# Securing the Power System Information Infrastructure

## IEC 62351 Application Notes

## Volume 2: From Requirements to Solutions

## September 2024

| | |
|---|---|
| Version | 1.0 |
| Date | 2024-09-27 |

# Contents

## Figures

## Tables

# 1 Introduction

## 1.1 Motivation

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:

- Volume 1: Overview of the IEC 62351 series of cybersecurity standards
- Volume 2: From Requirements to Solutions: addressing specific cybersecurity requirements, which are know from IEC 62443 and also the NIST CSFW, with IEC 62351 means
- Volume 3: Application Examples of IEC 62351.

This document is Volume 2. It uses commonly available cybersecurity frameworks like IEC 62443 [11] and the NIST Cybersecurity Framework [9] to correlate between cybersecurity standards describing the "what" with IEC 62351 describing the "how" for certain technical aspects.

The IEC 62351 application notes are intended to provide an overview of the framework [1] and examples [2] for utilizing specified IEC 62351 [3] functionality to secure a power system communication infrastructure as dedicated target domain. The focus is placed on deployment environments, which utilize IEC TC 57 defined communication standards like the telecontrol protocols IEC 60870-5 [4] or the control protocol IEC 61850 [5] and the corresponding data models. This comprises installations in the substation automation domain, distribution automation, equipment integration like decentralized energy resources, but is not limited to these. The goal is to show the contribution of different IEC 62351 parts in the setup and operation of power system automation.

The term "secure power system" addresses different aspects of operating a power system securely. One aspect is the protection of data in transit (communication) for monitoring, control, and maintenance of a power automation system. A technical precondition for this protection is the distribution and application of security key material and security policies to the authorized entity and therefore, the support for (component and user) authentication and authorization. A further aspect relates to the security of data at rest (integrity, confidentiality). Besides securing the monitoring of the power system functions, also the security monitoring during normal operation is considered to provide additional information for network management tools and to add support for anomaly or threat detection based on an enhanced view of the network. In addition, technical security measures are always accompanied by a security process, which also relies on the provided technical security measures.

Note that this document concentrates on the application of IEC 62351 and does not address the derivation of security requirements. More specifically, it is expected that power systems as a critical infrastructure are operated in accordance with an information security management like ISO 27001 [6]. Specifically, for power systems, ISO 27019 [7] provides an augmentation of the cybersecurity controls defined in ISO 27002 [8] to address the needs for the power system domain. Other examples targeting a security framework are provided by the NIST Cyber Security Framework [9] or the NISTIR 7628 for Guidelines on Smart Grid Security Controls [10]. In addition to the operation, an integrator may leverage parts of the IEC 62443 series [11] 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. The manufacturer may leverage further information for the development process. IEC 62351 in this respect specifies the necessary technology to address the derived requirements and to realize dedicated security controls. The following figure shows the interplay of security requirements stemming regulation like the European NIS Directive [12] or the US FERC [13] and the potential security measures defined in the ISO/IEC 270xx series, the IEC 62443 framework and IEC 62351 as domain specific security standard.

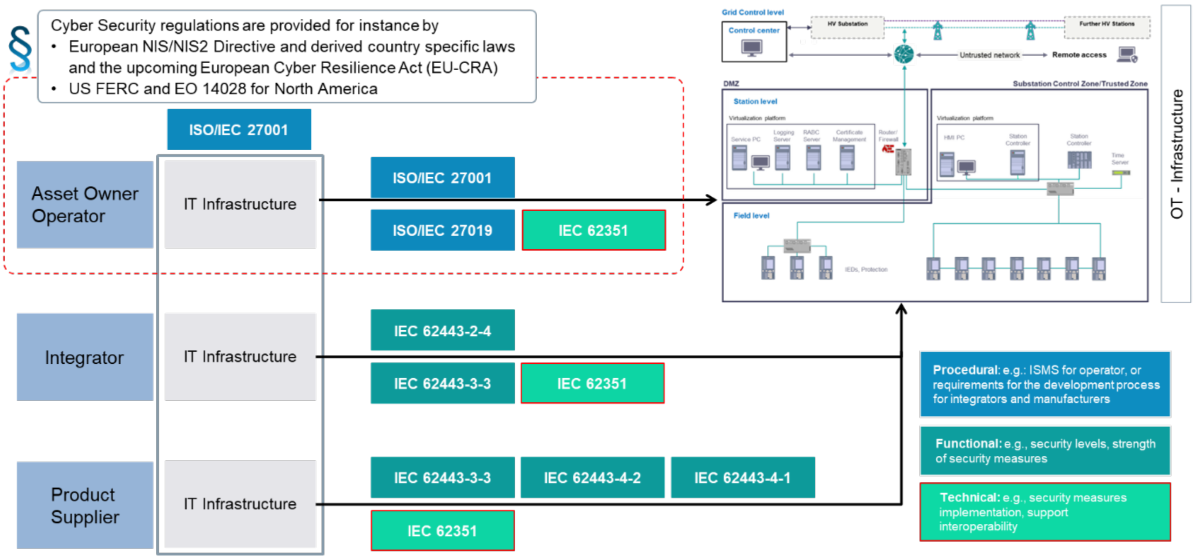


**Figure 1: Interplay of Cybersecurity Standards to address regulative requirements in the power system domain**

More insight into potential security threats and the derivation of security requirements based on a risk-based approach for the power system domain can also be found in [13]. 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.

