CEN-CENELEC-ETSI Coordination Group on Smart Energy Grids (CG-SEG)

Date: 2016-12

Secretariat: CCMC

Coordination Group on Smart Energy Grids

Cyber Security & Privacy

SEG-CG/CSP- Report-V09.pdf

Contents

Page

1 Foreword

This document has been prepared by CEN-CENELEC-ETSI Smart Energy Grid Coordination Group (SEG-CG) under the frame provided by CEN, CENELEC and ETSI.

The work done by the Cyber Security and Privacy (CSP) group within the SEG-CG has been continued after the closing of the mandate M/490 [1] with the purpose to follow-up on items found during the work performed under the mandate and to provide best practice examples on smart energy grid specific use case in order to show the applicability of existing standards.

2 Scope

The scope of the Smart Energy Grid Coordination Group (SEG-CG) is to advice on European requirements relating to Smart Energy Grid standardization. The work of the Cyber Security and Privacy (CSP) working group is based on the results of the Smart Grid Information Security (SGIS) working group [3],[4] which have addressed cyber security within the European Commission Smart Grid Mandate M/490 [1].

In this report, security standardization specific to Smart Energy Grid and security standardization targeting generic standards are further monitored and analysed with the focus on two specific use cases: decentralized energy resource (DER) and substation automation. It shows the applicability and interrelationship between these two groups of standards. Furthermore, the SGIS approach has been followed to show the applicability of different standards on the selected, specific use cases for Smart Energy Grid deployments. In this context, the applicability of the IEC 62443 framework is shown on the example of secure substation.

EU & US energy sector related documents are analysed to investigate and possibly identify means to be able to transpose a use case once it has been mapped to the SGAM [5] from a European cyber security context to a US one and vice-versa.

Results presented in this report are determined to help standardization organization to take-up respective findings and to help operator and integrator to apply cyber security standards in smart energy grid deployments.

3 Terms and Definitions

Smart Grid
A smart grid is an electricity network that can cost efficiently integrate the behavior and actions of all users connected to it – generators, consumers and those that do both – in order to ensure economically efficient, sustainable power system with low losses and high levels of quality and security of supply and safety.

Information Security
As defined in ISO/IEC 27002:2005 '*Information security is the protection of information from a wide range of threats in order to ensure business continuity, minimize business risk, and maximize return on investments and business opportunities.*'

Smart Grid Information Security – Security Level (SGIS-SL)
SGIS-SL objective is to create a bridge between electrical grid operations and information security. SGIS-SL is a classification of inherent risk, focusing on impact on the European Electrical Grid stability to which requirements can be attached. SGIS working group defined five SGIS Security Levels in this report.

Likelihood
Classical concepts of likelihood cannot be assessed in a generic sense and may not be known in an early stage of a risk assessment. It is describing a possibility that an event might occur; by nature this is difficult to measure or estimate and needs experienced experts to analyze in a specific context.

Smart Grid Architecture Model – SGAM
The Smart Grid Architecture Model (SGAM) is a reference model to analyze and visualize smart grid use cases in respect to interoperability, domains and zones.

SGAM Domain
One dimension of the Smart Grid Plane that covers the complete electrical energy conversion chain, partitioned into 5 domains: Bulk Generation, Transmission, Distribution, DER and Customers Premises.

SGAM Zone
One dimension of the Smart Grid Plane represents the hierarchical levels of power system management, partitioned into 6 zones: Process, Field, Station, Operation, Enterprise and Market [IEC 62357:2011].

Requirement Standard
Requirement standards are high to medium level requirement standards, neutral from technology. Those requirements do not provide technical implementation options. They describe 'what' is required.

Solution Standard
Solution standard are related to describe specific implementation options ideally addressing requirements from the requirement standards. The solution standards address (local) security implementation options, reflecting different security levels, and also interoperability. They describe 'how' functionality is required.

4 Symbols and Abbreviations

- **BES** Bulk Electric System
- **CIA** Confidentiality, Integrity, Availability
- **DER** Distributed Energy Resources
- **DSO** Distribution System Operator
- **EU** European Union

- **FDIS** Final Draft International Standard
- **GDOI** Group Domain of Interpretation
- **GOOSE** Generic Object Oriented Substation Event
- **ICT** Information and Communication Technology
- **IED** Intelligent Electronic Device
- **IS** International Standard
- **ISMS** Information Security Management System
- **LRM** Logical Reference Model
- **NIST** National Institute of Standards and Technology
- **PKI** Public Key Infrastructure
- **SGAM** Smart Grid Architecture Model
- **SGIS** Smart Grid Information Security
- **SGIS-SL** Smart Grid Information Security – Security Level
- **TR** Technical Report
- **TS** Technical Specification
- **TSO** Transmission System Operator
- **US** United States
- **WD** Working Document

5 Executive Summary

The objective of this report is to support Smart Energy Grid implementation in Europe by providing analyses on standards and best practice examples on applicability of these standards on energy grid deployments.

One common base line for the results presented in this report are the SGIS key elements, namely the Smart Grid Architecture Model (SGAM) [2], the SGIS Security Levels (SGIS-SL) [4].

Available security standards are increasingly applied to address functional, organizational or procedural requirements. Selecting the appropriate security standards to achieve a dedicated security level on a technical and organizational or procedural level is crucial for the reliability of a European Smart Energy Grid. The security standards investigated are partially continuative actions and partially new standards. For all a categorization in SGAM has been provided to show their immediate applicability. Also, it has been depicted, who is in the focus of a specific standard: vendor, integrator, or operator. Moreover, identified gaps in standards are listed provide a recommendation to standardization bodies for potential further actions.

Additionally, the applicability of standards to decentralized energy resources and secure substation use cases has been outlined and analyzed in order to provide respective recommendations. For this, the results of the SGIS [4] have been extended specifically for the use case security analysis methodology with intermediate steps going from use case ICT analysis, through risk levels and (standard) security requirements to solutions to secure the use case ICT architectures utilizing the security standards.

Furthermore, in the context of this analysis, the IEC 62443 [14] framework has been applied on the substation automation use case. The advantage in applying the IEC 62443 security framework with the security levels defined in IEC 62443-3-3 are pointed out. In combination with IEC 62351 [20], this allows a comprehensive protection concept on cyber security in the implementation and offers a reference model to address cyber security on system level.

EU & US energy sector related documents are analysed to investigate and possibly identify means to be able to transpose a use case once it has been mapped to the SGAM [5] from a European cyber security context to a US one and vice-versa.

Applying cyber security to smart energy grid deployments can provide substantial protection when it is built on international standards. However, it has to be stated that cyber security requires a continuous effort to incorporate existing and new technologies, architectures, use cases, policies, best practice or other forms of security diligence.

6 Smart Grid Set of Security Standards

The Smart Grid Set of Security Standards investigates into selected standards along the work already been done as part of the SG-CG SGIS in the phase 1 (2011-2012) [3] and phase 2 (2013-2014) [4]. The goal here is to focus on following the already identified standards as well as investigating into new, upcoming standards, to discuss their applicability and suitability for smart grid scenarios and use cases. As in the past, the goal, besides the discussion of applicability is the identification of potential gaps and based on this the interworking with the associated standardization committee in terms of feedback and proposals as far as possible.

6.1 Security Standards Supporting Smart Grid Reliable Operation

This section provides a further discussion of a set of security standards that have been selected for investigation based on their relation to the Smart Grid. Some of these standards have already been addressed during the two working phases of SGIS and are followed further as they are being developed further.

The selection of the security standards has been done targeting the support of reliable Smart Energy Grid operation by providing appropriate technical and organization counter measures against cyber attacks. The standards may not directly address reliability issues for failure cases (e.g. programming errors, incorrect control commands, breakdown of communication lines, power loss in the ICT systems, ...), which are distinct from cyber attacks. It should be noted that for reliable operation of a Smart Grid, standards are required to handle all possible failure cases ensuring system resilience even if accidental or malicious failures occur.

The documents considered in this section are categorized as requirements and solution standards. These standards have been investigated regarding their coverage of implementation details on a technical or operational level. Note, that interoperability of existing products complying with a specific solution standard is not part of the review. Based on this analysis it has been depicted for whom the standards are mostly relevant: product vendors, solution integrators, or operators. This helps architecture and solution designer in selecting the right standards to follow.

The applicability of the selected standards is shown later on in this document when discussing use cases.

6.1.1 Selected Security Standards

The security standards focused in this working period are distinguished into requirements standards (type 1) and solution standards (type 2 and type 3) as listed below. Please note that the distinction in requirements standards and solution standards is a simplification of the type1, 2 and 3 standards from SGIS phase 1 [3]. In the following the requirement standards summarize the abstract security requirements, while the solution standards describe a realization targeting interoperability between different vendor’s products.

Requirement standards considered (The ‘What’)

- ISO/IEC 27001 [10]: Information technology — Security techniques — Information security management systems — Requirements
- ISO/IEC 27002 [11]: Information technology — Security techniques — Code of practice for information security management ISO/IEC TR 27001
- ISO/IEC TR 27019 [12]: Information technology - Security techniques - Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry
- IEC 62443-2-4 [13]: Security for industrial automation and control systems - Network and system security - Part 2-4: Requirements for Industrial Automation Control Systems (IACS) solution suppliers
- IEC 62443-3-3 [14]: Security for industrial automation and control systems, Part 3-3: System security requirements and security levels
- IEC 62443-4-2 [15]: Security for industrial automation and control systems, Part 4-2: Technical Security Requirements for IACS Components
- IEEE 1686 [16]: Substation Intelligent Electronic Devices (IED) Cyber Security Capabilities

- IEEE C37.240 [17]: Cyber Security Requirements for Substation Automation, Protection and Control Systems

Solution standards considered (The 'How')

- ISO /IEC 15118: Road vehicles – Vehicle-to-Grid Communication Interface, Part 8 [18]: Physical and data link layer requirements for wireless communication
- ISO / IEC 61850-8-2 [19]: Communication networks and systems for power utility automation - Part 8-2: Specific communication service mapping (SCSM) - Mapping to Extensible Messaging Presence Protocol (XMPP)
- IEC 62351-x [20] Power systems management and associated information exchange – Data and communication security
- IEC 62743 [21] Industrial communication networks – Wireless communication network and communication profiles - ISA 100.11a
- IETF draft-weis-gdoi-iec62351-9: IEC 62351 Security Protocol support for the Group Domain of Interpretation (GDOI) [22]
- IETF draft-TLS1.3 TLS Version 1.3 [25]

6.1.2 Standards Coverage

The stated list of standards covers requirements and solution standards that provide different level of detail. These standards are analysed regarding their coverage following the approach from SGIS phase one as depicted in the Figure 1 below.

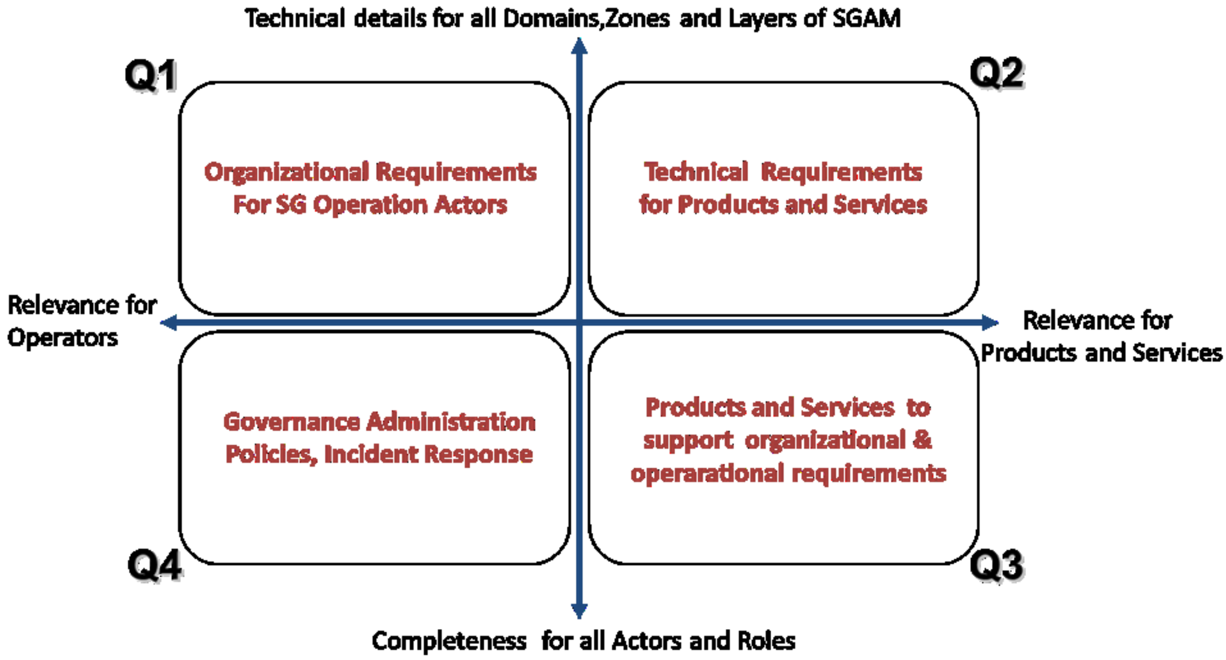


Figure 1: Security standard areas

While mapping a standard to the diagram in Figure 1, it is shown on an abstract level, which scope and to what level of detail the standards addresses each of the four quadrants. Moreover, also addressed is the relevance of the standards for organizations (Smart Grid operators) as well as products and services (product manufacturer and service providers).

Figure 2 below shows the mapping of the selected standards to the standards areas under the following terms:

- **Details for Operation**: The standard addresses organizational and procedural means applicable for all or selected actors. It may have implicit requirements for systems and components without addressing implementation options.
- **Relevance for Products**: The standard directly influences component and/or system functionality and needs to be considered during product design and/or development. It addresses technology to be used to integrate a security measure.
- **Design Details**: The standard describes the implementation of security means in details sufficient to achieve interoperability between different vendor's products for standards on a technical level and/or procedures to be followed for standards addressing organizational means.
- **Completeness**: The standard addresses not only one specific security measure but addresses the complete security framework, including technical and organizational means.

The colour code in the Figure 2 shows the origin domain of the considered standards. What can be clearly seen, based on the colouring, is that for Smart Grids standards from different domains are applicable.

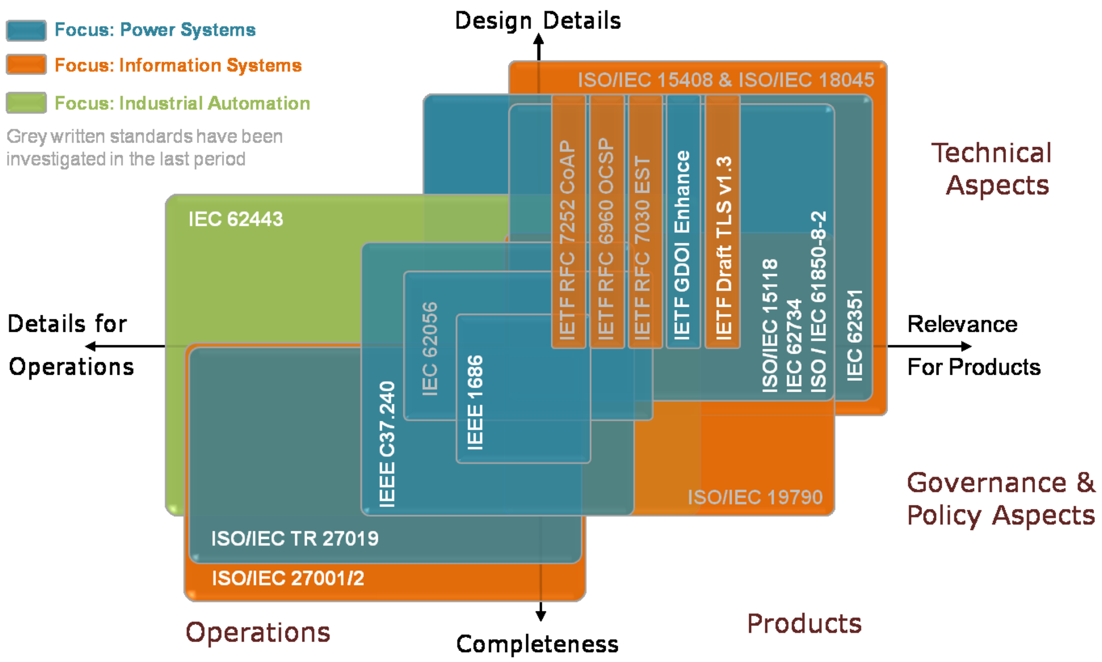


Figure 2: Security Standard Coverage

The following drawing Figure 2 shows the applicability and scope of each of the standards considered as part of this working period of the SGIS from a somewhat different perspective. The differentiation in the drawing is as following:

- **Guideline:** The document provides guidelines and best practice for security implementations. This may also comprise pre-requisites to be available for the implementation.
- **Requirement**: The document contains generic requirements for products, solutions or processes. No implementation specified.
- **Realization:** The document defines implementation of security measures (specific realizations). Note, if distinction possible, the level of detail of the document raises from left to right side of the column.
- **Vendor:** Standard addresses technical aspects relevant for products or components
- **Integrator:** Standard addresses integration aspects, which have implications on the technical design, are relevant for vendor processes (require certain features to be supported), or require product interoperability (e.g., protocol implementations).
- **Operator:** Standard addresses operational and/or procedural aspects, which are mainly focused on the service realization and provisioning on an operator site.

The colour code from Figure 2 is kept also in this picture. Some of the standards only cover partly a certain vertical area. The interpretation of a partly coverage is that the standard may not provide explicit requirements for the vendor / integrator / operator. Standards covering multiple horizontal areas address requirements and also provide solution approaches on an abstract level. For the implementation additional standards or guidelines may be necessary. *Note that section 6.3 lists further standards identified, which are not considered in Figure 2 and Figure 3.*

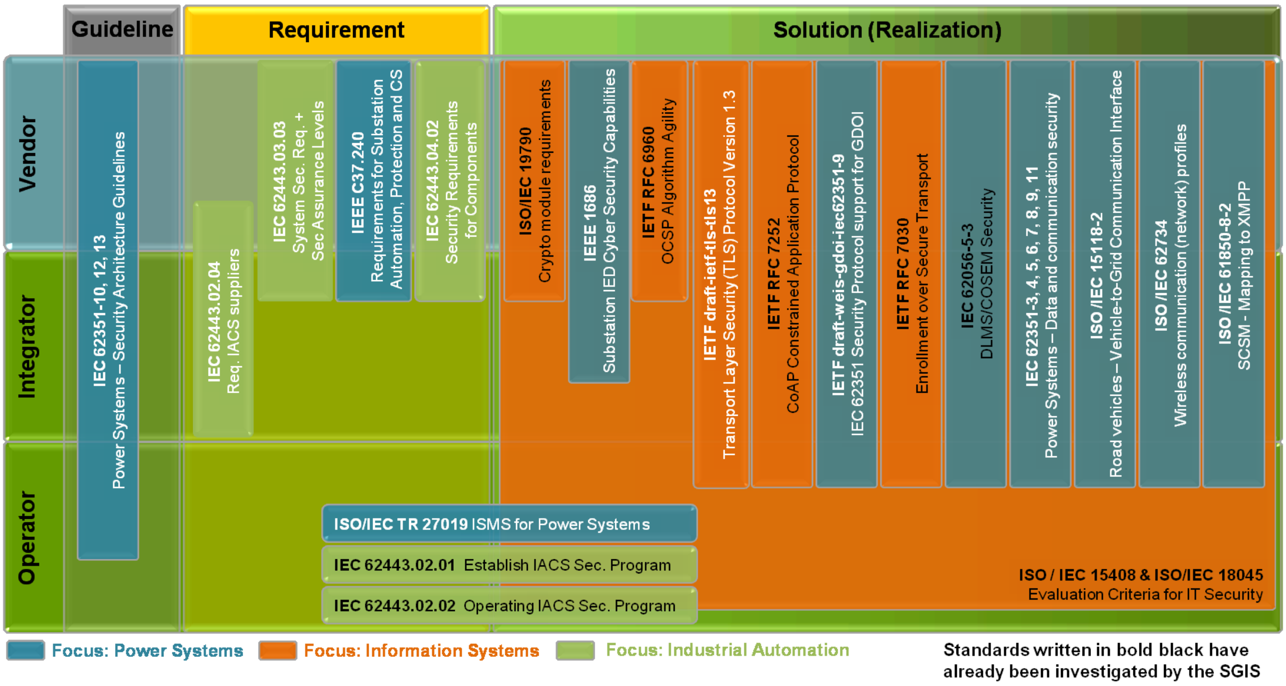
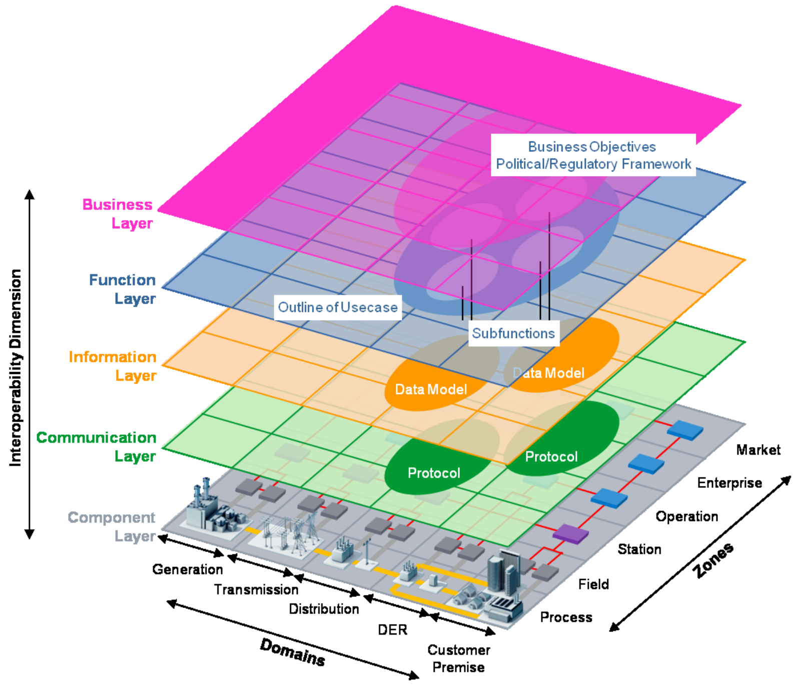


Figure 3: Security standard applicability

The goal of the introduction and the analysis is the support for the identification of suitable standards to secure a dedicated target use case relating to Smart Grid. The analysis focuses on the general applicability of the selected standards in the considered use case leading potentially to requirements to enhance the standards if necessary. Moreover, the use case specific analysis also allows pointing to further standards applicable and not considered for the analysis explicitly.

6.1.3 Standards Mapping to SGAM

Figure 4 depicts SGAM just to introduce abbreviations, which are used for the SGAM mapping in the following subsections.



SGAM Layer
- B – Business
- F – Function
- I – Information
- C – Communication
- Phy – Component

SGAM Domains
- G – Generation
- T – Transmission
- D – Distribution
- DER
- CP – Customer

SGAM Zones
- M – Market
- E – Enterprise
- O – Operation
- S – Station
- F – Field
- P – Process

Figure 4: Smart Grid Architecture Model – Layers, Domains, and Zones

Starting from section 6.2, the single requirements and solutions standards are investigated. They contain a short overview about the considered standard and a mapping to SGAM to analyse the applicability based on the selected use cases.

The following two subsections summarize the detailed investigation and show general applicability of the considered standards in SGAM. Note that some of the standards investigated are still under development (drafts or working documents). Hence, these may change as a result of their comment periods, impacting the output of this report or remove references to draft standards.

6.1.3.1 Mapping Requirement Standards to SGAM

The following table provides a generic mapping of the requirement standards to SGAM. Generic in this context refers to today's application or intended application in known use cases. Section 6.2 later on will do a mapping based on selected use cases to verify the generic view.

Standard	SGAM		
	Layer	Domains	Zones
ISO/IEC 27001	B, F, I	G, T, D, DER, CP	O, E, M
ISO/IEC 27002	B, F, I	G, T, D, DER, CP	E, M, O, S, F
ISO/IEC 27019	B, F, I	G, T, D, DER	E, O, S, F
IEC 62443-2-4 (CD)	F, I, C, Phy	T, D, DER, CP	E, O, S, F, P
IEC 62443-3-3 (IS)	F, I, C, Phy	T, D, DER, CP	P, F, S, O, E
IEC 62443-4-2 (WD)	F, I, C, Phy	D, DER, CP	P, F, S, O
IEEE 1686	Phy	G, T, D,	F,P
IEEE C37.240	Phy, C	G, T, D, DER	F.P

IEC 62443-2-1	B, F, I	G, T, D, DER	O, S, F

6.1.3.2 Mapping Solution Standards to SGAM

Standard (Status)	SGAM		
	Layer	Domains	Zones
ISO/IEC 15118-8 (CD)	F, I, C	T, D, DER, CP	M, E, O S, F, P
IEC 61850-8-2 (CD)	F, I, C	T, D, DER, CP	E, O, S, F, P
IEC 62056-5-3 (IS)	F, I, C	T, D, DER, CP	E, O, S, F, P
IEC 62351- 3 (IS)	I, C	G, T, D, DER, CP	E, O S, F
IEC 62351- 4 (TS)	I, C	G, T, D, DER, CP	E, O S, F
IEC 62351- 5 (TS)	I, C	G, T, D, DER, CP	E, O S, F
IEC 62351- 6 (TS)	I, C	G, T, D, DER, CP	E, O S, F
IEC 62351- 7 (TS)	I, C	G, T, D, DER, CP	E, O S, F
IEC 62351- 8 (TS)	F, I, C	G, T, D, DER, CP	E, O S, F
IEC 62351- 9 (2.CD)	F, I, C	G, T, D, DER, CP	E, O S, F
IEC 62351- 10 (TR)	B, F, I, C, Phy	G, T, D, DER, CP	M, E, O S, F
IEC 62351- 11 (CD)	F, I, C	G, T, D, DER, CP	E, O S, F
IEC 62351- 12 (DC)	I, C	G, T, D, DER, CP	M, E, O S, F
IEC 62351- 13 (DC)	I, C	G, T, D, DER, CP	M, E, O S, F, P
IEC 62351- 14 (NWIP)	I, C	G, T, D, DER, CP	M, E, O S, F, P
IEC 62734	I, C, Phy	G, T, D, DER, CP	E, O S, F
IETF I-D draft-ietf-tls-tls13 (Draft)	I, C	G, T, D, DER, CP	M, E, O S, F, P
IETF I-D draft-weis-gdoi-iec62351-9 (Draft)	I, C	G, T, D, DER, CP	M, E, O S, F, P

6.2 Detailed Standards Analysis

This section provides more insight into the selected standards. Each standard will be introduced with a small overview explaining the general goal of the standard as well as a status update regarding the document state. Gaps are listed, which have been initially discovered by investigating into the standards. These gaps may relate to technical shortcomings or missing coverage of dedicated requirements. The section is divided into security requirement and security solution standards.

