CEN-CENELEC-ETSI Smart Grid Coordination Group

Date: 2014-12

Secretariat: CCMC

SG-CG/M490/H_ Smart Grid Information Security

Contents

Page

Foreword 4
1 Scope 4
2 Terms and Definitions 5
3 Symbols and Abbreviations 5
4 Executive Summary 6
5 SGIS Key Elements 7
5.1 Smart Grid Architecture Model (SGAM) 7
5.1.1 Security View per Layer 9
5.2 SGIS Security Levels (SGIS-SL) 9
5.2.1 SGIS-SL High Level Recommendations 10
5.3 Selected Use Cases 11
6 Smart Grid Set of Security Standards 11
6.1 Security Standards Supporting Smart Grid Reliable Operation 12
6.1.1 Selected Security Standards 12
6.1.2 Standards Coverage 13
6.1.3 Standards Mapping to SGAM 16
6.2 Detailed Standards Analysis 18
6.2.1 Security Requirement Standards 19
6.2.2 Security Solution Standards 24
6.3 Security Standards mapping to Use Cases 32
6.3.1 Mapping of Requirement Standards 32
6.3.2 Mapping of Solution Standards 34
6.3.3 Identified standards not covered in the use case mapping and the gap analysis 34
6.4 Identification of Additional Security Standards to be Considered 35
7 European Set of Recommendation 36
7.1 European Set of Recommendations Overview 36
7.2 European Set of Recommendations Dashboard 39
7.3 Conclusion 40
7.4 Last Words 40
8 Applied Information Security on Smart Grid Use Cases 40
8.1 Transmission Substation Use Case 40
8.1.1 SGAM Mapping 40
8.1.2 Applied Cyber Security 43
8.1.3 Standards 43
8.1.4 Conclusion 44
8.2 Distribution Control Room Use Case 44
8.2.1 SGAM Mapping 44
8.2.2 Applied Cyber Security 47
8.2.3 Standards 47
8.2.4 Conclusion 48
8.3 Consumer Demand Management Use Case 48
8.3.1 SGAM Mapping 49
8.3.2 Applied Cyber Security 51
8.3.3 Standards 52
8.3.4 Conclusion 53
8.4 Distributed Energy Resources (DER) Control Use Case 53
8.4.1 SGAM Mapping 53
8.4.2 Applied Cyber Security 56
8.4.3 Standards 58

8.4.4 Measure implementation in the DER control use case ... 60
8.4.5 Conclusion ... 61
9 Privacy Protection ... 61
9.1 Analysis of expectable Effects of the proposed EU General Data Protection Regulation ... 62
9.1.1 Comparison of Current vs. Potential New Regulatory Regime ... 63
9.1.2 Country-specific Analyses ... 66
9.1.3 Expectable Effects of the New Data Protection Regulation on Smart Grids ... 70
9.2 Impact Assessment of Use Cases in Four Member States ... 73
9.2.1 SGIS Toolbox Methodology ... 73
9.2.2 Data Protection Impact Assessment Template ... 73
9.2.3 Data Security and Data Privacy ... 74
9.2.4 Generic Data Privacy Threats ... 75
9.3 Analysis of Emerging Privacy Technologies ... 76
9.3.1 Privacy by Design ... 76
9.3.2 Privacy in a Smart Grid ... 77
9.3.3 Privacy Enhancing Technologies ... 77
9.3.4 Privacy Enhanced Technologies in Smart Metering ... 78
9.3.5 Privacy Enhanced Technologies in Electric Vehicles ... 80
10 SGIS Framework (Former SGIS Toolbox) ... 81
11 Conclusion ... 82
Annex A – Additional Information on DER control use case ... 83
Annex B – Overview on Privacy Enhanced Technologies for Smart Metering ... 84
Annex C – Overview on Document Status of Investigated Standards ... 87
Annex D – Detailed Description of the SGIS Framework Steps ... 89
Annex E – References ... 93

Foreword

This document has been prepared by CEN-CENELEC-ETSI Smart Grid Coordination Group (SG-CG) under the Mandate M/490 [1] given to CEN, CENELEC and ETSI by the European Commission and the European Free Trade Association.

As quoted from the M/490 Mandate text, *'[…] The objective of this mandate is to develop or update a set of consistent standards within a common European framework […] that will achieve interoperability and will enable or facilitate the implementation in Europe of […] Smart Grid services and functionalities […]. It will answer the technical and organizational needs for sustainable 'state of the art' Smart Grid Information Security (SGIS), Data protection and privacy (DPP), […]. This will enable smart grid services through a Smart Grid information and communication system that is inherently secure by design within the critical infrastructure of transmission and distribution networks, as well as within the connected properties (buildings, charging station – to the final nodes). […]'*

The Mandate M/490 has been issued in March 2011 to be finalized by end of 2012. In the light of the discussions hold between the Smart Grid Coordination Group (SG-CG) and EC Reference (EG1) Group in July 2012, the need to iterate the European Commission Mandate M/490 was considered by both sides and an iteration of this Mandate has been initiated. The 2nd phase of this Mandate will be finalized by end of 2014.

1 Scope

The scope of the Smart Grid Information Security (SGIS) working group under the European Commission Smart Grid Mandate M/490 [1] is to support European Smart Grid deployment.

As quoted from the M/490 Mandate text: '*[…] It will answer the technical and organizational needs for sustainable 'state of the art' Smart Grid Information Security (SGIS), Data protection and privacy (DPP), enabling the collection, utilization, processing, storage, transmission and erasure of all information to be protected for all participating actors. This will enable smart grid services through a Smart Grid information and communication system that is inherently secure by design within the critical infrastructure of transmission and distribution networks, as well as within the connected properties (buildings, charging station – to the final nodes). This should be done in a way that is compatible with all relevant legal requirements, i.e. consumer data protection and privacy rights, metrology and daily business operations, and that is ensuring that rights of all consumers, including the vulnerable ones, are protected. […]*'

Cyber security requires an overall risk management approach where threats and measures are considered from technical, process and people point of view. The content presented in this report cannot provide a complete and definitive answer to the mandate's objective. The target of the work of the Smart Grid Information Security (SGIS) working group is to provide a high level guidance on how standards can be used to develop Smart Grid information security. In this light it presents concepts and tools to help stakeholders to integrate information security into daily business.

Privacy is a major concern of European Commission and member states as it addresses the need to protect consumers e.g. for the misuse of remote functionality or private data. This report will look into current data protection regulation in order to set the base line for further work on this topic.

It should be noted, that this report covers 'cyber security' and 'information security'[1]. However, in recent times, cyber security has been used dominantly by stakeholders.

[1] Cyber security by the nature of the term as well as common use relates to a property of cybernetic systems, often referred to as cyber-physical systems. The relevant distinction is that in information security the object of concern is the information, while in cyber security the object of concern are cyber-physical systems.

Securing the Smart Grid is a continuous effort. Elements presented here are purposed to help finding the first and right steps of a Smart Grid information security journey to an end to end security.

2 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 (SGIS)
As quoted from M/490 mandate, Smart Grid Information Security refers to*:'[…] technical and organizational needs for sustainable 'state of the art' Smart Grid Information Security (SGIS), Data protection and privacy (DPP), enabling the collection, utilization, processing, storage, transmission and erasure of all information to be protected for all participating actors.*'

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 analyse 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.

3 Symbols and Abbreviations

- **CIA** Confidentiality, Integrity, Availability
- **DPC** Data Privacy Class
- **DSO** Distribution System Operator
- **EST** Enrolment over Secure Transport

- **EU** European Union
- **FDIS** Final Draft International Standard
- **GDOI** Group Domain of Interpretation
- **GOOSE** Generic Object Oriented Substation Event
- **IED** Intelligent Electronic Device
- **IS** International Standard
- **ISMS** Information Security Management System
- **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

4 Executive Summary

The objective of this report is to support Smart Grid deployment in Europe providing Smart Grid Information Security guidance and standards to Smart Grid stakeholders.

One common base line for the results presented in this report are the SGIS key elements, namely the Smart Grid Architecture Model (SGAM), the SGIS Security Levels (SGIS-SL) and selected use cases.

Available security standards are increasingly applied to address functional, organizational or procedural requirements. Selecting the right 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 Grid. Beside a standardization landscape on security requirements, an analysis on selected standards presents gaps to be addressed. Additionally, a mapping of selected security standards to SGAM, showing their applicability in the different Smart Grid zones and domains on different layers, will help system designers and integrators in selecting the proper security standards to protect the Smart Grid system appropriately. Furthermore, selected use cases are used to investigate the standards more deeply regarding their application within the Smart Grid based on SGAM.

In order to support Smart Grid deployment with security by design, a set of recommendations has been derived closely linked to ENISA's set of recommendations. These recommendations are linked to the SGIS security levels and to the SGAM and guidance on recommendations is provided based on the respective security levels. Two additional domains have been found worth to be added during the analysis work: Situational Awareness and Liability. In this context, please keep in mind that security is an ongoing effort as a system cannot be secured by applying security measures once in a time only.

A SGIS Framework is proposed as a new methodology for a risk assessment which strongly links to ENISA's threat landscape (see ENISA/EG2: "Proposal for a list of security measures for smart grids" report [8]) in order to derive measures linked to threats in a pragmatic way.

Data Privacy and Data protection, particular in the context of smart metering, is crucial for a sustainable business. The forthcoming EU General Data Protection Regulation has been analysed to understand the potential impact on organizational and functional requirements and its relationship with the current sector-specific regime in four member states examined.

The Smart Grid Task Force Expert Group 2 (SGTF EG2) has developed a Data Protection Impact Assessment (DPIA) template. The main elements of the DPIA template specifically relevant to privacy for the individual have been considered and recommendations developed on how to improve the data protection aspect of the personal information in the SGIS Framework. It is suggested that data protection impact assessment is considered separately in the pre-assessment of the SGIS Framework, since an identical approach to security cannot be applied for data privacy. Additionally, an analysis on emerging Privacy Enhanced Technologies to support privacy by design is presented.

In conclusion, standards needed to establish the base of a Smart Grid Information Security are available, but it needs continuous effort to incorporate existing and new technologies, architectures, use cases, policies, best practice or other forms of security diligence.

5 SGIS Key Elements

5.1 Smart Grid Architecture Model (SGAM)

Information presented in this chapter is an extract from the Smart Grid Reference Architecture working group report from the 1st phase of Mandate M/490 [3]. The SGAM consists of five consistent layers representing business objectives and processes, functions, information models, communication protocols and components. These five layers represent an abstract version of the interoperability categories introduced in the Reference Architecture working group report. Each layer covers the smart grid plane, which is spanned by smart grid domains and zones. The intention of this model is to allow the presentation of the current state of implementations in the electrical grid, but furthermore to present the evolution to future smart grid scenarios by supporting the principles universality, localization, consistency, flexibility and interoperability

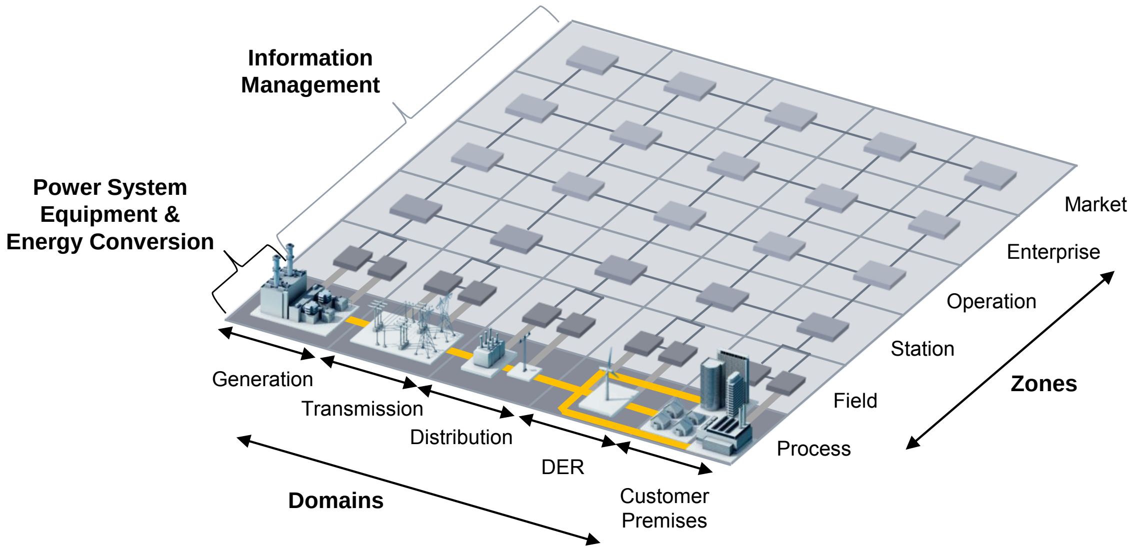


Figure 1: Smart Grid Plane

The Smart Grid Plane covers the complete electrical energy conversion chain.

Domains	Description
Bulk Generation	Representing generation of electrical energy in bulk quantities, such as by fossil, nuclear and hydro power plants, off-shore wind farms, large scale photovoltaic (PV) power– typically connected to the transmission system
Transmission	Representing the infrastructure and organization which transports electricity over long distances
Distribution	Representing the infrastructure and organization which distributes electricity to customers
DER	Representing distributed electrical resources, directly connected to the public distribution grid, applying small-scale power generation technologies (typically in the range of 3 kW to 10.000 kW). These distributed electrical resources can be directly controlled by DSO
Customer Premises	Hosting both - end users of electricity, also producers of electricity. The premises include industrial, commercial and home facilities (e.g. chemical plants, airports, harbors, shopping centers, homes). Also generation in form of e.g. photovoltaic generation, electric vehicles storage, batteries, micro turbines… are hosted

Zones	Description
Process	Including both - primary equipment of the power system (e.g. generators, transformers, circuit breakers, overhead lines, cables, electrical loads …) - as well as physical energy conversion (electricity, solar, heat, water, wind …).
Field	Including equipment to protect, control and monitor the process of the power system, e.g. protection relays, bay controller, any kind of intelligent electronic devices which acquire and use process data from the power system.
Station	Representing the aggregation level for fields, e.g. for data concentration, substation automation…
Operation	Hosting power system control operation in the respective domain, e.g. distribution management systems (DMS), energy management systems (EMS) in generation and transmission systems, microgrid management systems, virtual power plant management systems (aggregating several DER), electric vehicle (EV) fleet charging management systems.
Enterprise	Includes commercial and organizational processes, services and infrastructures for enterprises (utilities, service providers, energy traders …), e.g. asset management, staff training, customer relation management, billing and procurement.
Market	Reflecting the market operations possible along the energy conversion chain, e.g. energy trading, mass market, retail market...