This volume of the IEC 62351 application notes concentrates on the mapping of IEC 62351 defined security measures to a set of exemplary but typical security requirements seen in power automation installations comprising substation automation, transmission and distribution networks, equipment integration and further.

To make the application more visible, an illustrative application scenario is used on the base of a substation, in which most security requirements collude. Here, most of the technology specified in IEC TC 57 is applied, which allows to discuss the application of IEC 62351 more concisely. Volume 3 of the IEC 62351 Application notes [2] provides more examples and describes selected use cases for applying security functionalities specified in IEC 62351 like securing remote control, role-based access control, and smart authentication.

This document is structured as following. Clause 1.2 describes the target audience. Clause 1.3 defines the utilized terms, which have not been specified in other part. Clause 2.1 motivates the derivation of security requirements based on a risk-based approach and provides abstract security requirements, which are taken for the further elaboration on IEC 62351 application. Clause 2.3 is the main part of this document and discusses the application of IEC 62351 parts to address the abstract security requirements. For this the product development steps are being followed starting with the use case analysis and the definition of (here example) security requirements and the utilization of different IEC 62351 through the lifecycle to address the derived requirements. The different steps contain take away's as summary on the application of specific IEC 62351 parts.

## 1.2 Target Audience

Target audience for this document are system architects, operator, integrator, and manufacturer of power automation system components, who oversee planning and operating components of the digital grid. Note that this document only provides an overview about the provided functionalities, but not necessarily 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.

For more insight into the structure and content of the IEC 62351 framework, the reader is referred to Volume 1 of the application notes. For more specific examples on the application of selected IEC 62351 parts, Volume 3 of the application notes should be consulted.

## 1.3 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 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 Planning for cybersecurity implementation

## 2.1 Prerequisite: Analysis of risks and derivation of security requirements

A necessary prerequisite before applying any security measures is the definition of security requirements. Besides the derivation of security requirements from existing requirement specifications (e.g., from regulation, standard frameworks, guidelines, or tenders), this is typically done based on a risk-based approach considering the specific needs of the use case and the intended operational environment. There are different approaches available to perform a threat and risk analysis. As an example, ISO 27005 [15] provides a framework for risk management, while STRIDE (Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege) [16] provides an approach for threat modeling. It is assumed that the reader has an appropriate process in place.

For the definition of security requirements targeting the power system automation domain, the reader is referred to the standards ISO 27001 [6] for an information security management framework, ISO 27019 [7] for an augmentation of the security controls defined in ISO 27002 [8] for power systems, and IEC 62443 [11] during the target architecture definition process (specifically IEC 62443-2-4) and the determination of the required security controls. IEC 62351 specifically concerns manufacturers, integrators and operators and addresses technical security requirements for systems in its part 3-3 and for components in part 4-2. Likewise, the NIST Cyber Security Framework (NIST CSFW [9]) addresses security in a holistic view, covering processes of an organization and technology.

It should be noted that these standards are continuously being updated, so it is possible that a particular reference has been updated or the numbering changed: it is impossible to keep up with all changes.

To illustrate the application of IEC 62351, substation automation is taken as generic use case as outlined in section 1.1 To concentrate on the application of IEC 62351, the following generic security requirements are assumed to be met for substation automation. As stated before, security requirements in general may be posed though regulative requirements for critical infrastructures.  Moreover, specific security requirements have to be derived for the specific environment as outcome of a risk assessment.

They reflect typical security requirements for communication systems, which can also be found for instance in ISO/IEC 27001/19 and IEC 62443-3-3 (systems) and IEC 62443-4-2 (devices) and the NIST CSFW as outlined below the requirements.

Note: These security requirements do not constitute normative requirements, but they can easily be mapped to security requirements from IEC 62443 and the NIST CSFW. The listed requirements should not be considered complete. They are used here to show how IEC 62351 can be applied.

[R 1] Communication endpoints shall authenticate, when sessions are established. This typically results in mutual authentication.

[R 2] Role-based access control shall be done at least for remote access and should be supported in substation internal access.

[R 3] Communication that crosses the substation perimeter is to be secured regarding confidentiality and integrity.

[R 4] Interactions based on TCP/IP links in station level zone shall be secured at least regarding integrity and optionally for confidentiality.

[R 5] Interactions based on serial links shall be protected regarding the integrity of the communication.

[R 6] Communication in the process bus zone shall be protected regarding the integrity of communicated data.

[R 7] Security state of the components and the communication shall be monitored. Depending on detected cyber security events an eventing/alarming procedure is required on a technical level as well as a reaction plan on organizational level.

