivity models (online and offline).

4.3.4 IEC 62351-9: Key Management

This part of IEC 62351 specifies cryptographic key management, primarily focused on the management of long-term keys, which are most often asymmetric key pairs, such as X.509 public-key certificates and corresponding private keys. As certificates build the base this document builds a foundation for many IEC 62351 services. Symmetric key management is also considered but only with respect to session keys for group-based communication as applied in IEC 62351-6. The objective of this document is to define requirements and technologies to achieve interoperability of key management by specifying or limiting key management options to be used.

This document assumes that an organization (or group of organizations) has defined a security policy to select the type of keys and cryptographic algorithms that will be utilized, which may have to align with other standards or regulatory requirements. This document therefore specifies only the management techniques for these selected key and cryptography infrastructures and has a relation to several other IEC 62351 parts.

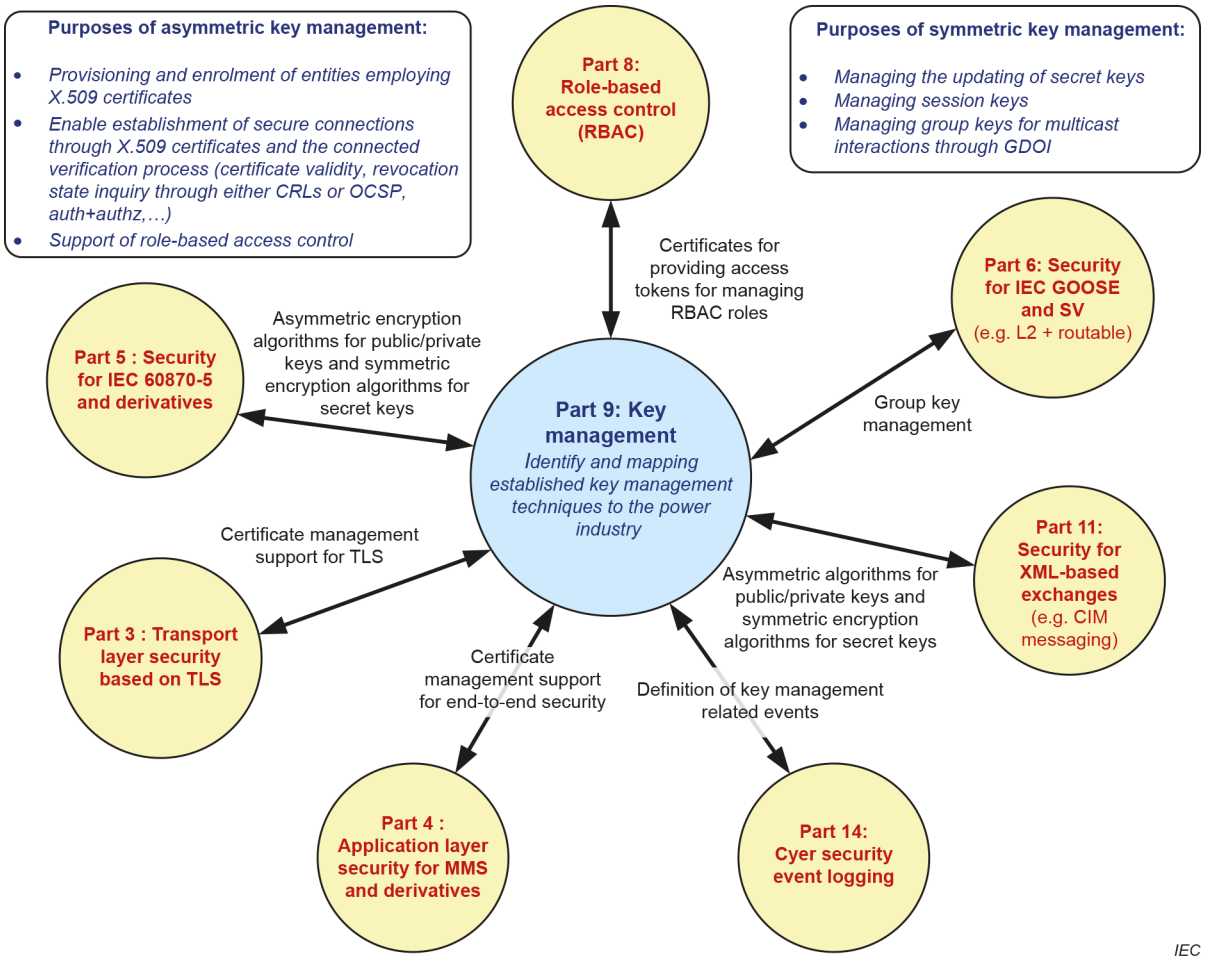

Figure 12: Relation of the key management to other IEC 62351 parts

Regarding asymmetric credentials IEC 62351-9 specifies the mandatory and optional components for certificates (similar to a certificate profile) and their verification. This information is one base for the application in the context of IEC 62351-3, IEC 62351-4, IEC 62351-8, and further. Moreover, the management of certificates is addressed by different techniques for enrollment (like EST and SCEP) and revocation handling via CRLs and OCSP.