SGAM Layers Overview:

Layers	Description
Business	Represents business cases which describe and justify a perceived business need
Function	Represents use cases including logical functions or services independent from physical implementations
Information	Represents information objects or data models required to fulfill functions and to be exchanged by communication
Communication	Represents protocols and mechanisms for the exchange of information between components
Component	Represents physical components which host functions, information and communication means

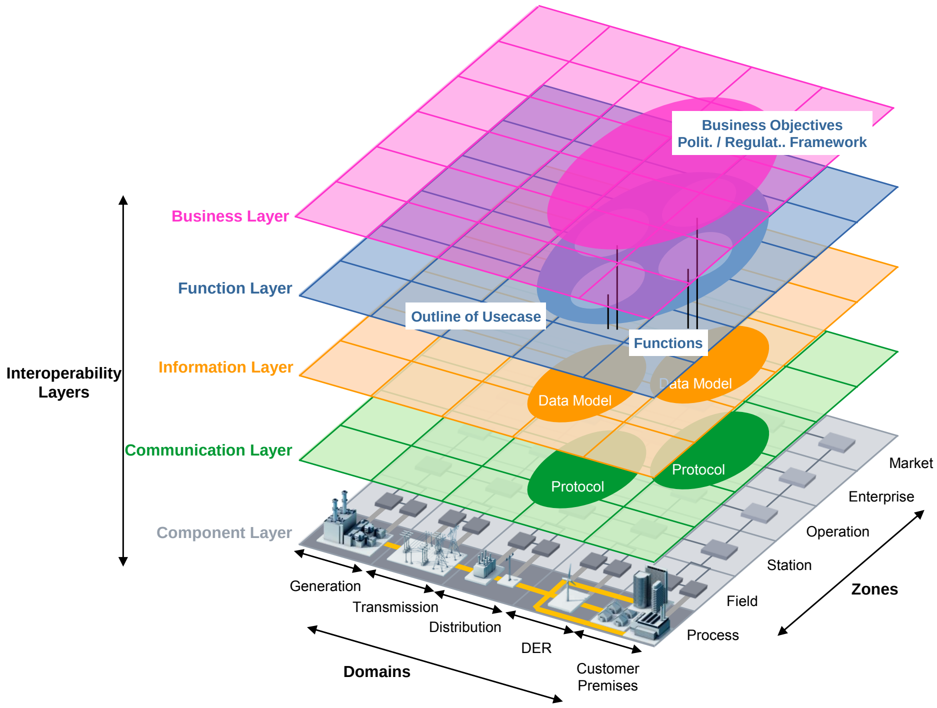


Figure 2: SGAM Layers

5.1.1 Security View per Layer

In order to efficiently build Smart Grids inherently secure by design, security should be involved at all levels of the Smart Grid in order to secure Smart Grid operations and related IT operations. Translating this fact into the SGAM means that information security should be considered in all domains, zones, and layers.

In order to incorporate this into the model without denaturing or over sizing it, additional layers have been proposed in the 1st phase of Mandate M/490 with the Reference Architecture working group. One additional layer could be slipped under each SGAM layer. This is called the **Security View per Layer**.

The Smart Grid is a system of systems connected and interacting with each other. As exposed previously, their security requirements will vary depending on the SGAM Domain/Zone the systems are located. The Security View per Layer is a conceptual representation used to illustrate this.

5.2 SGIS Security Levels (SGIS-SL)

SGIS - Security Levels (SGIS-SL) have been defined in the 1st phase of Mandate M/490 with the objective to create a bridge between electrical grid operations and information security in order to increase the Grid resiliency [6]. Additionally, European Commission M/490 mandate and Smart Grid stakeholders have required some guidance on Smart Grid information security.

Installed capacity at the European level is more than 800 GW. At country level, the country size and electrical network architecture will obviously have an impact on the amount of power managed. For latest detailed information on installed capacity you can refer to the ENTSO-E web site (www.entsoe.eu). Additionally European Electrical Grid stakeholders have estimated that a loss of power of 10 GW or more could lead to a pan European incident, depending on which area of the European electrical grid is impacted.

European Electrical Grid stability has been chosen as reference to define SGIS Security Level (SGIS-SL) and create a bridge between electrical operations and information security. Thus focus is made on power loss caused by ICT systems failures.

Security Level	Security Level Name	Europeans Grid Stability Scenario Security Level Examples
5	Highly Critical	Assets whose disruption could lead to a power loss above 10 GW Pan European Incident
4	Critical	Assets whose disruption could lead to a power loss from above 1 GW to 10 GW European / Country Incident
3	High	Assets whose disruption could lead to a power loss from above 100 MW to 1 GW Country / Regional Incident
2	Medium	Assets whose disruption could lead to a power loss from 1 MW to 100 MW Regional / Town Incident
1	Low	Assets whose disruption could lead to a power loss under 1 MW Town / Neighborhood Incident

Figure 3: SGIS-SL description

Example definitions of SGIS Security Levels are given considering the European Electrical Grid has a whole system. The different elements of this system have different level of criticality evaluated thru the prism of their disruption and associated potential power loss and systemic impact. Thus SGIS Security Levels here reflect assets criticality from a European Electrical Grid stability point of view and their associated different security needs.

5.2.1 SGIS-SL High Level Recommendations

The European Commission M/490 mandate and Smart Grid stakeholders have required some guidance on Smart Grid information security. Therefore, SGIS-SL guidance is estimated for each SGAM Domain/Zone cell given the kind of equipment used there to manage power and its maximum potential power loss associated in a global Pan-European Electrical Grid stability scenario for a given location using values defined above in section 5.2, Figure 3.

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 4: High level security view per layer and recommendations

** Please note values proposed are guidance examples only*

Values proposed in Figure 4 are a first input for each cell and are to be seen as rough high level estimations of potential power loss due to SGIS incidents. They are proposed to help people identifying most critical areas where security matters most from a Pan-European Electrical Grid stability point of view. They will have to be validated through more formal exercise as detailed later.

Even if guidance is provided, Smart Grid stakeholders are recommended to perform the exercise by themselves. Smart Grid stakeholders are encouraged to perform a complete risk assessment to identify their risks. Their risk assessment results can be compared to the proposed values to support the risk assessment exercise.

5.3 Selected Use Cases

SGIS is working on standards, European set of recommendations, SGIS Framework and Privacy topics. As one of the common base line following use cases are selected:

- Transmission Substation
- Distribution Control Room
- Consumer Demand Management – Direct load/generation management
- Distributed Energy Resources (DER) Control

These use cases have been chosen to provide an overview on how to deal with Smart Grid Information Security issues in various Smart Grid areas. They are not exhaustive. They have been chosen as valuable illustrative examples.

A detailed outline with SGAM and analysis by applying information security on these use cases will be presented in chapter 8.

6 Smart Grid Set of Security Standards

Smart Grid Set of Security Standards investigates into selected standards and their suitability in selected use cases and follows the identified gaps regarding their resolution in the associated standardization committees.

In the 1st phase of the Mandate M/490, SGIS already investigated into selected security standards applicable to securing the Smart Grid core during its first working period. The result is available within the reports of the working group ‘First Set of Standards’ (cf. [5]) as well as the working group ‘Smart Grid Information Security’ (cf. [6]). The focus was set on ISO/IEC 27001, ISO/IEC 27002, IEC 62351, NERC CIP (US Standard), NIST IR-7628 (US Guidelines). From the list of these standards, only IEC 62351 is followed further in this second working period. From the ISO/IEC 27000 series, the focus is set additionally on the ISO/IEC TR 27019 as an energy automation domain specific standard extending ISO/IEC 27002.

The second working period of the SGIS further investigates into selected security standards applicable in smart grid that also relate to adjacent domains like industrial automation. Additionally, security standards from ISO, IEC and IETF targeting the implementation of security measures are taken into account. The selected standards are divided into requirements and solution standards and are listed in section 6.1.1. These standards will be investigated in general regarding their application area, status, and maturity in a similar manner as has been done in the 1st phase of the Mandate M/490.

Note that, as in phase 1 of the SGIS work, the selected set of standards provides a subset of security standards applicable in Smart Grid, which have been acknowledged as important for the considered use cases.

The process of the gap analysis of the standards as listed above will proceed in basically three steps

1. Further investigation into selected standards from phase 1 (IEC 62351, ISO/IEC TR 27019)
2. Applicability analysis for the remaining set of security standards
3. Identification of further security standards to be investigated

A clear mapping of selected security standards to SGAM, showing their applicability in the different Smart Grid zones and domains on different layers will support system designers and integrators in selecting the proper security standards to protect their Smart Grid system appropriately. In addition, it is intended to support the definition of audit processes of smart grid environments by providing a clear view of applicable and relevant standards in SGAM areas.

Selected use cases will be used to investigate the standards more deeply regarding their application within the Smart Grid based on SGAM. For identified gaps, recommendations will be provided to standardization as far as possible.

6.1 Security Standards Supporting Smart Grid Reliable Operation

This section provides an introduction into the set of security standards that have been selected for investigation based on their relation to the Smart Grid during the preparation of SGIS phase 2. The selection of security standards was partly based on dedicated standards, which had been identified already in SGIS phase 1 for further investigation. Reports from the European Task Force on Smart Grid privacy and security and Joint Working Group have also been used as inputs for this study. Moreover, the set of use cases also influenced the standard selection. Note that the security standard have also been selected with the goal to support reliable Smart 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.

Note that the same restriction as in SGIS phase 1 applies regarding the coverage of security standards. As stated above, the standards addressed have been selected based on the phase 1 analysis and also based on the use cases. It has been acknowledged that the list of standards may not be complete and that there are certainly more standards contributing to smart grid security, which also needs to be investigated. Due to the limited time of this activity, only the standards in the sections below have been analyzed. Nevertheless, further standards have been identified during the analysis of the use cases and are listed for further investigation in section 6.3.3 (derived from the use cases) and section 6.4 (suggested by experts). Besides the investigation into the standards coverage, also the mapping of the set of security standards to SGAM is addressed, showing their applicability in the different Smart Grid zones and domains on a general level.

While this section provides the overview information, section 6.3 addresses a use case specific analysis about the applicability of the selected security standards. This will be used to identify gaps in the standards with relation to the use cases on one hand and also to identify deviations regarding the SGAM mapping.

In conjunction with the European set of security requirements, also provided by the SG-CG, the selected security standards shall help to address these requirements.

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.

Requirement standards considered (The ‘What’)

- ISO/IEC 15408 [12]: Information technology — Security techniques — Evaluation Criteria for IT security
- ISO/IEC 18045 [13] Information technology — Security techniques — Methodology for IT Security Evaluation
- ISO/IEC 19790 [14]: Information technology — Security techniques — Security requirements for cryptographic modules

- ISO/IEC TR 27019 [15]: 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 [17]: 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 [18]: Security for industrial automation and control systems, Part 3-3: System security requirements and security levels
- IEC 62443-4-2 [19]: Security for industrial automation and control systems, Part 4-2: Technical Security Requirements for IACS Components
- *IEC 62443-2-1 [16]: Security for industrial automation and control systems - Network and system security - Part 2-1: Industrial automation and control system security management system*
- IEEE 1686 [20]: Substation Intelligent Electronic Devices (IED) Cyber Security Capabilities
- IEEE C37.240 [21]: Cyber Security Requirements for Substation Automation, Protection and Control Systems

Solution standards considered (The ‘How’)

- ISO /IEC 15118-2 Road vehicles – Vehicle-to-Grid Communication Interface, Part 2 [22]: Technical protocol description and Open Systems Interconnections (OSI) layer requirements
- IEC 62351-x Power systems management and associated information exchange – Data and communication security [23]
- IEC 62056-5-3 DLMS/COSEM Security [24]
- IETF RFC 6960 Online Certificate Status Protocol [25]
- IETF RFC 7252: CoAP Constrained Application Protocol [26]
- IETF draft-weis-gdoi-iec62351-9: IEC 62351 Security Protocol support for the Group Domain of Interpretation (GDOI) [27]
- IETF RFC 7030: Enrollment over Secure Transport [28]

6.1.2 Standards Coverage

The stated list of standards covers requirements and solution standards that provide different level of detail. These standards are analyzed regarding their coverage following the approach from SGIS phase one as depicted in the Figure 5 below.

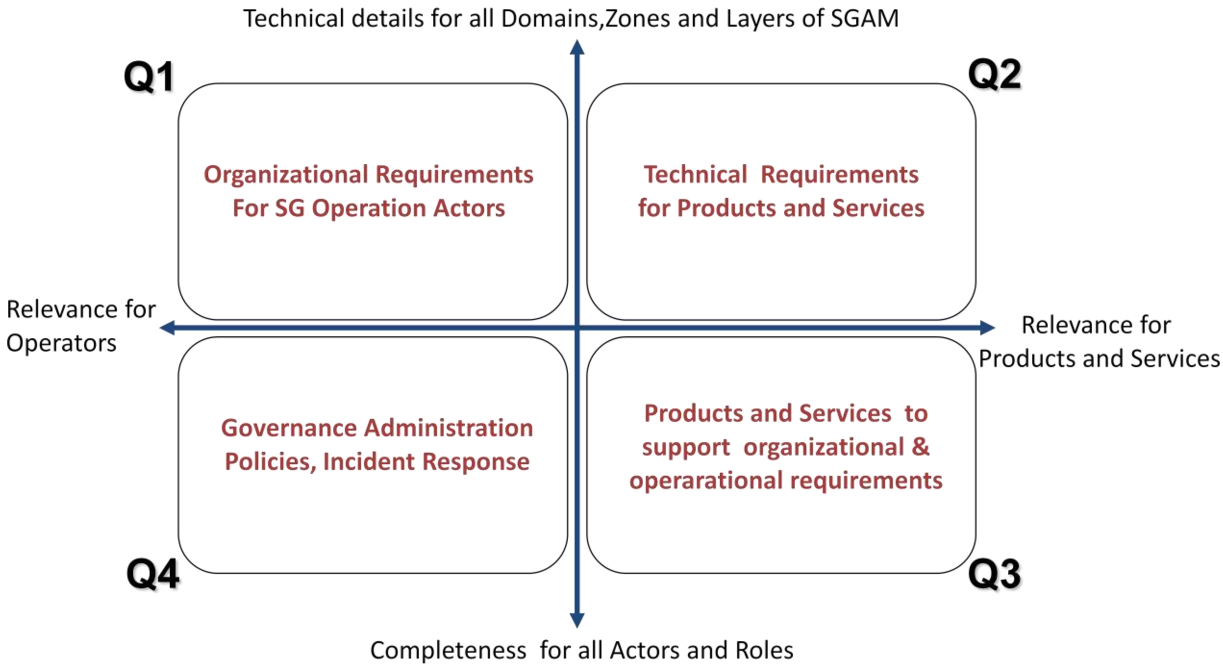


Figure 5: Security standard areas

While mapping a standard to the diagram in Figure 5, 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 6 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 color code in the Figure 6 shows the origin domain of the considered standards. What can be clearly seen, based on the coloring, is that for Smart Grids standards from different domains are applicable.