The generic requirements relate on one hand to the communication (on transport and application layer) and result in an enhancement of the utilized protocols to incorporate the required security functionality. On the other hand, the requirements may lead to additional functional elements to be considered in the substation as deployment infrastructure. An example additional element may be a PKI component, to provide certificates for substation components.

The following table maps the generic requirements to specific requirements found in the context of IEC 62443 (focusing on the technical parts -3-3 and -4-2) and the NIST CSFW 2.0.

**Table 1: Mapping of generic technical requirements to controls from existing frameworks**

| Generic Requirement | IEC 62443-3-3/-4-2 | NIST CSFW 2.0 |
|---|---|---|
| **[R 1]**: Endpoint authentication during communication (mutually) | **IEC 62443-3-3:2013** SR 2.1, SR 2.2, SR 2.3, SR 2.4, SR 2.5, SR 2.6, SR 2.7<br>**IEC 62443-4-2:2019** CR 2.1, CR 2.2, CR 2.3, CR 2.5, CR 2.6, CR 2.7 | **PR.AA-01**: Identities and credentials for authorized users, services, and hardware are managed by the organization<br>**PR.AA-02:** Identities are proofed and bound to credentials based on the context of interactions<br>**PR.AA-03:** Users, services, and hardware are authenticated<br>**PR.AA-04:** Identity assertions are protected, conveyed, and verified |
| **[R 2]**: Authorization of remote access based on roles or attributes | **IEC 62443-3-3:2013** SR 2.1, SR 2.2, SR 2.3, SR 2.4, SR 2.5, SR 2.6, SR 2.7<br>**IEC 62443-4-2:2019** CR 2.1, CR 2.2, CR 2.3, CR 2.5, CR 2.6, CR 2.7 | **PR.AA-05:** Access permissions, entitlements, and authorizations are defined in a policy, managed, enforced, and reviewed, and incorporate the principles of least privilege and separation of duties |
| **[R 3]**: Communication integrity and confidentiality across zones | **IEC 62443-3-3:2013** SR 3.1, SR 3.8, SR 4.1<br>**IEC 62443-4-2:2019** CR 3.1, CR 3.8, CR 4.1 | **PR.DS-01:** The confidentiality, integrity, and availability of data-at-rest are protected<br>PR.DS-02: The confidentiality, integrity, and availability of data-in-transit are protected<br>PR.DS-10: The confidentiality, integrity, and availability of data-in-use are protected<br>**PR.IR-01:** Networks and environments are protected from unauthorized logical access and usage<br>**PR.IR-03:** Mechanisms are implemented to achieve resilience requirements in normal and adverse situations |
| **[R 4]**: TCP-based communication integrity and optional confidentiality in same zone | **IEC 62443-3-3:2013** SR 3.1, SR 3.8, SR 4.1<br>**IEC 62443-4-2:2019** CR 3.1, CR 3.8, CR 4.1 | **PR.DS-01:** The confidentiality, integrity, and availability of data-at-rest are protected<br>**PR.DS-02:** The confidentiality, integrity, and availability of data-in-transit are protected<br>**PR.DS-10:** The confidentiality, integrity, and availability of data-in-use are protected |

| Generic Requirement | IEC 62443-3-3/-4-2 | NIST CSFW 2.0 |
|---|---|---|
| | | **PR.IR-01:** Networks and environments are protected from unauthorized logical access and usage |
| **[R 5]**: Serial link communication integrity | **IEC 62443-3-3:2013** SR 3.1, SR 3.8<br>**IEC 62443-4-2:2019** CR 3.1, CR 3.8 | **PR.DS-01:** The confidentiality, integrity, and availability of data-at-rest are protected<br>**PR.DS-02:** The confidentiality, integrity, and availability of data-in-transit are protected<br>**PR.DS-10:** The confidentiality, integrity, and availability of data-in-use are protected<br>**PR.IR-01:** Networks and environments are protected from unauthorized logical access and usage |
| [**R 6]**: Process zone communication integrity | **IEC 62443-3-3:2013** SR 5.1, SR 5.2, SR 5.4<br>**IEC 62443-4-2:2019** CR 5.1, CR5.2, CR 5.4 | **PR.IR-01:** Networks and environments are protected from unauthorized logical access and usage<br>**PR.IR-03:** Mechanisms are implemented to achieve resilience requirements in normal and adverse situations |
| **[R 7]:** Monitoring of component security and security event handling | **IEC 62443-3-3:2013** SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1, SR 6.2<br>**IEC 62443-4-2:2019** CR 2.8, CR 2.9, CR 2.10, CR 2.11, CR 3.9, CR 6.1, CR 6.2 | **DE.CM:** Continuous Monitoring, Assets are monitored to find anomalies, indicators of compromise, and other potentially adverse events<br>**DE.AE:** Adverse Event Analysis, Anomalies, indicators of compromise, and other potentially adverse events are analyzed to characterize the events and detect cybersecurity incidents<br>**RC.RP:** Incident Recovery Plan Execution, Restoration activities are performed to ensure operational availability of systems and services affected by cybersecurity incidents<br>**RC.CO:** Incident Recovery Communication, Restoration activities are coordinated with internal and external parties |

## 2.2 Application of IEC 62351 to support security along systems lifecycle

As outlined in volume 1 of the application notes[1], IEC 62351 consist of multiple parts, either addressing the security of specific target communication protocols and the associated data exchange or the provisioning of the necessary infrastructure to enable the security and monitor its use. In the following, the application of different IEC 62351 parts will be motivated by relying on one example scenario, in which most of the technology defined in IEC TC57 is applied. Figure 2 below takes substation automation as example. This also aligns with IEC 62351-10, in which substation automation is taken as example for placing security controls.