6.2.1 Security Requirement Standards

The following subsections investigate into selected security requirements standards.

6.2.1.1 ISO/IEC 27000-Family: Information Security Management Systems

This family of standards specifies requirements for an information security management system (abbr. ISMS). Its main standard is ISO/IEC 27001 which specifies the requirements for an ISMS. Additionally several standards co-exist which are all in support of ISO/IEC 27001.

Since the previous publication of this report a new revision of ISO/IEC 27001 and ISO/IEC 27002 were published and in the meantime two additional corrections have been applied.

ISO/IEC 27001 is a generic information security management system standard that is ‘to be applicable to all organizations, regardless of type, size or nature’, therefore can also be used in the Energy sector.

ISO/IEC 27002:2013 is a code of practice and only acts as guidance on possible control objectives and the way these control objectives can be implemented.

Within this family of standards ISO/IEC TR 27019 is specific to the Energy sector. The current published version of ISO/IEC TR 27019 is a sector-specific extension to ISO/IEC 27002 describing the code of practice for information security controls. Hence, ISO/IEC TR 27019 also includes all of the controls listed in ISO/IEC 27002. The scope of ISO/IEC TR 27019 is defined as ‘process control systems used by the energy utility industry for controlling and monitoring the generation, transmission, storage and distribution of electric power, gas and heat in combination with the control of supporting processes.’ Therefore not all zones and domains of the Smart Grid are covered.

ISO/IEC TR 27019 was previously approved as a Technical Report in 2013 and is currently under revision which will bring several major changes.

27019 will change from a Technical Report (TR) to an International Standard (IS). The current draft of ISO/IEC 27019 applies and conforms with the requirements specified in ISO/IEC 27009. ISO/IEC 27009 specifies the sector-specific application of ISO/IEC 27001; his includes addition, refinement or interpretation of requirements contained in ISO/IEC 27001 and its controls in Annex A.

By conforming to ISO/IEC 27019 it will be possible to specify requirements in ISO/IEC 27019 which are sector-specific. These additions, refinements or interpretations shall not contradicting or invalidating generic requirements specified in ISO/IEC 27001. At the moment, the current draft incorporates only a single additional requirement requesting the so called Statement-of-Applicability (SoA) to contain the controls defined by 27019.

Based on this circumstance, it is expected that the current title “Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry” might get rid of the “Guidelines”.

6.2.1.1.1 Status

	Description	Standardization Status
ISO/IEC 27001:2013/Cor 2:2015	Information technology — Security techniques — Information security management systems — Requirements	New release in 2013 with two additional corrigenda
ISO/IEC 27002:2013/Cor 2:2015	Information technology — Security techniques — Code of practice for information security controls	New release in 2013 with two additional corrigenda
ISO/IEC 27009	Information technology — Security techniques — Sector-specific application of ISO/IEC 27001 – Requirements	The document was approved during DIS balloting in 2015 and should be published in 2016.
ISO/IEC TR 27019:2013	Information Technology — Security techniques — Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry	Published in 2013. ISO/IEC TR 27019 is aligned to the previous version of ISO/IEC 27002:2005

	Description	Standardization Status
ISO/IEC 27019	Information Technology — Security techniques — Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry	Currently under revision 2nd Working Draft, January 2016

6.2.1.1.2 Identified Gaps

There have been no gaps identified.

6.2.1.2 IEC 62443: Industrial communication networks – Network and system security

Specific requirements and side conditions of industrial and energy automation systems like high availability, planned configuration (engineering info), long life cycles, unattended operation, real-time operation, and communication, as well as safety requirements have to be considered when designing a security solution. The IT (information technology) security requirements defined in IEC 62443 can be mapped to different automation domains, including energy automation, railway automation, building automation, process automation, and others. IEC 62443 is not a single specification, but provides a relatively complete framework of specifications. The individual parts cover common definitions, and metrics, requirements on setup of a security organization (ISMS related), and processes, defining technical requirements on a secure system, and to secure system components. The different parts are grouped into four clusters that cover

- common definitions, and metrics
- requirements on setup of a security organization (ISMS related), and solution supplier and service provider processes
- technical requirements and methodology on a secure system at system-wide level
- and requirements to the secure development lifecycle of system components, and security requirements to such components at a technical level (broken down from the system-wide requirements).

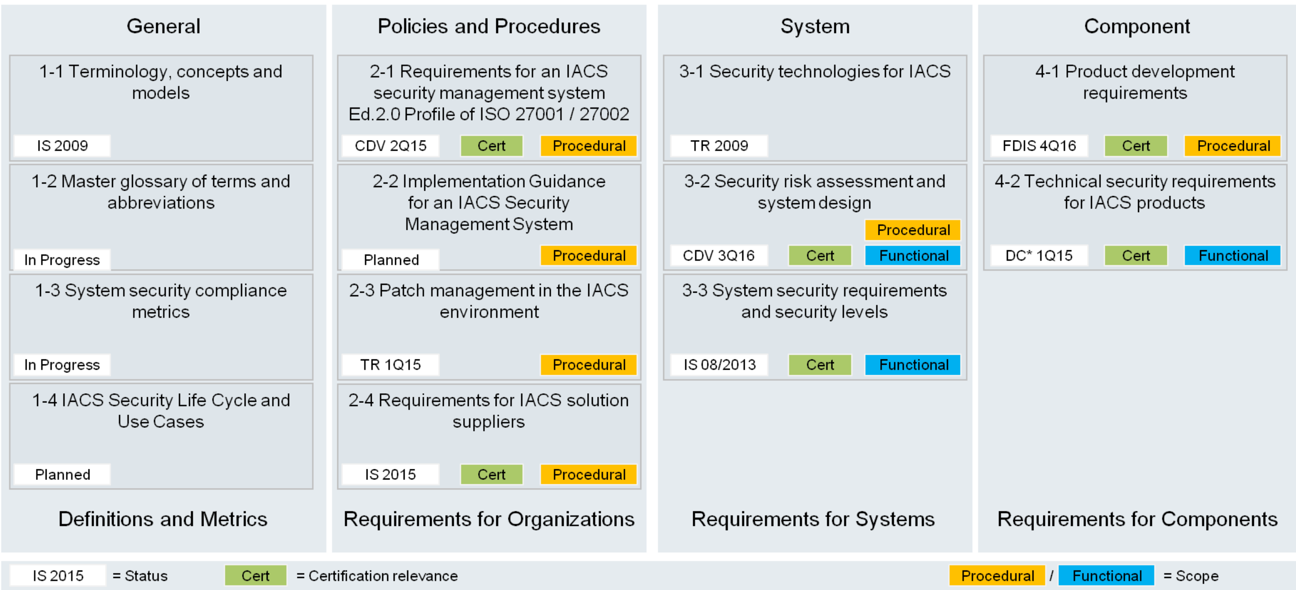


Figure 5: IEC 62443 framework overview and targets

As shown in Figure 5 the parts are in different states of completion and address both procedural/organizational and functional requirements. Several parts of the IEC62443 framework are intended to serve as basis certification or assessment activities. To provide an overall approach for certified IACS security,

- the IEC62443-4-x series target the secure development process and appropriate security features for individual components of an automation system,
- IEC62443-2-4 and -3-3 focus on a securely designed system (based on the components covered by the IEC62443-4-x series) and secure processes and procedures of solution suppliers for such system, or maintenance/upgrade service providers,
- and IEC62443-2-1 addresses security aspects in secure operation, strongly based on the security controls defined by ISO/IEC 27001/2.

IEC 62443-3-3 and IEC 62443-4-2 are very similar in their requirements content, contained in the following requirement groups:

- Authentication control — *Account management, PKI, etc.*
- Use control — *Authorization, session management, audits, etc.*
- System integrity — *Communication, session & data integrity, malware protection, etc.*
- Data confidentiality — *Data encryption and secure purging of old data*
- Restricted data flow — *Network, applications and device partitions*
- Timely response — *Monitoring, logging and timely response*
- Resource availability — *Smart resource management, system backup, etc.*

In addition IEC 62443-4-2 adds the following requirement groups:

- Application requirements — *malware protection mechanisms, mobile code extra security*
- Embedded requirements — *secure booting, malicious code protection, etc.*
- Host device requirements — *secure booting, malicious code protection, etc.*
- Network device requirements — *authentication, RBAC, secure booting, etc.*

According to IEC 62443 a complex automation system is structured into zones that are connected by so-called “conduits”. For each zone, the targeted security level (SL) is derived from a threat and risk analysis. The threat and risk analysis evaluates the exposure of a zone to attacks as well as the criticality of assets of a zone. IEC 62443-3-2 defines security levels and zones for the secure system design. IEC 62443-3-3 lists security requirements that must be met to reach a certain SL. From the structure, each security requirement consists of a baseline requirement and zero or more requirement enhancements (REs) to strengthen security and thus increase the SL.

Note that IEC 62443-3-3 is intended for solutions, not for components. Hence, when designing a control system to meet the set of SRs associated with specific SL-Ts, it is not necessary that every component of the proposed control system support every system requirement to the level mandated in this standard. Compensating countermeasures can be employed to provide the needed functionality to other subsystems, such that the overall SL-T requirements are met at the control system level. Inclusion of compensating countermeasures during the design phase should be accompanied by comprehensive documentation so that the resulting achieved control system SL, SL-A (control system), fully reflects the intended security capabilities inherent in the design. Similarly, during certification testing and/or post-installation audits, compensating countermeasures can be utilized and documented in order to meet the overall control system SL.

Four security levels (SL) have been defined by IEC62443-3-3. These primarily select the applicable requirements of IEC62443-3-3 (their number increasing with increasing SL), but the requirements are organized into security levels to target different high-level categories of attackers:

SL	Description
1	Protection against casual, or coincidental violation
2	Protection against intentional violation using simple means, low resources, generic skills, low motivation
3	Protection against intentional violation using sophisticated means, moderate resources, IACS specific skills, moderate motivation
4	Protection against intentional violation using sophisticated means, extended resources, IACS specific skills, high motivation

For each security level, IEC62443 part 3-3 defines a set of requirements. Seven foundational requirements (FR) group specific requirements of a certain category as there are:

FR	Description
1	Identification and authentication control
2	Use control
3	System integrity
4	Data confidentiality
5	Restricted data flow
6	Timely response to events
7	Resource availability

6.2.1.2.1 Status

	Description	Standardization Status
IEC 62443-2-4	Requirements for Security Programs for IACS Integration and Maintenance Service Providers	IS 2015
IEC 62443-3-2	Security risk assessment and system design	CDV: 11/2016
IEC 62443-3-3	System security requirements and security levels	IS 2013
IEC 62443-4-1	Product development requirements	CDV, FDIS end of 2016
IEC 62443-4-2	Technical security requirements for IACS products	DC

6.2.1.2.2 Identified Gaps

Privacy by design is currently not considered as design criteria in IEC 62443.

6.2.1.3 IEEE 1686: Intelligent Electronic Devices (IED) Cyber Security Capabilities

This document targets the description of Intelligent Electronic Devices (IEDs) Cyber Security Capabilities. The standard defines functions and features that must be provided in substation intelligent electronic devices to accommodate critical infrastructure protection programs. It addresses security in terms of access, operation, configuration, firmware revision, and data retrieval from IEDs. Security functionality with respect to confidentiality of the transmission of data is not part of this standard. It serves as a procurement specification for new IEDs or analysis of existing IEDs. IEEE 1686-2014 also provides a table of compliance in the annex. This table is intended to be used by vendors to indicate a level of compliance with the requirements.

Outside the scope of the standard is the determination of the system security architecture. It only addresses embedded security features of the IED and the associated IED configuration software. The system aspects are addressed by the IEEE C37.240.

6.2.1.3.1 Status

The first document was initially released in 2007 and the second edition has been updated in 2014. The standard does not contain requirements targeting the interoperability of different systems. In contrast to the 2007 version, the scope has been broadened from the consideration of pure Substation IEDs to IEDs in general. A Matrix is available at the end to state which requirements is met by the device claiming conformity.

	Description	Standardization Status
IEEE 1686	Substation Intelligent Electronic Devices (IED) Cyber Security Standards	Approved in 2014

6.2.1.3.2 Identified Gaps

No gaps have been identified so far.

6.2.1.4 IEEE C37.240: Cyber Security Requirements for Substation Automation, Protection and Control Systems

IEEE C37.240 addresses technical requirements for substation cyber security. It is intended to present sound engineering practices that can be applied to achieve high levels of cyber security of automation, protection and control systems independent of voltage level or criticality of cyber assets. Cyber security in the context of this document includes trust and assurance of data in motion, data at rest and incident response. Main topics addressed comprise:

- Requirements for system security architecture with common network components and communication links
- Remote IED access systems including the role of a Remote IED Access Gateway (RIAG)
- Connection Monitoring Authority (CMA) and Connection Controlling Authority (CCA)
- User authentication and authorization, protection of data in motion, and device configuration management.
- Security event auditing, analysis and security testing.

6.2.1.4.1 Status

The standard is approved and reference several others standards like IEC62351 but also IEEE P1686 for all cyber security IED specific features.

	Description	Standardization Status
IEEE C37.240	Cyber Security Requirements for Substation Automation, Protection and Control Systems	Approved in 2014

6.2.1.4.2 Identified Gaps

There have been no gaps identified.

6.2.2 Security Solution Standards

The following subsections investigate into selected security solution standards.

6.2.2.1 ISO /IEC 15118 Road Vehicles – Vehicle-to-Grid Communication Interface

The set of ISO/IEC 15118 parts addresses the vehicle to grid interface for the charging infrastructure. The different parts comprise the requirements, use cases, and the specification of the communication interface for plug and charge and inductive charging. Security is an integral part of this set of standard and utilizes existing security technology as far as possible. Notably, the security measure in the standardized parts completely relies on elliptic curve based certificates to address the involved constraint devices as well as lifetime of the components.

While the communication stack has already been defined for wired charging, the definition of the complete communication stack for wireless charging is currently on going. Here, the goal is to have as less as possible deviations from the general (wired) approach. Regarding the security, the new use cases, involving not only PLC based communication, but also wireless communication require a review of the security and trust assumptions and mechanisms already defined.

6.2.2.1.1 Status

ISO/IEC 15118	Definition of Security Services for	Standardization Status
Part 1	General information and use-case definition	Standard published 2013
Part 2	Network and application protocol requirements	Standard published 2014
Part 3	Physical and data link layer requirements	Standard published 2015
Part 4	Network and application protocol conformance test	Standard published 2015
Part 5	Physical layer and data link layer conformance test	CD, 12/2014
Part 6	General information and use-case definition for wireless communication	DIS, 07/2015
Part 7	Network and application protocol requirements for wireless communication	CD, 05/2015
Part 8	Physical layer and data link layer requirements for wireless communication	CD, 07/2015

6.2.2.1.2 Identified Gaps

ISO/IEC 15118 relies on certificates and corresponding private keys. The management and storage of these credentials is currently out of scope of the standard. To address a dedicated security level in the charging infrastructure, recommendations should be given, how to address these issues.

6.2.2.2 IEC 62351-x Power Systems Management and Associated Information Exchange – Data and Communication Security

IEC 62351 is maintained in IEC TC57 WG15 and defines explicit security measures to protect data exchange in power systems. Besides the specification of security measures, parts of the standard also provide general guidelines for designing power systems with security in mind. The set of IEC 62351 parts covers different scenarios and applies directly to substation automation deploying IEC 61850 and IEC 60870-x protocols as well as in adjacent communication protocols supporting energy automation, like ICCP (TASE.2) used for inter-control center communication. It also targets the integration of DER via classical protocols and already considers the application of web based services for DER integration.

Main topics addressed in these scenarios comprise:

- Mutual authentication for communicating entities in power systems using power system specific communication means (see mapping below)

- Security (integrity and confidentiality) data exchange between the communicating entities, realized as transport security or application layer security for serial and routed protocols
- Role-based Access Control
- Security monitoring and event logging
- Security architecture design recommendations

The following Figure 6 shows the applicability of IEC 62351 in the context of other standard frameworks.

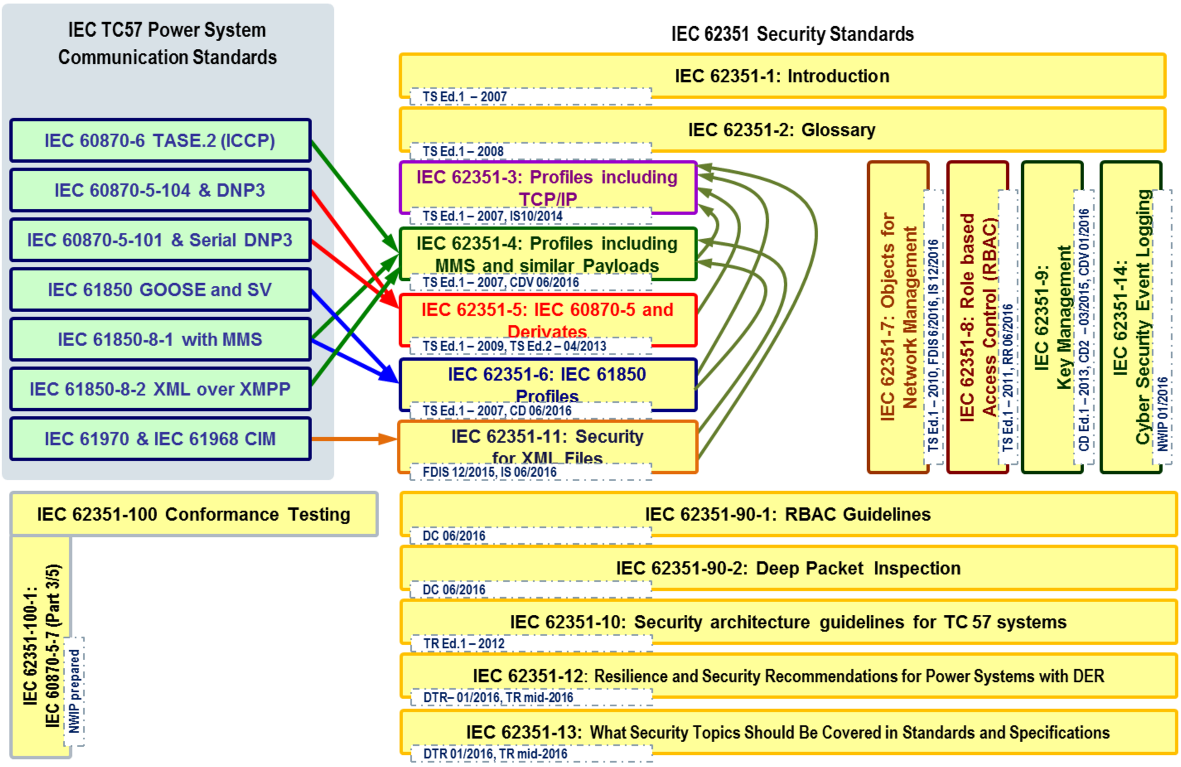


Figure 6: IEC 62351 Overview and mapping to protected communication standards

A clear goal of IEC62351 is the assurance of end-to-end security, which can be achieved on different OSI levels. The standard comprises multiple parts that are in different state of completion (see next subsection). While the focus was placed on the security of data in motion, the security for data at rest will be considered in newer parts as well.

6.2.2.2.1 Status

The following table indicates the status of each IEC 62351 part.

IEC 62351	Definition of Security Services for	Standardization Status
1	Introduction and overview	Technical Specification (TS, 2007) Update needed
2	Glossary of terms	Technical Specification Ed. 1 (TS, 2008) Edition 2 is currently being prepared
3	Security for profiles including TCP/IP	International Standard Ed.1 (IS, 2014)
4	Security for profiles including MMS	Technical Specification (TS, 2007) Work on International Standard Ed. 1 is started CDV in 07/2016, IS expected in 06/2017

IEC 62351	Definition of Security Services for	Standardization Status
5	Security for IEC 60870-5 and Derivatives	Technical Specification Ed. 2 (TS, 2013) Work on International Standard in preparation, also addressing identified issues
6	Security for IEC 61850 profiles	Technical Specification (TS, 2007) International Standard in preparation, will align with IEC/TR 61850-90-5, will be developed in parallel to part 4, as there are normative references CDV in 07/2016 in parallel with Part 4
7	Network and system management (NSM) data object models	Technical Specification (TS, 2010) International Standard in progress CDV in 12/2015
8	Role-Based Access Control for Power systems management	Technical Specification (TS, 2011) Update planned upon further development of IEC/TR 62351-90-1 Revision Request for International Standard by 06/2016
9	Credential Management	International Standard in progress CDV in 02/2016
10	Security Architecture Guidelines	Technical Report (TR, 2012)
11	Security for XML File	International Standard in progress FDIS in 12/2015 IS 06/2016
12	Resilience and Security Recommendations for Power Systems with DER	Technical Report in 04/2016
13	What Security Topics Should Be Covered in Standards and Specifications	Technical Report in progress This part is likely to serve as input for the newly founded ACSec DTR in 02/2016
14	Security Event Logging and Reporting	New Proposal in progress NWIP by 06/2016
90-1	Guidelines for using Part 8 Roles	Technical Report in progress WD 03/2016 DC 06/2016
90-2	Deep Packet Inspection	Technical Report in progress DC 09/2016
100-1	Conformance test cases for IEC 62351-5 and companion standards	Technical Specification in preparation NWIP by 05/2016

Besides the work on existing parts there are further issues continuously identified, which are specific to security in power systems, and which may need further definition in terms of TS/IS/TR documents.

6.2.2.2.2 Identified Gaps

As pointed out in the previous section, there have been issues identified for further work. Additionally, it is recommended to also take device security into account. While the current set of standards mainly focuses on communication security, the security of the devices producing the data, attached to a communication network need to be taken into account as well. As for several other parts, it may not be necessary to reinvent technology here but profiling would be an option.

6.2.2.3 IEC 62734: Wireless communication

This standard specifies a method of reliable and secure wireless operation for non-critical monitoring, alerting, supervisory control, open loop control, and closed loop control applications. This standard defines a protocol suite, including system management, gateway considerations, and security specifications, for low-data-rate wireless connectivity with fixed, portable, and slowly-moving devices, often operating under severe energy and power constraints.

The concept behind this standard is the adoption of PHY and MAC layer of IEEE 802.15.4 (that is also the physical layer of Zigbee protocol) defining a complete suite of protocol, covering the whole ISO/OSI seven layer stack.

This is a wireless solution standard dedicated to industrial systems but because it defines in a very complete manner all the details for the lifecycle of end systems, and it relays on a widely used and low cost hardware platform (that includes an hardware encryption engine) it candidates for the use inside a home automation environment.

From the security perspective this standard includes all the needed specification (also the key management and enrolment features).

This standard specifies the following:

- Physical layer service definition and protocol specification
- Data-link layer service definition and protocol specification
- Network layer service definition and protocol specification
- Transport layer service definition and protocol specification
- Application layer service definition and protocol specification, including support for protocol tunneling and gateways
- Security and security management (including key management)
- Provisioning and configuration
- Network management
- Additive communication role profiles (i.e., one or more can be selected concurrently).

In other words the adoption of this standard will somehow “hide” the underling IEEE 802.15.4 PHY/MAC standard because of the full coverage of the specifications needing.

6.2.2.3.1 Status

	Description	Standardization Status
IEC 62734	Industrial networks - Wireless communication network and communication profiles - ISA 100.11a	Publication 2014-10-28

6.2.2.3.2 Identified Gaps

No gaps identified so far.

6.2.2.4 IETF draft-ietf-tls-tls13: TLS Version 1.3

Transport Layer Security (TLS) is a widely used and endorsed security protocol to protect TCP based traffic. Historically, it is the successor of the Secure Socket Layer (SSL) and is meanwhile available in version 1.2 as RFC 5246. This RFC has been released in 2008 and has been updated since then. There are currently efforts in the IETF to update TLS to version 1.3 to address recent advances in cryptography and also to simplify the protocol state machine. These changes specifically comprise beyond others:

- Changes in supported/required cipher suites (e.g., support for static RSA and DH key exchange as well as for non-AEAD ciphers has been removed)
- Simplifications in the TLS handshake and session handling through
    - removal of renegotiation and ChangeCipherSpec exchanges
    - removal of session resumption in favour of utilization of tickets
- Prohibition of negotiation of SSL for backward compatibility
- Changes in handshake to provide faster setup (just 1.5 roundtrips)
- Removed support for compression.

Beyond other use cases, TLS is being profiled and utilized in the context of IEC 62351 to protect TCP-based power systems automation communication. As this requires the consideration of further advancements of this protocol as well as ensuring backward compatibility also with existing implementations utilizing TLS version prior to version 1.3, it is being monitored here.

6.2.2.4.1 Status

The Internet-Draft is in review and will expire September, 2016.

	Description	Standardization Status
draft-ietf-tls-tls13	TLS version 1.3 specification	Working Draft

6.2.2.4.2 Identified Gaps

There have been no gaps identified. However, the draft is in the review phase. Once published, it will have an influence to IEC 62351-3 as TLS1.3 provides certain changes to be considered in the profiling of TLS. This relates to the handshake, the session management, and also the supported cipher suites.

6.2.2.5 IETF draft-weis-gdoi-iec62351-9: GDOI Protocol Support for IEC 62351 Security Services

The Internet Draft (I-D) with the title GDOI Protocol Support for IEC 62351 Security Services amends RFC 6407 with payload definitions to support protocols using GDOI in the IEC 62351 series of standards. The abstract outlines this: *The IEC 61850 power utility automation family of standards describes methods using Ethernet and IP for distributing control and data frames within and between substations. The IEC 61850-90-5 and IEC 62351-9 standards specify the use of the Group Domain of Interpretation (GDOI) protocol (RFC 6407) to distribute security transforms for some IEC 61850 security protocols. This memo defines GDOI payloads to support those security protocols.*

GDOI is currently defined as group key management protocol in IEC TR 61850-90-5 and IEC 62351-9. Furthermore, it is a key distribution protocol for VPN technologies based on group keys. It is already in use in many installations, especially to protect traffic between substations or between substations and control centers.