In addition, IEC 63251-9 defines the application of the group-based key management GDOI (Group Domain of Interpretation, IETF RFC 6407) to manage security parameters for multicast communication. The specifically is provided for GOOSE and Sampled Values as specified in IEC 62351-6 and to time synchronization with PTP as specified in IEEE 1588.

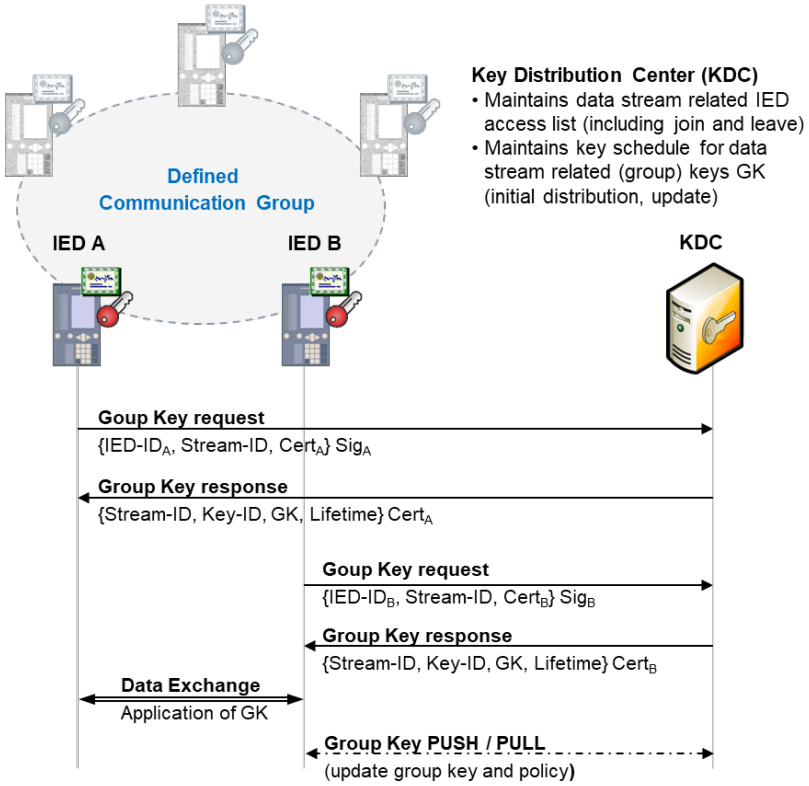

Figure 13: Approach for centralized group-based key management using GDOI

As other IEC 62351 specification, this document also defines security events for specific conditions which could identify issues which might require error handling. However, the actions of the organization in response to these error conditions are beyond the scope of this document and are expected to be defined by the organizations security policy.

In the future, as public-key cryptography may be endangered by the advances in quantum computers, this document will also consider post-quantum cryptography. In the meantime, IEC 62351-90-4 will provide guidelines on the migration towards stronger cryptographic algorithms.

4.3.5 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. Namely how to send and receive security events securely, how to forward security events or logs, how to query logs, etc. All features needed to support organizations to comply with cyber security regulations and standards.

Digital systems have typically used Syslog to log relevant system events. Syslog has become the de-facto standard to log system events. Unfortunately, there are many different Syslog flavours and Syslog event data is not standardized.

The purpose of this standard is to guarantee interoperability among different vendors by specifying Syslog content, Syslog communication protection and a global list of event Ids to be able to support features such querying, filtering, reporting and localization in multi-vendor environments.

4.3.6 IEC 62351-15: Deep Packet Inspection

IEC 62351-15 is a technical specification that aims to solve the Deep Packet Inspection vs confidentiality dilemma. In this context, several techniques are proposed to solve the problem for all the main power systems protocols domains, taking into account some of the different requirements that the network owner may pose.

As confidential data increasingly sent over public networks or even supposedly private networks, the need for encryption increases accordingly. At the same time, these network owners often need to be able to assess whether only authorized data has been sent and/or whether this confidential data has been modified. Therefore, they need some mechanism to securely view the decrypted payload up through the application layer without compromising its security. DPI network monitoring is an answer to allowing such assessments, but DPI also raises its own security risks, namely, how to ensure the decrypted data is secure when/while the assessment takes place.