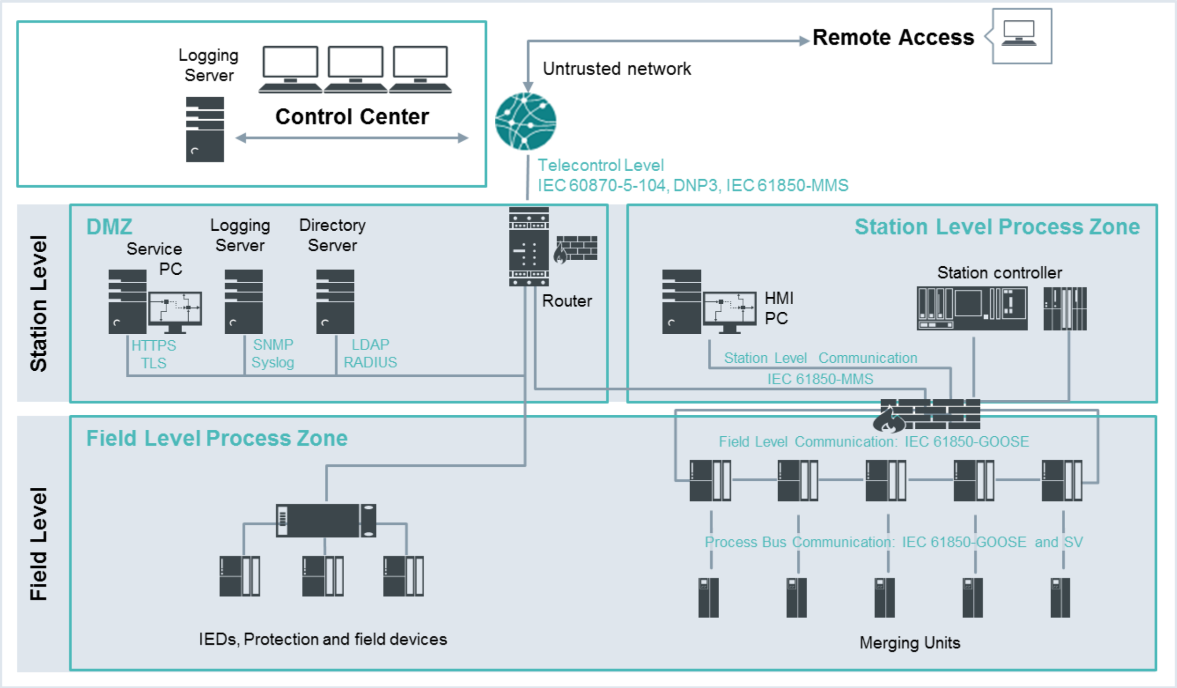


**Figure 2: Overview on a substation automation setup as example**

Based on an example substation automation setup, the following architectural boundary conditions can be assumed:

- A substation is divided into different zones in order to separate the information exchange according to the administrative boundaries and the process conditions. This approach is also being followed in IEC 62351-10. Zones selected are
    - **DMZ** building the transition zone between internal and external communication. Moreover, several security relevant components, like a directory, logging services, historian server and certain PKI services are typically placed here.
    - **Station level process zone** to provide oversight of the substation status based on measurement from the field level process zone as well as control of IEDs in the field level process zone. This zone is expected to use IEC 61850 with MMS for communication, e.g., between the substation controller, HMI and the field level devices.
    - **Field level process zone** encapsulates the real-time communication parts, utilizing protection devices. They communicate using IEC 61850 GOOSE and SV to communicate measured values and status information.

- Substation external communication with a control center is performed using protocols like IEC 61850, IEC 60870-5-104, or DNP3 (IEEE 1815).

- Remote access, e.g., for maintenance is performed using protocols like RDP, IPSec (VPN-based access) or other terminating in the DMZ to enable maintenance or engineering operations.

The application of IEC 62351 to support cybersecurity in substation automation contributes in different deployment phases of a substation. These phases involve different stakeholders as there are:

- **Operator**: is typically also the asset owner and defines the requirements on functional and operational level for the target solution. This also includes security requirements to cope with his security policy.

- **Integrator**: responsible for the product/component selection and integration into the requested target solution. This comprises the definition of security features to be supported in the components.

- **Manufacturer** developing, producing, and providing the requested components.

Focus for the following discussion are the operator (asset owner) and the integrator as they need to address security in the overall system design.