The GDOI protocol is typically used when group-key management is needed, either in a pull or push scenario. In IEC 61850-90-5, GDOI is utilized for key management to protect the transmission of synchrophasor data. Beyond that, GDOI will be the protocol of choice for group key management and distribution in IEC 62351 and defined in part 9. It will be used to distribute keys to protect GOOSE and Sampled Value (SV) data according to IEC 62351-6.

6.2.2.5.1 Status

The Internet-Draft is in review and expired on September 22nd , 2016.

	Description	Standardization Status
draft-weis-gdoi-iec62351-9	GDOI Protocol Support for IEC 62351 Security Services	Working Draft

6.2.2.5.2 Identified Gaps

There have been no gaps identified. However, the draft is in the review phase.

6.3 Identification of Additional Security Standards to be Considered

Further security standards or draft standards have been identified or have been recommended by experts, during the course of investigating into the topic as such, which also address security in the target domain and may be directly applicable.

SGAM Layer	Standard	Comments
B, F, I	IEC 62443-2-1	Security for industrial automation and control systems - Network and system security - Part 2-1: Industrial automation and control system security management system
F, I, C	ISA 100.11a	Industrial communication networks – Wireless communication network and communication profiles
C	ISO 24759	Test requirements for cryptographic modules
C	ISO 18367	Algorithm and security mechanisms conformance testing
C	ISO 17825	Testing methods for the mitigation of non-invasive attack classes against crypto modules
B, F,I	ISO 27005	Information technology -- Security techniques -- Information security risk management
B, F,I	ISO 31000:2009	Risk management
B, F,I	ISO 30104	Physical security attacks, mitigation techniques and security requirements
B, F,I	NIST SP 800-39	Managing Information Security Risk

7 Applied Cyber Security on Smart Energy Grid Use Cases

The Applied Cyber Security on Smart Energy Grid Use Cases provides a set of guidelines on how to deploy security standards.

In Chapter 8 of 2014 SGIS report [4] some use case examples were presented in a synthesized way with the objective to illustrate how to use the SGIS methodology, i.e. the SGAM [2] and the European set of recommendations dashboard for going from a smart grid use case to security standards. The use case SGAM mapping presented in [4] provided some information to understand the functional and technical details of the use cases. The European set of recommendations dashboard in [4] has been designed to propose a pragmatic and easy way to deal with information security in smart grid use cases.

Starting from the outcome of the SGIS report [4], the work hereby reported is aimed at extending the use case security analysis methodology with intermediate steps going from use case ICT analysis, through risk levels and (standard) security requirements to solutions to secure the use case ICT architectures.

Figure 7 provides an overall view of the security analysis process of Smart Energy System use cases.

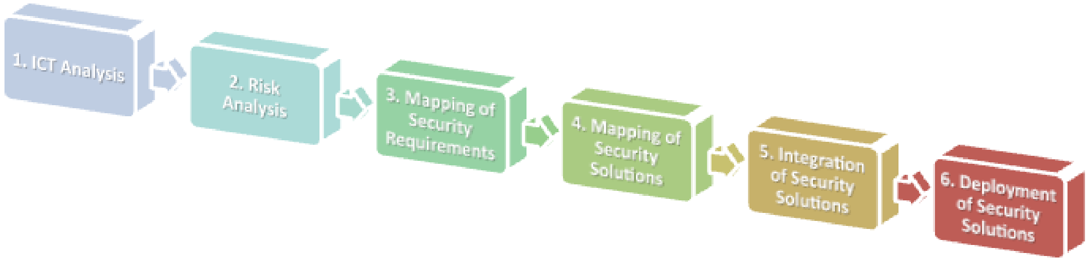


Figure 7: Security Analysis Process

The Use Case ICT Analysis is the starting step addressing the detailed specification of the use case architecture. A high level view of the use case architecture is achieved by mapping the use case assets over the SGAM layers. Key outcomes from the use case ICT analysis are the use case **ICT architecture**, its **logical communication interfaces** and the **communication protocols** to be used for the information exchanges.

The second step is the use case risk analysis providing details on the use case impacts and use case specific threats to the component and system functions, resulting in **risk level** assignments to use case information assets.

Given the architecture and security details collected in the two analysis steps, the mapping of (standard) **security requirements** represents the third step of the security process, followed by the mapping of (standard) **security solutions** in the fourth step.

In order to come up with a system level view of the use case security, in the step five the use case solution standards are integrated in the use case ICT architecture, resulting in the use case **secure architecture**.

Finally the deployment details of use case solution standards are given in step 6 producing a set of interface specific **recommendations** on the security solution application.

The specific aim of this security analysis methodology is to drive the use case owners in the deployment of security standards.

In Section 7.1 the extended methodology has been applied to the DER control use case introduced in [4] highlighting the key issues related to the deployment of security solutions.

The use of the SGAM Toolbox [6] as a formal support to the application of the methodology is included in Section 7.2.

Furthermore the substation automation use case introduced in [4][3] is used in Section 7.3 to illustrate how the standard IEC 62443-3-3 supports some intermediate steps of the security analysis methodology.

From the application of the extended security analysis methodology to use cases a set of recommendations will be derived in Chapter 7.4 and future development items of some IEC 62351 Technical Reports identified.

7.1 Application of the security analysis process to DER Control Use Case

This section presents the step-by-step application of the security analysis methodology to the DER control use case, highlighting the rationale underlying each security analysis step.

7.1.1 DER Control Use Case – ICT Analysis

The SGIS report [4] showed how the DER Control architectural aspects could be mapped over the five layers of the SGAM model. In the Function Layers the actors of the use case were placed into the Transmission, Distribution and DER domains. The control zones varied from the Market zone of the Aggregator to the Field zone of the control functions of the OLTC (On Load Tap Changer), Capacitor bank, DER and Flexible Load. The Generation and Load Forecast functions were placed in the cell Enterprise zone/Distribution domain. The

EMS (Energy Management System) and DMS (Distribution Management System) control functions were in the Operation zone hosting all the active grid operation functions. The Substation Automation System and the Medium Voltage Grid Control functions were located in the Station zone. In Figure 8 the mapping of the DER Control Use Case architecture over the SGAM communication layer is reported, including the communication protocols used for the required information exchanges.

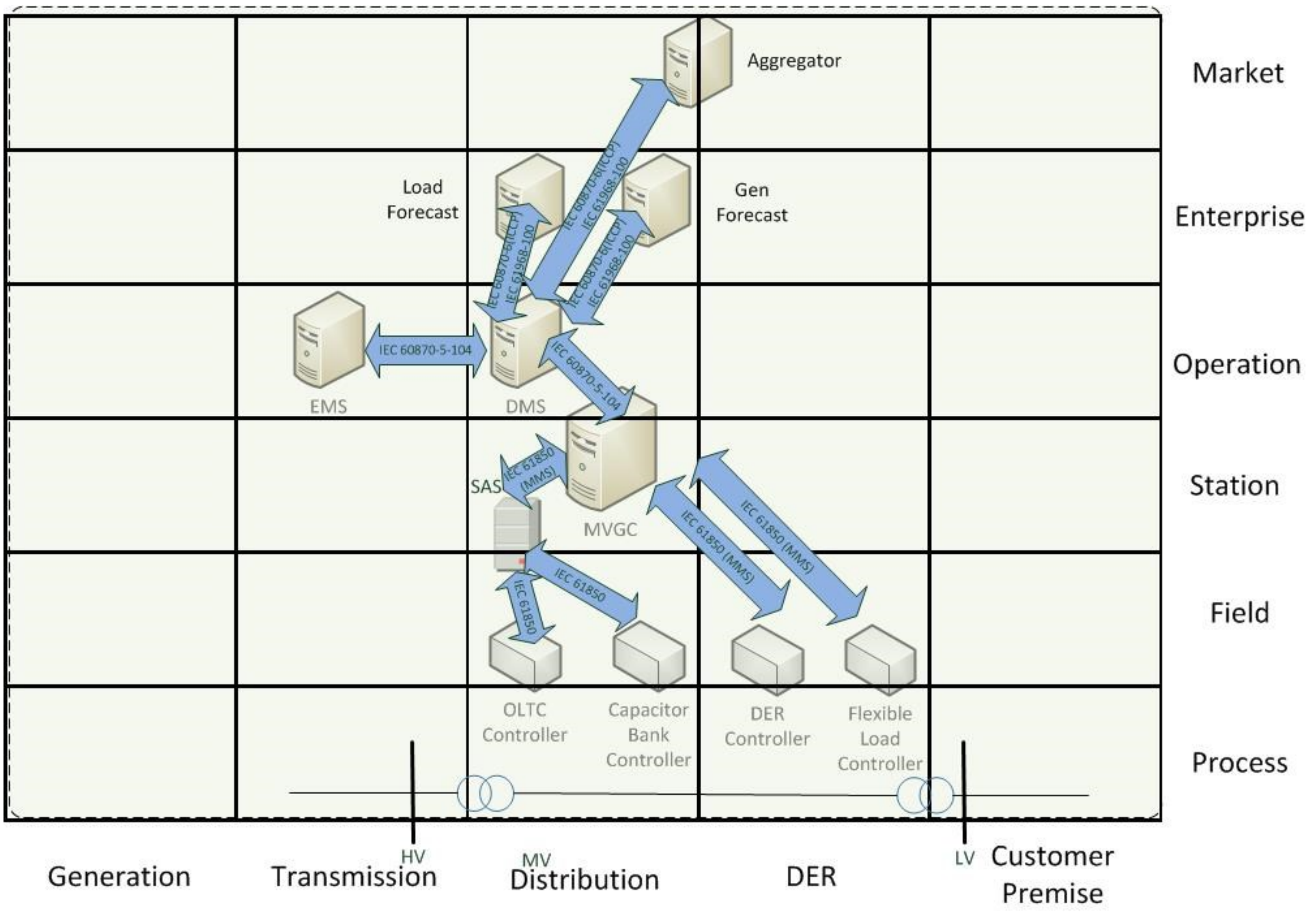


Figure 8: DER Control Use Case – Mapping of SGAM Communication Layer

Since the DER may be outside the responsibility area of the utility and the optimization algorithm requires inputs from actors external to the Distribution System Operator, the resulting overall architecture span over a multi-domain cyber space interconnecting a variety of ICT entities and network segments.

The use case mapping over the SGAM layers is a good mean for communicating a high level view of the use case control functions. However, in order to get it eligible for security risk analysis the SGAM mapping has to be complemented by deeper ICT modeling of the use case as well as benchmark grid data. A comprehensive list of use case details enabling a well-informed risk analysis is provided in Table 1, where green rows indicate power related items and blue ones refer to ICT related information. As can be understood from the item list in Table 1, before of moving to the risk analysis step a benchmark grid has to be defined as part of the use case specification, detailing the system size, its electrical connections, ICT links and associated information exchanges.

Parameter	Description
Geographical area	Geographical extension of the area covered by the grid service: multi-nation, nation, region, province, city
Population density	# of people in the area
Regulation	Applicable regulations
Grid size	Installed grid capacity
DER penetration	Total amount of Power from Renewable Energy Sources (RES)
DER size	Installed DER capacity
Grid topology	# HV/MV substations
	# MV loads
	# MV/LV substations
	# generators
	# storage devices
	# MV lines
Grid model parameters	Electrical parameters of grid components
DER model parameters	Electrical parameters of DER
Telecontrol Network Topology	# control centers
	# substation links per center
	# DER links per substation
Communication Network Topology	# gateways per network
	# communication (internal and external) interfaces per device
Data exchanges	Data models
	Communication protocol exchanges
	Communication interfaces
	Application message sequencing
	Data frequency
	Communication performance requirements
	Communication bandwidth requirements (traffic profile)

Table 1: Use case details enabling cyber risk analysis

In Figure 9 the Logical Interfaces of the DER Control Use Case are presented. The identification of the use case Logical Interfaces is driven by security engineering principles [24]. Each logical interface exposes typical features: we have the local network for the communications inside the primary substation, the DSO control network for Primary substation – DSO control centre information flows, a wired or wireless network for DER – Primary substation data exchange and the TSO process network and External/Enterprise network used by the DSO Control centre in order to communicate with TSO Control Centre and Aggregator, Load/Generation forecast respectively. The ICT maintenance and monitor operations are performed through a fully decoupled ICT maintenance network.

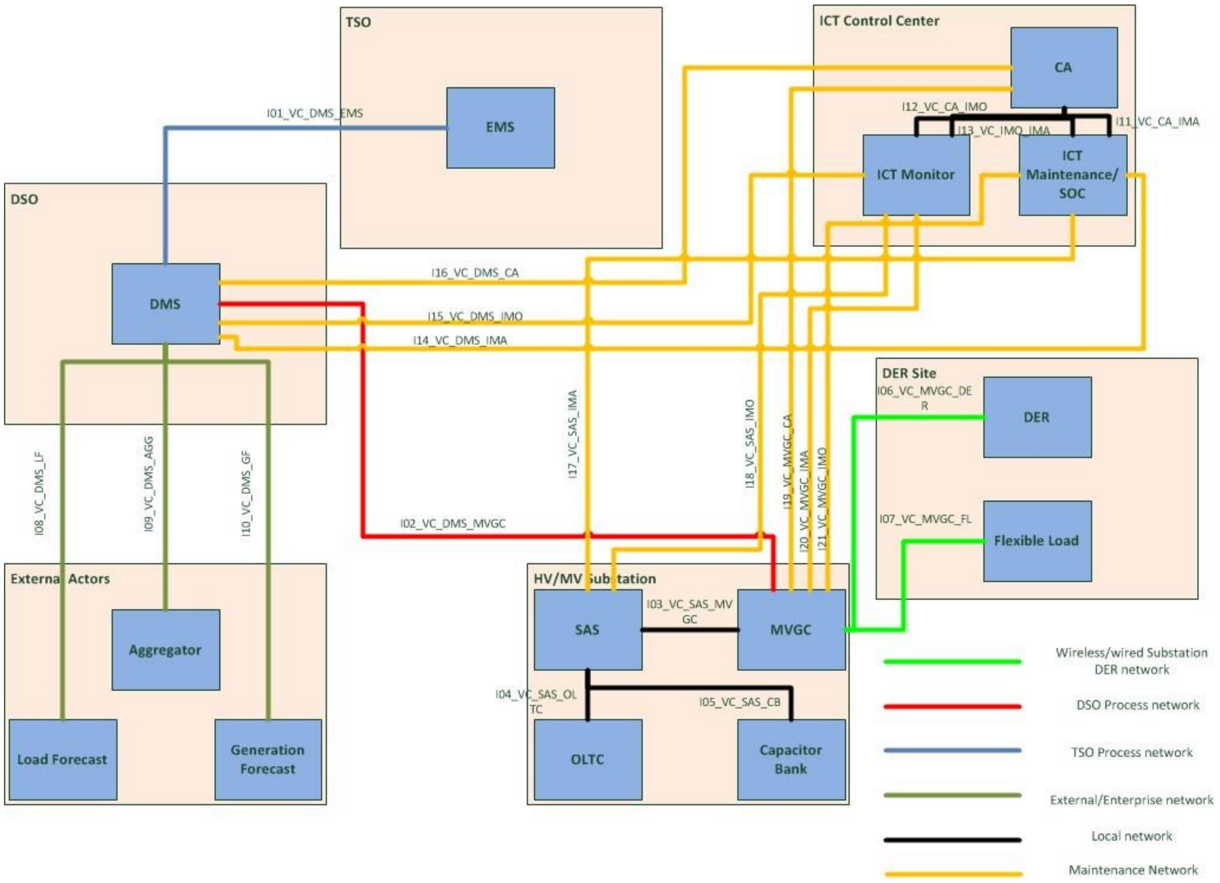


Figure 9: DER Control Use Case - Logical Interfaces

In Table 2 the list of the use case logical interfaces are presented together with a short description. Each interface is identified by a reference number, the reference control function (i.e. VC for Voltage Control) and the pair of entities constituting the link ends. The mapping of the DER Control use case interfaces with the interface categories of the NIST LRM [9] is reported in the third column of Table 2: as highlighted by the blue cells, the mapping of the DER Control use case required an extension of the NIST LRM with a new logical interface, 16 bis, for the information flows between the external DER and flexible load controllers and the medium voltage grid control device in the Primary Substation. A full description of the DER Control use case mapping over the NIST LRM logical interface categories can be found in [27].

Interfaces	Description	NIST LRM Interface Category
I01_VC_DMS_EMS	Interface used by the TSO for send TSO signal	6: Interface between control systems in different organizations
I02_VC_DMS_MVGC	Interface used by the DMS for exchange data with MVGC	1: Interface between control systems and equipment with high availability, and with compute and/or bandwidth constraints
I03_VC_SAS_MVGC	Interface used by the MVGC for exchange data with SAS (send setpoint and obtain measurements)	12: Interface between sensor networks and control systems
I04_VC_SAS_OLTC	Interface used by the SAS for exchange data with OLTC (send setpoint and obtain measurements)	12: Interface between sensor networks and control systems
I05_VC_SAS_CB	Interface used by the SAS for exchange data with Capacitor Bank (send setpoint and obtain measurements)	12: Interface between sensor networks and control systems
I06_VC_MVGC_DER	Interface used by the MVGC for exchange data with DER (send setpoint and obtain measurements)	16bis: Interface between external systems and substation equipment

Interfaces	Description	NIST LRM Interface Category
I07_VC_MVGC_FL	Interface used by the MVGC for exchange data with Flexible load (send setpoint and obtain measurements)	16bis: Interface between external systems and substation equipment
I08_VC_DMS_LF	Interface used by the DMS for exchange data with Load Forecast (updated data related to the forecast of the load customer consumption)	8: Interface between back office systems not under common management authority
I09_VC_DMS_AGG	Interface used by the DMS for exchange data with Aggregator (updated data related to the cost)	8: Interface between back office systems not under common management authority
I10_VC_DMS_GF	Interface used by the DMS for exchange data with Generation Forecast (updated data related to the forecast of the generation)	8: Interface between back office systems not under common management authority
I11_VC_CA_IMA	Interface used by the Certification Authority for exchange data with ICT and Security Maintenance (new certificates, check of certificates) and used by the ICT and Security Maintenance for maintenance purpose	22: Interface between security/network/system management consoles and all networks and systems
I12_VC_CA_IMO	Interface used by the Certification Authority for exchange data with ICT Monitor Systems (new certificates, check of certificates) and used by the Monitor server in order to obtain monitor information	22: Interface between security/network/system management consoles and all networks and systems
I13_VC_IMO_IMA	Interface used by the ICT and Security Maintenance for maintenance of the ICT Monitor Systems and used by the Monitor server in order to obtain monitor information	22: Interface between security/network/system management consoles and all networks and systems
I14_VC_DMS_IMA	Interface used by the ICT and Security Maintenance for DMS maintenance purpose	22: Interface between security/network/system management consoles and all networks and systems
I15_VC_DMS_IMO	Interface used by the Monitor Server in order to obtain monitor information related to DMS and used for provide to DMS a subset of the monitor information related to the ICT network status	22: Interface between security/network/system management consoles and all networks and systems
I16_VC_DMS_CA	Interface used by the Certification Authority for exchange data with DMS (new certificates, check of certificates)	22: Interface between security/network/system management consoles and all networks and systems
I17_VC_SAS_IMA	Interface used by the ICT and Security Maintenance for SAS maintenance purpose	22: Interface between security/network/system management consoles and all networks and systems
I18_VC_SAS_IMO	Interface used by the Monitor Server in order to obtain monitor information related to SAS	22: Interface between security/network/system management consoles and all networks and systems
I19_VC_MVGC_CA	Interface used by the Certification Authority for exchange data with MVGC (new certificates, check of certificates)	22: Interface between security/network/system management consoles and all networks and systems
I20_VC_MVGC_IMA	Interface used by the ICT and Security Maintenance for MVGC maintenance purpose	22: Interface between security/network/system management consoles and all networks and systems

Interfaces	Description	NIST LRM Interface Category
I21_VC_MVGC_IMO	Interface used by the Monitor Server in order to obtain monitor information related to MVGC	22: Interface between security/network/system management consoles and all networks and systems

Table 2: Logical Interfaces

7.1.2 DER Control Use Case – Risk Analysis

The risk analysis investigates the failure modes caused by cyber attacks to the ICT infrastructure supporting DER control functions and how they impact on grid operation. Typical approaches for a threat and risk analysis or threat modeling are described in [26]. With reference to SGIS security levels defined in the SGIS phase 1, the impact and likelihood levels associated to the information assets and scenarios related to the DER Control use case have been evaluated in order to obtain the corresponding SGIS levels [3]. Combining the impact levels with the likelihood level the High (3) and Critical (4) security levels have been assigned to the DER Control use case, depending on the information assets/security scenarios under consideration.
For a detailed discussion about the challenges of the use case risk analysis please refer to [27] and [28]. What is more relevant here to remark is that the security levels assigned to the use case assets by considering the benchmark grid and ICT details of the use case will drive the identification of the security requirements and the deployment of the security solutions in the next steps of the analysis process.

7.1.3 DER Control Use Case – Mapping of Security Requirements

From the outcome of the risk analysis a set of security requirements have to be associated to the use case information assets. In the SGIS report the European Recommendation Dashboard has been used to prioritize the security domains most relevant for the DER Control Use Case [3]. With the focus on the technical security issues, i.e. the information, communication and component SGAM layers, the following security domains have achieved a high priority by the application of the European Dashboard to the DER Control security levels 3 and 4:

- Secure lifecycle process for smart grid components and operating procedures
- Continuity of operations
- **Information systems security**
- Network security
- Resilient and robust design of critical core functionalities and infrastructures
- Situational Awareness**.**

The European security domains can be linked to security requirements defined in security standards. For example by taking as a reference the requirement categorization defined in [9], the following groups of security requirements are linked to the priority Information system security:

- Access Control (SG.AC)
- Identification and Authentication (SG.IA)
- Smart Grid Information System and Communication Protection (SG.SC)
- Smart Grid Information System and Information Integrity (SG.SI)
- Cryptography and Key Management.

According to the NIST LRM security concept in Figure 15, a full set of security requirements can be associated to the DER Control use case categories mapped in Table 2, by following the formal approach illustrated in Annex B.

7.1.4 DER Control Use Case – Mapping of Security Solutions

The technical security requirements associated to the use case information assets guide the selection of the relevant security solutions among the plethora of available security standards. In the SGIS report [3] a list of security standards have been mapped on the European security dashboard. As for the use case requirements addressing the Information system security and Situational Awareness priorities the solution standard IEC 62351 plays a central role.

IEC 62351-5, that is specified for securing the operation of all protocols based on or derived from the standard IEC 60870-5 (Transmission protocols in telecontrol equipment and systems), shall be referenced. This part focuses only on application layer authentication (on a message-by-message basis) and transport layer security via the IEC 62351-3.

IEC 62351-6 provides security specifications for use of IEC 61850. For MMS communications, it refers to IEC 62351-4. Furthermore, Part 6 suggests one additional cipher suite based on specifications of Part 4 in order to allow less CPU utilization for devices within substations.

IEC 62351-4 contains a set of mandatory and optional security specifications to be implemented for ISO 9506 – Manufacturing Message Specification (MMS) based applications. The communication security, specified in this technical specification, shall be mapped into two types of profiles (application profiles and transport profiles) according to the mapping to different layers of OSI Reference Model. For transport profiles, the usage of encryption and peer authentication shall be referred to IEC 62351-3.

IEC 62351 Parts 7-14-8-9 are used for ICT monitoring, ICT logging, role based access control and credential management functions, respectively.

Use Case Interface	Communication Protocols	Security Standards
I01_VC_DMS_EMS	IEC 60870-5-104	IEC 62351-5 IEC 62351-3
I02_VC_DMS_MVGC	IEC 60870-5-104	IEC 62351-5 IEC 62351-3
I03_VC_SAS_MVGC	IEC 61850-8-1 (MMS)	IEC 62351-4 IEC 62351-3
I04_VC_SAS_OLTC	IEC 61850-8-1 (MMS, GOOSE)	IEC 62351-4 IEC 62351-3 IEC 62351-6
I05_VC_SAS_CB	IEC 61850-8-1 (MMS, GOOSE)	IEC 62351-4 IEC 62351-3 IEC 62351-6
I06/7_VC_MVGC_DER	IEC 61850-8-1 (MMS, IP GOOSE)	IEC 62351-4 IEC 62351-3
I11_VC_CA_IMA	HTTPS SSH LDAP (Lightweight Directory Access Protocol) Online Certificate Status Protocol (OCSP) Trust Anchor Management Protocol (TAMP)	IEC 62351-3 IEC 62351-9
I12_VC_CA_IMO	Simple Network Management Protocol (SNMP) Online Certificate Status Protocol (OCSP) Trust Anchor Management Protocol (TAMP)	IEC 62351-7 IEC 62351-14 IEC 62351-9
I13_VC_IMO_IMA	HTTPS SSH LDAP (Lightweight Directory Access Protocol) Simple Network Management Protocol (SNMP)	IEC 62351-3 IEC 62351-7 IEC 62351-14
I14_VC_DMS_IMA	HTTPS SSH LDAP (Lightweight Directory Access Protocol)	IEC 62351-3

Use Case Interface	Communication Protocols	Security Standards
I15_VC_DMS_IMO	Simple Network Management Protocol (SNMP)	IEC 62351-7 IEC 62351-14
I16_VC_DMS_CA	Online Certificate Status Protocol (OCSP) Trust Anchor Management Protocol (TAMP)	IEC 62351-9
I17_VC_SAS_IMA	HTTPS SSH LDAP (Lightweight Directory Access Protocol)	IEC 62351-3
I18_VC_SAS_IMO	Simple Network Management Protocol (SNMP)	IEC 62351-7 IEC 62351-14
I19_VC_MVGC_CA	Online Certificate Status Protocol (OCSP) Trust Anchor Management Protocol (TAMP)	IEC 62351-9
I20_VC_MVGC_IMA	HTTPS SSH LDAP (Lightweight Directory Access Protocol)	IEC 62351-3
I21_VC_MVGC_IMO	Simple Network Management Protocol (SNMP)	IEC 62351-7 IEC 62351-14

Table 3: DER Control Use Case Logical Interfaces - Mapping of security solutions

Depending on the required security levels of the use case information assets, different implementation of the security measures will be deployed. This aspect will be further discussed in the following sections.