Deep Packet Inspection (DPI) includes a variety of techniques that could allow authorized network owners to assess encrypted data with the goals of visibility, anomaly and intrusion detection for a given network in scope. In the security landscape, DPI is becoming a core security control used for overall visibility, threat management, and ultimately risk mitigation. This is complementary to other network and system monitoring types as described in IEC 62351-7 and IEC 62351-14.

4.3.7 IEC 62351-16: MAC Security

This standard is a work-in-progress and specifies Media Access Control Security (MACsec) as a method for the security of OSI Layer 2 IEC 61850 protocols. This document is self-contained and meant to complement existing methods found in IEC 62351-6. Part 16 identifies how to implement MACsec with a focus on interoperability between devices both inside and outside substations in such a way as to provide low-latency encryption optimized for embedded devices to enable confidentiality for Layer 2 GOOSE and Sampled Values.

Part 16 is intended to define a profile for MACSEC security in a similar way as IEC 62351-3 profiles TLS. In addition, different key management approaches (MACSEC, GDOI) are considered to provide the relevant security parameters.

4.4 IEC 61351 Parts 10, 12, 13: Cybersecurity Technical Reports

4.4.1 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. Furthermore, the relation and mapping of these security controls to the general system architecture of power systems is provided as guideline to support system integrators to securely deploy power generation, transmission, and distribution systems applying available standards.

Figure 14 illustrates the IEC TC57 architecture used as a base for applying cybersecurity.

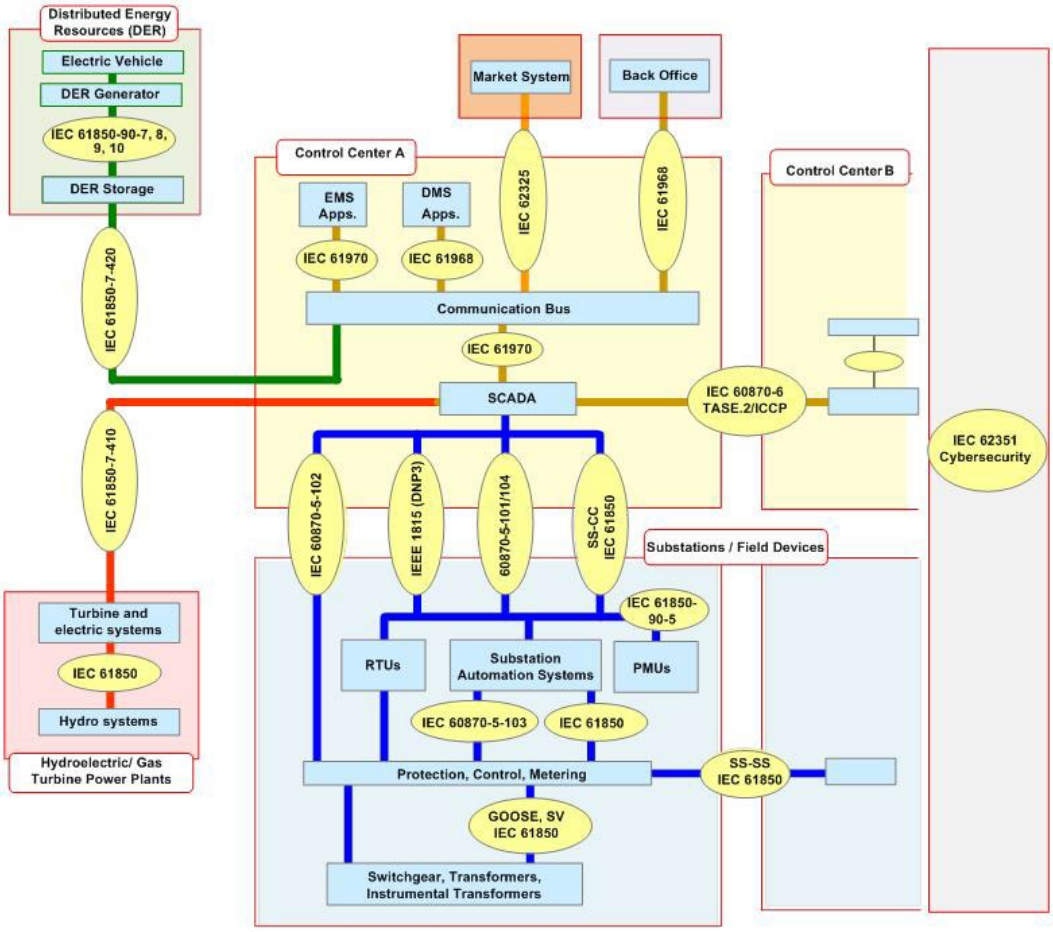

Figure 14: IEC TC57 Communication Standards Architecture

4.4.2 IEC/TR 62351-12: Resilience for Power Systems with DER Systems

This document 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.