The deployment and operation phases can be roughly described as:

1. **Determination and evaluation of potential risks** for the operational use case, i.e. in the context here the operation of a substation. This is typically done by the operator.
2. **Derivation of system and security requirements** based on the risk evaluation. This is typically done by the operator.
3. **System and security architecture design** (here the substation) to address the system and security requirements. This is typically done by the integrator.
4. **System realization**: This phase specifically includes the component selection and the setup of a solution/system. This is typically done by the integrator aligned with the operator, using components from manufacturers providing the requested (security) functionalities.
5. **System engineering** (and commissioning) according to the target operational environment. This is typically done by the operator in conjunction with the integrator. Consequently, this also relates to security relevant tasks like setup of the security infrastructure to support credentials allowing identification and authentication of communication peers as well the definition of allowed components and communication protocols. Note that this step includes on one hand technical measures for an operator defined security policy (e.g., RBAC). On the other hand, there may be additions to the operator’s security process, based on implemented security measures.
6. **Operation and maintenance**: In the main phase, data exchange security is based on the provided credentials and security policy configuration. In this phase the security of the communicating peers (authenticity and authorization) and the exchanged data (integrity and confidentiality) is in focus, based on the appropriate selection of security measures. Besides the substation automation operation, also the security management has to be performed in parallel to ensure the validity of utilized credentials (and security policies), but also to monitor and log security relevant events. Note that this phase comprises the normal operation but also maintenance and service and is therefore relevant for the operator.

Note that the participants in the different phases may vary, so the description above may be taken as example.

The phases 1 and 2 are already addressed in section 2 before on an abstract level. The following subsections build on the generic requirements and address the phases 3-6 to show how IEC 62351 supports the different phases.

## 2.3 System design considerations

### 2.3.1 General design considerations

During the design of a system security architecture IEC 62351-10 provides support for the by discussing general security considerations for setting up an architecture following security-by-design. With this it relates directly to the security requirements [R 1] to [R 7] and can be mapped to the substation automation architecture in Figure 2. Certain design aspects are already visible in the substation automation architecture like the separation into zones with different security requirements. Besides the internal separation, a DMZ has been placed into the substation to shield the devices residing in the substation from unauthorized external access but also have a clear separation for the process network on the internal side. Typically, in the DMZ reside services for remote access, the historian, and infrastructure services like a directory, RADIUS server, or PKI components. Further security measures like network access control for IEDs participating in the network may be taken additionally.

To enable the substation for secure operation necessary security functionality as well as parameter distribution and configuration needs to be enabled and supported by the components. As seen in the IEC 62351 overview, several parts relate to securing the communication protocols, as there are Parts 3/4/5/6. Common to all IEC 62351 parts is the need for security credentials for component and/or user authentication. The credentials used are typically X.509 certificates. This requires on one hand additional infrastructure components to manage these certificates; on the other hand, the substation components consequently need to support the necessary management interfaces to interact with the management components.

### 2.3.2 Management of authentication credentials (targets [R 1])

To support IEC 62351 security measures, all considered components are expected to possess an X.509 certificate, a corresponding private key and a trusted root CA certificate, which are employed for mutual authentication. Mutual authentication can be applied in different communication relations, for instance for communication using IEC 60870-5-101/-104, IEC 61850 MMS, as well as GOOSE and SV in the substation and routed variants.

To support mutual authentication, IEC 62351-9 specifies the management of security credentials of asymmetric keys but also for symmetric keys. For the asymmetric keys the interaction with a Public Key Infrastructure (PKI) to issue and manage certificates is defined. The standard itself leaves the placement of the certificate management in the overall architecture open. Essentially there are different approaches possible by either operating a PKI directly within the substation, solely managing the certificates for devices residing in the substation.

The next hierarchical level of the PKI typically resides in the control center, which may also be used to issue substation internal certificates. Note that the latter requires to have consistent connection to be able to maintain the installed certificates. The PKI in the control center may also be used for fall back situations if the substation PKI is not operating or to construct a PKI hierarchy. Part 9 defines how to utilize SCEP (Simple Certificate Enrollment Protocol) and EST (Enrollment over Secure Transport) as protocols for certificate management to interact with a PKI. Specifically, the infrastructure managing the operational device certificates needs to support both protocols, to allow integration of devices supporting typically only a single protocol.

The endpoints (IEDs) requesting certificates only need to support one of the enrollment protocols. The decision which one to use depends on the type of credential to be used (RSA-based certificate, ECDSA-based certificate) and the connectivity to the PKI component. In this regard, SCEP supports RSA-certificates, while EST supports both types. Which type of certificate is used depends on the security policy of the operator and needs to be considered by the integrator.

Furthermore, during the system design it is necessary to determine the trust relations between the components. This relates to the definition of one or a set of trusted root CA as well as the distribution of component specific credentials, which are derived from a trusted root CA. The selection of a trusted root CA is not described in IEC 62351 and is expected to be done by the operator based on his security policy. This information is expected to be determined by the system integrator based on the security requirements provided operational security boundary conditions from the operator. The selected trusted root CA certificates are typically part of the engineering information.