7.1.5 DER Control Use Case – Integration of Security Solutions

An overview of the use case secure architecture is presented in Figure 10 where, starting from the security requirements of the use case, the main solution standards have been integrated into the DER Control component architecture. We see as the main communication channels are protected by means of the authentication and encryption mechanisms recommended by IEC 62351 parts 3-4-5-6 (represented by a lock). A digital certificate based system (Certification Authority – CA in the picture) is deployed in order to guarantee the authentication of the different parties exchanging information, as recommended by IEC 62351-9. In order to monitor and detect anomalies a structure for capturing and analyzing monitoring objects and log information is developed where different monitor agents are scattered over the ICT architecture, according to IEC 62351-7 and IEC 62351-14. These agents may perform local analysis and create alarms and/or report values to server agents placed at the ICT maintenance center where a global view of the ICT systems is supervised by operators and correlation functions are performed enabling the application of automatic recovery measures.

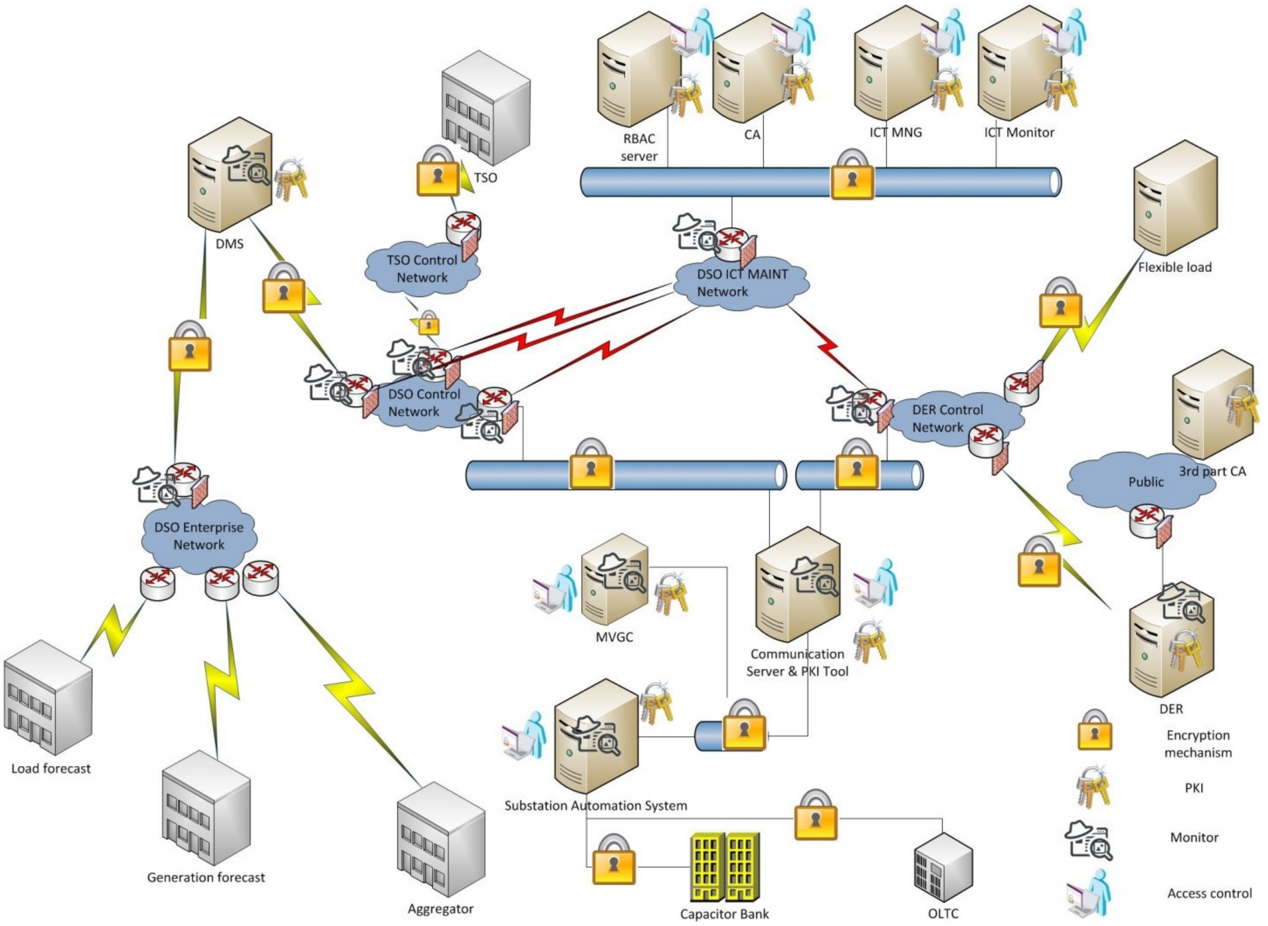


Figure 10: DER Control Use Case - Secure Architecture

7.1.6 DER Control Use Case – Deployment of Security Solutions

In order to explain the application of the deployment step to the DER Control Use Case, let us focus the analysis on the security standards of the MVGC logical interfaces, starting from the interface I06_VC_MVGC_DER, i.e. the interface used by the MVGC for exchanging data with DER (sending setpoints and getting measurements) using a 7-layer MMS connection-oriented mechanism.

IEC 62351-4 contains a set of mandatory and optional security specifications to be implemented for ISO 9506 – Manufacturing Message Specification (MMS) based applications. The communication security, specified in this technical specification, shall be mapped into two types of profiles, i.e. application profiles and transport profiles according to the addressed layers of the OSI Reference Model. For the transport profiles, the usage of encryption and peer authentication shall be referred to IEC 62351-3. To conform to IEC 62351-3, the communication peers of MVGC and DER should both provide the valid certificates with the recommended size. Both two sides also should specify at least one common cipher suite to agree on the algorithms used for data compression and encryption. Additionally, the timeframe configured for session resumption and session renegotiation shall be aligned with the Certificate Revocation List (CRL) refresh time.

With regard to the application profiles, the secure profile shall be indicated and configured to allow establishment of a MMS connection/association depending on the required security level. To convey/verify the association, the parameters including presentation address, profile used indication (for DER use case, it shall be SECURE) and ACSE authentication parameters (containing user information value) shall be configured. In hence, the peer entity authentication shall occur during the association set-up to counter the specific security threats of unauthorized access to information. Also it is important to configure the logging of security related violations in a separate log.

The MVGC interface I21_VC_MVGC_IMO requires the deployment of the IEC 62351-7. To conform to IEC 62351-7 which defines network and system management (NSM) data objects used to monitor and control the networks and end systems, and to detect possible security intrusions, the DER use case architecture is integrated with the ICT management infrastructure as shown in Figure 11.

The ICT management infrastructure supports the functions typically provided by Network and Security Operation Centers, and related to the monitoring and control of the network devices (routers, switches, firewalls etc.) in the DSO Control Center LAN, Substation LANs and DSO Control networks. Such communication devices are connected to the ICT maintenance network (see the red network in Figure 11) so that the network monitoring information, such as network configuration information, network backup monitoring, communication performance and failure report, that are provided by IETF standard NSM data objects (shown as blue hats in Figure 11) are collected centrally by an ICT Monitor server.

As shown in Figure 11 the value of the IEC 62351-7 integration relies in extending the ICT monitoring to the control IED with NSM data objects (shown as red hats in Figure 11) that are specific of the application protocols. Further transport level objects has been identified as relevant to the security monitoring, currently not included in IETF standard (shown as yellow hats in Figure 11).

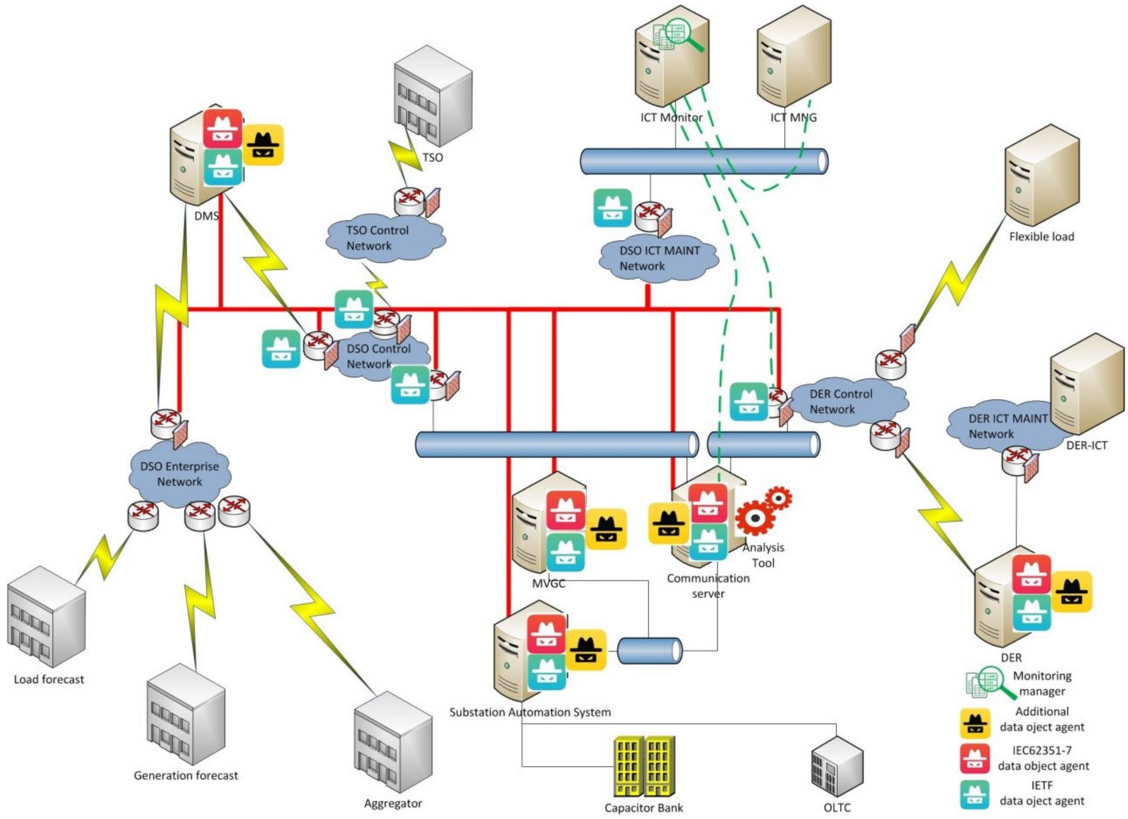


Figure 11: DER Control use case – architecture of ICT-DSO monitoring and management

The generation of the NSM data objects related to the communication performances is done by an analysis tool that calculates the object values from the network traces. In the DER control use case architecture the analysis function is onboard to the communication server within the substation network.

7.2 A formal approach supporting the security analysis process

One of the major aspects when considering smart grid security is to follow a consistent approach that integrates security by design. Thus, this chapter outlines a formal approach on how to deal with security over all stages of the development process.

The ideas presented in this section are a brief summary of existing concepts. Further more practical information on domain specific and standards based development of smart grid systems can be found in [29],

[30] or [31]. However, the described process is aligned with the concepts of the SGAM and comprises the first three steps of the security analysis process:

1.) ICT Analysis: Formal description of a fundamental system architecture in context of the SGAM. It comprises both, a functional analysis (SGAM Business and SGAM Function Layer) and an architectural description (SGAM Information, Communication and Component Layer). A special focus is put on the identification and description of Information Objects as fundamental asset for protection.

2.) Risk Analysis: Evaluation of Impact and Likelihood for potential cyber attacks. This step yields the SGIS Levels for particular components of the architecture.

3.) Mapping of Security Requirements: Derivation of certain Security Requirements for all interfaces within the architectural solution.

Figure 12 depicts the discussed steps together with their corresponding outcomes. The individual steps are described in more detail in the following. In addition, for the purpose of understanding, the appendix contains a complete example that demonstrates the application of the formalisation as a whole. For this example, the free to use SGAM-Toolbox [5] has been used for modelling.

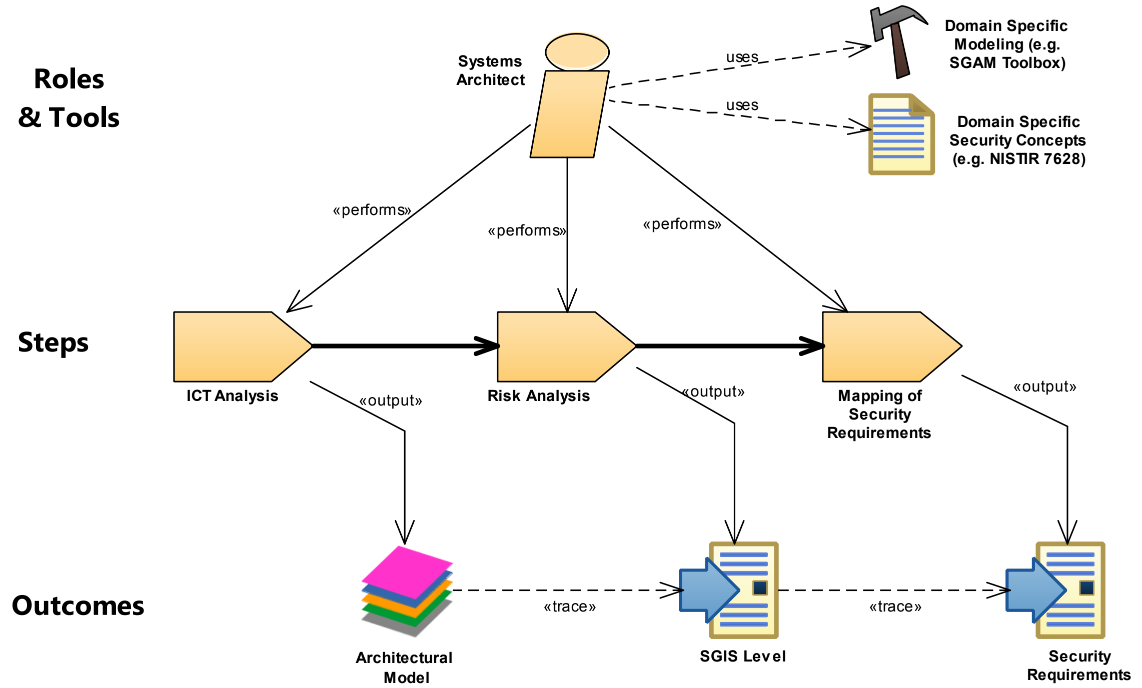


Figure 12: First steps of the security analysis process

7.2.1 ICT Analysis

The ICT Analysis step can be decomposed into two parts. First, a functional analysis aims at identification and specification of functionality to be realized. Moreover, particular Information Objects as important asset for protection are identified. The basic results of the functional analysis are the SGAM Business and Function Layer. Next, the architecture development describes a particular architectural solution to deliver the preliminary described functionality. The solution is described within the lower three SGAM layers. It comprises several components, which are connected via interfaces.

Each of these two parts consists of several tasks as depicted in Figure 13. A brief description of each task is given in the following. More detailed explanations can be found in [29].

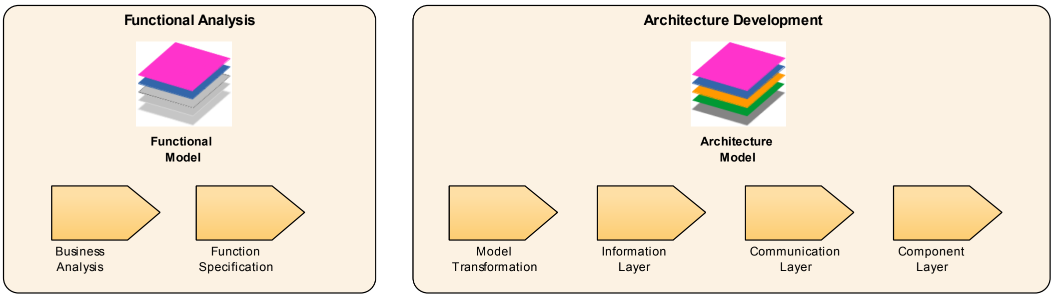


Figure 13: ICT Analysis

The Functional Analysis part comprises two tasks:

- Task 1.1 - "Business Analysis": The initial task takes place on height of the SGAM Business Layer. This layer is used to identify particular Business Actors (BA), which refer to physical or legal persons and their individual Business Goals (BG). Moreover, Business Cases (BC) are described that aim at balancing the needs between certain BAs. It is important to notice that the SGAM Business Layer not only comprises commercial aspects, much more it is also used to consider regulatory constraints. However, making particular BCs explicit is a rather important task in order to provide a complete picture as basis for the risk assessment.

- Task 1.2 – "Function Specification": On basis of the BCs, specific functionality can be derived and described on level of the SGAM function layer. For this step a staged approach is used. In accordance with the M/490 concepts in a first step High Level Use Cases (HLUC) can be defined. Typically, every BC comprises several HLUCs. An appropriate way for describing these HLUCs is to utilize the IEC 62559-2 Use Case template [7]. For a more detailed description each HLUC can be decomposed into more granular Primary Use Cases (PUC) with each being described in detail. This detailed description at least should cover the involved Logical Actors and the Information Object Flows in between. These Information Object Flows describe information being exchanged and thus yield information assets to be protected. In terms of the SGAM, for every HLUC one corresponding SGAM Function Layer should be developed. Here, all involved Logical Actors and their according PUCs can be aligned within the SGAM plane.

The Functional Analysis delivers a functional model. A logical view on every single HLUC is given as composition of several PUCs and their concerning Logical Actors (SGAM Function Layer). Moreover, the detailed description of every PUC delivers the information objects being exchanged as important asset for protection.

On basis of this functional model, a particular architectural solution can be developed. The Architecture Development part comprises the following tasks:

- Task 2.1 – "Model Transformation": In a first step the Logical Actors from the functional model are mapped onto specific physical components. This mapping represents a model transformation, which is not necessary a 1:1 mapping (e.g. a logical actor can be realized by a compound of physical components or, vice versa, logical actors can be realized as Software which is deployed on one physical computer that can host different software artefacts). It is a good practice to rely on well-defined actors such as those specified by the NISTIR Logical Reference Model (NIST LRM) [9]. The NIST LRM delivers best practice architecture solutions comprising actors and interfaces in between. Moreover, it provides detailed security considerations for particular interfaces. To be more precise, every Interface is associated with one or more Interface Categories. Furthermore, for every Interface Category very detailed security requirements are supplied.

- Task 2.2 – "Information Layer": This task yields the SGAM Information Layer, which describes information exchanges ("Business Context View") and data models being used ("Canonical Data

Model View"). The Information Layer is built upon the components derived in the previous step. The information flows can be derived on basis of the detailed description of particular PUCs from the functional model and the relation between components and Logical Actors. Subsequent to the development of the Business Context View, the used data models for information exchange can be defined within the Canonical Data Model.

- Task 2.3 – "Communication Layer": Similar to the Information Layer, the Communication Layer can be developed. The Information Layer describes information flows between particular components. On basis of these identified information flows, the used communication protocols can be defined within the Communication Layer.

- Task 2.4 – "Component Layer": The point-to-point communication has been specified within the Information- respectively the Communication Layer. On basis of this information, an appropriate Network Topology can be described within the Component Layer. The description on this layer rather serves as top-level view on the network architecture than as complete description. However, by utilizing appropriate modelling tools, more detailed in-depth descriptions can be developed.

The ICT analysis yields a description of a particular Smart Grid system. In alignment with the SGAM it comprises Business Aspects (SGAM Business Layer), Functional Aspects (SGAM Function Layer) and Architectural Aspects (SGAM Information, Communication and Component Layer). By following the process as described and maintaining the transformation relations between the particular layers, a consistent description can be obtained. To better illustrate this concept, Figure 14 depicts the overall model. This illustration can be interpreted as "front view" onto the SGAM cube. Here, the Functional Model comprises the SGAM Business Layer and the SGAM Function Layer. The Architectural Model comprises the lower three SGAM layers. Even if in these layers the same components are used, they are focusing on different aspects (information, communication, technology). However, it is important to notice that the relations between two or more components are associated with particular interfaces that play a major role in the subsequent considerations on security.

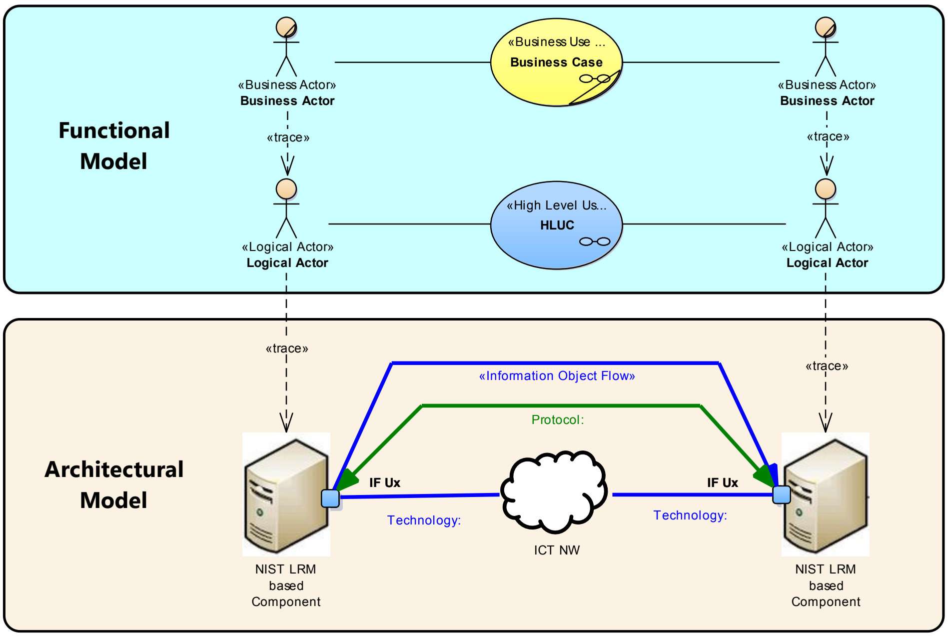


Figure 14: SGAM based System Model

7.2.2 Risk Analysis

The arising risk for a system can be derived on basis of the two factors impact and likelihood for a successful attack. Thus, these two factors need to be determined. The Smart Grid Information Security Report [3] suggests using a components' position within the SGAM plane as indication for the potential impact. For identification of the likelihood proposals exist [31] that suggest utilizing different Attack Probability Indicator such as reachability, hackers' motivation or systems maturity. However, a profound risk assessment requires detailed and individual considerations, which exceed the scope of this report. Further information on conducting risk assessments can be found for example in [26].

7.2.3 Mapping of Security Requirements

When considering security requirements it is a good approach to not reinvent the wheel but reuse approved work such as the NIST LRM. The NIST LRM is built up from particular actors and their interfaces. Moreover, each of these interfaces is assigned to one or more Interface Categories, which again is associated with a certain set of security requirements (Figure 15). Thus, putting the components from the architectural model in relation with particular actors from the NIST LRM, the according security requirements directly can be obtained. As these requirements are intended as High Level Security Requirements, further particularization is necessary. This can be done by considerations on basis of the preliminary made risk assessment.

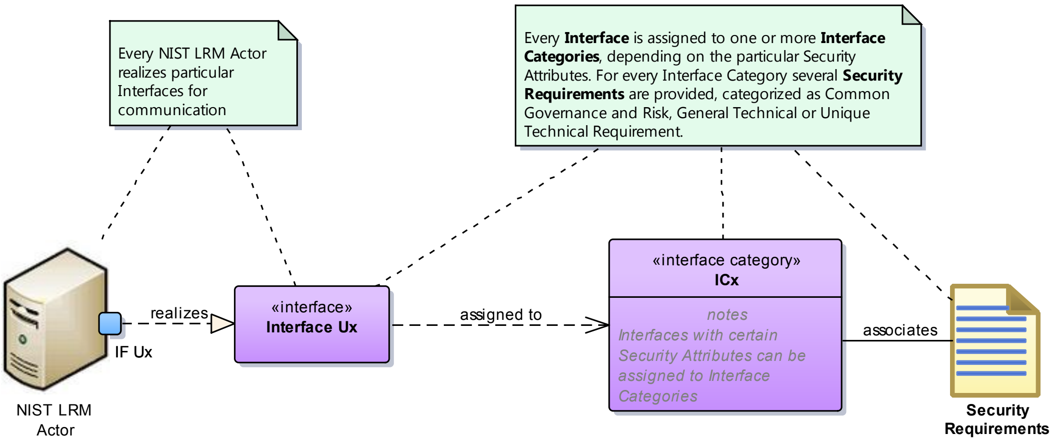


Figure 15: NIST LRM Security Concept

However, if a particular component (and its interfaces) can't be found within the NIST LRM, it can be added without breaking the underlying concepts. Thus, the interfaces of the newly introduced component can be manually related to the existing Interface Categories on basis of their original description. As a consequence, the security requirements of the identified Interface Category can be applied.

7.3 Substation Automation Use Case: Application of IEC 62443

Industrial Automation Control Systems (IACS) monitor and control automation systems in different automation domains. As networked automation control systems are exposed to external systems, they have to be protected against attacks to prevent manipulation of control operations. The three basic security requirements are confidentiality, integrity, and availability. However, in automation systems, the OT environment, these priorities are reversed: Availability has typically the highest priority, followed by integrity that, however, often overlaps with availability when considering the impact of an integrity violation. Confidentiality is often no strong requirement for control communication, but depends on the actual system and use case.

Security requirements have been discussed as part of the former SGIS working periods and resulted in the definition of the SGIS security levels (see [4][3]), which provide guidance for zones and domains in the SGAM, based on the criticality correlated with a pan-European Grid as shown in Figure 16. These security levels describe impact levels, which have to be taken into account when performing a threat and risk analysis.