4.4.2.1 Resilience of Power Systems with DER

While recognizing that the resilience of the power system to anomalous conditions has many components and extends far beyond the impacts of DER systems, the focus of this document is the role of DER systems in grid resiliency, including:

- **DER System Resilience**: The cyber security and engineering strategies for designing and installing DER systems to provide DER resilience to anomalous power system events and cyber attacks.
- **Grid Resilience for Planning with Significant Numbers of DER Interconnections**: The cyber security and engineering strategies for promoting grid resilience by studying the impact of and planning for interconnecting DER systems with the grid to promote grid resilience.

- **Grid Resilience for Operations with Significant Capacity of DER Generation and Storage:** The cyber security and engineering strategies for operating the grid with significantly large numbers and capacities of DER systems that can impact grid reliability and security.

Grid resilience responds to the overarching concern: *"The critical infrastructure, the Smart Electric Grid, must be resilient - to be protected against both physical and cyber problems when possible, but also to cope with and recover from the inevitable disruptive event, no matter what the cause of that problem is - cyber, physical, malicious, or inadvertent."* Resiliency of the grid is often associated only with making the grid able to withstand and recover from severe weather, equipment failures, intermittency challenges of renewable DER systems, and other physical events, but resiliency should also include the ability of the cyber-physical grid to withstand and recover from malicious and inadvertent cyber events.

The term “cyber-physical grid” implies that the power system consists of both cyber and physical assets that are tightly intertwined. Both the cyber assets and the physical assets must be protected in order for the grid to be resilient. But protection of these assets is not enough: these cyber and physical assets must also be used in combination to detect, cope with, and recover from both cyber and physical attacks into order to truly improve the resiliency of the power system infrastructure.

DER systems can be viewed as both potentially disruptive to power system operations as well as capable of increasing power system stability – if appropriately engineered and operated. If both the cyber and the physical components of power systems, including their interconnected DER systems, were well designed and implemented with embedded cyber security, and were interconnected and operated using good engineering strategies, they would significantly improve the resiliency of the power system.

4.4.2.2 DER Architecture

However, the goal of engineering and operating DER systems in a resilient manner within a complex power system environment is a challenge. In general, utilities will not be able to directly monitor all DER systems nor have real-time control over most DER systems. In many scenarios, the DER operators have additional purposes for their DER systems in addition to providing energy to the grid.

Therefore, the control and management of DER systems will of necessity be hierarchical, since central control of thousands if not millions of DER systems distributed throughout the grid is impractical. This hierarchical architecture may involve many different configurations and management scenarios but can be modeled as consisting of five (5) levels based on a selected set of domains, layers, and zones of the Smart Grid Architecture Model (SGAM), as illustrated in Figure 15 and described in a (draft) White Paper developed by the Smart Grid Interoperability Panel (SGIP)[3]. For instance, small residential PV systems may not include sophisticated Facilities DER Energy Management Systems (FDEMS), while large industrial and commercial sites could include multiple FDEMS and even multiple levels of FDEMS. Some DER systems will be managed by Retail Energy Providers through demand response programs, while others may be managed (not necessarily directly controlled) by utilities through financial and operational contracts or tariffs with DER owners.

[3] Diagrams of these 5 levels have been discussed and updated by the SGIP DRGS DEWG and by IEC TC57 WG17. They utilize the European Smart Grid Architecture Model (SGAM) structure. The draft White Paper can be found at http://iectc57.ucaiug.org/wg17/TF-MDER/Shared%20Documents/SGIP%20DRGS%20documents/DRGS%20Subgroup%20B%20White%20Paper%20-%20Categorizing%20Use%20Cases%20in%20Hierarchical%20DER%20Systems%2001-14-2014.docx