An additional component to support certificate handling inside the substation is a server providing the revocation state (Certificate revocation List, CRL) for the utilized certificates in the substation. This information is queried by the components when validating received certificates. IEC 62351 requires support for a CRL. Alternatively, the status check may be performed using the Online Certificate Status Protocol (OCSP) to fetch the status of a single certificate. In this case the CRL server (residing in the DMZ) would be configured to work as OCSP responder substation internally.

In addition to certificate management, IEC 62351-9 also defines the management of symmetric keys utilized to secure IEC 61850 GOOSE communication. This requires a key distribution service (typically provided by a key distribution center – KDC), which may be collocated with an existing security infrastructure component like a local PKI or a standalone component. The KDC is the base to secure IEC 61850 GOOSE communication using a so-called group-based communication approach, in which all entities share a symmetric group key. To support group-based secure communication the actual trust groups sharing the same symmetric group key, need to be defined. For this it is necessary to provide the KDC with at least the following information is expected during the engineering:

- the certificates corresponding to the IEDs forming a group. Based on this information and the component authentication, the group key is distributed (see also the management of authentication credentials above regarding information for certificate verification).
- configuration of a key renewal interval to allow for an update of the group key (depending on the operator’s security policy)

Note that it is most likely that the components handle different certificate/private key pairs and root CA certificates to fulfil their operational purpose. The number of certificates utilized by a component depends on the security policy of the operator. It may be the case that distinct authentication credentials for a dedicated purpose are needed. An example may be certificates, which are used, if the device acts as client or server or related to a specific application. In addition, different certificates may be used to protect the transport layer (e.g., TLS) or the application layer (e.g., IEC 61850).

Note that for the different functionalities supporting the management of credentials for authentication and authorization may collapse on a single physical component. The functional split into components depends on the selected products by the integrator.

Volume 3 of the IEC 62351 Application notes [2] provide more information on the certificate management by providing more detailed information about the PKI components and potential approaches for certificate enrollment for manufacturer and operator.

Take away: IEC 62351-9 provides the base for management of authentication credentials for direct communication as well as for group-based communication. Authentication for direct communication is typically based on X.509 certificates and IEC 62351-9 describes the management of these certificates throughout the lifecycle of components.

### 2.3.3 Role based access control (targets [R 2])

Besides the identification and authentication of users and components, authorization to perform certain actions is typically required. To enable this, IEC 62351-8 specifies options for role-based access control. The authorization information is provided as access token, which is bound to the authentication of the user/component. IEC 62351-8 supports the engineering by already defining a set of roles to be supported. Further roles may be defined to address specific requirements of a substation operator. To enable an interoperable exchange of role definition information IEC 62351-8 provides an exchange format for roles specified by the operator. Roles are defined by assigning permissions to a newly defined role. Information about defined roles must be distributed to all components, which need to recognize the specific role. In case of the substation scenario outlined in Figure 2, components are typically protection devices and RTUs on field level but also components like HMIs or substation controller on station level.

The exchange format is defined using the standard XACML, which is expected to be supported by engineering tools or the components directly. To assign a role to a user, further information is necessary. Besides the role information also the area of responsibility (AoR) is to be defined. An example for this value may be the location of the specific substation as “Germany.Bavaria.Munich.Perlach”. This information (defined roles, AoR) must be provided to the components in the substation for verification of the applicability of a presented role as well as in the access token used for RBAC. In addition, all components need to be configured with a trusted issuer for the RBAC access tokens. In case of certificates it may be the same or the same set of root CA. The role assignment tool must be configured with the role definition as well as the AoR information. This tool must also allow to specify the validity period of the access tokens. If the role information is part of a certificate, the role assignment to a user or component must be included during the management of authentication credentials stated above.

To ease the application of RBAC in terms of necessary infrastructure and know how support, IEC 62351-8 allows to start integrating RBAC by means of the already known login process using username/password combinations. Following this approach uses the IEC 62351-8 defined PULL procedure, which allows the accessed device to query the necessary RBAC information from a central repository, using LDAP or RADIUS protocol. Using a directory service based on LDAP in the backend even allows for utilizes certificates carrying the RBAC information in the backend communication, without involving the subjects/components in the certificate handling itself. This has the advantage for already existing devices, not providing means for a certificate-based user authentication. Alternatively, IEC 62351-8 defines fetching the RBAC information by the subject upfront. This information can then be provided to the accessed component directly. This approach is called PUSH. PUSH has the advantage, that the components (IEDs) do not need to have an own connection to a central repository. As a further variant also the combination of both, e.g., PULL for long term credentials (like a public key certificate) and PUSH for short term credentials (like an attribute certificate) is possible. The decision if PULL or PUSH or a combination of both is realized for RBAC depends on the integration into a potentially existing operational environment and the provided functionality by the selected components. Depending on the selected approach additional components are necessary for storing the RBAC information like a RADIUS or LDAP server. Moreover, depending on the chosen access token type, PKI components are necessary for managing public key certificates or attribute certificates containing RBAC information. Note that IEC 62351-8 offers different profiles for RBAC handling, which allow easy integration into existing infrastructures. This requires matching the profiles supported by components with the desired functionality in the target system (e.g., when RBAC is done based on X.509 certificates, this functionality consequently needs to be supported by the components in the substation and by the system engineering.