SGIS-SL HIGH LEVEL GUIDANCE					
3 – 4	3 – 4	3 – 4	2 – 3	2 – 3	**MARKET**
3 – 4	3 – 4	3 – 4	2 – 3	2 – 3	**ENTREPRISE**
3 – 4	5	3 – 4	3	2 – 3	**OPERATION**
2 – 3	4	2	1 – 2	2	**STATION**
2 – 3	3	2	1 – 2	1	**FIELD**
2 – 3	2	2	1 – 2	1	**PROCESSES**
GENERATION	**TRANSMISSION**	**DISTRIBUTION**	**DER**	**CUSTOMER**	
DOMAINS					

Figure 16: Overview SGIS - Security Impact Level

The IEC 62443 series defines four different security levels based on the assumed strength of an attacker, which allow the derivation of security capabilities to cope with the specific strength of an attacker. The derived security capabilities in turn help to decrease the likelihood of a successful attack and thus directly relate to the SGIS security impact levels. The main focus of this section is to provide examples for the applicability of the IEC 62443 approach to define target specific security architectures, addressing a dedicated security level. An overview about the IEC 62443 security levels and the foundational requirements has already been given in section 6.2.1.2.

This section elaborates on the secure substation automation use case and discusses applicability of the IEC 62443-3-3 security requirements to the use case. Realization approaches for selected security requirements in the area of authentication and access control are given for selected IEC 62443 security levels.

In the six-step use case security analysis process presented in Section **Error! Reference source not found.**, the following substation automation discussion assumes that results from step 1 (ICT Analysis) and step 2 (Risk Analysis) are available. For example, the architecture as shown in Figure 19 would result from step 1. The content of this section focuses on:

- Step 3: Mapping of security requirements, where the scope is on IEC 62443-3-3 security requirements and their mapping to the substation use case.
- Steps 4 and 5: Mapping and integration of security solutions, where different realizations for selected IEC 62443-3-3 requirements and their integration into a secure architecture are discussed.

Note that in IEC TR 62351-10 [22], different use cases are discussed regarding their security considerations. This specifically includes a mapping of realization examples for security controls to different security domains as presented in table 4 of IEC TR 62351-10 [22]. A similar approach can be taken for mapping realization examples of IEC 62443-3-3 security controls to security levels. Section 6.4.3 will provide input to such mapping for FR1 – identification and authentication control.

Please note: IEC 62443-3-3 states in chapter “4.2 Support of essential functions”, special considerations for essential functions are the following:

- An essential function is a “function or capability that is required to maintain health, safety, the environment and availability for the equipment under control.”
- Security measures shall not adversely affect essential functions of a high availability IACS unless supported by a risk assessment.
- NOTE: See IEC 62443-2-1 regarding the documentation requirements associated with the risk assessment required to support instances where security measures may affect essential functions.
- When reading, specifying and implementing the SRs described in this standard, implementation of security measures should not cause loss of protection, loss of control, loss of view or loss of other essential functions. After a risk analysis, some facilities may determine certain types of security measures may halt continuous operations, but security measures shall not result in loss of protection that could result in health, safety and environmental (HSE) consequences.

Of course, if a system integrator uses products that are e.g. SL-2 capable, but does not configure them properly (as described by the products), the resulting solution might also not reach SL-2. This is also true for the asset owner: if the solution is not operated as described by the system integrator, the security of the solution will most likely degrade over time. As depicted in Figure 17, IEC 62443 introduces the different states of SLs:

- SL-T describes the target SLs, which is determined by a threat and risk analysis
- SL-C describes the reachable or capable SL by the chosen equipment
- SL-A describes the achieved SLs in the interplay of system components in the target operative environment.

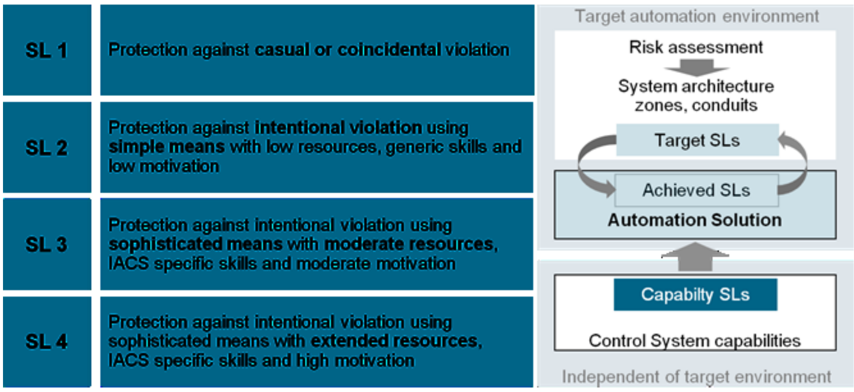


Figure 17: Security Levels - From targeted SL to achieved SL

Due to the varying operational environments and impact for substations, it is not possible to pick a common security level for substation automation systems. Due to typical setups, however, the main focus in the following is placed on security requirements to achieve SL 2, and additional SL3 requirements for dedicated target use cases.

In general, all of the seven foundational requirements (FR) categories of IEC 62443-3-3 apply to substation automation. The focus in this document is placed on the foundational requirement FR 1 “Identification and authentication control” and here specifically on the supplemental requirements human user authentication and device authentication as specific examples for the applicability of the security level concept of IEC 62443-3-3 in the energy automation domain. Note that for complete system architecture all foundational requirements and their supplemental requirements have to be addressed.

7.3.1 Use Case Overview

The substation use case used throughout this section can be mapped to the layers, domains, and zones defined in the SGAM model. Applicable domains are transmission and distribution, where the system used within this use case lies in one of these domains, or between them. The scope of IEC 62443-3-3 is a technical one, hence the information and communication layers are in focus. A mapping for substation automation into the SGAM model zones is shown in Figure 18.

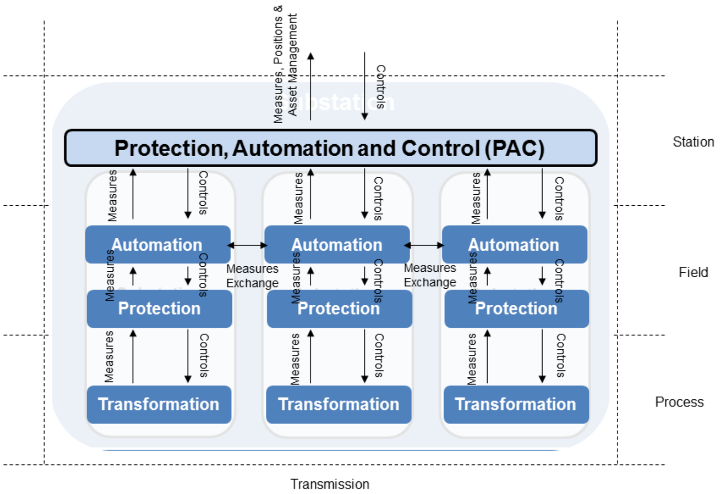


Figure 18: Substation automation use case - information layer mapping

Substation automation systems typically comprise different types of components that may come from different product suppliers, including, as sketched in Figure 18 and in Figure 19 within the control system box:

1. Embedded controllers like IEDs or similar field devices. Clearly, protection relays are among the most critical devices in substation automation systems, as they control the power lines and trip the circuit breakers if a fault is detected.
2. Substation controllers that concentrate data to and from the protection relays and provide automation, telecontrol and communication functions.
3. Local Human-Machine Interface (HMI) stations for visualization, monitoring and control of the process in the substation.
4. Applications running on standard-OS host devices, like workstations for engineering, parameterization and commissioning.
5. Additional network equipment that does not provide automation functions but realizes the networking between the automation components. This typically includes industrial-grade switches, routers, firewalls, or time servers.

An example substation design including the above listed components is shown in Figure 19. The components are grouped into secure zones, where one or several substation control zones group IEDs, substation controllers, and local HMI. All network communication to and from the substation control zone(s) passes through a demilitarized zone (DMZ) that is protected by firewalls. Common communication endpoints with the substation are a central control center where process-related communication is exchanged, or remote access for the purpose of remote maintenance or diagnostics.

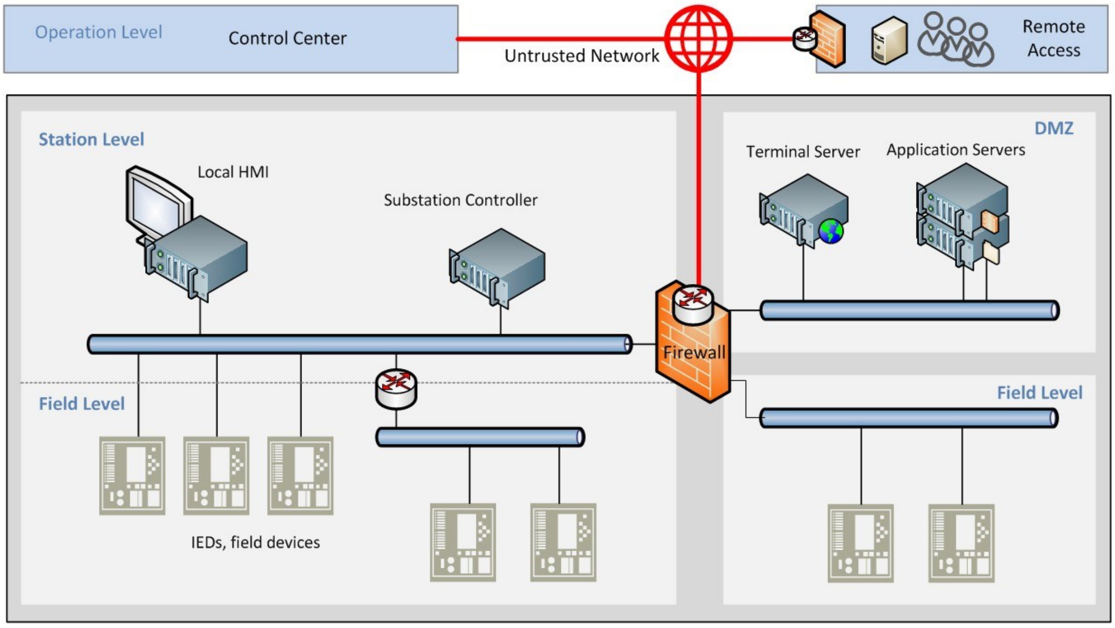


Figure 19: Generic substation composition

The IEC 62443 framework differentiates involved stakeholders that contribute to secure development, integration and operation of an industrial automation control system into three roles for product or component suppliers, system or solution integrators and asset owners (operators). See Figure 20, and its source in [13]. Considering the above system overview for substation automation, it shows that this approach maps well to substation automation where the same product or component types are designed into an automation control system for the energy distribution process.

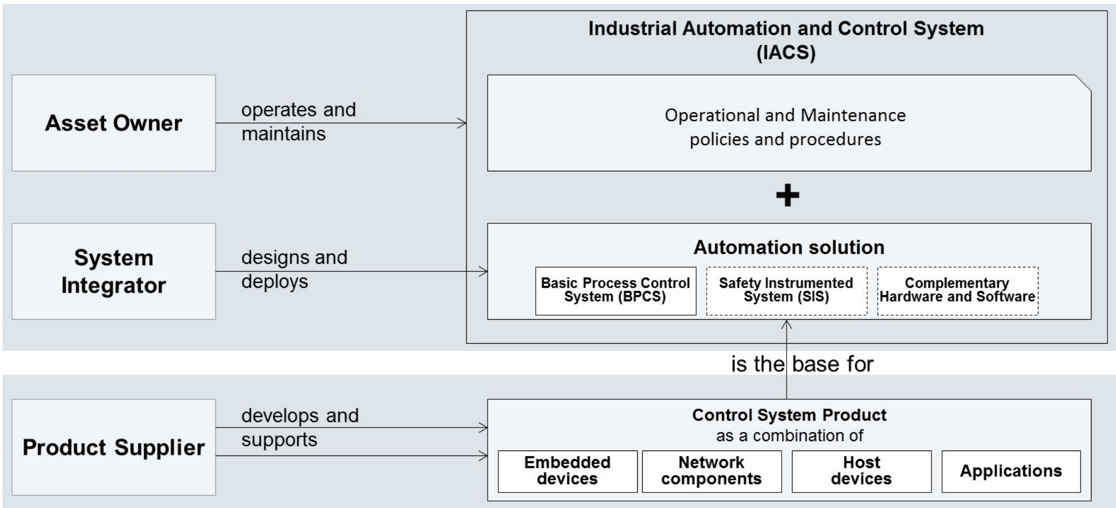


Figure 20: Roles contributing to automation control system security

In general, the IEC 62443 security requirements, including those provided by IEC 62443-3-3, largely apply to substation automation. Minor differences to industrial process automation can be identified like the fact that substation automation focuses on protection, instead of actively influencing the controlled process. In summary, this leads to the conclusion that the majority of IEC 62443-3-3 requirements can be applied to substation automation in a straight-forward way, with a small number of security requirements that either does not apply to this use case or needs to be interpreted differently.

7.3.2 Typical realization challenges

For substation automation systems, the realization of security functions underlies a number of limitations that stem from the typically constrained operational environment and lifecycle related considerations. An overview of such specifics can be found in [22], section 4.2. In the context of discussing realization approaches in the remainder of this section, especially the following challenges are mentioned:

- High availability requirements at least for a subset of substation components, especially including the IEDs and substation automation controllers that need to directly interact with the energy distribution process, if needed.
- Greatly varying needs regarding the availability of communication interfaces, where for example communication with a control center requires high availability, whereas remote access is temporary and possibly only needed in rare cases.
- Installation in remote physical locations with high maintenance effort in cases where local access is needed, or with potentially limited connection bandwidth.
- Very long lifetime (e.g. 15-30 years) where components stay in operation, leading to specific challenges and the need for suitable migration concepts.
- Large technical variety among the different components types that for example limit unified authentication and account management.

7.3.3 Applicability of IEC 62443-3-3 Security Levels

Due to the varying operational environments and impact for substations, it is not possible to pick a common IEC 62443-3-3 security level for substation automation systems. Due to typical setups, however, the main focus in the following is placed on the security requirements to achieve SL 2, and optional SL3 requirements for dedicated target use cases.

Figure 19 shows an example blueprint of a secure substation automation, where the substation components are separated by different secure zones. The core substation automation functionality is typically located in one secure zone (station and field level), where specific deployments may optionally introduce a separation between the station and field level. For all communication to and from the substation automation zone, a de-militarized zone is realized. This may reside in the same physical location as the station level, or may be separated with VPN tunnels to ensuring secure communication. Deployments may have several instances of the station and field level, resulting in several parallel zones. These may for example be physically separated, with connectivity through one central station zone or through the DMZ.

When assigning security levels to such setup, options are to assign the same security level to the whole system, or to assign an individual security level to each secure zone.

The SL concept is applied to the overall secure zone, which allows the case that a component used within a zone with given security level can come with a capability security level SL-C that is lower than the SL-T of the zone. This especially allows to accommodate systems where legacy components are in use and appropriate migration concepts are necessary. In such case, the SL-T can be achieved by applying appropriate compensating countermeasures that allow the zone to meet the applicable security requirements despite the component with lower SL-C.

In theory, it would also be possible to assign a higher security level SL to a component within a zone (an example would be to introduce a logical zone within the station zone that just contains a single engineering work station and that targets SL3, whereas the station zone itself targets SL2).

Furthermore, IEC 62443 security levels can be assigned as an SL-vector, where for each of the seven foundational requirements (FR) groups (see section 6.2.1.2) of the specification are assigned an individual SL resulting in the following format:

SL-x ([FR,]domain) = { IAC UC SI DC RDF TRE RA }

where x indicates whether the target, capability, or achieved SL type is used. An example for a substation automation system would be the following:

SL-T (substation automation) = { 2 2 2 1 2 2 2}

which means that the target SL for a given substation automation system is SL2, with the exception of data confidentiality capabilities that are classified as less critical for the system and are only applied at SL1.

For assigning a target security level to a given substation automation system and its intended operational environment, a typical approach would be

- to identify protection goals in the areas of confidentiality, integrity and availability, and to determine the resulting impact for violation of protection goals.
- based on the identified protection goals and impact, to perform a cyber security threat and risk analysis where the resulting risk for identified threats to each part of the system are estimated based on their likelihood and impact.
- to use the resulting risks as input to SL determination.

Security threat and risk analysis based on common methodologies like the one described in ISO 27005 can provide suitable justification why a certain SL is assigned to a given system. The above described approaches to not choose an overall SL for a substation automation system but to use individual SLs (whether per component and secure zone, or per FR) introduce additional complexity for SL assignment and hence require additional and more fine-grained justification for why a certain SL is assigned to a specific part of the system.

In summary, the following recommendations concerning the security level concept introduced by IEC 62443 are made:

- For the secure substation use case, no common security level can be assumed. However, a practical approach can be to start with assuming a security level of SL2 and assess based on the given operational environment and criticality (aligned with a determined SGIS-SL if available) whether additional SL3 capabilities should be targeted.
- It is recommended to keep differentiation of SL assignment within the substation automation system simple, as justification of fine-grained SL differentiation within the system may be difficult in practice.

To better relate the different sources for security levels and their applicability to following general recommendations are provided:

- Relate the SGIS-SL security levels defined in [3] and their mapping to the SGAM model with the IEC 62443-3-3 security levels.
- Relate the security domains and protection levels introduced by [22], including the realization examples of [22] table 4, with the IEC62443-3-3 security levels.

7.3.4 Considerations for authentication

This section discusses security requirements focused on the authentication of software processes and human users within the system-wide context. Different realization examples within the substation automation context are detailed and put in relation to the requirements' corresponding security levels.

Security requirements related to authentication of human users, software processes and devices are summarized in the foundational requirements FR1 chapter within IEC 62443-3-3 [14]. The security requirements are structured in basic ones, and in requirements enhancements that increase the required capabilities along an increasing security level.

The IEC 62443-3-3 security requirement SR 1.1 covers the identification and authentication of human users, as shown in Table 4 below. Such authentication is already required at SL1, but for this security level, group accounts are allowed to be used. For SL2, the required capabilities include that unique user authentication is available, e.g. through the configuration and use of individual accounts for each user having access to the substation automation system. There is no differentiation in the requirement for whether the user access takes place locally, or remote.

IEC 62443-3-3 Security Requirements	SL 1	SL 2	SL 3	SL 4
FR 1 - Identification and authentication control				
SR 1.1 – **Human user** identification and authentication	✔	✔	✔	✔
SR 1.1 RE 1 – Unique identification and authentication		✔	✔	✔
SR 1.1 RE 2 – Multifactor authentication for untrusted networks			✔	✔
SR 1.1 RE 3 – Multifactor authentication for all networks				✔
SR 1.2 – **Software process and device** identification and authentication		✔	✔	✔
SR 1.2 RE 1 – Unique identification and authentication			✔	✔

Table 4: IEC 62443-3-3 example requirements authentication

With SL3, additional multi-factor authentication is required based on the SL2 capability of unique user authentication. Here, a differentiation regarding the location of the authentication is made, as SL3 requires multi-factor authentication for access through untrusted networks. This applies to remote access that will typically be performed through untrusted or less trusted communication infrastructure. SL4 in addition requires the capability for multi-factor authentication for all human user access to the system, so this would also apply to HMI or engineering workstations within the secure substation zone.

7.3.5 User Authentication

When looking at the different component types within substation automation, it shows that user authentication can in principle take place in a number of different places, and can be realized by a number of different technologies. Typical places where user authentication may be performed include

- Authentication at the OS level with standard OS level user accounts. Standard-OS based substation components commonly include HMI stations, engineering workstations, or remote access servers. They may also include standard-OS based station controllers.

- Authentication at the application level as part of an application account management. Such user accounts may be application specific, or may be integrated with OS-level accounts.

- Authentication at embedded devices. Such authentication is not common in current deployments. Hence, it may be performed instead remotely and indirectly through the corresponding engineering applications. In such case, the engineering application would handle the user account management at application level. Authentication between the application and the embedded controller maps to software process and device authentication covered by SR 1.2.

- Authentication at network devices, including switches and routers. In this device class, a common approach is to map users to roles (e.g. admin, operator, user) granting different rights on the components, instead of performing unique user management directly within these devices.

For addressing authentication in substation automation systems to meet a certain SL the respective security requirements have to be met at the system level and not directly per each component. As a result, this allows for a range of realization options that target a given security level.

In the following, different realization approaches are discussed for the example use case of local engineering access to an IED device as depicted in Figure 21. The realization approaches target SR 1.1 with a security level of SL2:

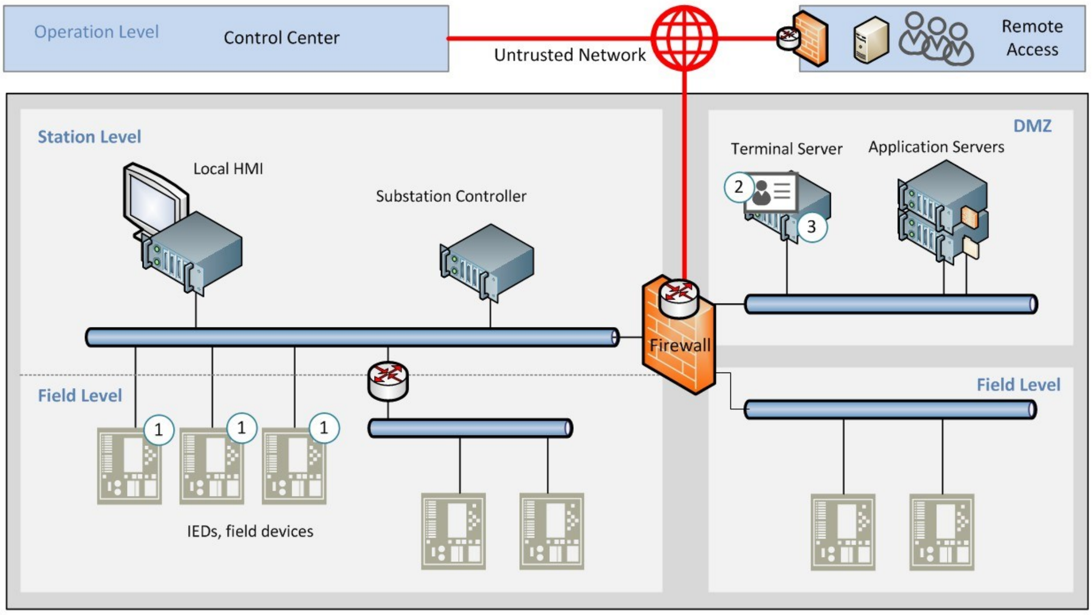


Figure 21: Example locations for authenticating engineering access

Example: Engineering access to an IED from within the substation automation zone, or substation DMZ.

- Realization approach 1: The IED itself may target SL2 and perform user authentication internally. Such realization is uncommon in current IED realizations. Furthermore, as there may be a substantial number of parallel IED devices within a substation deployment, directly performing user account management locally on each such device, is not recommended from a security perspective as this would introduce a significant risk of configuration errors, lack of synchronization, and unneeded user accounts in the system (conflicting with other IEC 62443-3-3 requirements like SR 7.7 – least functionality, or with secure maintenance requirements as identified in IEC 62443-2-4 [13]).

  With such realization, centralizing and unifying account management, e.g. through a central authentication, authorization and accounting (AAA) server and backend protocols like RADIUS would be needed in addition. Other approaches for future consideration to address this issue, include the use of methods based on X.509 public-key and attribute certificates as described in IEC 62351-8 [23] for use in the energy automation domain.

- Realization approach 2: Engineering access to an IED is performed through a corresponding engineering application that may perform unique user authentication of service technicians. With such setup, the authentication is not performed in the IED, but on the engineering workstation where the engineering application is installed and from where users actually perform their engineering tasks. The application account management can also be integrated with the OS-level account management of the workstation, which would support centralization of user accounts.

Here, it is important to implement a system design that allows engineering access to the IED only from dedicated engineering workstations to avoid bypassing of the authentication step. This can be achieved for example by secure engineering protocol communication (with process-level authentication between the IED and the engineering application) and by appropriate network configuration that blocks access to the IED from outside the secure zone where the IEDs are located.

- Realization approach 3: In cases where the engineering application does not support unique authentication at application level, the OS-level account management of the engineering workstation can be used as fallback to ensure that service technicians are uniquely authenticated. A drawback with such approach is that in cases where it is required to trace former user activities (a capability required by SR 2.8), correlation of logs would be needed. The account activity (user login/logoff) would be logged by the OS account management of the workstation, whereas actions performed through the engineering application would be found in the application logs.

Realization Example	Target SL	Communication Protocols	Security Measures
Approach 1	SL 2	Engineering (device specific), https, ssh	IEC TS 62351-8: • Purely certificate based using push method with X.509 user/attribute certificates. • Username/PW based with pull method to fetch X.509 user/attribute certificate from central repository.
Approach 2	SL 2	Engineering (device specific), https, ssh	Application level authentication (standalone or centralized), software process authentication, secure zone, firewall
Approach 3	SL 2	Engineering (device specific), https, ssh	OS level authentication (standalone or centralized), software process authentication, secure zone, firewall

Table 5: Summary of realization examples for user authentication

A summary of the above realization options that target SL2 is given in **Table 5**. To target a SL3 realization in addition, the local implementation must for example support dedicated security hardware to hold the user credentials.

7.3.6 Software process authentication

In substation automation, numerous software processes control the communication between system components. Such communication can be separated in communication internal to a secure (e.g. substation automation) zone, and in communication that is exchanged between secure zones. Examples for the latter that are shown in Figure 19 include control centers, or remote access for engineering and maintenance purposes.

Typical communication protocols are TCP/IP based and include a mix of generic (e.g. http/https, snmp) as well as energy automation specific (e.g. IEC 61850 [19], or 60870-5-104, see Figure 22) examples. For communication between substation automation and control center components, IEC 60870-5-104 for the exchange of process related information or commands to the substation, is commonplace, see also **Table 3**. An example for software process communication is an automated process that collects substation log data from a repository hosted in the substation’s DMZ. Especially in the remote access case, the communication is expected to traverse an untrusted network environment that interconnects the communicating endpoints.