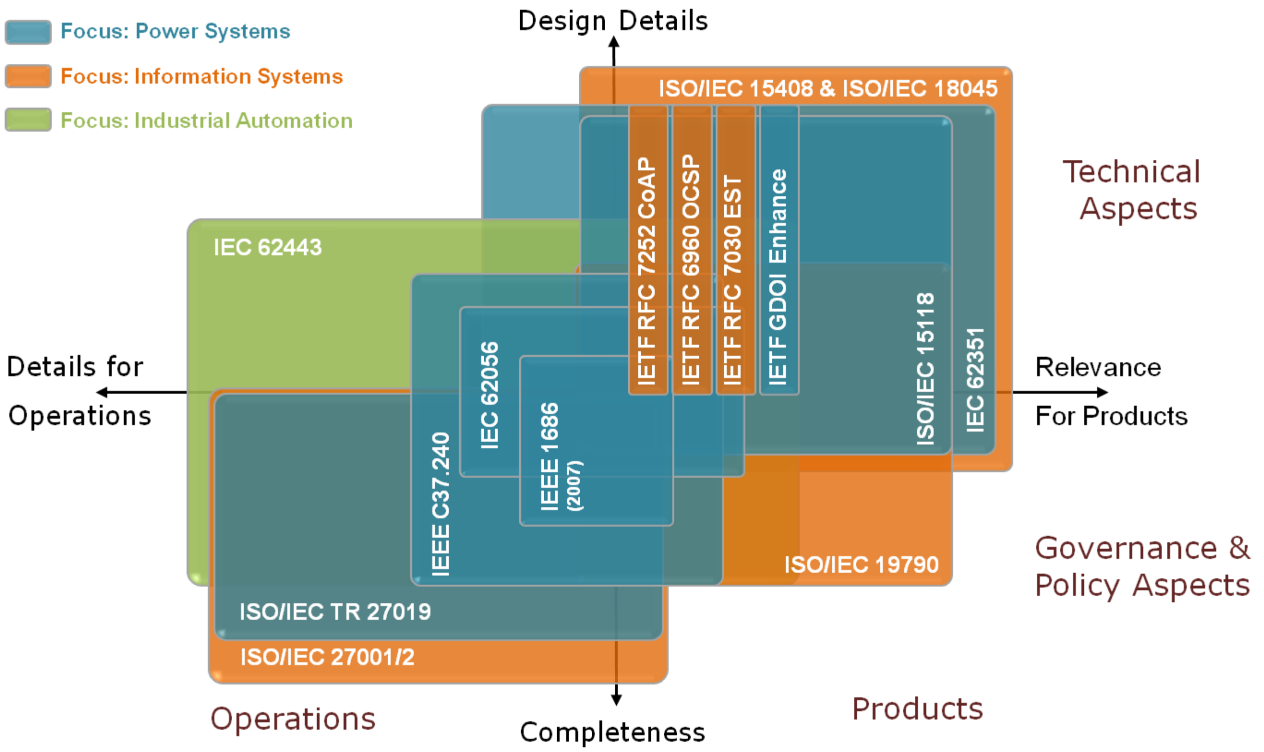


Figure 6: Security Standard Coverage

The following drawing Figure 6 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 color code from Figure 6 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 6.3.3 and section 6.4 list further standards identified, which are not considered in Figure 6 and Figure 7.

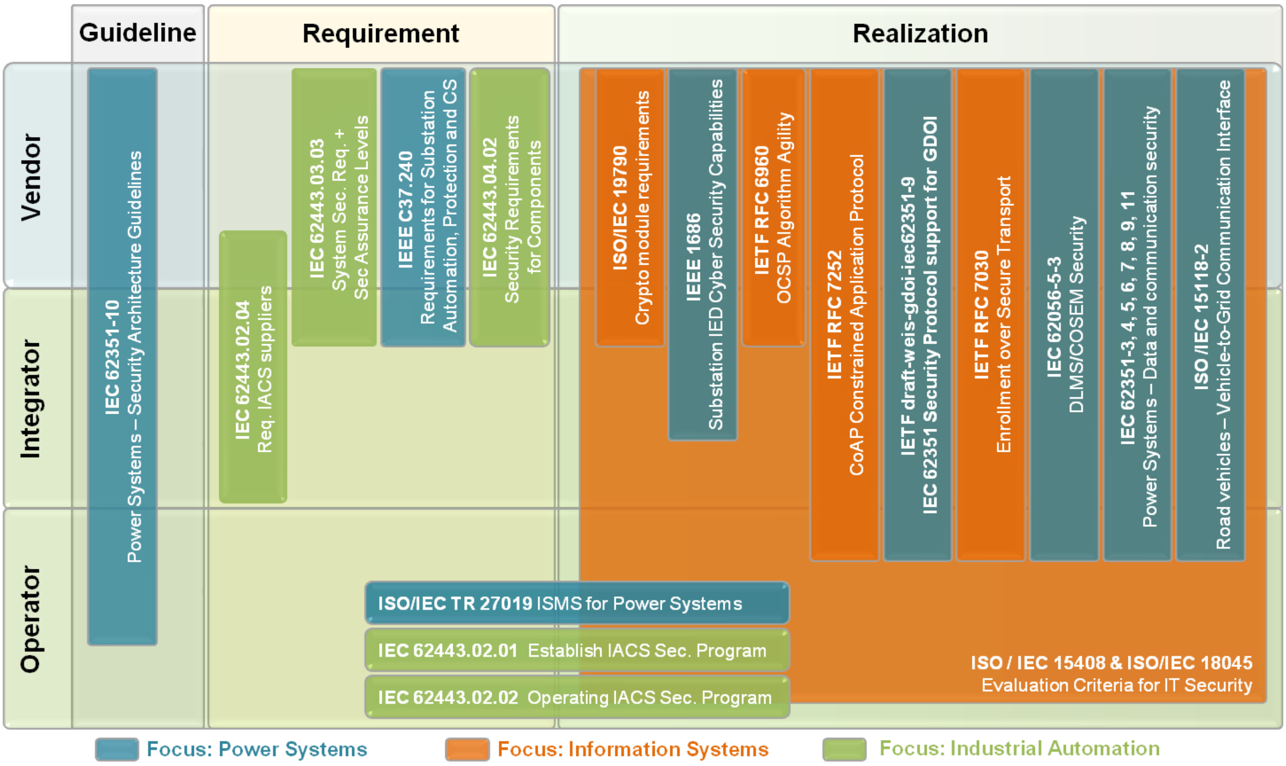
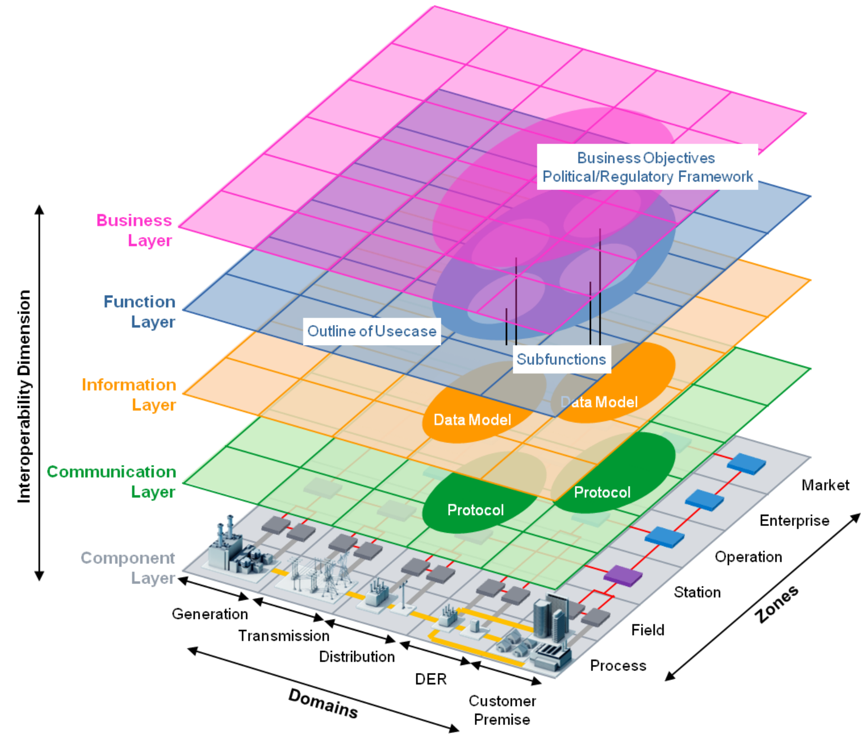


Figure 7: Security standard applicability

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 8 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 8: 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 analyze 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 15408 – 1	N.A.	N.A.	N.A.
ISO/IEC 15408 – 2	F, I, C, Phy	G, T, D, DER, CP	P, F, S, O
ISO/IEC 15408 – 3	F, I, C, Phy	G, T, D, DER, CP	F, S, O
ISO/IEC 18045	N.A	N.A	N.A
ISO/IEC 19790	Phy, C	G, T, D, DER, CP	P, F, S
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	SGAM		
	Layer	Domains	Zones
ISO/IEC 15118-2 (FDIS)	F, I, C	T, D, DER, CP	M, E, O S, F, P
IEC 62056-5-3 (IS)	F, I, C	T, D, DER, CP	O S, F, P
IEC 62351- 3 (TS)	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 (TS)	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 (WD)	F, I, C	G, T, D, DER, CP	E, O S, F
IETF RFC 6960 OCSP	I, C	G, T, D, DER, CP	M, E, O S, F
IETF RFC 7252	I, C	G, T, D, DER, CP	M, E, O S, F, P
IETF I-D draft-weis-gdoi-iec62351-9	I, C	G, T, D, DER, CP	M, E, O S, F, P
IETF RFC 7030 EST	I, C	G, T, D, DER, CP	M, E, O S, F

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. An overview of the standardization status of all investigated documents can be found in Annex C. 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 15408 + ISO/IEC 18045: Evaluation Criteria for IT security

ISO/IEC 15408 defines common criteria to rate the correctness and effectiveness of implemented security functions, covering the whole development and production process. ISO/IEC 18045 defines the methodology for the evaluation.

The product (Target of Evaluation - TOE) comprises assets that need to be protected (secret keys, user data, user SW, etc.) against threats.

The way it is done is described using Security Functional Requirements (the What?, taken from Part 2) and Security Assurance Requirements (the How well?, taken from Part 3).

Seven assurance levels (EAL) are available (involving each time more details in the description and corresponding higher attacker potential).

ISO/IEC JTC1 SC27 has made an international version of the Common Criteria standard (Version 3.1 - Revision 3): ISO/IEC 15408 and ISO/IEC 18045.

6.2.1.1.1 Status

ISO/IEC 15408	Description	Standardization Status
Part 1	Introduction and General Model (Principles)	IS (2009)
Part 2	Security Functional Requirements	IS (2008)
Part 3	Security Assurance Requirements	IS (2008)

	Description	Standardization Status
ISO/IEC 18045	Methodology for IT security evaluation	IS (2008)

6.2.1.1.2 Identified Gaps

As the Common Criteria (CC) have been updated in March 2013 to Version 3.1 - Revision 4, ISO/IEC is considering updating ISO/IEC 15408 and ISO/IEC 18045 to take into account the modifications between CC V3.1 Revision 3 and CC V3.1 Revision 4.

Several expert groups utilizing CC, among others Global Platform, have identified that the composite certification scheme of CC does not always fit with the new domains where CC is applied; among others it is difficult to maintain composite certificates when software does not change but a change is brought to the hardware. The components used in the smart grid realm will typically involve a combination of hardware, firmware and applicative software. Composite evaluation also refers to a hierarchical evaluation, in which the underlying part has already been evaluated. There are existing examples that fit to the composite evaluation approach like the Smart Meter Protection profile of the German BSI. It may be the case that for Smart Grid devices, a new composition scheme is required as well.

To ensure a consistent level of protection, Protection Profiles will need to be developed for relevant smart grid components.

6.2.1.2 ISO/IEC 19790: Security Requirements for Cryptographic Modules

ISO/IEC 19790, developed by ISO SC 27 WG3, was first published in 2006 as an international equivalent to the U.S. FIPS 140-2 specification that coordinates the requirements used for procurement of cryptographic modules by departments and agencies of the U.S. federal government, completed with additional requirements for mitigation of attacks at the highest security level. ISO 19790 addresses a specific part of the security chain (chip procurement), which is neither directly covered by ISO/IEC 15408 and ISO/IEC 18045, nor suitable to be addressed through the common criteria process.

ISO 19790 defines 4 levels of security from 1 to 4, ranging from preventing various kind of insecurity in production-grade components to physically tamper-resistant featuring robustness against environmental attacks. The considered requirements cover the documentation and design assurance of the cryptographic module, its ports and interfaces, its state machine, authentication and key management aspects, physical security features, its operational environment, EMI/EMC aspects, self-tests and mitigation of attacks.

6.2.1.2.1 Status

The September 2012 revision of the standard initially aimed to align with the FIPS 140-3 revision which was so delayed that the ISO/IEC effort took precedence and started to develop independently. Note however that currently FIPS 140-2 still tends to be used as the de facto standard.

6.2.1.2.2 Identified Gaps

SC27 WG3 is currently working on the following standards that relate to ISO 19790:

Number	Name	Status 10/2013
ISO 24759	Test requirements for cryptographic modules	Published 2008 – under first revision. Now DIS ballot Publication Q2 2014
ISO 18367	Algorithm and security mechanisms conformance testing	First release Text for 2nd WD
ISO 17825	Testing methods for the mitigation of non-invasive attack classes against crypto modules	First release Text for 4th WD (first CD to be decided)
ISO 30104 Technical Specification	Physical security attacks, mitigation techniques and security requirements	First release Text for 3rd Preliminary Draft Technical Specification

Though ISO/IEC 19790 cannot provide sufficient conditions to guarantee that a module conforming to its requirements is secure (security of the module or system could be ensured by security evaluation as per ISO/IEC 15408), a common set of security requirements for the cryptographic modules to be used in tomorrow's critical infrastructures will be a key enabler to consistent, interoperable and affordable deployments.

6.2.1.3 ISO 270xx: Information Security Management System

This section discusses the information security management system related standards applicable for the Smart Grid domain. These are ISO/IEC 27001 and ISO/IEC 27002 as the base standards and ISO/IEC TR 27019 as a domain specific mapping of ISO/IEC27002 to the energy systems domain.

ISO/IEC 27001:2013 is a generic Information Security Management System Standard that is 'to be applicable to all organizations, regardless of type, size or nature'.

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.

ISO/IEC TR 27019 is a sector-specific extension to ISO/IEC 27002 describing the code of practice for information security controls, based on ISO/IEC 27001. 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.

6.2.1.3.1 Status

At the moment ISO/IEC TR 27019 is aligned to the previous version of ISO/IEC 27001:2005. SC27 hast recently started a study period to determine the future scope and possible content of the next version of ISO/IECTR 27019 and the alignment with the current version of ISO/IEC 27002:2013 as well as the development into an IS. The results of this study period will be presented in autumn 2014.

	Description	Standardization Status
ISO/IEC 27001	Information technology — Security techniques — Information security management systems — Requirements	New release in 2013
ISO/IEC TR 27002	Information technology — Security techniques — Code of practice for information security controls	New release in 2013
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	Published. ISO/IEC TR 27019 is aligned to the previous version of ISO/IEC 27002:2005
ISO/IEC 27009	Information technology — Security techniques — Sector-specific application of ISO/IEC 27001	Draft available

6.2.1.3.2 Identified Gaps

There have been no gaps identified.

6.2.1.4 IEC 62443-2-1: Industrial Automation and Control System Security Management System

This standard has been developed by IEC TC65 WG10 in collaboration with ISA 99. The document addresses the implementation, management and operation of an IACS security system, based on ISO/IEC27001:2005 and ISO/IEC 27002:2005. The goal is to describe specifics for industrial control systems, which are to be adhered in addition to ISO/IEC 27002:2005 addressing general business and information technology systems. Hence, the goal is to describe this part as profile of ISO/IEC 27002:2005.

6.2.1.4.1 Status

Edition 2 of IEC 62443-2-1 is currently available as draft for comments. There will be a revision period to address the received comments. Note that IEC 62443-2-1 is aligned to ISO/IEC 27002:2005. In 2013 a revision of ISO/IEC 27001 and ISO/IEC 27002 has been done. Since the structure of both documents has changed, the consequences for IEC 62443-2-1 are currently being addressed and will be reflected in the next draft of 62443-2-1.

There is also the relation to ISO 27019 addressing the ISO 27002 mapping to process control systems in the energy utility industry (see also section 6.2.1.3).

6.2.1.5 IEC 62443-2-4: Requirements for Security Programs for IACS Integration and Maintenance Service Providers

This standard has been developed by IEC TC65 WG10 in collaboration with the International Instrumentation Users Association (WIB) and ISA 99.

This part of the IEC 62443 series defines requirements for the security programs of integration and maintenance IACS (Industrial Automation Control Systems) service providers. The requirements (policy, procedure, practice and personnel related) are defined in terms of the capabilities that these security programs are required to provide.

It also specifies a maturity model that sets benchmarks for meeting these requirements. These benchmarks are defined by maturity levels, based on the CMMI-SVC model (CMMI for services, see also [11]).