To support RBAC a directory server may be placed in the substation's DMZ. It supports RBAC management within the substation and may work in conjunction with a directory server in the control center. This supports situations, in which the user management is performed on control center level, while the role assignment is done on substation level. Note that to ensure operation with RBAC also in emergency cases specific enhancements in the architecture may need to be considered by the integrator. This may be addressed by providing a read only domain controller to replicate certain information from the active directory in the control center. Alternatively, the RBAC handling may be solely done within the substation utilizing emergency accounts.

Volume 3 of the IEC 62351 Application notes [2] provides specific examples for role-based access control for remote access scenarios. In addition, a realization option for a combined authentication and authorization option is described, which not only performs the role-base access control part but also the system state of the accessing component (e.g., a service technicians' laptop).

Take away: IEC 62351-8 provides the different profiles to support authorization. Selection of a profile or of multiple profiles depends on the target operational environment and may be done based on already existing components or based on a specific technical approach (e.g., relying on X.509 certificates for authorization decisions).

### 2.3.4 Enabling secure communication and application interaction (targets [R 3] through [R 6])

Secure communication is supported by applying the issued component credentials (certificates and corresponding private keys, trusted root CA), which are used in the context of authentication and key agreement. In power system automation different communication stacks are used as there are serial communication, or TCP/IP based communication. In addition to transport security, also security on the application becomes necessary, especially if the application requires security features independent from the transport layer.

TCP/IP based communication (e.g., IEC 61850 MMS, IEC 60870-5-104, IEEE 1815) is protected by utilizing TLS as additional communication protocol according to IEC 62351-3. The general support of TLS options is determined in the IEC 62351-3 and relates to the configuration of at least the following information

- assigned ports on which a TLS server runs (typically dependent on the protected protocol)
- accepted certificates during the TLS handshake phase based on the trusted root CAs as well as certificate revocation check information.
- session management information like session resumption and session renegotiation intervals
- selection of optional cipher suites in addition to the mandatory cipher suites specified.
- security policy for handling failed authentication during the TLS handshake (potential graceful degradation, etc.)
- handling of security events provided during the validation of certificates or during communication.

In addition to the transport security also application layer security may be necessary. The necessity for application layer security depends on the use case and may be related to a dedicated authorization of a requestor on application layer or on the possibility that the communication link between the communicating peers spans multiple (maybe even TLS protected) communication hops. Both use cases require an end-to-end security. IEC 62351-4 provides two different security profiles. The A-profile allows for user authentication and potentially authorization in single transport hop scenarios, while the E2E-profile provides in addition a secured session on application layer and targets multi-hop scenarios. The latter can be used for instance when integrating equipment over publish-subscribe mechanisms, which are defined in IEC 61850-8-2. Note that the E2E-profile is intended to replace the A-profile in the long run, also for single hop communication as it provides a higher security. Also for telecontrol communication using IEC 60870-5-104 application layer security can be provided as outlined in IEC 62351-5.

Protection of serial communication (e.g., IEC 60870-5-101) requires the definition of a set of symmetric keys and associated security policies between the different entities. The configuration of security services for serial communication contains at least:

- symmetric session keys used to authenticate the requestor in a challenge response procedure before the responder performs a critical command.
- symmetric update key to provide means to update the session keys after a defined interval
- the security policy should contain at least
    - the selection of the key update key method, which is either symmetric or asymmetric. In case of asymmetric, the certificates of the receiver need to be available at the requestor side. Note that the update using certificates is only possible with RSA based certificates.
    - the number of re-key runs before changing the update key either per symmetric or asymmetric approach

The third type of transport relates to multicast communication using IEC 61850 GOOSE. In the substation IEC 61850 GOOSE communication is performed in the field-level process zone using multicast Ethernet. Routable IEC 61850 GOOSE (R-GOOSE) and IEC 61850 SV (R-SV) can be applied to facilitate communication, e.g., between substations on top of UDP/IP. IEC 62351 provides support for the necessary key management in IEC 62351-9. The application of the negotiated symmetric group key on a per message base is outlined in IEC 62351-6. The configuration of security services for multicast communication contains at least:

- definition of communication groups sharing the same symmetric key
- definition of key update intervals to refresh the group key
- accepted certificates on the infrastructure side for component authentication.

The security policy determining the security services used (which on what layer) are expected to be provided by the operator and instantiated by the integrator.

Take away: Different parts of IEC 62351 target communication security. IEC 61850 MMS related security is addressed using the IEC 62351-4 (combined with IEC 62351-3). Security relevant for multicast communication using IEC  61850 GOOSE is addressed in IEC 62351-6. Security relevant for telecontrol using IEC 60870-5 is targeted in IEC 62351-5 (combined with IEC 62351-3). Authentication and authorization support is as described above.