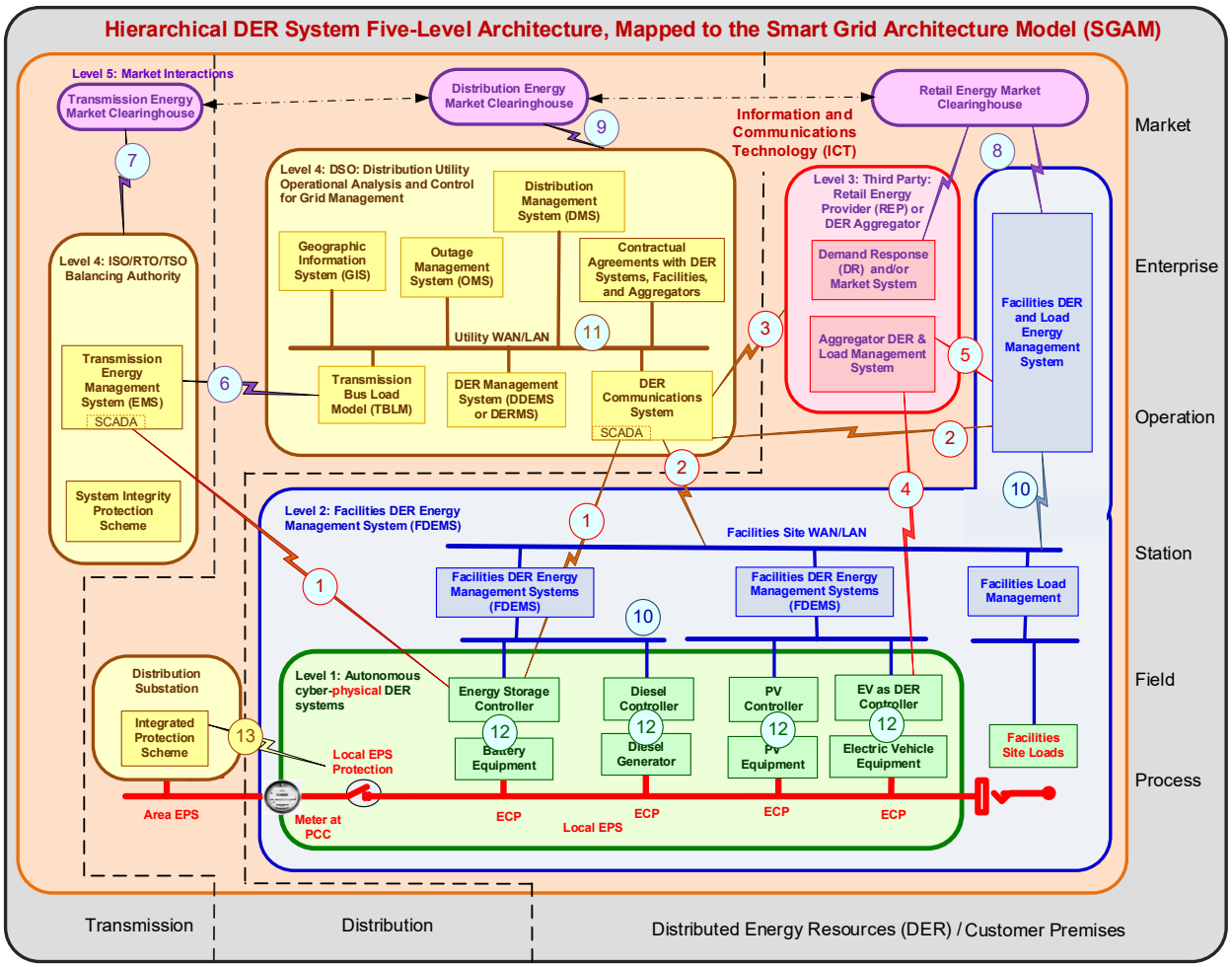

Figure 15: Five-Level Hierarchical DER System Architecture

4.4.2.3 DER Systems as Cyber-Physical Systems

DER systems are cyber-physical systems that are designed to provide electrical generation and/or energy storage within the distribution power system, but where resilience to adverse external forces is one primary goal. Both physical and cyber actions can have "real-world" impacts. Physically, generation systems have been protected against causing these real-world impacts since Thomas Edison pulled the switch in Pearl Station in 1882 to light up Wall Street for the first time in history. From the start, they included fuses to avoid voltage spikes from burning them down. They included voltage regulators to ensure the voltage remained in the proper range within the light bulbs. They used multiple generators so that one could be taken down while the other was maintained. Eventually transmission systems were designed with redundancy, monitoring, protection, and control to improve reliability.

Distribution systems have lagged transmission in automation, based on the concept that disruptions had limited impact on the loads of just a few customers and that extensive automation could not be cost-justified. However with the paradigm shift of increasing generation being supplied via DER systems and with the ever-increasing importance of electric power in the world economy, the impact of loss of DER generation is becoming an increasing concern.