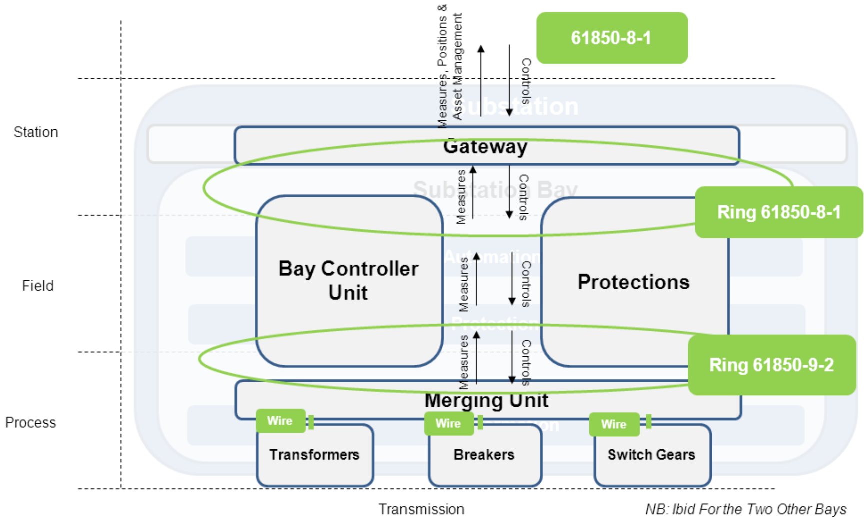


Figure 22: Transmission substation use case (one bay) - communication layer mapping

To design a substation automation system with capabilities targeting IEC 62443-3-3 SL2, authentication of software processes between the substation automation system and the control center zone (assumed to be a trusted zone of the same or higher SL) is needed. See also SR 1.2 in Table 4.

From a secure system design perspective, authentication of communicating software processes across a potentially untrusted network infrastructure can typically be achieved in two ways:

1. The communicating components, e.g. a station automation controller and the corresponding server in the control center, authenticate each other through an authentication method integrated with the communication protocol itself, like the TLS handshake used within IEC 62351 [20].

2. Both communicating components are located within secure zones, and the communication between these zones is secured and authenticated. This is typically achieved through a secure IPsec based VPN that can be established between the firewalls at the borders of the respective zones, or between dedicated appliances at these locations.

The main difference between the two approaches is that in the first case the communication is secured end-to-end, where the control center server directly authenticates the station automation controller in the substation and vice versa. In the second case, communication between the two zones is secured in a generic way, which means that the server knows the received communication originates from the secure substation automation zone (and vice versa). Hence, the server relies on the fact that the substation zone ensures the authenticity of the station automation controller.

For realization in deployments targeting SL2, securing communication between secure zones is considered a reasonable approach. In addition to an IPsec or similar VPN tunnel interconnecting all communication between the zones, appropriate firewall configuration can further limit the substation attack surface, e.g. through restricting IEC 60870-5-104 communication to the IP addresses of the respective control center components and the station automation controller.

When looking at SL3, SR1.2 RE(1) requires unique software process authentication. Here, the second approach as additional measure would be preferable, where the software processes traversing secure zone boundaries perform cryptographic authentication at the communication protocol level. For the IEC 60870-5-104 example, a realization approach is to support IEC 62351 based secure communication. This adds cryptographic protection based on the TLS protocol to IEC 60870-5-104. Within the IEC 62351 framework, part 4 realizes end-to-end protection based on TLS for IEC 60870-5-104. **Table 6** below summarizes the two approaches.

Realization Example	Target SL	Communication Protocols	Security Measures
Approach 1	SL 3	IEC 60870-5-104	IEC TS 62351-5, mutual authentication based on X.509 certificates. Certificates may be enhanced with RBAC information according to IEC 62351-8.
Approach 2	SL 2	IEC 60870-5-104	IPsec VPN (mutually authenticated), secure zones, firewall

Table 6: Summary of realization examples for software process authentication

7.3.7 Considerations for remote access

The IEC 62443-3-3 specification does not formulate requirements specifically for remote access to a system or secure zone. It provides

- requirements for generic security capabilities that also apply to remote access,
- and requirements that apply to the entry and exit points of secure zones in a generic way.

This section discusses the requirements of FR1 – "User identification and authentication" that focus on authenticating human users (see Table 4). These requirements in FR1 apply to the system in general. Hence, they need to be addressed for all human users that interact with the system, either locally or remote.

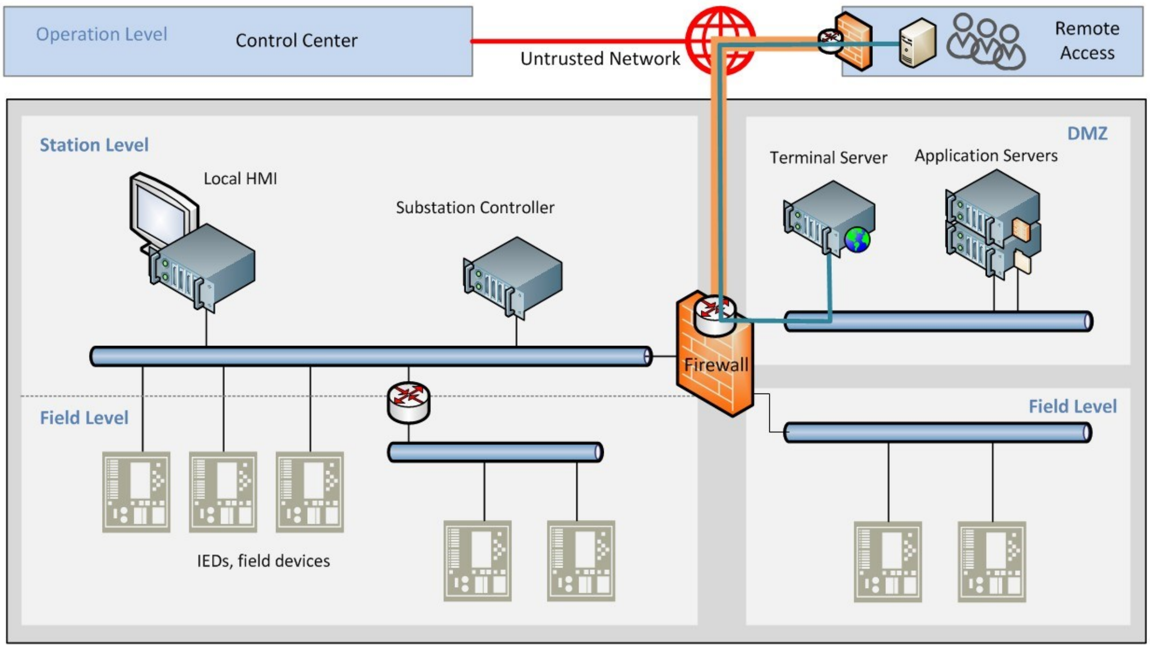


Figure 23: Remote access overview

Adding remote access capabilities as shown in Figure 23 to a system typically introduces additional user accounts for human users to the system. Remote access solutions are based on different technical realizations and infrastructure. Here, clear scoping is required to identify which parts of the remote access solution belong to the target system scope being subject to IEC 62443-3-3 conformance. The following options may occur:

- Remote access components are within the scope of the target system. These components are subject to applicable IEC 62443-3-3 security requirements.

  Example: a target system device may be accessible through an ssh connection. The ssh connection (conduit) and the remote device terminating ssh are within the scope of the target system.

- Remote access components partially lie within the scope of the target system. Applicable IEC 62443-3-3 requirements need to be met by those components within the scope of the target system.

  Example: The remote access solution, besides external IT infrastructure, uses an IPsec VPN tunnel that terminates at the border of the target system zone (e.g. at the DMZ). The component terminating the IPsec VPN tunnel at the target system falls into the scope of the target system, whereas all other remote access infrastructure is defined external to the target system.

Especially the second option shows that, depending on the actual realization, it may be difficult to apply all applicable security requirements to remote access in the same way as it is done for the substation automation system itself. Furthermore, as IEC 62443-3-3 is developed for industrial automation control systems, their direct application to regular IT infrastructure may not be feasible.

Still, the substation automation system itself has to meet the required capabilities of the assigned security level. A recommended approach to deal with such setup and choose a suitable realization is to perform a security threat and risk analysis for the planned remote access solution within the substation automation system context. Based on the resulting risks and risk levels, realizations may or may add an additional level of authentication within the substation environment. This may for example be an additional authentication step for all remote users that is enforced by a terminal server located within the substation DMZ.

7.4 Summary of Recommendations

As discussed in the beginning of chapter 7, to determine the risk level of specific scenarios a threat and impact analysis is the starting point. In order to achieve reliable outcome, different inputs are necessary to the risk analysis, like the underlying ICT architecture, the applied communication and network technologies, the effect of a successful attack, and benefit for an attacker. The current approach takes the SGIS security level as impact categorization as one input for the risk analysis. Based on the security analysis, security requirements and measures can be derived and ideally mapped to existing standards, as shown in the two examples for DER Control and Substation Automation.

To better relate the different sources for security levels and their applicability the following general recommendations are provided:

- Relate the SGIS-SL security levels defined in [4] and their mapping to the SGAM model with the IEC 62443-3-3 security levels.

- Relate the security domains and protection levels introduced by [22], including the realization examples of IEC 62351-10 [22] table 4, with the IEC 62443-3-3 security levels [14]. This approach has been successfully done in the context of IEC 62351-12 [24] by mapping the security guidelines for the integration of DER to the NISTIR 7628 requirements and also to the security requirements for the four different security levels in IEC 62443-3-3. This mapping provides a domain specific characterization of the described security requirements.

As shown in the applicability example in Section 7.3, the IEC 62443 security requirements framework covers the complete secure substation automation lifecycle, where different parts of the framework address different stakeholders. Especially relevant are the parts 62443-3-3 for a secure technical solution, and 62443-2-4 for its secure integration and maintenance. These parts are available as international standards.

IEC 62443-3-3 introduces a security level (SL) that cannot be assigned without considering the individual criticality and operational environment of each deployment. For considering realization approaches for a secure substation automation system, it seems reasonable to start with assuming a security level of SL2 and assess based on the given criticality and operational environment (aligned with a determined SGIS-SL if available) whether additional SL3 capabilities should be targeted.

Security levels can be assigned to different parts of a substation automation system, or also per each of the seven categories of requirements in IEC 62443-3-3 (FR). Here, it is recommended to keep such SL differentiation as simple as possible. Justification of fine-grained SL differentiation within the system may be difficult in practice.

In general, realizations and applicable requirements should be motivated by an IT security threat and risk analysis to evaluate and classify the specific risks. Such analysis should also cover any remote access capabilities, as these strongly impact conformance of the overall substation automation solution with the security requirements.

Another interesting finding of the standard application to use cases is the relations between IEC 62443-3-3 security levels and the IEC 62351 solution standards: depending on the security level assigned to a given communication interface, the deployment of the IEC 62351 may implement simpler or more complex configurations and/or architectures. Typical examples are the choice of the end-to-end communication security profile in the deployment of Parts 3/4/5/6, the layout and the configuration of the monitoring architecture in the deployment of Part 7, or the type of digital certification management architecture in the deployment of Part 9.

7.4.1 Links with IEC 62351

Specific links and possible extensions of the security guidelines in IEC 62351-10 and IEC 62351-12 are provided in the following sections.

7.4.1.1 Links of findings with IEC 62351-10

The IEC 62351-10 Technical report [22], released on October 2012, presents security architecture guidelines for power systems based on essential security controls. 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. This is a very important task for the usability of security standards, complementing the detailed, specific technical aspects defined in the other parts. As electric power infrastructures are introducing many infrastructural and organisation changes, such guidelines should be extended in time by following the sector structural evolution.

The application of security standards in this report has highlighted the need to extend the security domain by including all the actors of smart grids, such as DER and microgrid owners, commercial and residential prosumers, aggregators and providers of energy services and final customers participating to energy efficiency programs, having the need to communicate each other for different purposes. Following the security analysis methodology applied in Section 7 sample use cases could be identified and used in a next edition of IEC 62351-10 to update the security domains and the integration of security controls in their respective secure architectures (see e.g. Figure 10 and Figure 11).

7.4.1.2 Links of finding with IEC 62351-12

IEC 62351-12 [24] (see also Section 6.2.2.2) provides resiliency guidelines that recognize the need for integrating cyber security techniques with engineering and operational strategies for power systems with connected DER systems in order to improve resistance to attacks, failures, and natural disasters. It addresses system resilience in the different parts of the power grid and for different stakeholders, including:

- DER system resilience: designing and installing DER systems to provide DER resilience to anomalous power system events and cyber attacks.
- Grid resilience for grid planning with significant numbers of DER interconnections: promoting grid resilience by studying the impact of and planning for interconnecting DER systems with the grid to promote grid resilience.
- Grid resilience for grid operations with significant capacity of DER generation and storage: operating the grid with significantly large numbers and capacities of DER systems that can impact grid reliability and security.

With its scope IEC 62351-12 is directly applicable and supports the different steps of the security analysis described in Section 7.1 by providing cyber security requirements for design and engineering of DER integration from a domain level perspective. The standard addresses this by dividing the DER integration into different parts, which in turn are also mapped to SGAM. On the other hand, IEC 62351-12 also follows the NISTIR 7628 approach by defining logical interfaces between system components. Besides the analysis of the

DER scenarios IEC 62351-12 also maps the identified security requirements to the security requirements provided in NISTIR 7628 [9] and IEC 62443-3-3 [14]. This relates to the security analysis provided in this section in two ways:

- NISTIR 7628 identifies logical system interfaces and connected security requirements for the smart grid. As stated above, this approach is also taken here.

- The mapping to IEC 62443-3-3 helps determining appropriate technical security measures to reach a target security level required for the operation of the DER.

The DER use cases addressed in Section 7 of this document utilize the approach of logical interface identification between components to be able to map the identified security requirements to dedicated solution security standards to show their applicability. Note that this is being done for specific use cases and thus provide more fine grained requirements, which in turn can already be mapped to specific security measures. This is done by utilizing specifically different parts of IEC 62351, for protecting communication of control or monitoring or event information.

One specific target example of applying IEC 62443-3-3 in the context of this section was the handling of FR 1 – Identification and authentication control with the focus on user and process authentication. For all interfaces requiring an authentication as part of the telecontrol communication, IEC 62351-3 related security measures in conjunction with the connected telecontrol protocol (IEC 60870-5 or IEC 61850) security measures (specified in IEC 62351-4 and IEC 62351-5) are recommended. Specifically IEC 62351-3 requires the application of mutually authenticated TLS connections, for which both sides have to possess X.509 compliant certificates and corresponding private keys. This already targets unique authentication and identification required to achieve SL2. To achieve SL3 with multifactor authentication the local implementation must for example support dedicated security hardware (e.g., smart card), to hold the private key and perform the associated operations. Moreover, in conjunction with measures described in IEC 62351-8 role based access control can directly be supported as part of the X.509 certificates.

8 EU & US Analysis

The objective of this chapter is, through the analysis of cyber security for the energy sector related documents, see section 8.1, to investigate and possibly identify means to be able to transpose a use case once it has been mapped to the SGAM, see section 8.3.1, from a European cyber security context to a US one and vice-versa.

The documents that will be analyzed are complex one’s, reflecting a complex reality. The present chapter is a first attempt to see if and how this EU and US transposition could be done. For this first work, the content of these documents may have to be simplified in order to facilitate the work to be done in this chapter, the objective being to evaluate if such an approach is relevant and could be defined, not to define a complete and exhaustive transposition plan between all these documents.

Such an exhaustive plan would require much more work to be done. The content on this chapter is only an exploratory first attempt, not a definitive plan.

8.1 Analyzed Documents

8.1.1 SGIS Report (2014)

In 2014, CEN-CENELEC and ETSI published a report from the SG-CG/SGIS working group [4]. The chapters 7 & 8 of this report introduced the recommendations made by the ENISA and European Commission Smart Grid Task Force Expert Group 2 (EG2) ad hoc group and presented a methodology using a “cyber security dashboard” to use the use case identified SGIS Security Level (cf. §8.2.2) to prioritize actions to be taken and to identify standards that could be used to put in place these recommendations. For a better understanding of the following content, readers are encouraged to have a look at these chapters.

This document will be used as EU reference document for the study to be made in this chapter.

8.1.2 NERC CIP

The North American Electric Reliability Corporation (NERC) is a non-for-profit international regulatory authority whose mission is to assure the reliability of the bulk power system in North America. NERC CIP [8] standard is one of the mandatory standards issued by the NERC in order to protect critical infrastructures and is used to secure bulk electric systems. NERC CIP V5 is the version of this standard that will be used in this chapter.

CIP-002-5.1 — Cyber Security — Bulk Electric System (BES) Cyber System Categorization document will be used as US reference document for the study to be made in this chapter. For a better understanding of the following content, readers are encouraged to have a look at this document, more particularly the "*Attachment 1*" section.

8.1.3 NISTIR 7628

As expressed in SGIP "Introduction to NISTIR 7628 Guidelines for Smart Grid Cyber Security" document [9], NISTIR 7628 document contains "[…] *guidelines* [that] *are not prescriptive, nor mandatory. They are advisory, intended to facilitate each organization's effort to develop a cyber security strategy effectively focused on prevention, detection, response and recovery*". For a better understanding of the following content, readers are encouraged to have a look at this document.

NISTIR 7628 Revision 1 will be used as US reference document for the study to be made in this chapter.

8.2 Key Elements

8.2.1 Smart Grid Architecture Model (SGAM)

For more details about the SGAM please refer to SGIS Report (2014), chapter 5.1.

8.2.2 SGIS Security Levels (SGIS-SL)

For more details about SGIS Security Levels (SGIS-SL) please refer to SGIS Report (2014), chapter 5.2.

8.3 SGIS-SL & NERC CIP V5 Analysis

8.3.1 SGIS-SL & SGAM

According to SGIS Report (2014) [4], see section 5.2.1, SGIS-SL can be mapped to the SGAM as presented in the Figure 24 hereunder.

Figure 24*: SGIS-SL SGAM Mapping*

8.3.2 NERC CIP V5 & SGAM

The "*Attachment 1*" section of NERCIP V5, CIP-002-5.1 [8] document, defines impact rating criteria (Low, Medium and High) that are to be used in BES Cyber System Categorization. Using these criteria NERC CIP V5 applicability and impact rating could be mapped to the SGAM as presented in the Figure 25 hereunder:

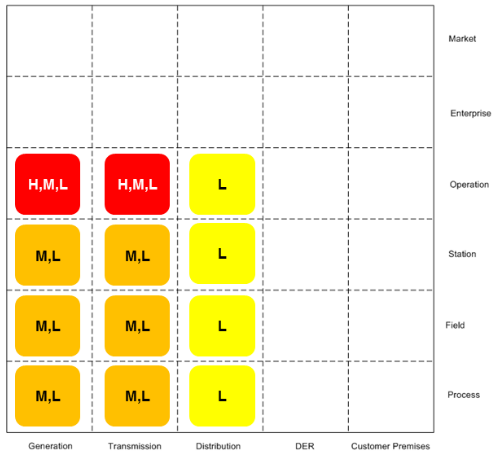


Figure 25*: NERC CIP V5 SGAM Mapping*

8.3.3 EU & US Portability Scale

According to SGIS-SL and NERC CIP V5 Impact rating definition power security scales could be defined for EU and US as presented in the Figure 26 hereunder:

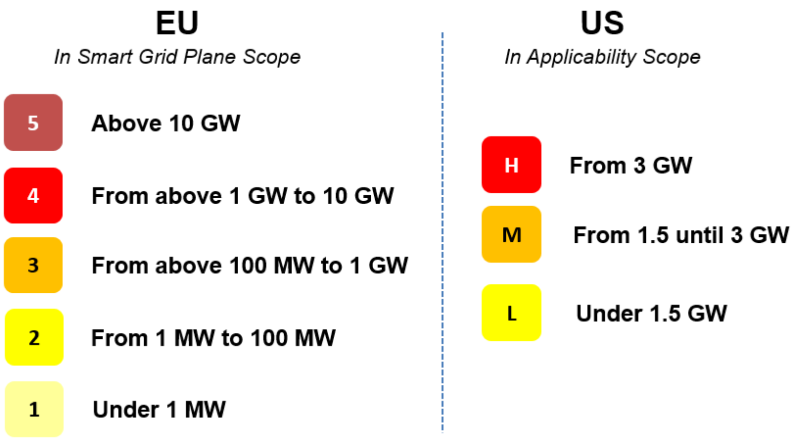


Figure 26: *EU & US Power Security Scales*

These EU & US scales are note fully aligned. In order to be able to easily transpose a use case from an EU context to a US one and vice versa a scale that could be used in both contexts would be useful. Such an EU & US portability scale can be found in Figure 27 hereunder.

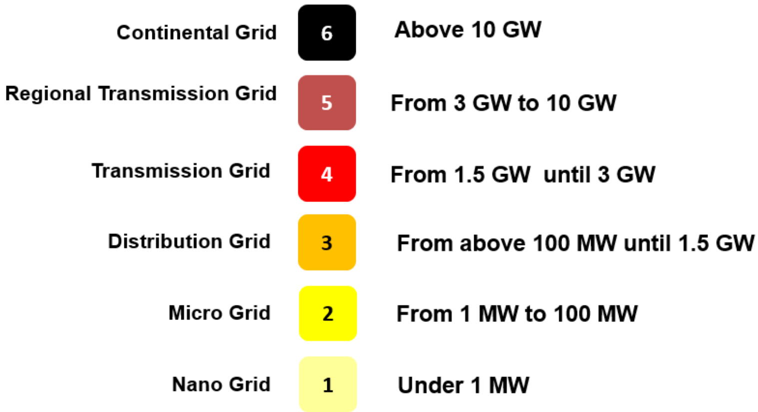


Figure 27: *EU & US Portability Scale*

8.3.4 EU & US Use Case Portability Reference Map

Using the EU & US portability scale previously defined and using the work done in section 8.3.1 and section 8.3.2 above it is now possible to define an EU & US Use Case Portability Reference Map that is presented in Figure 28 hereunder.

Figure 28: EU & US Use Case Portability Reference Map

Compared to the SGIS-SL SGAM mapping, this map uses the notion of Maximum Security Level (value will range from 1 to Max value) rather than to provide a range. This change is needed to ensure compatibility with NERC CIP SGAM mapping but has also been found meaningful to provide more flexibility based on power scale to map future Smart Grid use cases that may have not been thought about when defining this EU & US portability map.

8.3.5 Conclusion

The portability scale defined is EU SGIS-SL and US NERC CIP V5 compatible. It can be used to identify security requirements for a given use case either in EU or US cyber security context once the use case has been mapped to the SGAM. Same comments apply to the reference map.

Using this map, once a use case is mapped to the SGAM, it is really easy to identify what would be needed from a cyber security context either in EU ENISA and European Commission Smart Grid Task Force Expert

Group 2 (EG2) context or in US NERC CIP context. Even if each context could be used separately, the use of a common reference map will help to translate from a context to the other.

Additionally, as standards are also mapped to the SGAM (cf. §6 Smart Grid Set of Security Standards) using this methodology will also help identify which standards could be used to support the deployment of the requirements.

8.4 SGIS-SL & NISTIR 7628 Rev1

8.4.1 NISTIR 7628 Rev1 Impact Levels

NISTIR 7628 defines Impact Levels for the grid. The way they are defined differs significantly from the way SGIS-SL are defined. The latter being based on load levels while this is not the case for NISTIR 7628 Rev1 Impact Levels.

NISTIR 7628 Rev1 defines 22 Logical Interface Categories (LIC). For details of the LICs including definitions, please refer to NISTIR 7628 Rev1 §2. For each LIC, Impact Levels are assigned based on the three cybersecurity objectives of confidentiality, integrity and availability (see NISTIR 7628 Rev1 §2.2):

- A loss of confidentiality is the unauthorized disclosure of information.
- A loss of integrity is the unauthorized modification or destruction of information.
- A loss of availability is the disruption of access to or use of information or an information system

The Figure 29 hereunder gives the risk levels for each LIC (see NISTIR 7628 Rev1 §3.3 Table 3.2 for more details).

Logical Interface Category	Confidentiality	Integrity	Availability
1	L	H	H
2	L	H	M
3	L	H	H
4	L	H	M
5	L	H	H
6	L	H	M
7	H	H	L
8	H	H	L
9	H	H	M
10	L	H	M
11	L	M	M
12	L	M	M
13	H	H	L
14	H	H	H
15	L	M	M
16	H	M	L
17	L	H	M
18	M	H	L
19	L	H	M
20	L	H	M
21	L	H	M
22	H	H	H

Figure 29: Smart Grid Impact Levels (Source NISTIR 7628 Rev1)

The use of LIC and C,I,A Impact Levels in NISTIR 7628 Rev1 do not allow an easy and smooth way to translate a use case mapped to the SGAM from the European cyber security context to a US one referring to NISTIR 7628 Rev1.

8.4.2 Crosswalk of NERC CIP and NISTIR 7628 Rev1

NISTIR 7628 Rev1 Appendix A presents a crosswalk of cyber security documents including NERC CIP V3. Using this Appendix one can identify for a given NISTIR security control the NERC CIP V3 requirement it could be used for.

8.5 Conclusion

Section 8.4 presents a way to translate a use case from EU ENISA and European Commission Smart Grid Task Force Expert Group 2 (EG2) to US NERC CIP context and vice versa.

Rather than to solely have to choose from either an EU or an US set of requirements, Smart Grid stakeholders could also use the present study, for a given use case, to identify most relevant requirements for their use case that could be picked either in EU or US cyber security context or both.

Additionally as the portability reference map is compatible with SGAM and as standards are mapped to the SGAM, Smart Grid stakeholders will also be able to identify which standards could be used to support their efforts.

9 Closing Remarks

Smart Grids are depending on a variety of technologies used with a high degree on heterogeneity and complexity. At the same pace as technologies evolve the security and standards used in Smart Grid develop. The application of these standards in deployments offers appropriate means to protect against risk identified. This report is striving into this direction by applying cyber security standards on the example of specific use cases in order to give guidance for security implementation. Smart Grid stakeholders can use proposed guidance on applied use cases, decentralized energy resources and substation automation, or apply the methodology to their related use cases.

However, it must be noted, that cyber security is a continuous process, as both, cyber security measures and threats are constantly evolving.