Service providers are required to identify the maturity level associated with their implementation of each requirement.

Functional areas covered:

- Solution staffing
- Security incidents
- Security tools and evaluations
- Architecture
- SIS (safety instrumented system)
- Wireless
- Account management
- Malware protection
- Backup/Restore
- Patch Management

Profiles are used to organize requirements: Base Profile (BP), Enhanced Profile #1 (EP1), Enhanced Profile #2 (EP2).

6.2.1.5.1 Status

	Description	Standardization Status
IEC 62443-2-4	Requirements for Security Programs for IACS Integration and Maintenance Service Providers	Committee Draft for Vote (CDV) January 2014

6.2.1.5.2 Identified Gaps

Privacy by design is missing.

6.2.1.6 IEC 62443-3-3: System Security Requirements and Security Levels

This standard has been developed by ISA99 WG4 TG2 in cooperation with IEC TC65/WG10.

This part of the IEC 62443 series provides detailed technical control system requirements (SRs) associated with the seven foundational requirements (FRs) described in IEC 62443-1-1, including defining the requirements for control system capability security levels, SL-C(control system).

Foundational Requirements:

a) Identification and authentication control (IAC),

b) Use control (UC),

c) System integrity (SI),

d) Data confidentiality (DC),

e) Restricted data flow (RDF),

f) Timely response to events (TRE),

g) Resource availability (RA).

Each SR has a baseline requirement and zero or more requirement enhancements (REs) to strengthen security.

The baseline requirement and REs, if present, are mapped to the control system capability security level, SL-C (FR, control system) 1 to 4 (enhancing attacker resources, skills and motivation).

6.2.1.6.1 Status

	Description	Standardization Status
IEC 62443-3-3	System security requirements and security levels	IS (August 2013)

6.2.1.6.2 Identified Gaps

The following gaps have been identified:

- Privacy is missing.
- Tamper resistance is inconsistently required.

6.2.1.7 IEC 62443-4-2: Technical Security Requirements for IACS Components

This standard is being developed by ISA99 WG4 TG4 in cooperation with IEC TC65/WG10

This document prescribes the security requirements for the components which are used to build control systems and thus are derived from the requirements for industrial automation and control systems defined in ISA 62443-3-3 and assigns system security levels (SLs) to the system under consideration (SuC).

It expands the SRs and REs defined in ISA 62443-3-3 into a series of Component Requirements (CRs) and REs for the components contained within an IACS.

Components: applications, host devices, embedded devices and network devices

The baseline requirement and REs, if present, are mapped to the component capability security level, SL-C (FR, component) 1 to 4. The component capability security level, SL-C (FR, component) 1 to 4 is derived from the control system capability security level defined for the associated SR in ISA 62443-3-3.

6.2.1.7.1 Status

	Description	Standardization Status
IEC 62443-4-2	Technical Security Requirements for IACS Components	DC (December 2013)

6.2.1.7.2 Identified Gaps

The current work on -4-2 is driven by the content of -3-3. There is opportunity to address the gaps identified for -3-3 in the work on -4-2 and the first draft shows some indication that this is done.

6.2.1.8 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.

6.2.1.8.1 Status

The first document was initially released in 2007 and the second edition is targeted for 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.

	Description	Standardization Status
IEEE 1686	Substation Intelligent Electronic Devices (IED) Cyber Security Standards	Working Draft currently in Ballot phase

6.2.1.8.2 Identified Gaps

No gaps have been identified so far.

6.2.1.9 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.

6.2.1.9.1 Status

The standard is currently in balloting stage. The standard relies on 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	Working Draft

6.2.1.9.2 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 15118-2 Road Vehicles – Vehicle-to-Grid Communication Interface

ISO/FDIS 15118-2 is maintained in ISO/TC 22/SC 3. It belongs to ISO standards catalogue Electric road vehicles. It specifies the communication between battery electric vehicles or plug-in hybrid electric vehicles and the electric vehicle supply equipment. It defines messages, data model, XML/EXI based data representation format, usage of vehicle to grid transfer protocol, transport layer security, TCP and IPv6.

The ISO/IEC 15118 security concept builds on TLS for protection of communication between the charging spot and the electric vehicle. Here certificate based authentication is required from the server side (charging spot). The use case plug-and-charge additionally requires a certificate based authentication based on credentials available in the electric vehicle. As there is some communication on application layer, which has an end-to-end character, beyond the scope of the charging spot, this communication is protected by XML digital signatures. An example is the provisioning of contract certificates and corresponding private keys for the plug and charge use case.

6.2.2.1.1 Status

ISO/IEC 15118	Definition of Security Services for	Standardization Status
Part 2	Network and application protocol requirements	IS (March 2014)

The standard has close relation with the remaining parts of ISO/IEC 15118, as there are:

ISO/IEC 15118	Definition of Security Services for	Standardization Status
Part 1	General information and use-case definition	Standard published
Part 3	Physical and data link layer requirements	Enquiry stage, close of voting
Part 4	Network and application protocol conformance test	Proposal stage, New project approved
Part 5	Physical layer and data link layer conformance test	Proposal stage, New project approved
Part 6	General information and use-case definition for wireless	Preparatory stage, New project registered in TC/SC work program
Part 7	Network and application protocol requirements for wireless communication	Preparatory stage, New project registered in TC/SC work program
Part 8	Physical layer and data link layer requirements for wireless communication	Preparatory stage, New project registered in TC/SC work program

6.2.2.1.2 Identified Gaps

The following gaps have been identified so far:

- No references to meter standards e.g. IEC 62056.
- Limited length of X.509v3 certificates (base64Binary (max length: 1200))
- Off-line case
- Service, parameterization, installation
- No recommendation for signature devices
- Missing privacy considerations
- The TLS cipher suites to be supported state TLS_ECDHE_ECDSA _WITH_AES_128_CBC_SHA256. Since this cipher suite is part of NSA suite-B profile (RFC 5430), the remaining cipher suites of this profile may be included as well. This needs to be checked.

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 the communication in power systems. It 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. The following Figure 9 shows the applicability of IEC 62351 in the context of other standard frameworks.

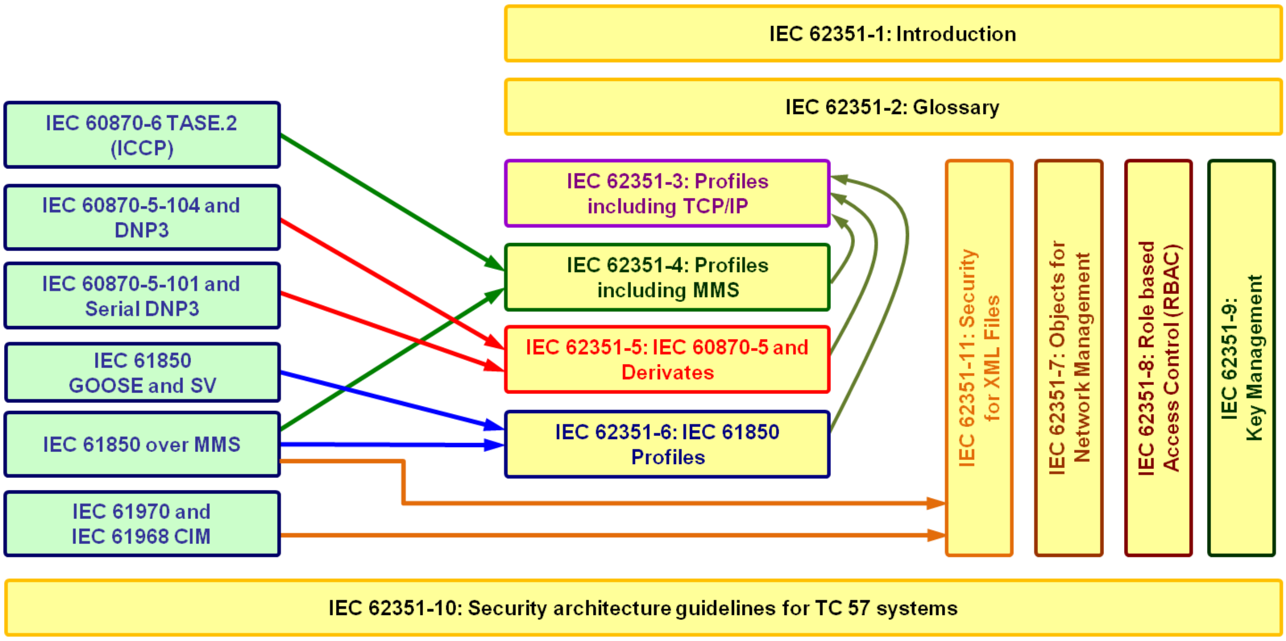


Figure 9: IEC 62351 applicability

A clear goal of the standardization of IEC62351 is the assurance of end-to-end security. 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
Part 1	Introduction and overview	Technical Specification (TS)
Part 2	Glossary of terms	TS, Edition 2 is currently being prepared
Part 3	Profiles including TCP/IP	TS, edition 2 FDIS in August 2014
Part 4	Profiles including MMS	TS, work on edition 2 is started. CD in 05/2015
Part 5	Security for IEC 60870-5 and Derivatives	TS in edition 2
Part 6	Security for IEC 61850	TS, edition 2 will align with IEC 61850-90-5 TR, WD available
Part 7	Network and system management (NSM) data object models	TS, edition 2 work started to enhance MIBs and provide mapping to protocols like SNMP, CD in 09/2014

Part 8	Role-Based Access Control for Power systems management	TS (2011), Amendment planned explaining usage as TR in IEC 62351-90-1
Part 9	Credential Management	Work in Progress, next CD in 09/2014
Part 10	Security Architecture Guidelines	Technical Report (TR, 2012), Amendment planned for dedicated use cases like DER in a separate document
Part 11	XML Security	CD published in 06/2014

Besides the work on the existing parts there is also further work being prepared as part of the IEC TC 57 WG 15 work:

Preliminary or new work Items	
Conformity Test	Targets a technical specification
Cyber security recommendations for DER	Targets enhancements of IEC 62351-10 with detailed examples for selected use cases. Note that this part is planned to be worked out as Technical Report IEC 62351-12.
Suggestions for what security topics to Include in Standards and Specifications	Target is a whitepaper to raise awareness for providing security considerations for standards not targeting specific security solutions. Note that this part is planned to be worked out as Technical Report IEC 62351-13.
RBAC Management Guidelines	Targets the management of roles in an energy automation environment, especially the categorization of roles and rights for an easier definition of custom roles. This will result in a TR (most likely IEC 62351-90-1).

6.2.2.2.2 Identified Gaps

This section describes gaps identified during the mapping of the considered standard to SGAM and to the different use cases. Identified gaps relate either to missing or insufficient functionality support or to necessary updates of functionality through recent developments in cryptography.

Note that gaps have already been identified for different IEC 62351 parts, which have already been stated in the report of the first working period of the SGIS. As these gaps have been reported to IEC TC57 WG 15 already and are being observed for the edition 2 development for the parts, they are not repeated here. Some of the identified gaps have been addressed by IEC TC57 WG15 in the context of edition 2 evolvements of dedicated parts. An example is the new revision of IEC 62351-3, which recently was voted 100% in favor. The issues raised by the SGIS in phase 1 have been addressed.

The focus for the gap analysis here is placed on new developments and parts, which have not received comments during SGIS phase 1.

- Comments on IEC 62351-7
    - Currently edition 2 is prepared providing a more consistent mapping of potential security events to MIBs building the base for the mapping to SNMP. The mapping to IEC 61850 is intended too and would be necessary to utilize the NSM also in a pure IEC 61850 context.
- Comments on IEC 62351-8
    - For interoperability reasons a mandatory profile for RBAC support is necessary
    - Transport profiles also for other protocols than TCP/IP (e.g., application for UDP/IP or even Ethernet based communication, like IEC 61850 GOOSE) may be outlined.
    - Usage examples for the role/right mapping and the application for online and offline actions. An example may be the handling of rights bound to a dedicated object.

    - Categorization of rights and roles to allow easier administration, addressing device management and operation are necessary to have a unified RBAC approach.
- Comments on IEC 62351-9
    - Describe migration path towards PKI based solution
    - Consider IETF RFC 7030 (Enrollment over Secure Transport, EST) for the enrollment of certificates additionally to SCEP and CMC. EST is an enhancement for the client utilizing CMC.
- Comments on IEC 62351-10
    - Intention to provide additional annexes describing security for dedicated smart grid areas, the first one is most likely DER. The work is currently based on a contribution to NIST. Nevertheless, the European view on DER needs to be incorporated as well. Germany will provide its view through the national committee. The enhancement may result in a separate TR part of IEC 62351.
- Comments on IEC 62351-11
    - Security (sensitivity labeling) necessary, cryptographic protection and enforcement of labeling necessary
    - Rely on XML security as much as possible → provide profiling

6.2.2.3 IEC 62056-5-3 DLMS/COSEM Security

IEC 62056-5-3:2013 (publication date 2013-06-05) specifies the DLMS/COSEM application layer in terms of structure, services and protocols for COSEM clients and servers, and defines how to use the DLMS/COSEM application layer in various communication profiles. It defines services for establishing and releasing application associations, and data communication services for accessing the methods and attributes of COSEM interface objects, defined in IEC 62056-6-2. It cancels and replaces IEC 62056-5-3 published in 2006. It constitutes a technical revision.

The standard defines how to use the COSEM application layer in various communication profiles. It specifies how various communication profiles can be constructed for exchanging data with metering equipment using the COSEM interface model, and what are the necessary elements to specify in each communication profile. Moreover, it specifies the symmetric key cryptographic algorithms and usage and amends the DLMS service and protocol specifications.

The standard is the suite of standards developed and maintained by the DLMS User Association.

6.2.2.3.1 Status

IEC 62056-5-3:2013 was published in 2013-06-05. The IEC technical committee is TC 13 Electrical Energy measurement, tariff- and load control. Related ICS codes are 17.220 (Electricity, magnetism, electrical and magnetic measurements), 35.110 (Networking) and 91.140.50 (Electricity supply systems). The standard contains 368 pages and its stability date is 2017.