A number of other technological changes have also taken place. As with many power system equipment, cyber controllers and embedded firmware have now been added to modern DER systems, thus blurring the distinction between power system devices and information systems. This additional automation helps to protect the equipment as well as to provide additional capabilities.

But at the same time, the cyber controllers and embedded firmware now can also be the cause real-world impacts due to both malicious cyber attacks as well as inadvertent cyber events. These cyber systems need to be protected from cyber threats, especially those that could cause harm to the physical devices or to the power system they are interconnected with. This need for cyber security of cyber assets is generally accepted – what is not well understood is how best to provide the required resiliency by combining the protections and capabilities provided by cyber technologies with the physical engineering technologies built into power system design and functions for over 100 years.

4.4.3 IEC/TR 62351-13: What Security Topics Should Be Covered in Standards and Specifications

IEC 62351-13 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. These suggestions cannot be prescriptive for every standard, since individual standards and specifications may legitimately have very different focuses, but it should be expected that the combination of such standards and specifications used in any implementation should cover these security topics. These suggestions could therefore be used as a checklist for the combination of standards and specifications used in implementations of systems.

This document is also being used as the basis for WG15 to assess the adequacy of cyber security in the standards developed by other TC57 working groups.

Some key items from that document include the following guidelines.

Cyber security clause: Even if the standard does not directly involve cyber security (e.g. an information model standard), the document should state that in a "cyber security requirements" clause. However, even a statement on where to find the relevant security policies and procedures would be beneficial, such as ISO/IEC 27019, NISTIR 7628, NERC CIPs, etc.

Key cyber security guidelines: All standards that do include some cyber security requirements should adhere to the following guidelines:

- Do not re-invent security requirements if they can be found in well-established standards.
- Include risk assessment: Threats, vulnerabilities, and failure scenarios along with possible impacts. This should include not only deliberate attacks but also inadvertent events such as equipment failures, natural disasters, and mistakes.
- Cover the following requirements and state where they are covered – in this standard or in a referenced standard:
  - **Authentication** of the systems, devices, and applications which are sending and receiving data, is generally the most important security requirement.
  - **Authorization** ensures that the requesting system has the right to view, receive, update, create, and/or delete the data. This is usually provided by Role-Based Access Control (RBAC).
  - **Non-repudiation** ensures that some entity cannot deny having received or acted upon a message.
  - **Accountability**, enhances non-repudiation by ensuring that all records of actions are traceable to their authors and are kept securely
  - **Data integrity** of all interactions and of information within the systems, is also critical. Data integrity of messages usually implies the need for authentication of the source of

the data, and the ability to detect tampering since it is not possible to prevent messages from being destroyed or modified, but it is possible to detect these actions.

- **Confidentiality** is usually required for financial, market, corporate, or private data, but is not usually necessary for normal power system operational data exchanges.
- **Availability** of the interactions can range from milliseconds to hours or days. Unlike the other cyber security requirements, availability generally relies on engineering design, configuration management, redundancy, functional analysis, communication network analysis, and engineering practices.

End-to-end security: Even if the standard does not cover all communications layers, the standard should state that security should be end-to-end, and provide either normative or informative references to other standards. End-to-end security not only addresses all communication layers, but should cover security policies, procedures, and technologies to ensure the secure and interoperable exchange of information between entities.

- Different security solutions and implementations by different vendors need to be interoperable. In particular, the interconnection of different security domains requires the mutual agreement between the parties about their security policies. Common minimum agreements on security policies will be required.
- Interconnection of security domains will also require the mutual agreement between the parties about their security policies, with common minimum agreements on security policies.

Security designed into the system from the beginning: security technologies should be designed into systems from the beginning, rather than being added "on top" of the system at a later date. Without such integrated security, the system will almost invariably have security "holes".

Note that the consideration of security during the creation of specifications has been taken over in the IEC Guide 120.

4.5 IEC 62351 Parts 90-x: Technical Reports

A number of technical reports have been developed. These usually involve use cases and discussions of the cybersecurity issues, and often act as stepping stones to the development or updating of IEC 62351 standards.

- IEC/TR 62351-90-1: Guidelines for Using Part 8 Roles
- IEC/TR 62351-90-2 Deep Packet Inspection
- IEC/TR 62351-90-3 Guidelines for Network Management
- IEC/TR 62351-90-4: Migration support to stronger cryptographic algorithms

4.6 IEC 62351 Parts 100-x: Conformance testing

4.6.1 IEC/TS 62351-100-3: Conformance test cases for IEC 62351-3

This technical specification which is part of the IEC 62351 series describes test cases of data and communication security for telecontrol equipment, Substation Automation Systems [SAS] and telecontrol systems, including front-end functions of SCADA.