Annex A– References

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

[1] M/490 EN - Smart Grid Mandate - Standardization Mandate to European Standardization

[2] SG-CG/M490/K_ SGAM usage and examples, SGAM User Manual - Applying, testing & refining the Smart Grid Architecture Model (SGAM) Version 3.0 ftp://ftp.cencenelec.eu/EN/EuropeanStandardization/HotTopics/SmartGrids/SGCG_Methodology_SGAMUserManual.pdf

[3] SG-CG/M490/H_ Smart Grid Information Security (Phase 1) ftp://ftp.cen.eu/EN/EuropeanStandardization/HotTopics/SmartGrids/Security.pdf

[4] SG-CG/M490/H_Smart Grid Information Security (Phase 2) ftp://ftp.cencenelec.eu/EN/EuropeanStandardization/HotTopics/SmartGrids/SGCG_SGIS_Report.pdf

[5] SGAM-Toolbox, www.en-trust.at/SGAM-Toolbox

[6] Christian Neureiter, Introduction to the “SGAM Toolbox”, Version 0.4, 2014-04-27, http://www.en-trust.at/wp-content/uploads/Introduction-to-SGAM-Toolbox1.pdf

[7] IEC 62559-2, Use case methodology - Part 2: Definition of the templates for use cases, actor list and requirements list

[8] NERC CIP, http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx

[9] NISTIR 7628, Guidelines for Smart Grid Cyber Security http://csrc.nist.gov/publications/PubsNISTIRs.html

[10] ISO/IEC 27001: Information technology — Security techniques — Information security management systems — Requirements

[11] ISO/IEC 27002: Information technology — Security techniques — Code of practice for information security management

[12] ISO/IEC TR 27019: Information technology — Security techniques — Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry

[13] IEC 62443-2-4: Security for industrial automation and control systems - Network and system security - Part 2-4: Requirements for Industrial Automation Control Systems (IACS) solution suppliers

[14] IEC 62443-3-3: Security for industrial automation and control systems, Part 3-3: System security requirements and security levels

[15] IEC 62443-4-2: Security for industrial automation and control systems, Part 4-2: Technical Security Requirements for IACS Components

[16] IEEE 1686: Substation Intelligent Electronic Devices (IED) Cyber Security Capabilities

[17] IEEE C37.240: Cyber Security Requirements for Substation Automation, Protection and Control Systems

[18] ISO /IEC 15118 Road vehicles – Vehicle-to-Grid Communication Interface, Part 8: Technical protocol description and Open Systems Interconnections (OSI) layer requirements

[19] IEC 61850-8-2 Communication networks and systems for power utility automation - Part 8-2: Specific communication service mapping (SCSM) - Mapping to Extensible Messaging Presence Protocol (XMPP)

[20] IEC 62351-x Power systems management and associated information exchange – Data and communication security

[21] IEC 62734 Wireless communication network and communication profiles - ISA 100.11a

[22] IEC TR 62351-10 Power systems management and associated information exchange – Data and communication security – Part 10: Security architecture guidelines, IEC, 2012

[23] IEC TR 62351-8 Power systems management and associated information exchange – Data and communication security – Part 8: Role-Based Access Control, IEC, 2011

[24] IEC TR 62351-12 Power systems management and associated information exchange – Data and communication security – Part 12: Resilience and security recommendations for power systems with distributed energy resources (DER) cyber-physical systems

[25] IETF draft-ietf-tls-tls13: The Transport Layer Security (TLS) Protocol Version 1.3

[26] NIST SP 800-30 rev.1: Guidance for conducting risk assessments of federal information systems and organizations, amplifying the guidance in Special Publication 800-39, http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf

[27] SoES European Project, Deliverable D2 “International Standards and Policies – Map and Analysis”, www.soes-project.eu

[28] G. Dondossola, R. Terruggia, “Security of communications in voltage control for grids connecting Distributed Energy Resources: impact analysis and anomalous behaviours”, Cigrè Journal Science and Engineering Innovation In the Power Systems Industry Vol. 2, June 2015

[29] Christian Neureiter, Dominik Engel and Mathias Uslar , “Domain Specific and Model Based Systems Engineering in the Smart Grid as Prerequesite for Security by Design”, MDPI, Electronics 2016, 5(2), 24; doi:10.3390/electronics5020024

[30] Christian Neureiter, Mathias Uslar, Dominik Engel, and Goran Lastro, “A Standards-based Approach for Domain Specific Modelling of Smart Grid System Architectures”, IEEE Conference on System of Systems Engineering 2016, Kongsberg, Norway, 2016

[31] C. Dänekas, C. Neureiter, S. Rohjans, M. Uslar, and D. Engel, “Towards a Model-Driven-Architecture Process for Smart Grid Projects,” in Digital Enterprise Design & Management, P. Benghozi, D. Krob, A. Lonjon, and H. Panetto, Eds., Springer International Publishing, 2014, vol. 261, pp. 47-58

[32] C. Neureiter, G. Eibl, D. Engel, S. Schlegel, and M. Uslar, “A concept for engineering smart grid security requirements based on SGAM models,” Computer Science – Research and Development, pp. 1-7, 2014

[33] DISCERN European Project, Deliverable (D) No: 3.5 “IT security concept”, 2014 www.discern.eu

Annex B – Risk analysis based on NISTIR 7628 and SGAM models

We assume a very simple scenario for this example in the context of this report. It is fully in line with the ones previously produced in the SGCG-RAWG reports [31]. Within Section B1, we describe a quick mapping coming from IEC 62559 [7], a mapping of the NISTIR systems onto the SGAM from [32] and deriving a short table of requirements [33]. Section B.1 supports an extensive example in order to show the individual steps done for single interfaces, taking into account only a very simple scenario. Section B.2 of this report is in line with the methods proposed in Section 7.2 of this report and motivates the use of the Section 7.2 approach in the context of the SGAM toolbox, thus, implementing the methods and processes described within this report into a tool chain based on model-driven engineering [32].

B.1 Quick mapping of NIST and SGAM without tool support

Within a so called virtual power plant (VPP), different, mostly small distributed energy resources (DER) are combined to achieve a critical mass of generating capacity and, thus, to act as if they were a bigger single unit.

Trading of energy at markets or providing various ancillary services is one focus of this virtual power plant (e.g. frequency control, voltage control, grid recovery or contingency planning). Based on their the individual generation forecasts of the units, virtual power plant (VPP) operators contract with market participants and create schedules to operate their individual units for a so-called combined power grid product. To realize such a plan at operational level, generation and load has to be adapted to the needs of the market bid.

Typically, this is done by direct control of the individual plants (control unit for DER) or by providing incentives to the owners to behave appropriately. In Figure 30, the communication and data exchange of the actors in this use case is displayed in a so-called UML sequence diagram that is explained in the following paragraphs.

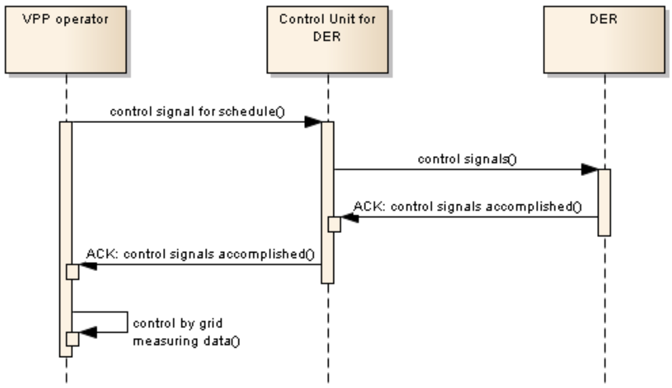


Figure 30: Example use case sequence diagram

Applying the NISTIR methodology [9], the following steps have to be taken to assess security requirements from NISTIR 7628 to this use case.

<u>Identifying and (formally) specifying the use case in PAS 62559 templates</u>

We start using the IEC PAS 62559 template [7] as recommended by SGCG Sustainable Processes group and specify the use case of the former paragraph. Because of the limitation of pages in this paper report, the definition of the use case is here reduced to the identified actors and sequence diagram.

The identified actors are: DER, VPP operator and Control Unit for DER. The sequence diagram of Figure 30 is useful to get an overview about the communication between the actors and to identify interfaces.

<u>Identification and mapping of LI, communication links and interface categories</u>

The identified actors and communication links have to be mapped on the NISTIR 7628 descriptions. Figure 31 shows the scenario as a so-called high-level diagram from NISTIR 7628. The DER is a Customer DER (CDER). It is controlled via the Customer EMS and the VPP Operator gets involved in the control process via the LMS/DRMS system. The communication links, U106 and U45 from the NISTIR 7628 annex, and their corresponding interface categories, e.g.10 and 15, are identified using the generic blueprint from the authors.

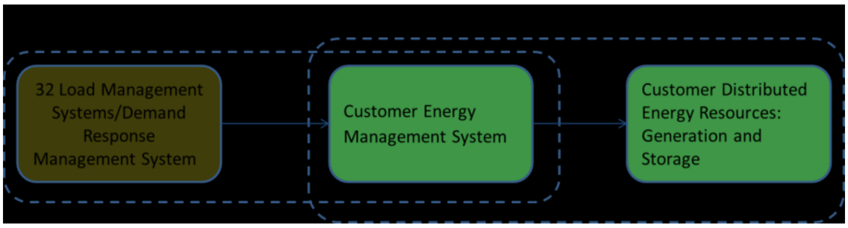


Figure 31: Interface categories and systems

The colours, used in Figure 31, reflect the domains of the LI diagrams. The system with number 32 LMS/DRMS (= yellow, domain operations) sends two different signals to the system number 5 Customer EMS (CEMS) (green = domain customer). After an appropriate ramp-up time the two signals, of tariffs and schedules, are submitted.

If the time to fulfil the schedule is reached, real-time measurements are used to check the fulfilment. If the schedule is not satisfied, direct control, using a control signal for the Customer DER, is initialized. Once the signals are sent to the CEMS, the CEMS decides how to react, based on pre-defined and engineered rule sets, and sends control signals to the CDER. After accomplishing the tasks, first, the CDER acknowledges to the CEMS and the CEMS acknowledges to the LMS/DRMS, as can be seen in Figure 30.

Integration of the LI onto the SGAM Functional Layer

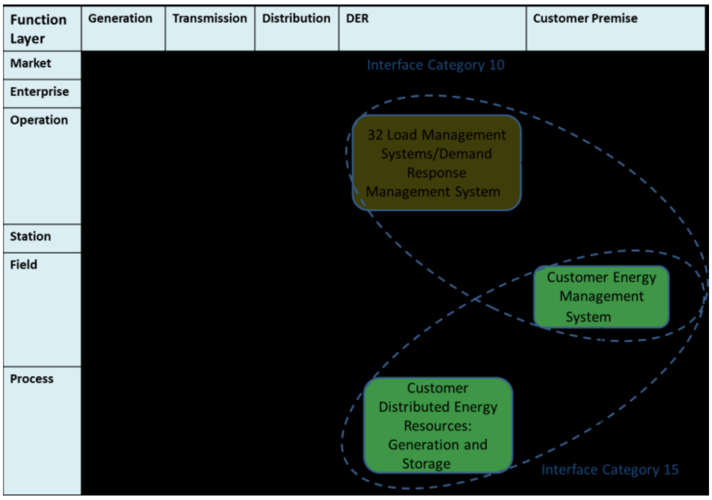


Figure 32: Mapped actors and interfaces

Within this step of the methodology [29], the mapping onto the SGAM layers is conducted. For this example, it is done in the Function Layer. Figure 32 provides an overview of the mapped actors as well as the corresponding communication links. Utilizing this kind of graphical representation makes it easier to check which domains are covered by which actors as well as to recognize the hierarchical zone they reside in.

Using the SG-CySecReq annex from NISTIR 7628

In the NISTIR 7628 the interfaces are categorized and for the different categories protection goals, like CIA analyses and high-level security requirements, are determined. Based on the previous identified interfaces and categories, Table 7 shows the corresponding SG-CySecReq and the resulting sum of these to obtain requirements for the communication from the LMS/DRMS to the CDER. In addition, security requirements from other standards can be used from the annex lookup tables of the NISTIR 7628 report [9].

Logical Interface Category:	**10**	**15**	**Result:**
Confidentiality:	Low	Low	**Low**
Integrity:	High	Medium	**High**
Availability:	Medium	Medium	**Medium**
Smart Grid Cyber Security Requirements:	AC-14 (Permitted Actions without Identification or Authentication)	AC-14	**AC-14**
	IA-04 (User Identification and Authentication)	IA-04	**IA-04**
	SC-05 (Denial-of-Service Protection)	SC-05	**SC-05**
	SC-06 (Resource Priority)	SC-06	**SC-06**
	SC-07 (Boundary Protection)	SC-07	**SC-07**
	SC-08 (Communication Integrity)	SC-08	**SC-08**
	SC-26 (Confidentiality of Information at Rest)	SC-26	**SC-26**
	SI-07 (Software and Information Integrity)	SI-07	**SI-07**
		SC-03 (Security Function Isolation)	**SC-03**
		SC-09 (Communication Confidentiality)	**SC-09**

Table 7: CIA and SG-CySecReq analysis for the DER SGAM example

In this step, the identified SG-CySecReq and their actors and communication links are mapped onto the individual further SGAM planes. Figure 33 shows where the high-level requirements are placed on the Business Layer.

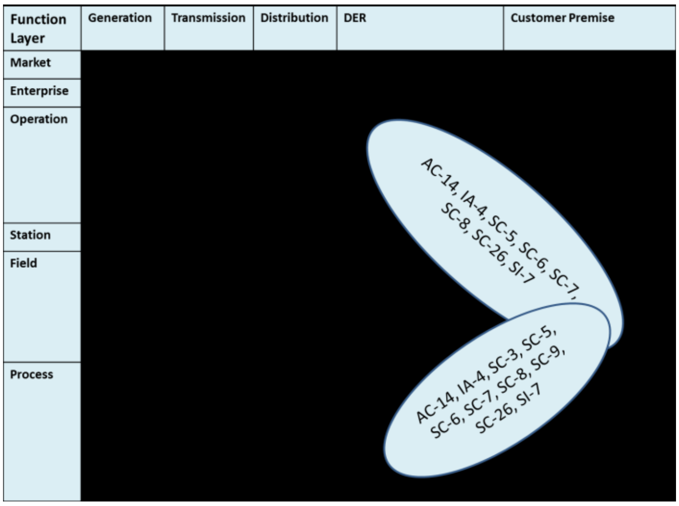


Figure 33: NISTIR 7628 requirements

Figure 34 shows the corresponding SG-CySecReq, from the SG-CySecReq classes. Additional aspects can be identified and assessed to the responsible architects for the individual layer, this is shown in the section B.2 for all the layers using the SGAM Toolbox as tool support.

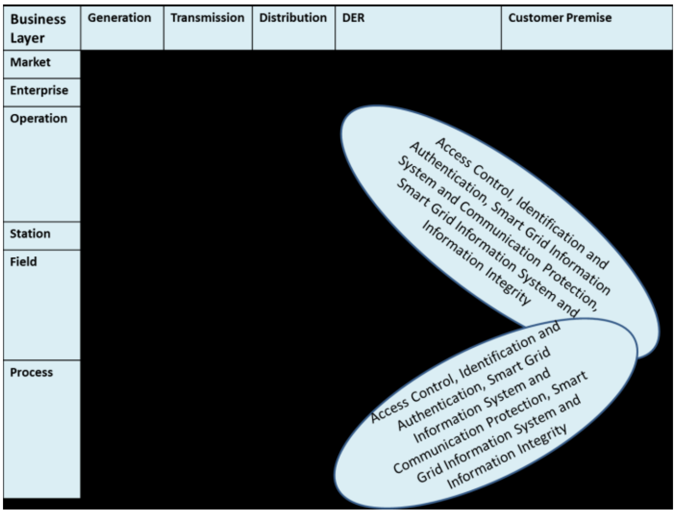


Figure 34: high-level security requirements

B.2 Security Analysis in the SGAM Toolbox

As outlined in Section 7, the ICT Analysis aims at identifying and describing

- ICT architecture
- Logical Interfaces
- Communication Protocols.

To provide a structured approach, the concepts of the SGAM are suitable for analysis and documentation. For modelling SGAM aligned Smart Grid architectures appropriate tools such as the publicly available and free-to-use SGAM-Toolbox[1] are available.

In the following it is described, how security analysis can be addressed during the step-by-step development of smart grid architectures. Contrasting to the originally proposed Use Case Mapping Process (UCMP) from [2] the suggested process is focusing on architecture development and, thus, realizes a more top-down approach.

Basically, the suggested process is separated into three parts. First, the Business Analysis delivers the SGAM Business Layer. It states the basis for identification of particular High Level Use Cases (HLUC) and furthermore is suitable for an initial risk assessment. Next, the Functional Analyses aims decomposing the HLUC into more granular Primary Use Cases (PUC). The detailed description of individual PUC delivers involved Logical Actors (LA) and Information Objects (IO) to be exchanged. These IO are an important asset for the subsequent risk analysis. The combination of all PUCs together with the involved Las delivers the SGAM Function Layer for one particular HLUC. Finally, the logical architecture is mapped onto a technical solution. Thus, all involved physical components together with their logical interfaces and the concerning communication protocols are identified. The resulting ICT architecture is depicted as SGAM Information, Communication and Component Layer.

B.2.1 Business Analysis

The *Business Analysis* focuses on strategic considerations on the motivation for realizing a particular system. Thus, individual *Business Actors*, their related *Business Goals* and appropriate *Business Cases* are modelled. The particular Business Cases identified aim at balancing the needs between different involved parties. At this stage first analysis can take place on basis of “What happens, if the realization of the Business Case fails?” considerations. Thus, appropriate quality requirements including security can be specified and attached to the BC. Moreover, on basis of the particular BC specific HLUC as technical realization of a BC can be defined.

[1] www.en-trust.at/SGAM-Toolbox

These HLUC can be described by means of IEC 62559 Use Case template [7] and state the basis of the subsequent functional analysis. Figure 35 depicts the concept of a resulting SGAM Business Layer.

The BC "Active Grid Operation" involves the three parties DSO, DER and Customer with each having his own Business Goals. The BC itself can be analysed and described in a more detailed manner, for example by means of *Business Process Modelling Notation (BPMN)* and other appropriate methods. Also, particular requirements introduced for example by regulation entities can be considered at this point.

On basis of these considerations an initial set of quality requirements (Non-functional Requirements) can be associated with the BC. This concept is illustrated simply by one "NF RQ: Security" requirement which rather serves as the root for numerous requirements than an individual one.

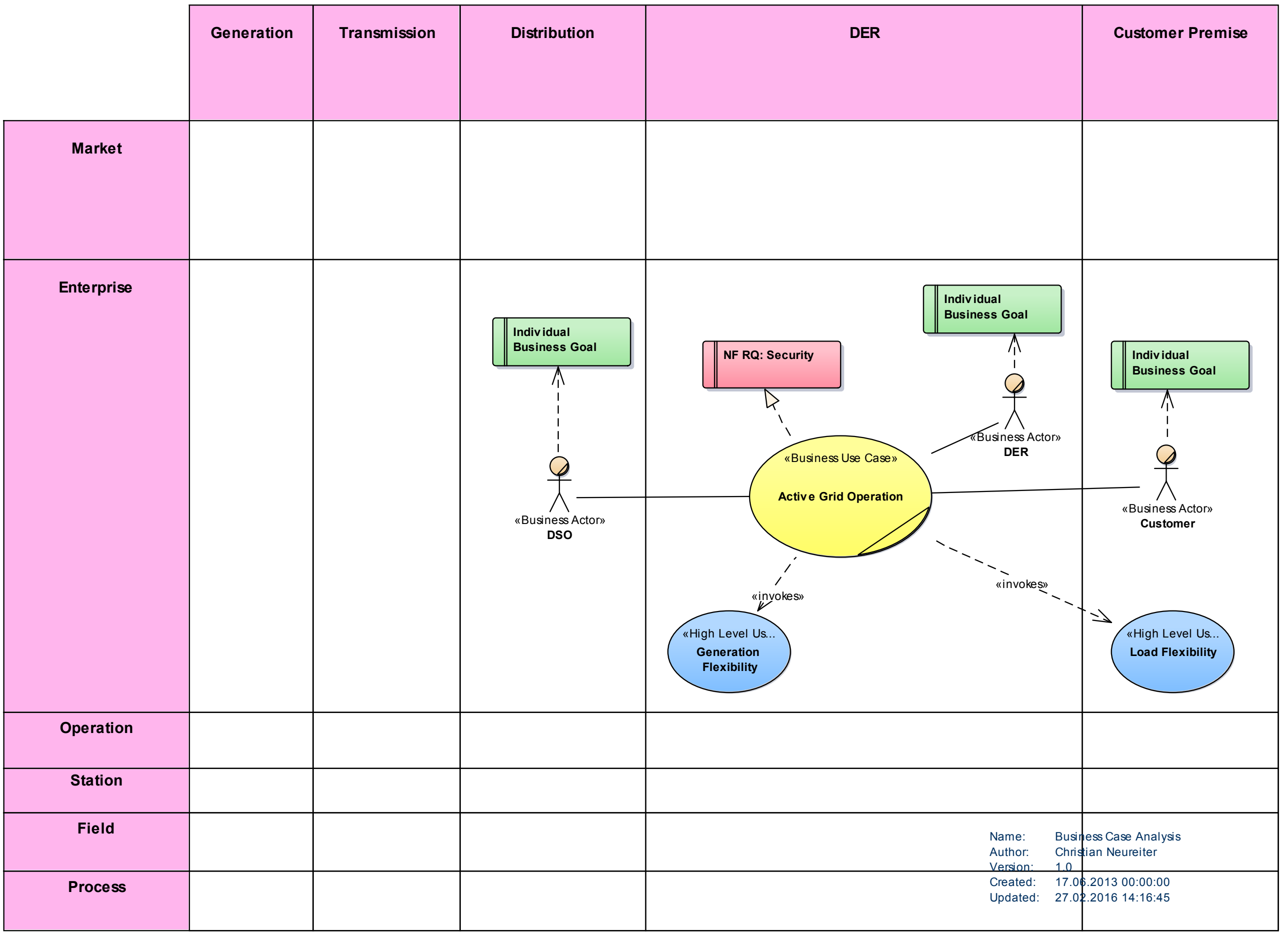


Figure 35: SGAM Business Layer

B.2.2 Functional Analysis

Having the HLUCs identified during the business analysis, the can be decomposed and described in more detail. Typically the HLUCs will be interrelated with different other HLUCs which can be described by classical UML modelling. Next, each of the individual HLUCs can be decomposed into more granular PUCs. Both, the interrelation of two HLUCs as well as the decomposition of one of them is depicted in Figure 36 which is based on the example from [2]. The cooperation of the individual PUCs for realizing the HLUC is denoted as UML Activity diagram on the right side of the image. Hereby the HLUC is represented as UML Activity comprising several UML Actions referring to the corresponding PUCs. In the example diagram the individual PUCs are executed sequentially, however, utilization of UML Activity Diagrams allows for any more detailed description with conditional flows or simultaneous paths as well.

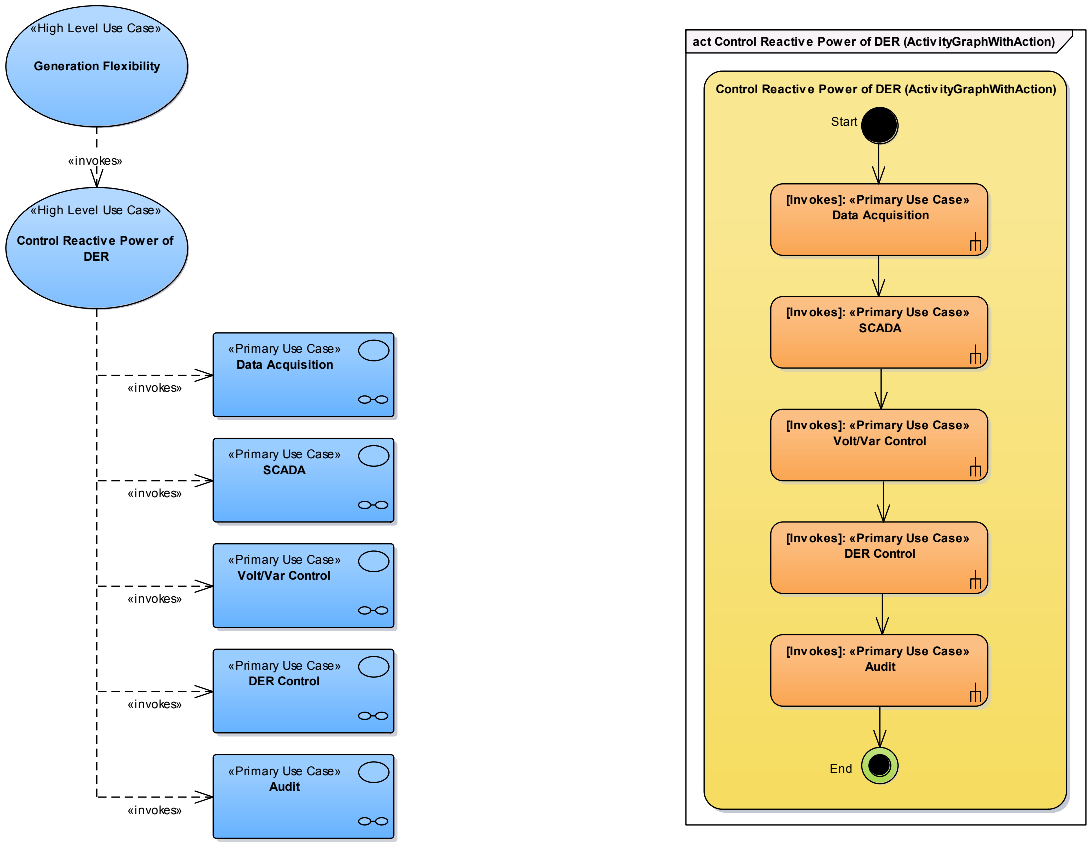


Figure 36: Decomposition of a single HLUC

Subsequent to the decomposition of the HLUCs, which yields the corresponding PUCs they can be described in more detail. The goal of this step is to identify involved *Logical Actors* (LA) on the one hand and *Information Objects* (IO) transmitted on the other hand. As the IOs represent an important assent in terms of security, a clear specification can be done in this step. The typical workflow goes as follows. First, on basis of a textual description of a PUC both, a UML Activity and a UML Sequence diagram can be generated. This is a feature most UML tools are able to do out of the box, which provides certain efficiency. Next, the Activity Diagram can be used for manually identify and describe the particular IOs.