IEC 62056	Definition of Security Services for	Standardization Status
-5-3	The DLMS/COSEM suite - Part 5-3: DLMS/COSEM application layer	Published, IS (06/2013)

The standard has close relation with the remaining parts of IEC 62056, as there are:

IEC 62056	Definition of Security Services for	Standardization Status
-1-0	Electricity metering data exchange - The DLMS/COSEM suite - Part 1-0: Smart metering standardization framework	ADIS 2013-11 , Approved for FDIS circulation
-21	Data exchange for meter reading, tariff and load	Published, 2002-07-17, former IEC 61107

IEC 62056	Definition of Security Services for	Standardization Status
	control, Direct local data exchange	
-3-1	The DLMS/COSEM suite - Part 3-1: Use of local area networks on twisted pair with carrier signaling	Published, 2013-08-20
-41	Data exchange for meter reading, tariff and load control, Data exchange using wide area networks. Public switched telephone network (PSTN) with LINK+ protocol	Published, 2002-04-18
-42	Electricity metering. Data exchange for meter reading, tariff and load control, Physical layer services and procedures for connection-oriented asynchronous data exchange	Published, 2002-07-16
-46	Data exchange for meter reading, tariff and load control - Part 46: Data link layer using HDLC protocol	2006-09-04
-47	Data exchange for meter reading, tariff and load control, COSEM transport layers for IPv4 networks	2007-06-29
-51	Data exchange for meter reading, tariff and load control, Application layer protocols	Published, 2002-03-27
-52	Data exchange for meter reading, tariff and load control, Communication protocols management distribution line message specification (DLMS) server	Published, 2002-03-27
-6-1	The DLMS/COSEM suite, Object Identification System (OBIS)	2013-09-30
-6-2	The DLMS/COSEM suite, COSEM interface classes	2013-09-30
-6-9 Ed. 1.0	Mapping between the Common Information Model CIM (IEC 61968-9) and DLMS/COSEM (IEC 62056) data models and message profiles	ANW 2012-09, Approved new work
-7-5	TARIFF AND LOAD CONTROL - Part 21: Direct local data exchange	ANW 2013-03, Approved new work
-7-6	The DLMS/COSEM suite, The 3-layer, connection-oriented HDLC based communication profile	2013-09-30
-8-20	The DLMS/COSEM Suite - Part 8-20: RF Mesh Communication Profile	ANW 2013-08, Approved new work
-8-3	The DLMS/COSEM suite, Communication profile for PLC S-FSK neighborhood networks	2013-09-30
-8-6	THE DLMS/COSEM SUITE - Part 8-X: DMT PLC profile for neighborhood networks	CD 2012-09, 1st Committee draft
-9-1	The DLMS/COSEM SUITE - Part 9-1: Communication Profile using web-services to access a COSEM Server via a COSEM Access Service (CAS)	ANW 2013-05, Approved new work
-9-7	The DLMS/COSEM suite, Communication profile for TCP-UDP/IP networks	2013-10-31

6.2.2.3.2 Identified Gaps

Comments to IEC 62056-5-3

- No definitions of key management of application level symmetric keys. This could be addressed by defining certificate profiles and an interaction with a PKI structure
- Embedding of the described application layer security mechanisms into an overall system security architecture not addressed. Note that this relates to the technical embedding in terms of a connection to the key management as stated above and also the operational handling.

6.2.2.4 IETF RFC 6960 Online Certificate Status Protocol

RFC 6960 specifies the Online Certificate Status Protocol (OCSP) as a key protocol for a X.509 Internet Public Key based Infrastructure. Beside Certificate Revocation Lists (CRLs), OSCP is a protocol which can be used to determine the current status of a digital certificate.
OSCP needs a server (OCSP responder) to retrieve certificate status information. A response is digitally signed. Information in detail is available from the IETF site (tools.ietf.org).

OSCP can be used where an OCSP server is already operated or an installation and operation practicable. The usage of OCSP in the scope of power systems (IEC TC57) is described in IEC 62351-9 (Data and Communication Security - Key Management). Furthermore, OSCP is typically in use to support secure e-mail transmission or TLS/SSL operation.

6.2.2.4.1 Status

RFC 6960 (OCSP) is an Internet Standards Track document.

	Description	Standardization Status
RFC 6960	Online Certificate Status Protocol	Published (06/ 2013)

6.2.2.4.2 Identified Gaps

There have been no gaps identified.

6.2.2.5 IETF RFC 7252: CoAP Constrained Application Protocol

The Constrained Application Protocol (CoAP) is an application-layer (web) protocol designed for resource-constrained networks and end-devices. The RESTful protocol design enables low overhead, simple caching mechanism, resource discovery as well as other features designed for an IoT (Internet of Things) environment. . The CoAP protocol is used in meshed-networks such as RF-Mesh or PLC-Mesh as well as in other networks running in a constrained environment. Typical use cases are in device and application management in networks for Distribution Automation (DA) or within an Advanced Metering Infrastructure (AMI). In terms of security, CoAP provides excellent capabilities for efficient monitoring and alarming in resource-constrained networks such as Distribution Automation, AMI and for sensor networks in general.

Security is considered in CoAP by providing a DTLS binding to CoAP, which can utilize pre-shared keys, raw public keys, or X.509 certificates for authentication and key agreement.

6.2.2.5.1 Status

The CoAP document has been approved in IETF as RFC 7252.

	Description	Standardization Status
RFC 7252	CoAP Constrained Application Protocol	Standard in 06/2014

6.2.2.5.2 Identified Gaps

There have been no gaps identified. The specification is already comprehensive and covering a broad variety on functionalities.

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

The Internet Draft (I-D) with the title *IEC 62351 Security Protocol support for GDOI* 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.*

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.

6.2.2.6.1 Status

The Internet-Draft is in review and will expire on November 17th, 2014.

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

6.2.2.6.2 Identified Gaps

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

6.2.2.7 IETF RFC 7030: Enrollment over Secure Transport

Enrollment over Secure Transport (EST) is a certificate management protocol for Public Key Infrastructure (PKI) clients over a secure transport. It supports client certificate and CA (Certificate Authority) certificate provisioning. In addition, EST supports client-generated public/private key pairs and key pairs generated by the CA. EST will replace the Simple Certificate Enrollment Protocol (SCEP) which is moving toward historical status. One reason is that SCEP does not support Next Generation Encryption.
Information in detail is available from the IETF site (tools.ietf.org).

The Enrollment over Secure Transport (EST) protocol covers a broad variety of use case scenarios, basically everywhere where a public key infrastructure and a CA are used to provide certificate and key management. Thus, EST should get into IEC 62351-9 (Data and Communication Security - Key Management) where SCEP is still the protocol of choice.

6.2.2.7.1 Status

RFC 7030 (EST) is an Internet Standards Track document.

	Description	Standardization Status

	Description	Standardization Status
RFC 7030	Enrollment over secure transport	Published (11/2013)

6.2.2.7.2 Identified Gaps

There have been no gaps identified.

6.3 Security Standards mapping to Use Cases

This section will rely on the use case as defined in chapter 8. In summary there are four use cases, which have been analyzed regarding the applicability of the standards stated in section 6.2:

- UC1: Transmission Substation
- UC2: Distribution Control Room
- UC3: Flexible and Consumer Demand Management
- UC4: Distributed Energy Resources (DER) Control

As these use cases have already been analyzed, an SGAM mapping and a description of actors, roles, and assets is available. This information will be used to evaluate, which and how the security standards are applicable within the use cases. The assumption is that at least not all of the standards are always directly applicable.

An example would be the utilization of IEC 61850 in the context of DER control. IEC 61850 should be secured by using IEC 62351 proposed means, like TLS (IEC 62351-3). TLS in the context of IEC 62351 requires X.509 certificates for mutual authentication. The provisioning with X.509 certificates is described in IEC 62351-9, which in turn may utilize EST (RFC 7030) as one option for the bootstrapping of certificates.

Note that in the following subsections the notion '(x)' is used when the selected standard is only indirectly applicable in the use case, while 'x' states direct standard applicability.

6.3.1 Mapping of Requirement Standards

The following table provides a mapping of the requirement standards to the use cases explained in section 8.

Standard	Use Case				Notes
	UC1: Transmission Substation	UC2: Distribution Control Room	UC3: Consumer Demand Management	UC4: Distributed Energy Resources (DER) Control	
ISO/IEC 15408 – 1	x	x	x	x	ISO 15408-1: General principles for security certification of products / systems
ISO/IEC 15408 – 2	x	x	x	x	ISO 15408-2: Design principles for security certification
ISO/IEC 15408 – 3	x	x	x	x	ISO 15408-3: Evaluation (testing) principles for security certification

Standard	Use Case				Notes
	UC1: Transmission Substation	UC2: Distribution Control Room	UC3: Consumer Demand Management	UC4: Distributed Energy Resources (DER) Control	
ISO/IEC 18045	x	x	x	x	ISO 18045: Methodology relevant for the entity in charge of security certification
ISO/IEC 19790	x	x	x	x	ISO 19790: Requirements for procurement of security components to be integrated in certified products/systems
ISO/IEC 27001	x	x	x	x	As ISO/IEC 27001:2013 is a Management System Standard, it is applicable to any of the Smart Grid use cases. ISO/IEC 27001:2013 provides the possibility to define the scope of a Management System based on the needs of the organization meaning any use case may be defined as a "Scope of the Management System".
ISO/IEC 27002	x	x	x	x	The application of all controls of ISO/IEC 27002:2013 is not a mandatory requirement of ISO/IEC 27001:2013 anymore. The controls contained in the standard may still be used, especially the implementation guidance in a best practice approach. Within a Management System, any control shall be determined based on the mandatory risk assessment and risk management process required by ISO/IEC 27001:2013.
ISO/IEC 27019	x	x	x	x	ISO/IEC TR 27019 is a Technical Report amending the controls of ISO/IEC 27002:2005. The note addressing ISO/IEC 27002:2013 applies. Please note that ISO/IEC TR 27019 is still based on the previous version of ISO/IEC 27002, namely the 2005 version. ISO/IEC JTC1 SC27 has started a study period on the necessary updates for ISO/IEC TR 27019 which is scheduled to produce results in autumn 2014.
IEC 62443-2-4 (CD)	(x)	(x)	(x)	(x)	Indirectly related
IEC 62443-3-3 (IS)	(x)	(x)	(x)	(x)	Applicable if security level categorization is required. In general support of security engineering through specific requirements related to strength of implementation.
IEC 62443-4-2 (WD)	(x)	(x)	(x)	(x)	Applicable if security level categorization required. In general support of security engineering through specific requirements related to strength of implementation.
IEEE 1686	x			x	
IEEE C37.240	x	x	x	x	
IEC 62443-2-1		(x)			

6.3.2 Mapping of Solution Standards

Standard	Use Case				
	UC1: Transmission Substation	UC2: Distribution Control Room	UC3: Consumer Demand Management	UC4: Distributed Energy Resources (DER) Control	Notes
ISO/IEC 15118-2 (IS)		x	x	x	Communication protocol for EV to supply equipment, UC2, UC3, UC4 have indirect link
IEC 62056-5-3 (IS)			x	x	For UC2/4: if COSEM interface objects are used
IEC 62351- 3 (TS)	x	x	x	x	If communication is done using IEC 61850
IEC 62351- 4 (TS)	x		x	x	If communication is done using IEC 61850
IEC 62351- 5 (TS)	x	x		x	To be applied for protection of IEC 60870-5 communication
IEC 62351- 6 (TS, WD Ed.2)	x			x	Edition 1 approach may not be applicable, but edition 2 addresses the shortcomings and make implementation more feasible.
IEC 62351- 7 (TS, CD Ed.2)	x			x	Applicability is related to the current Edition 2 work, which provides much more granularity than the edition 1 as well as the mapping to SNMP.
IEC 62351- 8 (TS)	x	x		x	May be used in conjunction with part 4, 5, 6
IEC 62351- 9 (CD)	x	(x)	(x)	x	Applicable if IEC 62351 services are used to protect IEC 61850 or IEC 60870 or IEEE 1815 communication.
IEC 62351- 10 (TR)	(x)			(x)	IEC 62351-10 is a technical report only.
IEC 62351- 11 (WD)	x	x	x	x	Protects XML based data exchange
IETF RFC 6960 OCSP	x	x	x	x	PKI base service for support of certificate based authentication (e.g., in the context of key management)
IETF RFC 7252		x	x	x	Communication of status, monitoring, and health check information in meshed- and constrained networks
IETF I-D draft-weis-gdoi-iec62351-9	x	x	x	x	Applicable for communication via GOOSE
IETF RFC 7030 EST	x	x	x	x	PKI base service for support of certificate based authentication (e.g., in the context of key management)

6.3.3 Identified standards not covered in the use case mapping and the gap analysis

This section lists security standards, which have been identified as important during the use case investigation with respect to standards application, but have not been dealt with, yet.

Standard	Use Case				Notes
	UC1: Transmission Substation	UC2: Distribution Control Room	UC3: Consumer Demand Management	UC4: Distributed Energy Resources (DER) Control	
SASL (Simple authentication and Security layer) RFC 4422		x	(x)	x	SASL provides authentication and is used in conjunction with XMPP. XMPP is intended to be used for DER integration.
End-to-End Signing and Object Encryption for XMPP, RFC 3923			x	x	Provides additional end-to-end security in XMPP applications. May be investigated in parallel to MMS security.
XMPP (eXtensible Messaging and Presence Protocol, RFC 6120			x	x	Not a purely security standard, but builds on existing security protocols like TLS and SASL
OAuth2 Framework, RFC 6749			x		Allows for authentication using a three party model.
ISO/IEC 29190			x	x	Information technology -- Security techniques – Privacy capability assessment model (status: CD)

6.4 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. These standards have not been investigated more deeply and are enumerated here for future investigation in addition to the standards listed in section 6.3.3.

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 European Set of Recommendation

The European set of recommendations objective is to support Smart Grid stakeholders in designing and building a European Smart Grid Infrastructure secure by design. As expressed in European Commission mandate M/490 [1]: *'[…] enable smart grid services through a Smart Grid information and communication system that is inherently secure by design within the critical infrastructure of transmission and distribution networks, as well as within the connected properties […].*'

Recommendations will be presented and linked to SGIS-Security Levels, SGAM domains, zones and layers, standards and use cases. Doing so will support the Smart Grid Coordination Group (SG-CG) framework [2][2] in assessing and supporting the development of standards to support European Smart Grid deployment mandate M/490 objective.

7.1 European Set of Recommendations Overview

In April 2014, ENISA and European Commission Smart Grid Task Force Expert Group 2 (EG2) ad hoc group, release a "Proposal for a list of security measures for Smart Grids" report [8].

For consistency of work at European level the choice has been made to work with the measures proposed in this report to define the European set of recommendations. During the analysis work two additional domains have been identified and have been found worth to be added: Situational Awareness and Liability.

An overview of the ENISA measures domains, a domain in ENISA report is a "family group" of measures and has no link with SGAM domains, is proposed in the table hereunder. Descriptions are quoted from ENISA report. This level of granularity is enough for the work aimed in this section and the next one, applied information security.

For complete measures details please refer to the "Proposal for a list of security measures for Smart Grids" report [8]. More details on Situational Awareness and Liability are presented after the table.

European Set of Recommendations Domains Overview
Security governance & risk management
Measures relevant to proper implementation and/or alignment with the security culture on collaborative chain of smart grid stakeholders.
Management of third parties
Measures relevant to the interaction with third parties, so that the smart grid operator can reach a true and sustainable integration to the smart grid as a whole.
Secure lifecycle process for smart grid components/systems and operating procedures
Measures relevant to the secure installation, configuration, operation, maintenance, and disposition, including secure disposal, of the smart grid components and systems. Therefore, the security measures included in this domain take into consideration among other things the proper configuration of the smart grid information systems and components or its change management procedures.
Personnel security, awareness and training
This domain ensures that employees of an organization operating and maintaining a smart grid receive adequate cyber security training to perform reliable operations on the smart grid.
Incident response & information exchange
This domain covers the possible security threats, vulnerabilities, and incidents affecting smart grids in order to provide an effective response in case of a potential disruption or incident.
Audit and accountability
This domain covers the implementation of an audit and accountability policy and associated controls in order to verify compliance with energy and smart grid specific legal requirements and organization policies.
Continuity of operations
This domain ensures the basic functions of the smart grid under a wide range of circumstances including hazards, threats and unexpected events.
Physical security
This domain covers the physical protection measures for the smart grid assets.
Information systems security
This domain covers the definition of measures to protect the information managed by the smart grid information systems using different technologies like firewalls, antivirus, intrusion detection and etc.
Network security
This domain covers the design and implementation of required security measures that protect the established communication channels among the smart grid information system and the segmentation between business and industrial networks.
Resilient and robust design of critical core functionalities and infrastructures
This domain covers the design of the functionalities offered by the network and the supporting infrastructures in a resilient way.
Situational Awareness
This domain covers principles for Smart Grid stakeholders to constantly be aware of their cyber security situation. This could be addressed thru three sub-domains: Anticipation, Monitoring and Response.
Liability
This domain covers principles for Smart Grid stakeholders in case of privacy or cyber security breach.