The goal of this part of IEC 62351 is to enable interoperability by providing a standard method of testing protocol implementations to verify that a device fulfils the requirement of the standard. Note

that conformity to the standard does not guarantee interoperability between devices using different implementations. It is expected that using this specification during testing will minimize the risk of non-interoperability. A basic condition for this interoperability is a passed conformance test of both devices.

The scope is the specification of common available procedures and definitions for conformance and/or interoperability testing to ensure conformity to the IEC 62351-3. The conformance test cases defined here are focused to verify the conformant integration of the underlying authentication/encryption protocol (TLS), as specified in IEC 62351-3, to protect TCP/IP based communications.

This technical specification is not intended to test the underlying authentication/encryption protocol required by IEC 62351-3 to be implemented over TCP/IP (TLS). The conformance testing of the authentication/encryption protocol over TCP/IP is outside the scope of this document.

This part of IEC 62351 deals with data and communication security conformance testing; therefore, other requirements, such as safety or EMC are not covered. These requirements are covered by other standards (if applicable) and the proof of compliance for these topics is done according to these standards.

4.6.2 IEC/TS 62351-100-4: Conformance testing for 62351-4 with IEC 61850

This part of IEC 62351, which is a technical specification, describes test procedures for interoperability conformance testing of data and communication security for power system automation and protection systems which implement MMS, IEC 61850-8-1 (MMS), IEC 61850-8-2 (XMPP) or any other protocol implementing IEC 62351-4:2018/AMD1:2020. The tests described in this document cover only E2E security testing and do not evaluate A-security[4] profile implementation. Thus, citing conformance to this document does not imply that any particular security level has been achieved by the corresponding product, or by the system in which it is used.

The goal of this document is to enable interoperability by providing a standard method of testing protocol implementations, but it does not guarantee the full interoperability of devices. It is expected that using this document during testing will minimize the risk of non-interoperability. Additional testing and assurance measures will be required to verify that a particular implementation of IEC 62351-4:2018/AMD1:2020 has correctly implemented all the security functions and that they can be assured to be present in the delivered products. This topic is covered in other IEC standards, for example IEC 62443.

The scope of this document is to specify available common procedures and definitions for conformance and/or interoperability testing of IEC 62351-4:2018/AMD1:2020.

This document deals mainly with cyber security conformance testing; therefore, other requirements, such as safety or EMC are not covered. These requirements are covered by other standards (if applicable) and the proof of compliance for these topics is done according to these standards.

T-profile testing should be performed prior to E2E security profile testing. T-profile testing is described in 62351-100-3 in the context of 61850-8-1. T-profile testing for IEC 61850-8-2 should be described in the corresponding IEC 61850-8-2 test specification.

4 A-profile is specified in IEC 62351-4:2020 for backward compatibility with IEC 62351-4:2007.

4.6.3 IEC/TS 62351 Part 100-5: Conformance testing for IEC 60870-5-7 (Part 3/5)

The scope of this technical specification is to specify common available procedures and definitions for conformance and/or interoperability testing of the IEC 62351-5, the IEC 60870-5-7 and their recommendations over the IEC 62351-3. These are the security extensions for IEC 60870-5 and derivatives.

IEC TC57 WG3 has developed a document for conformance testing of IEC 60870-5-101 and IEC 60870-5-104, respectively the IEC/TS 60870-5-601 and the IEC/TS 60870-5-604.

The same arguments for defining this proposed document are also valid for the 62351-5 and IEC 62351-3 applied to the IEC/TS 60870-5 series through the IEC/TS 60870-5-7 for secure data exchange. The widespread use of the IEC 60870-5 and the increasing use of its data communication security through the 62351 around the world justify the definition of test procedures for IEC 62351-5, IEC 60870-5-7, and their recommendations over IEC 62351-3 for profiles including TCP/IP.

4.6.4 IEC/TS 62351-100-6-1: Conformance testing for 62351-6 with IEC 61850-8-1 and 61850-9-2

IEC TS 62351-100-6, which is a technical specification, is part of the IEC 62351 suite of standards, which describes test cases for interoperability conformance testing of data and communication security for telecontrol equipment, Substation Automation Systems [SAS] and telecontrol systems which implement IEC TS62351-6. The tests described in this part do not evaluate the security of the implementation. Thus, citing conformance to this part does not imply that any particular security level has been achieved by the corresponding product, or by the system in which it is used.