### 2.3.5 Enabling security monitoring (targets [R 7])

During operation, a comprehensive security monitoring for power system components based on defined monitoring information and security events is necessary to operate the system reliably. The security monitoring contributes to the detection of potential threat to a system and thus enables an appropriate reaction in time. This requires at least the selection of components with adequate logging/monitoring capabilities and the definition of

- events and system properties to be monitored. Examples are failed authentication during a communication establishment, inability to update component associated keys, or events related to the physical environment like an unauthorized opening of a cabinet.
- counters and thresholds for dedicated events like failed authentication
- receiver information for monitoring (e.g., SNMP server) or event (e.g., syslog server) at the component side.

This is defined jointly by the operator and the integrator of the target system considering the component capabilities.

Take away: IEC 62351 provides support through the definition of monitoring events in IEC 62351-7, the definition of security events in IEC 62351-14. Moreover, IEC 62351-90-3 provides guidelines on how to handle security monitoring and eventing within a power automation system. Moreover, as the communication is increasingly security, IEC 62351-15 addresses monitoring of encrypted communication.

## 2.4 Operation

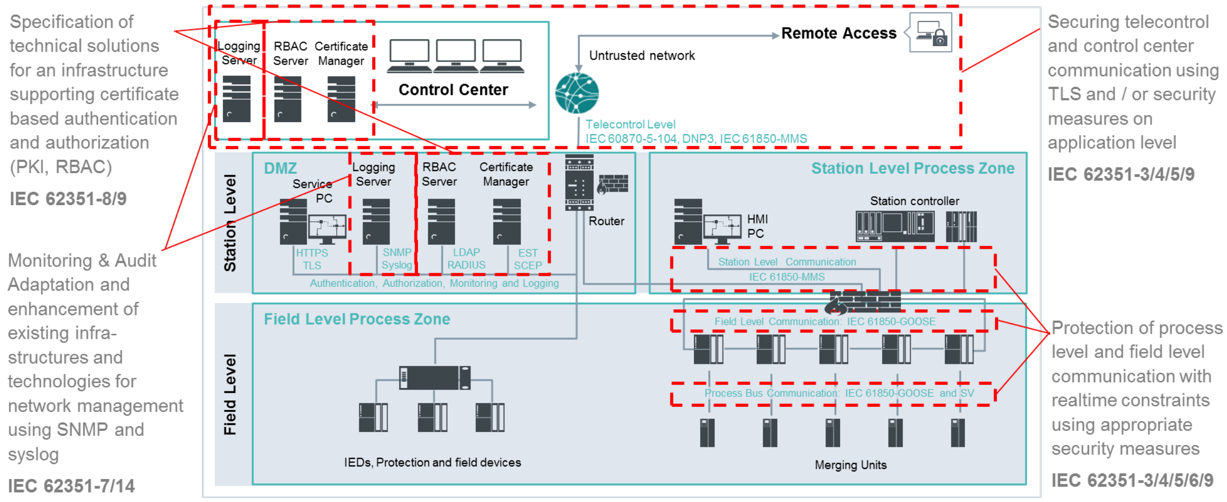
During normal operation the operator keeps track of the status and the monitoring results from the technical security controls as described above in section 2.3. Most importantly, the operator has to have appropriate processes in place to address at least:

- definition of a security policy specifying for instance authentication and authorization requirements for the target environment for human users and also between components of the system, security of data in transit and data at rest, certificate policies.
- investigate into advances in security to potentially adjust the applied security controls (vulnerability management).
- handle security events accordingly.
- Monitor vulnerabilities regarding the utilized components within his operational environment.
- apply firmware or software updates securely to considered components.

All of the procedural tasks typically derive from an information security management framework which had been used as base for the system design as discussed in sections 2 and 2.3.

## 2.5 Summary

Figure 3 below enhances the target use case substation automation introduced in Figure 2 with functionality provided in IEC 62351 parts. Note that the figure emphasizes the technical part supporting the security management through dedicated components for credential management and logging as well as the protection of communication in different parts of the substation or across the boundary of the substation.



Specification of technical solutions for an infrastructure supporting certificate based authentication and authorization (PKI, RBAC)

IEC 62351-8/9

Monitoring & Audit Adaptation and enhancement of existing infra-structures and technologies for network management using SNMP and syslog

IEC 62351-7/14

Securing telecontrol and control center communication using TLS and / or security measures on application level

IEC 62351-3/4/5/9

Protection of process level and field level communication with realtime constraints using appropriate security measures

IEC 62351-3/4/5/6/9

**Figure 3: Mapping of IEC 62351 to the substation automation scenario**

## References

[1] IEC 62351 Application Notes Volume 1: Motivation, Introduction, and Overview of IEC 62351

[2] IEC 62351 Application Notes Volume 3: Application Examples of IEC 62351

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

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

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

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

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

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

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

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

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

[12] European NIS Directive: https://www.enisa.europa.eu/topics/cybersecurity-policy/nis-directive-new

[13] US FERC Cyber & Grid Security, https://www.ferc.gov/industries/electric/indus-act/reliability/cybersecurity.asp

[14] 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

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

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