907 **Table 1*: European set of recommendations domains overview***

Situational Awareness:

Situational Awareness is about constantly being aware of what is happening within a given business, here the smart grid, in order to understand and monitor the information, alerts, events and/or incidents in it. Having a complete, accurate and up-to-date situational awareness will give a better rational response to crisis situations and improve the resilience of the given business. The Figure 10 hereunder illustrates the three situational awareness principles.

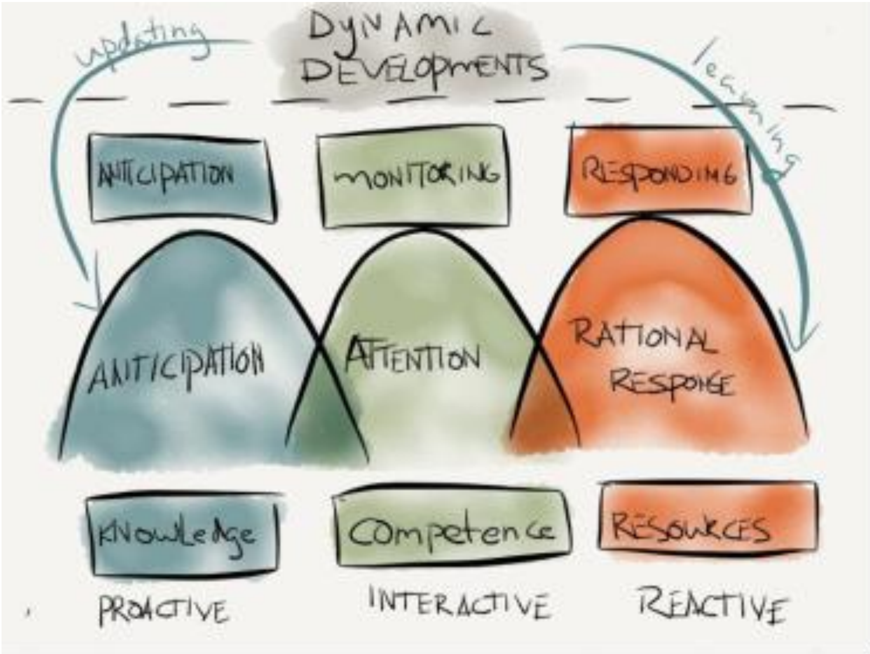


Figure 10: Situational Awareness Principles

The different three principles can be defined as follow:

1. Anticipation: intelligence gathering through information sharing with other utilities and ISAC's, threat and vulnerability analysis, information from CERT's, collaboration with governmental agencies etc.
2. Monitoring: Monitor the grid by gathering the data from the ICS and SCADA systems, detect the anomalies and send (analysis of the) alerts/events/incidents to the operator in the control center.
3. Respond: Respond rationally to the situation based on the analysis of the alert/event/incident as part of incident response management. If necessary escalate to crisis management.

Liability:

There is not always a clear picture of the liability of Smart Grid stakeholders in case of a cyber security incident in legislations. Nevertheless Smart Grid stakeholders should pay a specific attention to this non-technical point, especially as concerns about the topic are rising.

Note that in Netherlands, in order to provide a clear picture; a small team of legal experts has initiated an investigation with the following plan:

- Analyze in the criminal law, corporate law and the civil law what the as-is situation is of the liability for utilities in case of a cyber-security incident based on several use-cases
- Gather the conclusion, findings and gaps per use-case
- Describe the issues and (legal) recommendations for (change of) legislation and/or standards

- Describe the next steps

7.2 European Set of Recommendations Dashboard

Recommendations identified have to be linked to SGIS Security Levels and the SGAM, domains, zones and layers to integrate them in the SG-CG framework [2]. This is done using the dashboard hereunder:

European Set of Recommendations Domains		SGIS Security Levels					SGAM		
		1	2	3	4	5	Domains	Zones	Layers
ENISA Security Measures Domains	Security governance & risk management	***	***	***	***	***	All	All	Business, Function
	Third parties management	*	*	**	**	**	All	Station, Operation, Enterprise, Market	Business, Function
	Secure lifecycle process for smart grid components and operating procedures	**	**	***	***	***	All	All	Business, Function, Component
	Personnel security, awareness and training	*	*	**	**	***	All	All	Business, Function
	Incident response & information exchange	*	**	**	***	***	All	Station, Operation, Enterprise, Market	Business, Function
	Audit and accountability	*	*	**	**	***	All	Station, Operation, Enterprise, Market	All
	Continuity of operations	***	***	***	***	***	All	All	All
	Physical security	*	**	**	***	***	All	Process, Field, Station, Operation	Business, Function
	Information systems security	**	**	***	***	***	All	All	All
	Network security	**	**	***	***	***	All	All	Function, Information, Communication, Component
	Resilient and robust design of critical core functionalities and infrastructures	***	***	***	***	***	All	All	All
New	Situational Awareness	**	**	***	***	***	All	All	All
	Liability	*	**	**	***	***	All	All	Business, Function

Table 2*: European set of recommendations dashboard*

This dashboard contains three main columns: European Set of Recommendation Domains, SGIS Security Levels and SGAM and reads as follow:

- **European Set of Recommendation Domains** column presents the previously exposed recommendations domains.
- **SGIS Security Levels** column is using a three stars (*) system (*= low, **= medium, ***= high) to rank recommendations domains per security level. Then for a given security level recommendations can be prioritized. The objective here is to help stakeholders developing their cyber security strategy and program once they have identified their required security level using risk assessment or proposed recommended SGIS security levels (see section 5.2.1) per SGAM cell. This ranking can also be used to prioritize cyber security actions per smart grid stakeholders for a given use case, mapping the use case to the SGAM.
- **SGAM** column details in which domains, zones and layers a recommendations domain is applicable.

As standards are also presented using the SGAM [5], recommendations can then be linked to a given set of standards that could be used to deploy them. Then standards usage can be assessed and gaps or new standards needs identified.

This dashboard can also be used for use case analysis using use case SGAM mapping. SGAM can then be used as a common referential to present all information: use case details, SGIS security levels, recommendations and usable set of standards.

7.3 Conclusion

The current version of the European Set of Recommendations aims to propose a methodology linking cyber security recommendations to mandate M/490 objectives. Additional benefit of the proposed approach is that it can work whatever the recommendations might be. The dashboard would then just need to be updated but the process will remain the same.

7.4 Last Words

European Set of Recommendations should be reviewed yearly. This is a continuous process, as both, cyber security measures and forms of attacks are constantly evolving.

8 Applied Information Security on Smart Grid Use Cases

Use cases will be presented in this chapter in a synthesized way for the objective of this section is to illustrate SGIS methodology and not to provide fully detailed use cases description. Use cases will be presented using use case SGAM mapping.

Proposed use cases are examples and may not be representative of all related use cases. They are used for their demonstrative value to illustrate how to use proposed methodology.

The objective of use case SGAM mapping is to present all necessary information to describe a use case in a synthetic way using the different layers view. For more details about use case SGAM mapping, please refer to SG-CG/Methodology working group report.

Presented use cases SGAM mapping should provide all necessary information to understand the functional and technical details of the use cases.

The European set of recommendations dashboard has been designed to propose a pragmatic and easy way to deal with information security in Smart Grid use cases. This section illustrates how to use it.

The following use cases will be covered:

- Transmission Substation
- Distribution Control Room
- Consumer Demand Management
- Distributed Energy Resources (DER) Control

This section proposes a use case to security standards approach. A security standards to use cases approach is proposed in section 6.3. The objective of the present SG-CG/SGIS report is to propose cross-entries for standards and use cases.

8.1 Transmission Substation Use Case

Substations are a familiar sight alongside highways and in cities. Substations connect electricity flows from power plants and from the transmission lines and transform it from high to lower voltage. They distribute electricity to consumers and supervise and protect the distribution network to keep it working safely and efficiently, for example by using circuit breakers to cut power in case of a fault.

Their main functions are voltage transformation, network protection and switching of electrical power flows.

This use case describes a complete digital Substation Automation System (SAS) to illustrate the most complete cyber security coverage. SAS can also remain wired to HV equipment.

8.1.1 SGAM Mapping

The following figures represent the mapping of the use case to the SGAM layers:

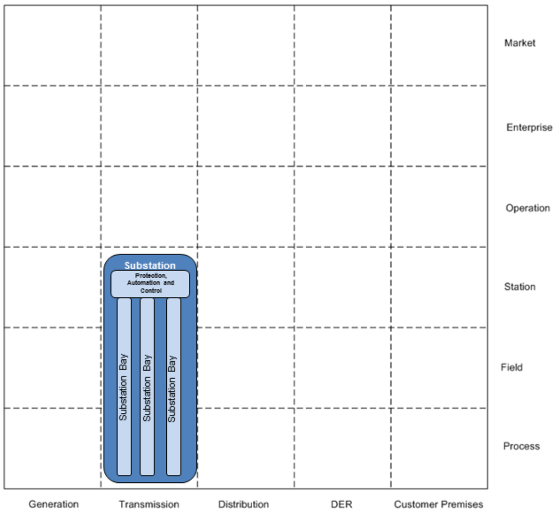


Figure 11: Transmission substation use case - business layer mapping

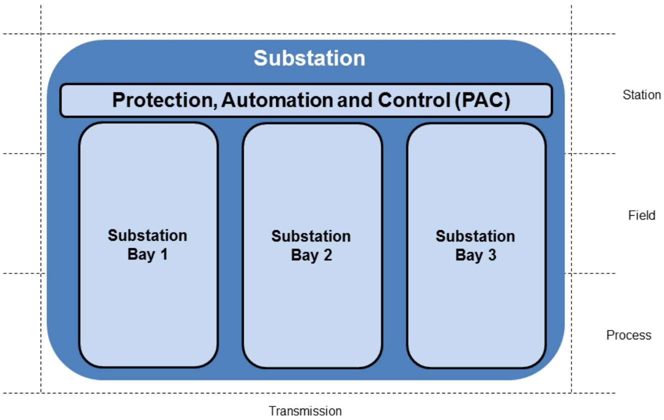


Figure 12: Transmission substation use case - business layer mapping

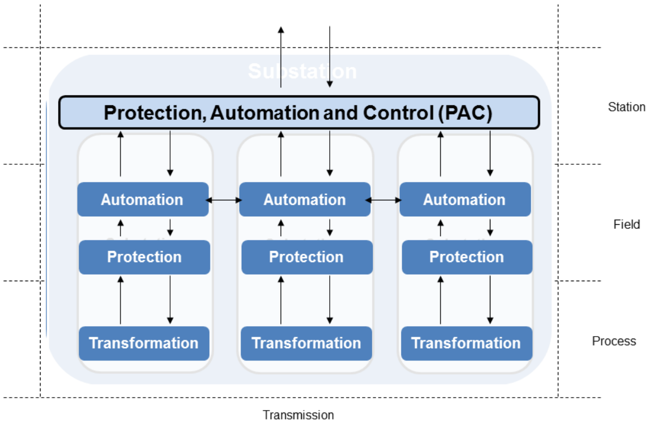


Figure 13: Transmission substation use case – function layer mapping

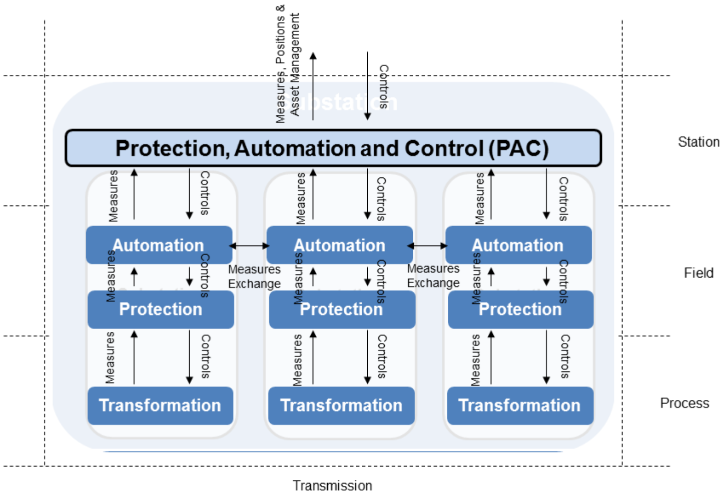


Figure 14: Transmission substation use case - information layer mapping

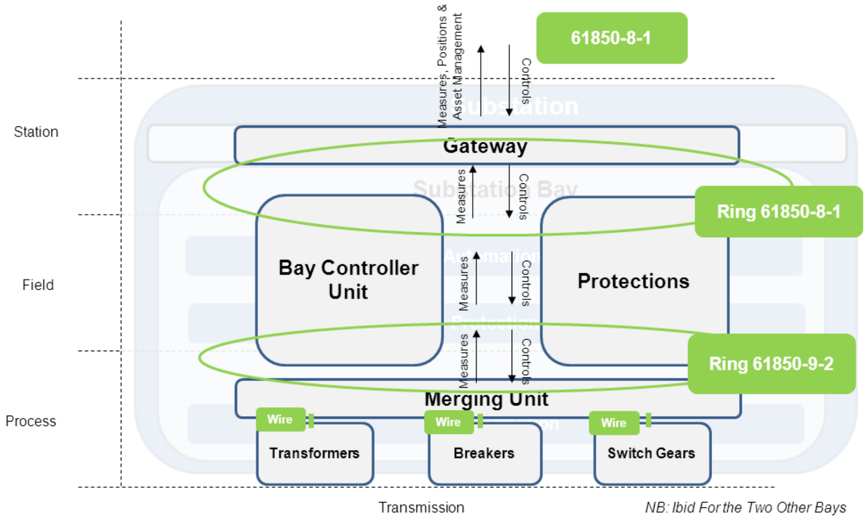


Figure 15: Transmission substation use case (one bay) - communication layer mapping

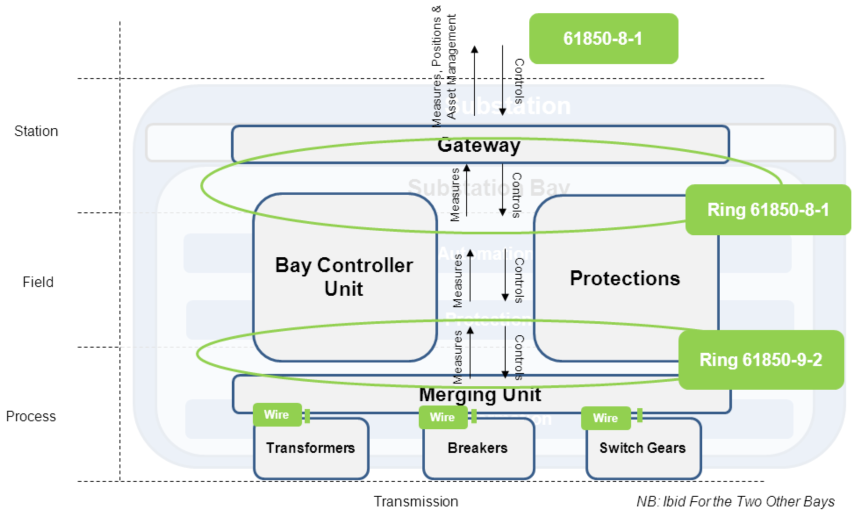


Figure 16: Transmission substation use case (one bay) - component layer mapping

8.1.2 Applied Cyber Security

8.1.2.1 Use Case Security Level

As shown in Figure 11, the transmission substation use case covers the following SGAM cells where according to section 5.2.1 Figure 4, the following security levels are proposed:

- Transmission, Station: 4
- Transmission, Field: 3
- Transmission, Process: 2

Transmission substations are critical Smart Grid components. Additionally it is considered as a system per itself for the present use case. Therefore choice is made to consider only one security level and to align on the highest one: **Use Case Security Level identified is: 4**

8.1.2.2 *Use Case Cyber Security Recommendations*

Using the European set of recommendations dashboard from section 7.2 Table 2 for SGIS Security Level 4, recommended cyber security domains can be prioritized. Then the following actions plan can be proposed to secure the transmission substation:

<u>High Priority Domains of Actions</u>

- Security governance & risk management
- Secure lifecycle process for smart grid components and operating procedures
- Incident response & information exchange
- Continuity of operations
- Physical security
- Information systems security
- Network security
- Resilient and robust design of critical core functionalities and infrastructures
- Situational Awareness
- Liability

<u>Medium Priority</u>

- Third parties management
- Personnel security, awareness and training
- Audit and accountability

<u>Low Priority</u>

- None

According to these findings a cyber security program and ad-hoc actions plans for each security recommendations domain could be defined. Identified priorities could be used to organize and manage the program and actions.