The goal of this part of IEC 62351 is to enable interoperability by providing a standard method of testing protocol implementations, but it does not guarantee the full interoperability of devices. It is expected that using this specification during testing will minimize the risk of non-interoperability. Additional testing and assurance measures will be required to verify that a particular implementation of IEC TC 62351-6 has correctly implemented all of the security functions and that they can be assured to be present in all delivered products. This topic is covered in other IEC standards, for example IEC 62443.

The scope of this document is to specify common available procedures and definitions for conformance and/or interoperability testing of IEC 62351-6, the IEC 61850-8-1, IEC 61850-9-2 and also their recommendations over IEC 62351-3 for profiles including TCP/IP and IEC 62351-4 for profiles including MMS. These are the security extensions for IEC 61850 and derivatives to enable unambiguous and standardized evaluation of IEC TS 62351-6 and its companion standards protocol implementations.

The detailed test cases per companion standard, containing among others mandatory and optional mandatory test cases per Secure Communication Application Function, secure ASDU (Application Service Data Unit) and transmission procedures, will become available as technical specifications (TS). Other functionality may need additional test cases, but this is outside the scope of this part of IEC 62351. For proper testing, it is recommended to define these additional test cases. This document is such a technical specification for the mentioned companion standard.

This document deals mainly with data and communication security conformance testing; therefore, other requirements, such as safety or EMC (Electromagnetic compatibility) are not covered. These requirements are covered by other standards (if applicable) and the proof of compliance for these topics is done according to these standards.

Annex A References

[1] IEC 62351-Series: “Power Systems Management and associated information exchange – Data and Communication Security, https://webstore.iec.ch/publication/6912

[2] IEC 60870-5: “Telecontrol equipment and systems - Part 5: Transmission protocols”, https://webstore.iec.ch/publication/3755; focus here are 101 and 104

[3] IEC 61850: “Communication networks and systems for power utility automation”, https://webstore.iec.ch/publication/6028

[4] ISO 27001: “Information technology - Security techniques - Information security management systems - Requirements”, https://webstore.iec.ch/publication/11286

[5] ISO 27019: “Information technology - Security techniques - Information security controls for the energy utility industry”, https://webstore.iec.ch/publication/61906

[6] ISO 27002: “Information technology - Security techniques - Code of practice for information security controls”, https://webstore.iec.ch/publication/11288

[7] ISO 27005: “Information technology - Security techniques – Information security risk management”, https://webstore.iec.ch/publication/63500

[8] NIST Cyber Security Framework, https://www.nist.gov/cyberframework

[9] NISTIR 7628: Guidelines for Smart Grid Cybersecurity, https://doi.org/10.6028/NIST.IR.7628r1

[10] IEC 62443 Series: “Industrial communication networks - Network and system security”

[11] IEC TC57 WG15: IEC 62351 Security Standards for the Power System Information Infrastructure, White Paper 02/2016, available on public IEC TC57 WG15 website: http://iectc57.ucaiug.org/IEC%20WG%20Shared%20Documents/WG15%20Public%20Documents/IEC%2062351%20Cyber%20Security%20Standards%20from%20WG15,%202-2016.docx

[12] IEC/IS 62351-9, Power systems management and associated information exchange – Data and communications security – Part 9: Cyber security key management for power system equipment, Edition 1.0, 2017-05

[13] ISO/IEC 9594-8, Information technology – Open Systems Interconnection – The Directory – Part 8: Public-key and attribute certificate frameworks

[14] BSI TR 03109-4, Smart Metering PKI – Public Key Infrastruktur für Smart Meter, Version 1.2.1, 2017-08

[15] Enrollment over Secure Transport – EST, RFC 7030, https://tools.ietf.org/html/rfc7030, 10-2013

[16] Simple Certificate Enrollment Protocol – SCEP, draft-nourse-scep-23, https://tools.ietf.org/html/draft-nourse-scep-23, 09-2011

[17] Whitepaper, Requirements for Secure Control and Telecommunication Systems, Version 2.0, 05/2018, BDEW - Federal Association of Energy and Water Industries and Energy Austria, Berlin, https://www.bdew.de/media/documents/Awh_20180507_OE-BDEW-Whitepaper-Secure-Systems.pdf

[18] IEC/TR 62351-8, Power systems management and associated information exchange – Data and communications security – Part 8: Role-based Access Control, Edition 1.0 2011-10

[19] IEC/TR 62351-10, Power systems management and associated information exchange – Data and communications security – Part 10: Security architecture guidelines, Edition 1.0 2012-10

[20] STRIDE Threat Modeling, https://docs.microsoft.com/en-us/previous-versions/commerce-server/ee823878(v=cs.20)

[21] IEC Guide 120, Security aspects - Guidelines for their inclusion in publications, 10/2023, https://webstore.iec.ch/publication/79273