In the final step, these IOs can be attached to the relations within the Sequence Diagram. Again, by having the analysis done basis of a model, the result is a complete representation of all information exchanges between the concerning actors. Also, as the information exchanged are model objects a consistency can be maintained. Figure 37 exemplary depicts the detailed description of the PUC “DER Control”.

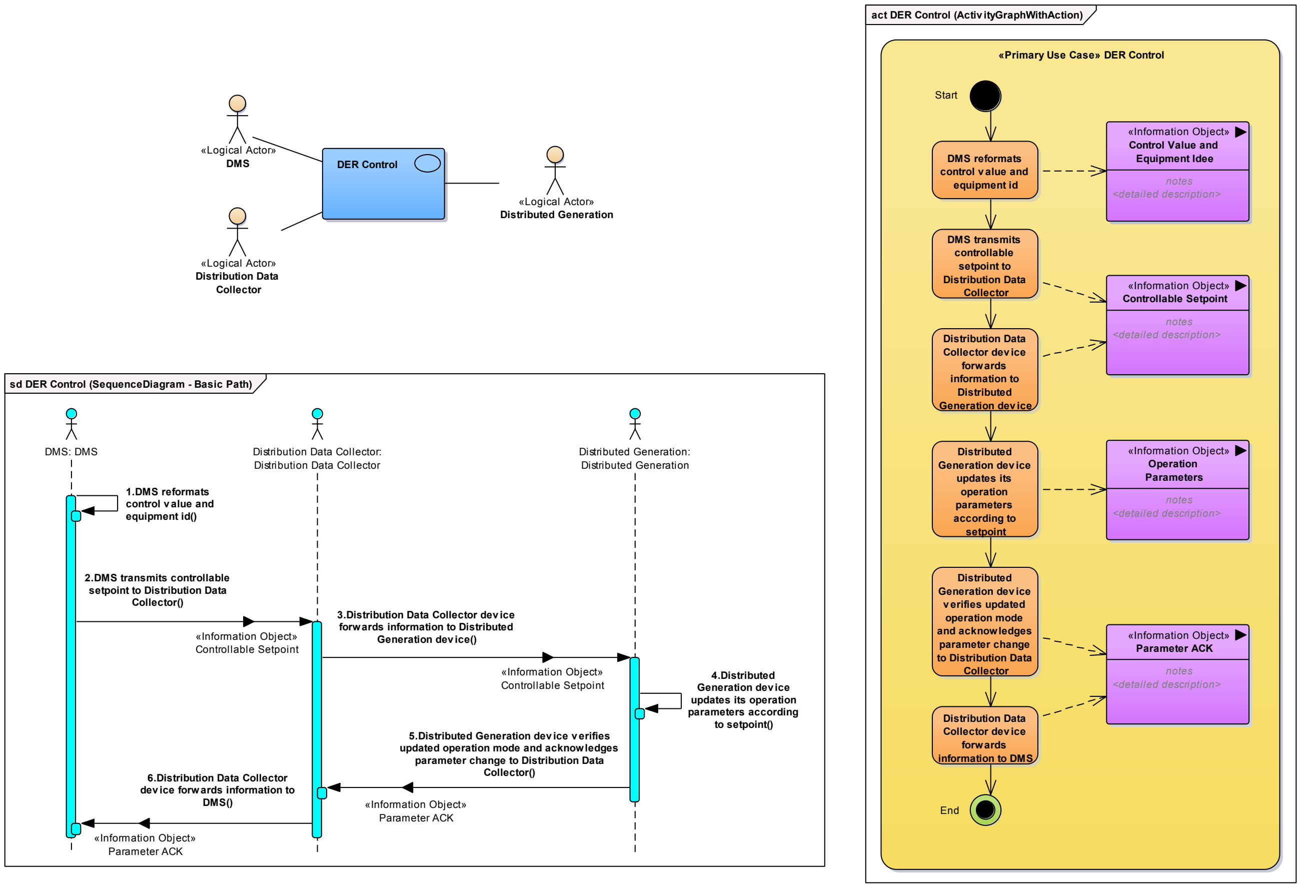


Figure 37: Process for HLUC

Doing a description as described for every single PUC from a HLUC yields the complete SGAM Function Layer for the HLUC as depict in Figure 38 for the HLUC “Control Reactive Power of DER”.

After this step, all Logical Actors involved are identified and associated with the concerning Primary Use Cases. Moreover, the detailed description of each PUC covers the Information Objects – as important asset in terms of privacy and security - exchanged. Again, it is deemed crucial to conduct the described analysis on basis of a model rather than individual drawings. Besides maintaining the consistency, the utilization of models emphasizes a complete picture as for example, after the step-by-step analysis of all PUC, for every actor all used information items can be assessed.

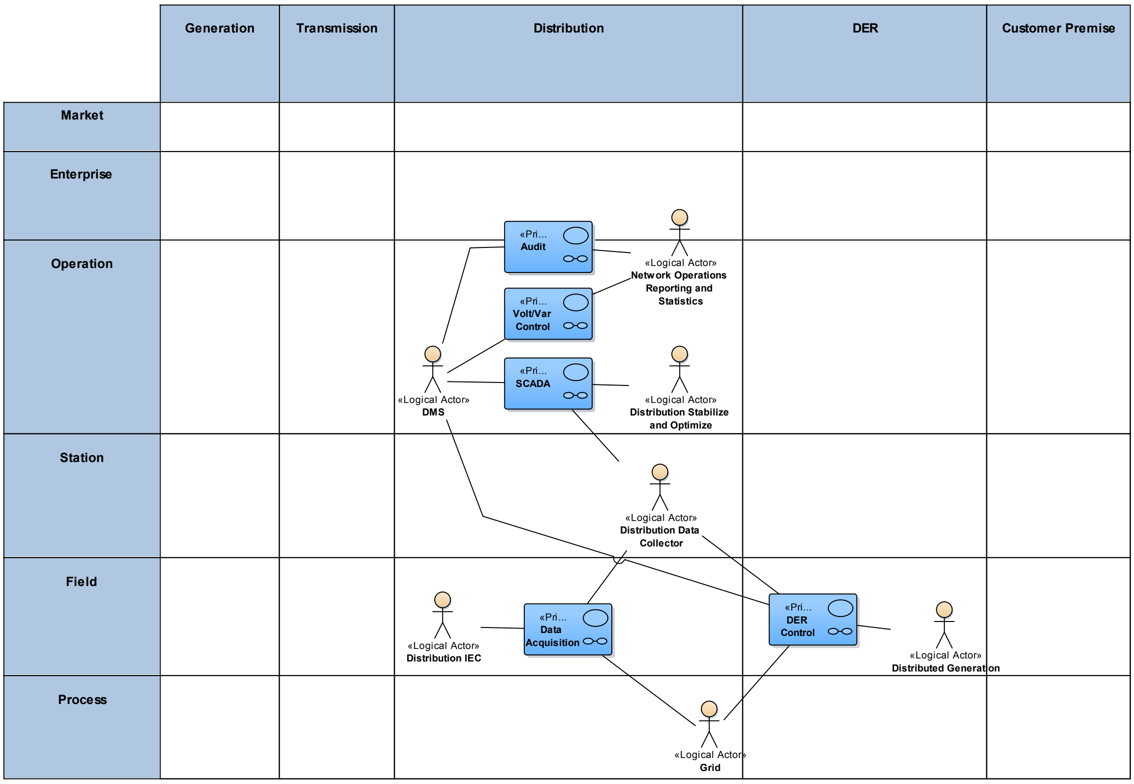


Figure 38: SGAM Function Layer for one HLUC

B.2.3 Architecture Development

The Architecture Development task aims at mapping the preliminary developed logical model onto a technical solution. This is an important step as the mapping not necessary is a 1:1 mapping. For instance, one logical actor can comprise several physical components or, in contrast, different logical actors can be realized by one particular component.

However, the goal of this mapping is to identify all of the used components. This enables one to build up the ICT architecture with all of the integrated interfaces. As all of the involved interfaces potentially can be subject of attack, a complete picture here is necessary.

After the mapping from LAs onto physical components, the knowledge from the detailed description of the PUCs can be utilized to develop the *Business Context View* of the SGAM Information Layer. The transmitted *Information Objects* hereby are instances of the elements earlier described. Figure 39 depicts the Business Context View for the example taken from [2].

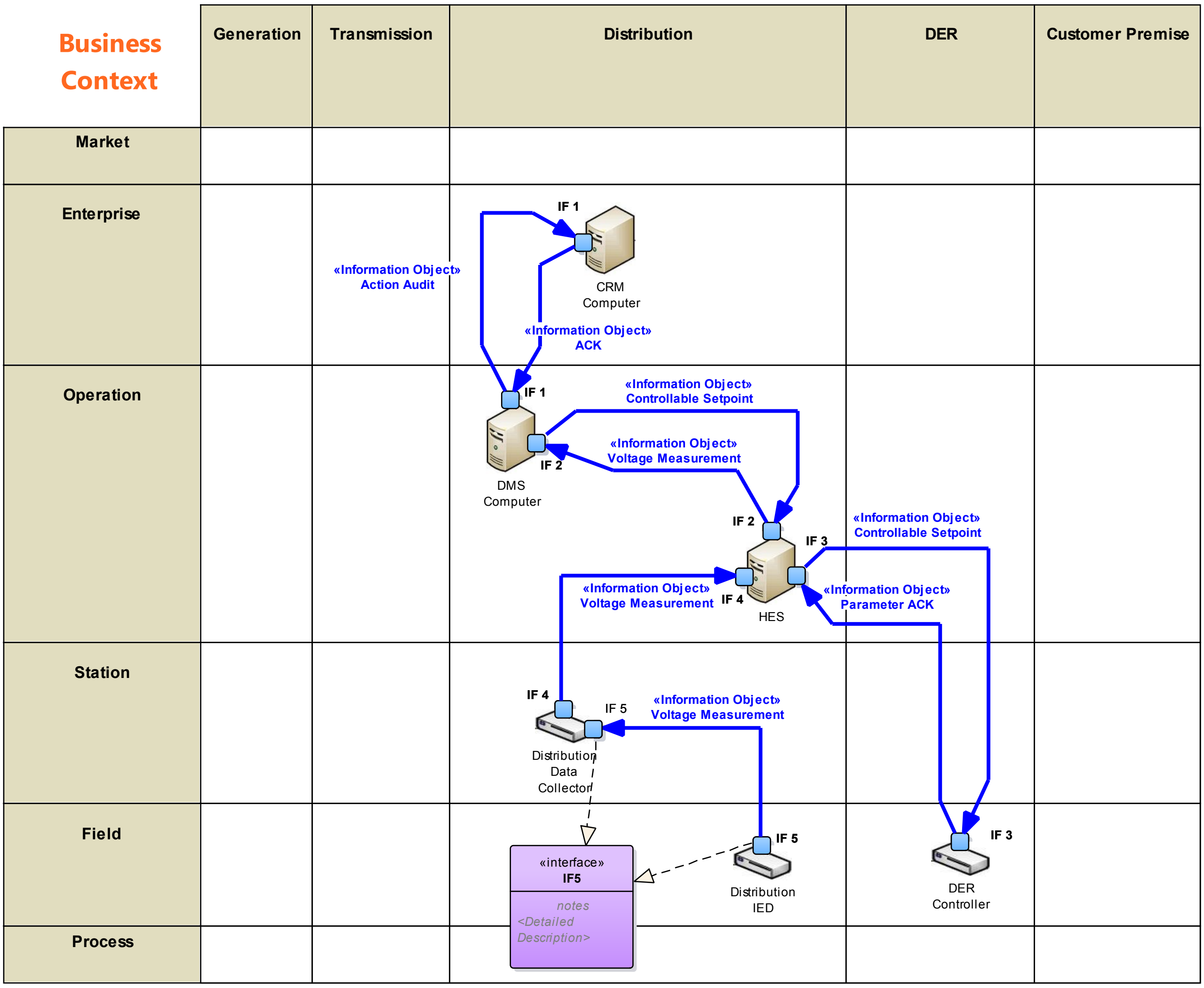


Figure 39: Business Context View (SGAM Information layer)

The *Information Object Flow* relations depicted in this image use particular interfaces of the individual components. These interfaces are described as *Ports* that are realizations of interfaces provided with a more detailed description. For IF 5 this instantiation is depicted within the graphic, even though no detailed description of this interface is provided. However, at this point one could benefit by reusing components and interfaces out of Reference Architecture Models such as the *NIST Logical Reference Model* (NIST LRM) as proposed in [9]. The interfaces used within the NIST LRM are assigned to specific Interface Categories, which have been subject to detailed security considerations. These considerations yield specific Security Requirements for every interface category. Thus, by reusing the well-defined actors from NIST LRM, together with the appropriate interfaces it is possible to obtain an initial set of Security Requirements. A model of the NIST LRM is already available and can be used for selection and instantiation of particular components, their interfaces and the corresponding security requirements[2].

The second view of the SGAM Information Layer, the *Canonical Data Model* delivers the possibility to assign an appropriate data model standard as depicted in Figure 40. Having the components positioned within the SGAM plane allows for selecting appropriate standards for example on basis of the online available IEC Smart Grid Standardsmap[3].

[2] www.en-trust.at/NISTIR

[3] smargridstandardsmap.com

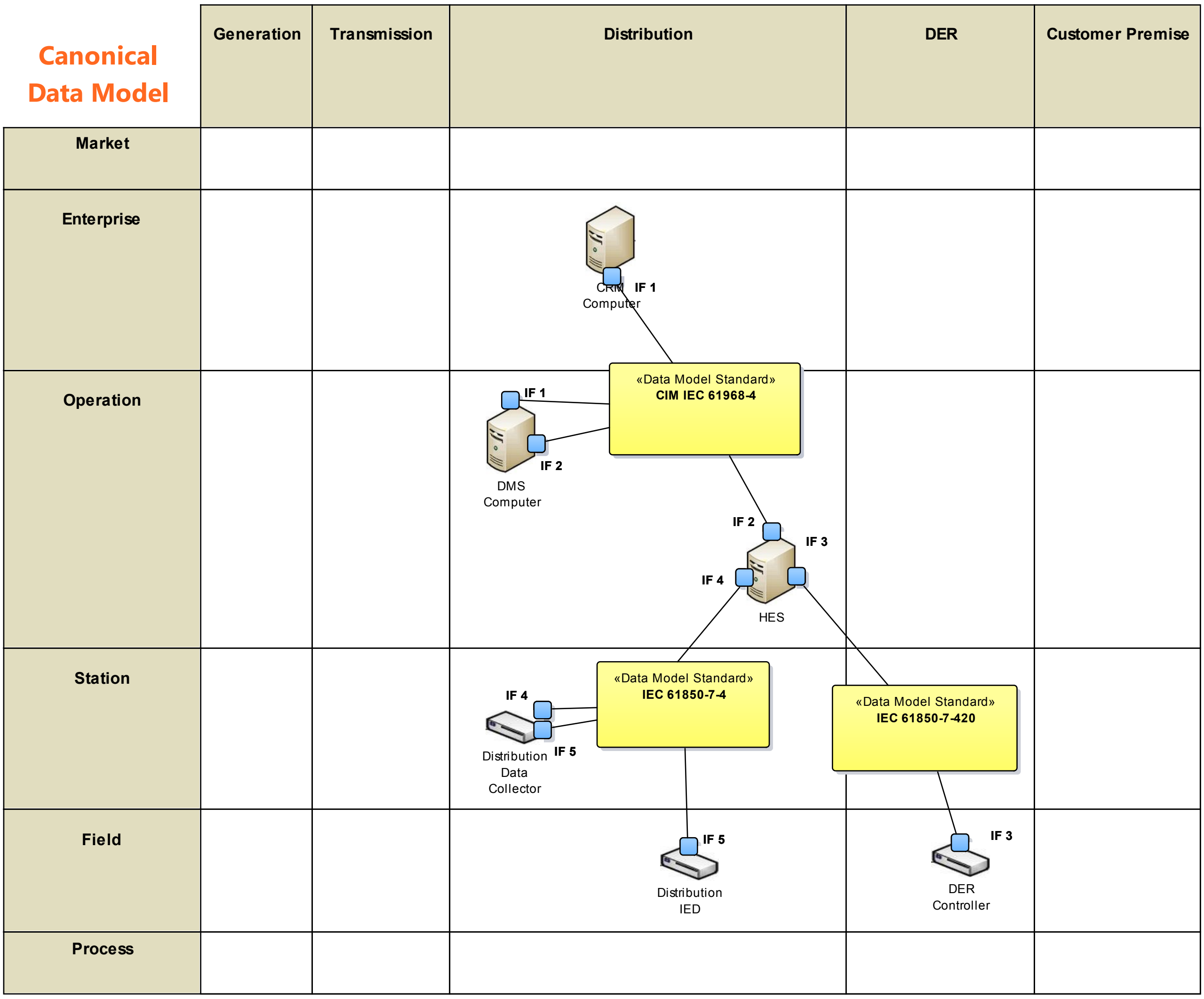


Figure 40: Canonical Data Model

Subsequent after analysing the Information Object Flows that yield the necessary interfaces, the communication paths can be defined and appropriate communication protocols can be chosen. Again, the ICE Smart Grid Standards map can deliver guidance for selecting appropriate communication protocol standards. The chosen standards can be depicted on height of the SGAM Communication Layer as depicted in Figure 41.

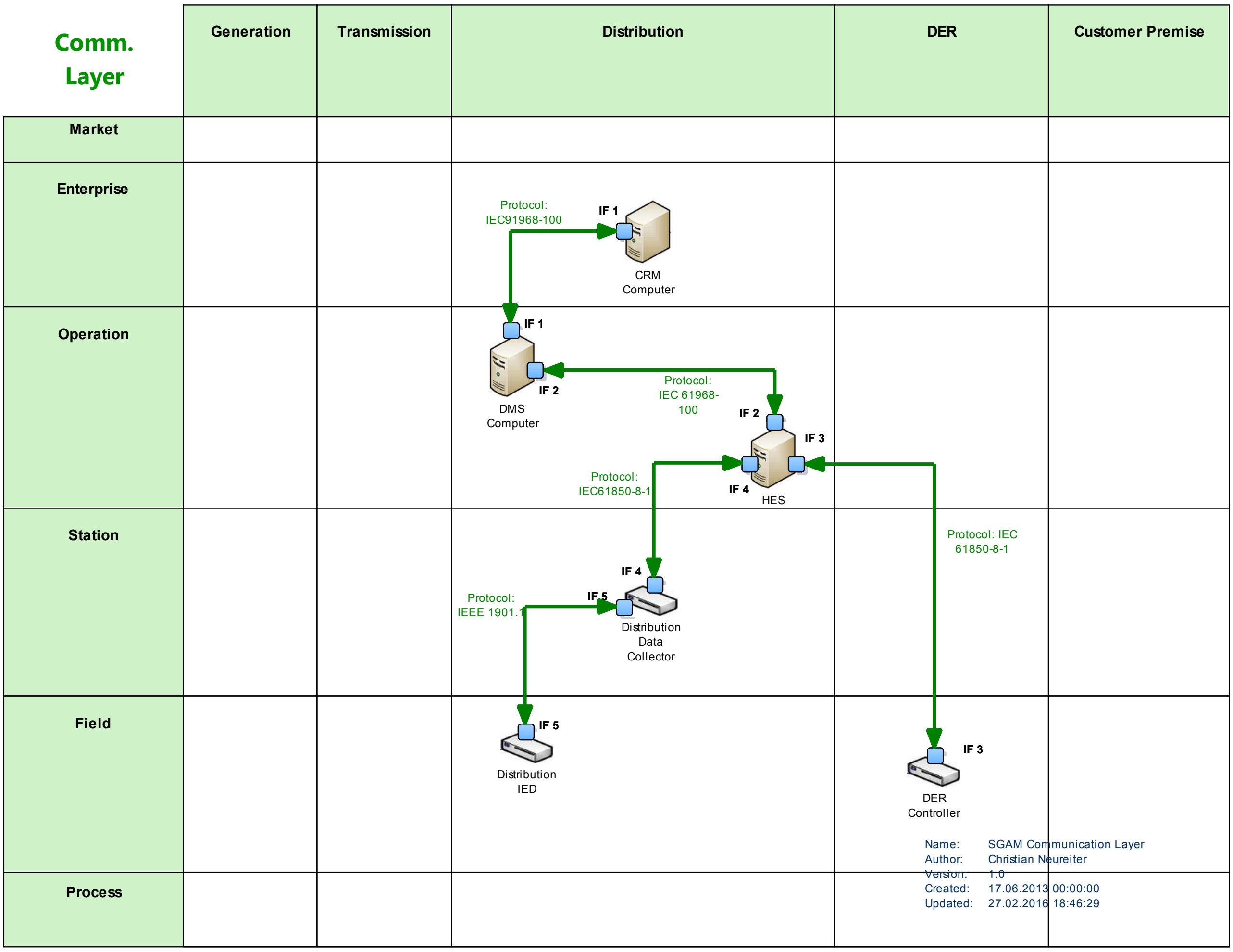


Figure 41: SGAM communication layer

Both, the SGAM Information Layer and the SGAM Communication Layer focus on a “component to component” communication with considerations on data models and communication protocols. However, the SGAM Component Layer is suited to develop the overall ICT architecture that also comprises components such as gateways or ICT networks. The integration of ICT networks also allows more detailed descriptions on the network topology with different segments or firewall rule sets later on.

Figure 42 delivers an example for the SGAM Component Layer. However, the interfaces identified and mentioned till now only comprise the directly involved components. The Security considerations and especially the later on derived requirements of course must be applied to the whole communication path together with the utilized network segments. The extension of the identified interfaces onto communication components such as gateways is not depicted in Figure 42, neither is a detailed description of the individual networks given here.

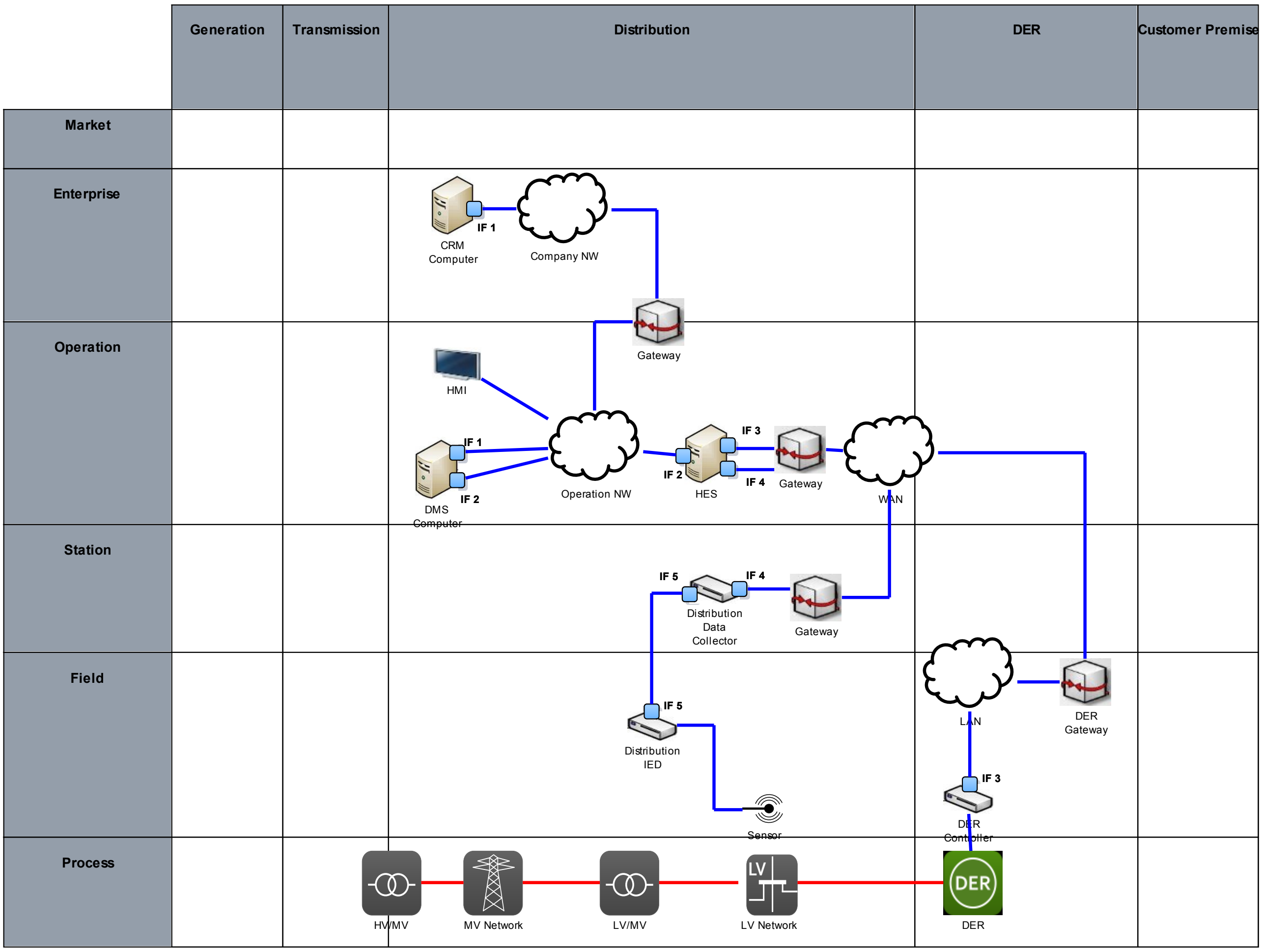


Figure 42: SGAM Component layer

The ICT Analysis Process as described here, shows how to step-by-step build up a Smart Grid system by utilizing the SGAM as architecture framework. It is explicitly explained how Use Cases can be described in detail in order to derive Information Objects as critical assets for privacy and security. Moreover, it is explained how the logical composition can be transferred into a technical architecture comprising interfaces, data model standards and communication protocols.

All of these identified elements are critical assets in terms of security and thus, state the basis for the security analysis. However, should be amended here that utilization of modelling is deemed crucial during considerations as described in order to maintain consistency. Moreover, it is suggested to rely during the development of particular architectures on well-described reference architectures such as the NIST LRM. The NIST LRM, for example, delivers best practice solutions for typical scenarios. These solutions are built upon well-described actors that also comprise exhaustive description of the interfaces used and their concerning security requirements.