8.1.3 Standards

A list of standards that could be used to support recommendations implementation can be selected from SG-CG set of standards report and present SGIS report. The selection can be made using SGAM mapping both for the use case and standards. Additionally any other relevant standard identified could also be selected.

For the transmission substation use case following standards could be selected:

- ISO/IEC 27002 for Information Security Best Practices Techniques
- ISO/IEC 27019 for ISO/IEC 27002 guidance in energy utility industry
- ISO/IEC 27005 for Risk Management Techniques

- IEC 62351-4 for IEC 61850-8-1 Security
- IEC 62351-6 for IEC 61850-8-1 and IEC 61850-9-2 Security

As security measures domains and security standards are mapped using SGAM domains, zones and layers, a correspondence can be established between them. Thus for a given domain of measures, available standards to support measures implementation can be identified.

The following dashboard can be used to identify which standards could be used per security recommendations domain:

European Set of Recommendations Domains		SGAM			Standards
		Domains	Zones	Layers	
ENISA Security Measures Domains	Security governance & risk management	All	All	Business, Function	ISO/IEC 27002, ISO/IEC 27019, ISO/IEC 27005
	Third parties management	All	Station, Operation, Enterprise, Market	Business, Function	ISO/IEC 27002, ISO/IEC 27019
	Secure lifecycle process for smart grid components and operating procedures	All	All	Business, Function, Component	ISO/IEC 27002, ISO/IEC 27019
	Personnel security, awareness and training	All	All	Business, Function	ISO/IEC 27002, ISO/IEC 27019
	Incident response & information exchange	All	Station, Operation, Enterprise, Market	Business, Function	ISO/IEC 27002, ISO/IEC 27019
	Audit and accountability	All	Station, Operation, Enterprise, Market	All	ISO/IEC 27002, ISO/IEC 27019
	Continuity of operations	All	All	All	ISO/IEC 27002, ISO/IEC 27019, IEC 62351-4, IEC 62351-6
	Physical security	All	Process, Field, Station, Operation	Business, Function	ISO/IEC 27002, ISO/IEC 27019
	Information systems security	All	All	All	ISO/IEC 27002, ISO/IEC 27019, IEC 62351-4, IEC 62351-6
	Network security	All	All	Function, Information, Communication, Component	ISO/IEC 27002, ISO/IEC 27019, IEC 62351-4, IEC 62351-6
	Resilient and robust design of critical core functionalities and infrastructures	All	All	All	ISO/IEC 27002, ISO/IEC 27019, IEC 62351-4, IEC 62351-6
New	Situational Awareness	All	All	All	
	Liability	All	All	Business, Function	

Table 3: Transmission substation use case – cyber security dashboard

8.1.4 Conclusion

Selected standards are not mandatory for the present use case but have been identified as relevant to cyber security for the transmission substation use case. Use case stakeholders now have a narrowed set of standards from which to start to put in place cyber security recommendations thru their prioritized actions plan program.

8.2 Distribution Control Room Use Case

Distribution control rooms are used to operate grid network operations at distribution level. Such control rooms usually gather a set of several business functions: SCADA, distribution network management, outage management, smart meters integration, distributed energy resources (DER) management among others. All these functions are associated to specific Smart Grid use cases to be managed.

For clarity reasons and to simplify the work presented here on SGIS Security Levels, cyber security recommendations and standards, the present use case will focus on DER Management function only.
Next DERMS will refer to Distributed Energy Resources Management System.

8.2.1 SGAM Mapping

The following figures represent the mapping of the use case to the SGAM layers:

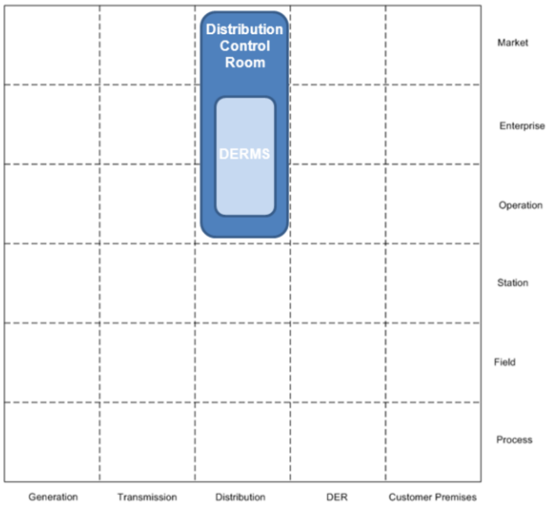


Figure 17: Distribution control room use case - business layer mapping

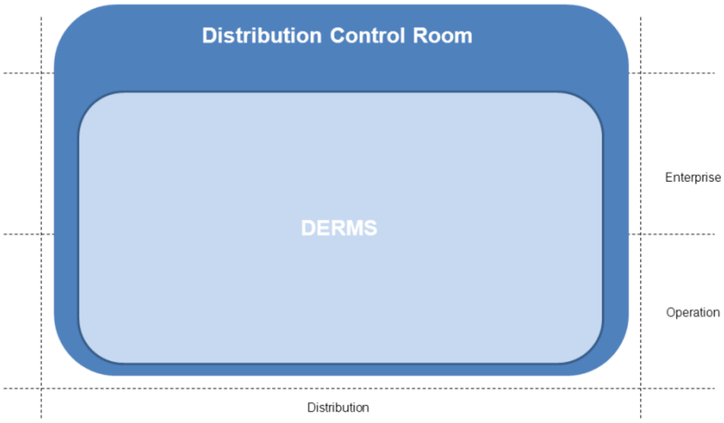


Figure 18: Distribution control room use case - business layer mapping

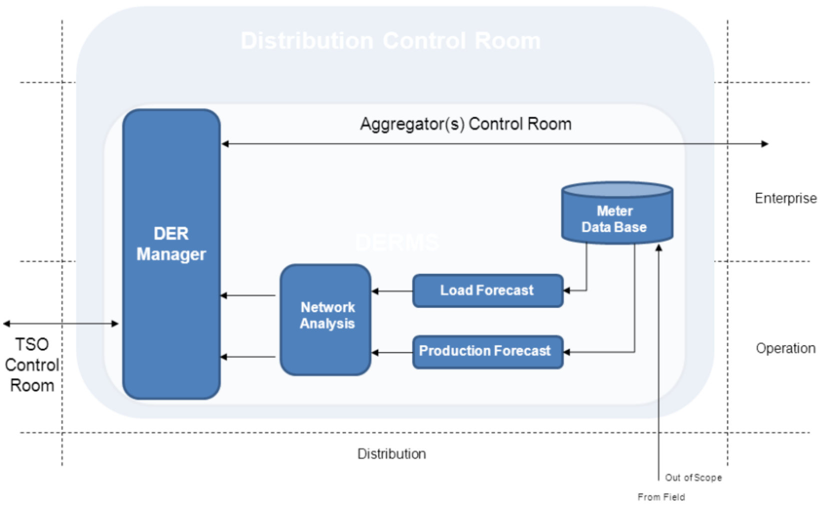


Figure 19: Distribution control room use case – function layer mapping

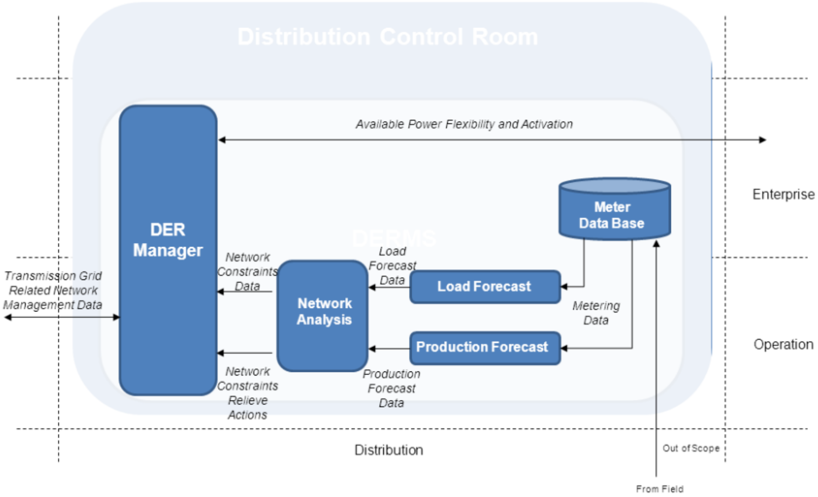


Figure 20: Distribution control room use case - information layer mapping

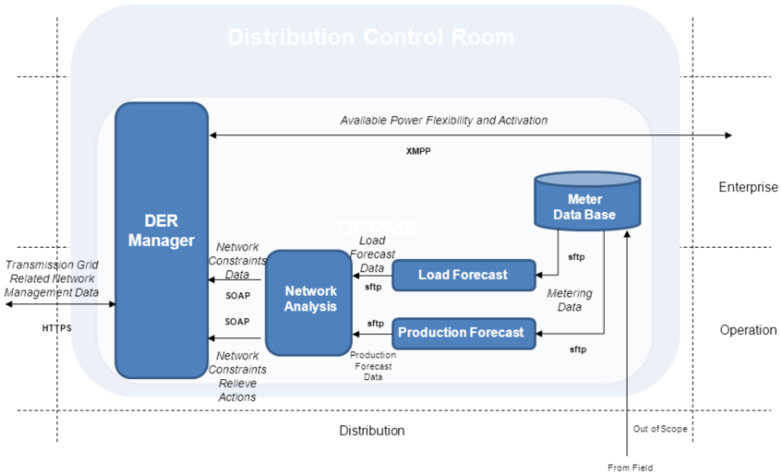


Figure 21: Distribution control room use case - communication layer mapping

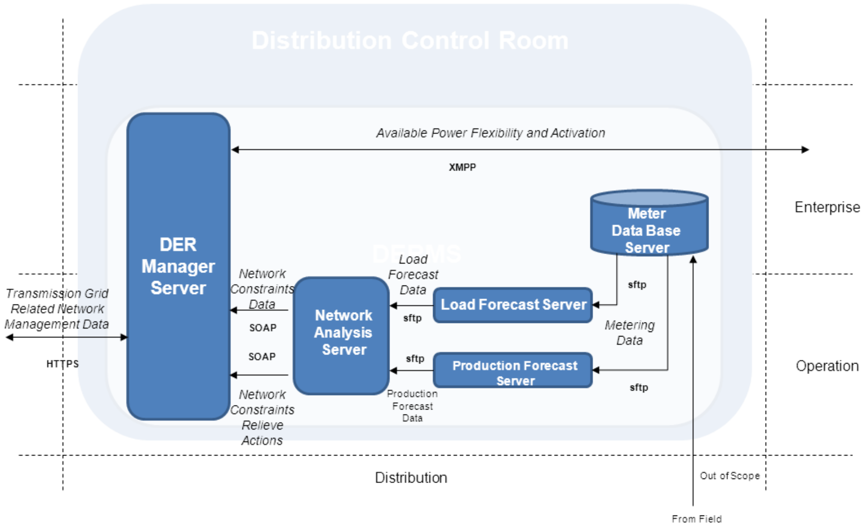


Figure 22: Distribution control room use case - component layer mapping

8.2.2 Applied Cyber Security

8.2.2.1 Use Case Security Level

As shown in Figure 17, the distribution control room use case covers the following SGAM cells where according to section 5.2.1 Figure 4, the following security levels are proposed:

- Distribution, Enterprise: 3 - 4
- Distribution, Operation: 3 - 4

For the present use case, the distribution control room is considered as a whole unique system with all involved stakeholders aligning on the same security level.

Choice is made to align on highest proposed security level: **Use Case security level identified is: 4**

8.2.2.2 *Use Case Cyber Security Recommendations*

Using the European set of recommendations dashboard from section 7.2 Table 2 for SGIS Security Level 4, recommended cyber security domains can be prioritized. Then the following actions plan can be proposed to secure the distribution control room:

High Priority Domains of Actions

- Security governance & risk management
- Secure lifecycle process for smart grid components and operating procedures
- Incident response & information exchange
- Continuity of operations
- Physical security
- Information systems security
- Network security
- Resilient and robust design of critical core functionalities and infrastructures
- Situational Awareness
- Liability

Medium Priority

- Third parties management
- Personnel security, awareness and training
- Audit and accountability

Low Priority

- None

According to these findings a cyber security program and ad-hoc actions plans for each security recommendations domain could be defined. Identified priorities could be used to organize and manage the program and actions.

8.2.3 Standards

A list of standards that could be used to support recommendations implementation can be selected from SG-CG set of standards report and present SGIS report. The selection can be made using SGAM mapping both for the use case and standards. Additionally any other relevant standard identified could also be selected.

For the distribution control room use case following standards could be selected:

- ISO/IEC 27002 for Information Security Best Practices Techniques
- ISO/IEC 27019 for ISO/IEC 27002 guidance in energy utility industry
- ISO/IEC 27005 for Risk Management Techniques

- HTTPS, (all relevant RFCs), for secure HTTP and SOAP communication
- SFTP, (all relevant RFCs), for secure FTP communication
- XMPP, (all relevant RFCs , especially RFC 6120), for secure XMPP communication

As security measures domains and security standards are mapped using SGAM domains, zones and layers, a correspondence can be established between them. Thus for a given domain of measures, available standards to support measures implementation can be identified.

The following dashboard can be used to identify which standards could be used per security recommendations domain:

European Set of Recommendations Domains		SGAM			Standards
		Domains	Zones	Layers	
ENISA Security Measures Domains	Security governance & risk management	All	All	Business, Function	ISO/IEC 27002, ISO/IEC 27019, ISO/IEC 27005
	Third parties management	All	Station, Operation, Enterprise, Market	Business, Function	ISO/IEC 27002, ISO/IEC 27019
	Secure lifecycle process for smart grid components and operating procedures	All	All	Business, Function, Component	ISO/IEC 27002, ISO/IEC 27019
	Personnel security, awareness and training	All	All	Business, Function	ISO/IEC 27002, ISO/IEC 27019
	Incident response & information exchange	All	Station, Operation, Enterprise, Market	Business, Function	ISO/IEC 27002, ISO/IEC 27019
	Audit and accountability	All	Station, Operation, Enterprise, Market	All	ISO/IEC 27002, ISO/IEC 27019
	Continuity of operations	All	All	All	ISO/IEC 27002, ISO/IEC 27019, HTTPS, SFTP, XMPP
	Physical security	All	Process, Field, Station, Operation	Business, Function	ISO/IEC 27002, ISO/IEC 27019
	Information systems security	All	All	All	ISO/IEC 27002, ISO/IEC 27019, HTTPS, SFTP, XMPP
	Network security	All	All	Function, Information, Communication, Component	ISO/IEC 27002, ISO/IEC 27019, HTTPS, SFTP, XMPP
	Resilient and robust design of critical core functionalities and infrastructures	All	All	All	ISO/IEC 27002, ISO/IEC 27019, HTTPS, SFTP, XMPP
New	Situational Awareness	All	All	All	
	Liability	All	All	Business, Function	

Table 4: Distribution control room use case – cyber security dashboard

8.2.4 Conclusion

Selected standards are not mandatory for the present use case but have been identified as relevant to cyber security for the distribution control room use case. Use case stakeholders now have a narrowed set of standards from which to start to put in place cyber security recommendations thru their prioritized actions plan program.

8.3 Consumer Demand Management Use Case

WG2-Sustainable Processes [4] provided following generic high level use case related to the consumer demand management within the DER cluster:

WGSP-2120	Direct load/generation management (Consumer demand management use case)

Direct load/generation management (WGSP-2120):
Demand Side Management signals and metrological information are sent to the Consumer Energy Manager (CEM) via an interface called Smart Grid Connection Point (SGCP).

This triggers a program that manages load by interacting with a number of in-home smart devices connected to the CEM. The following signals can be distinguished:

1. Direct load / generation / storage management (WGSP-2121)
2. Emergencies (WGSP-2122)
   a. Emergency load control
   b. Announce end of emergency load control

These functions can be labeled as a ‘Direct load control’ use case, following the definition of Eurelectric, which is referenced in the Sustainable Processes workgroup’s report.

8.3.1 SGAM Mapping

The figures below show the mapping of the direct load/generation management use case to the Smart Grid Architecture Model (SGAM) layers:

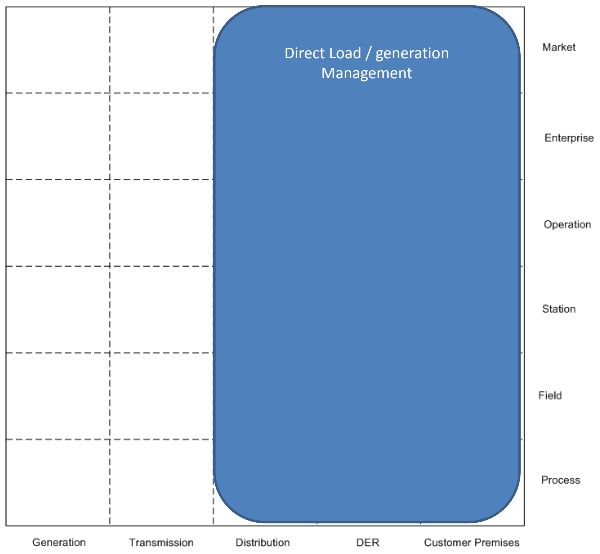


Figure 23: Direct load/generation management - business layer mapping

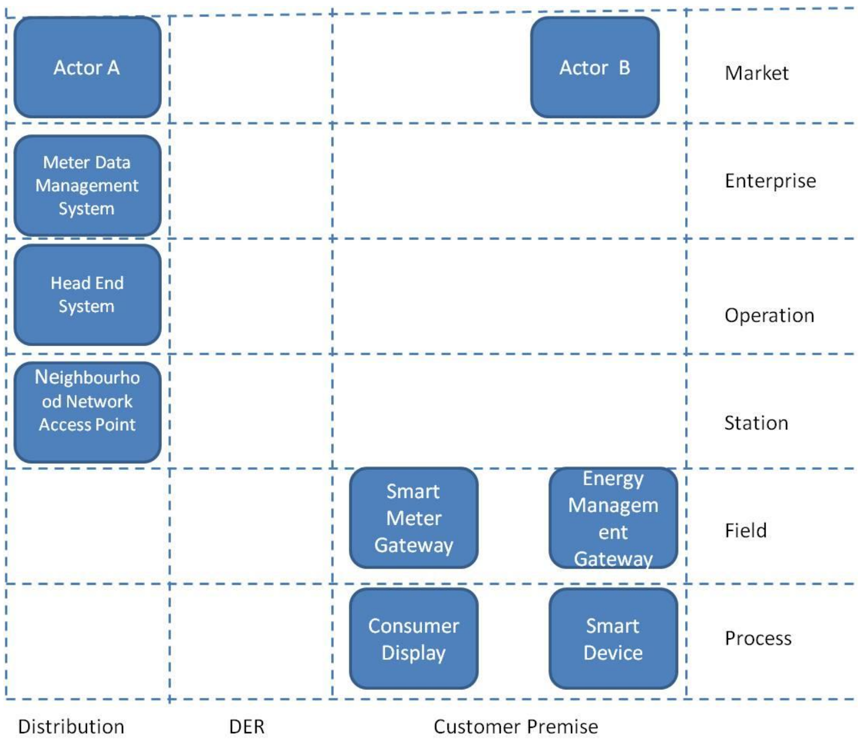


Figure 24: Direct load/generation management - function layer mapping

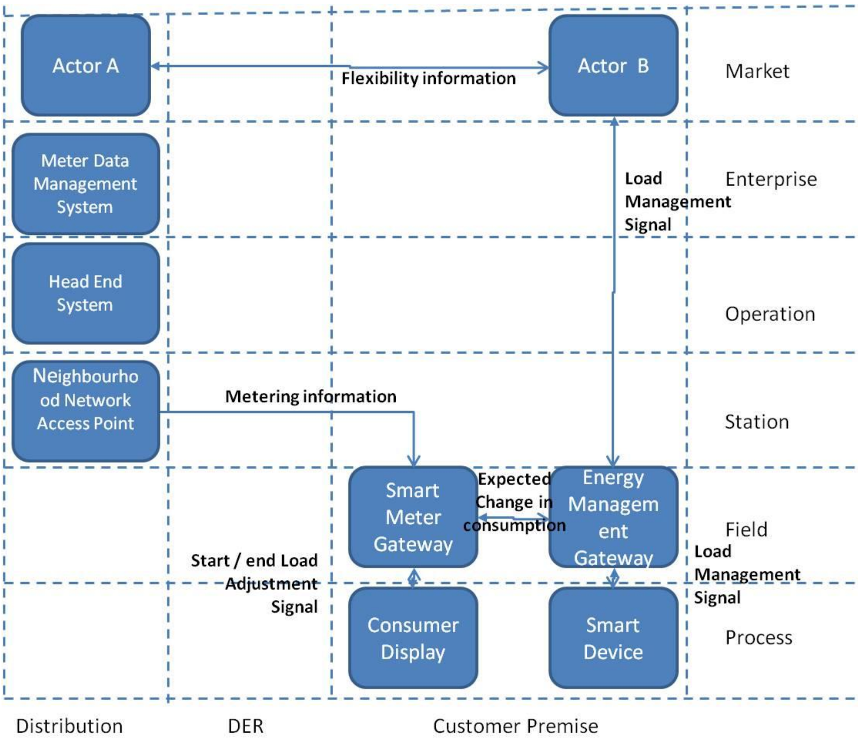


Figure 25: Direct load/generation management - information layer mapping

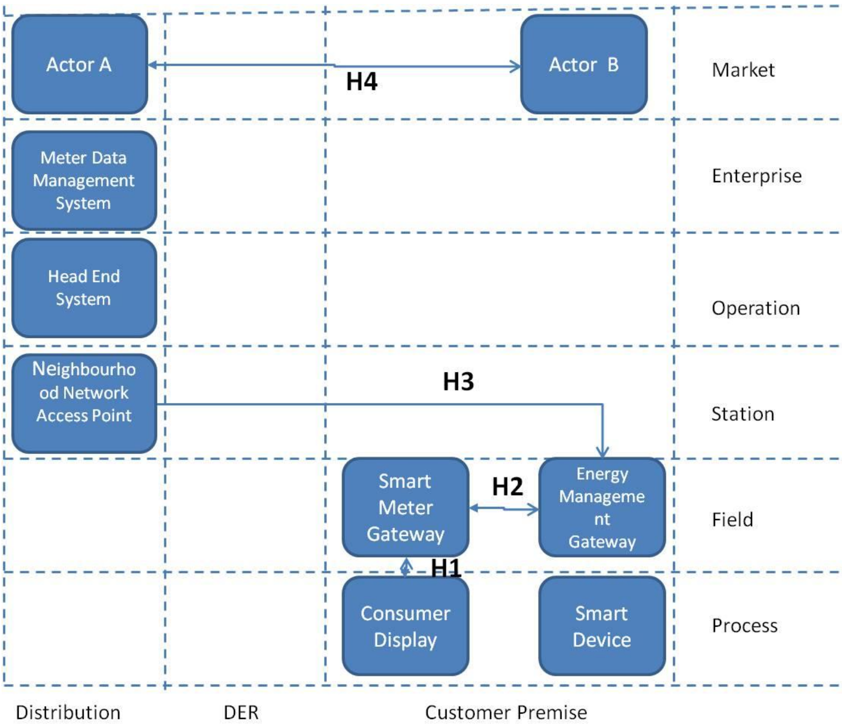


Figure 26: Direct load/generation management - communication layer mapping

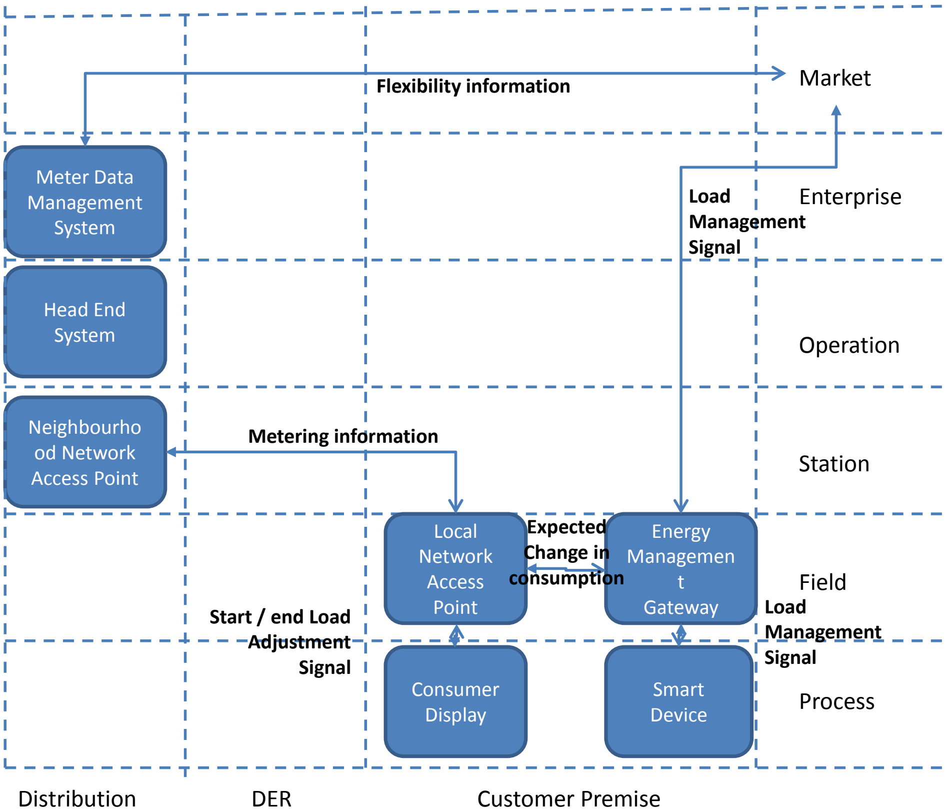


Figure 27: Direct load/generation management - component layer mapping

This use case has been developed to represent roles and interactions / interfaces in the market, marked as H1 – H4 which are described at the functional level. Specific communication protocols have not yet been included in the published use case; therefore these protocols do not appear on the communication layer mapping.

8.3.2 Applied Cyber Security

8.3.2.1 Use Case Security Level

As shown in Figure 23, he direct load/generation management use case covers the following SGAM cells where according to section 5.2.1 Figure 4, the following security levels are proposed:

- Distribution, Market: 3-4 — Customer, Market 2-3
- Distribution, Enterprise: 3-4 — Customer, Enterprise 2-3
- Distribution, Operation: 3 — Customer, Operation 2-3
- Distribution, Station: 2 — Customer, Station 2
- Distribution, Field: 2 — Customer, Field 1
- Distribution, Process: 2 — Customer, Process 1

Demand Side Management is an important Smart Grid component but it is an “ancillary service”; in case of real problems on the grid, the grid operator has alternative options. The security levels identified vary between 1 and 4, with the higher levels situated on the distribution side. Therefore choice is made to consider only one security level and to align between the highest one on the customer side (3) and the lower one on the distribution side (2): **Use Case Security Level identified is: 3**

8.3.2.2 Use Case Cyber Security Recommendations

Using the European set of recommendations dashboard from section 7.2 Table 2 for SGIS Security Level 3, recommended cyber security domains can be prioritized. Then the following actions plan can be proposed to secure the transmission substation:

High Priority Domains of Actions

- Security governance & risk management
- Secure lifecycle process for smart grid components and operating procedures
- Continuity of operations
- Information systems security
- Network security
- Situational Awareness
- Resilient and robust design of critical core functionalities and infrastructures

Medium Priority

- Third parties management
- Incident response & information exchange
- Personnel security, awareness and training
- Audit and accountability
- Physical security
- Liability

Low Priority

- None

According to these findings a cyber security program and ad-hoc actions plans for each security recommendations domain could be defined. Identified priorities could be used to organize and manage the program and actions.

8.3.3 Standards

A list of standards that could be used to support recommendations implementation can be selected from SG-CG set of standards report and present SGIS report. The selection can be made using SGAM mapping both for the use case and standards. Additionally any other relevant standard identified could also be selected.

Remark: as communication protocols have not (yet) been identified given the multitude of environments and the differences per country, no standards to secure them could be selected.

For the Direct load/generation management use case following standards could be selected:

- ISO/IEC 27002 for Information Security Best Practices Techniques
- ISO/IEC 27019 for ISO/IEC 27002 guidance in energy utility industry
- ISO/IEC 27005 for Risk Management Techniques

The following dashboard can be used to identify which standards could be used per security recommendations domain:

	European Set of Recommendations Domains	SGAM			Standards
		Domains	Zones	Layers	
ENISA Security Measures Domains	Security governance & risk management	All	All	Business, Function	ISO/IEC 27002, ISO/IEC 27019, ISO/IEC 27005
	Third parties management	All	Station, Operation, Enterprise, Market	Business, Function	ISO/IEC 27002, ISO/IEC 27019
	Secure lifecycle process for smart grid components and operating procedures	All	All	Business, Function, Component	ISO/IEC 27002, ISO/IEC 27019
	Personnel security, awareness and training	All	All	Business, Function	ISO/IEC 27002, ISO/IEC 27019
	Incident response & information exchange	All	Station, Operation, Enterprise, Market	Business, Function	ISO/IEC 27002, ISO/IEC 27019
	Audit and accountability	All	Station, Operation, Enterprise, Market	All	ISO/IEC 27002, ISO/IEC 27019
	Continuity of operations	All	All	All	ISO/IEC 27002, ISO/IEC 27019
	Physical security	All	Process, Field, Station, Operation	Business, Function	ISO/IEC 27002, ISO/IEC 27019
	Information systems security	All	All	All	ISO/IEC 27002, ISO/IEC 27019
	Network security	All	All	Function, Information, Communication, Component	ISO/IEC 27002, ISO/IEC 27019
	Resilient and robust design of critical core functionalities and infrastructures	All	All	All	
New	Situational Awareness	All	All	All	
	Liability	All	All	Business, Function	

Figure 28: Transmission substation use case – cyber security dashboard

8.3.4 Conclusion

Selected standards are not mandatory for the present use case but have been identified as relevant to cyber security for the direct load/generation management use case. Use case stakeholders now have a narrowed set of standards from which to start to put in place cyber security recommendations thru their prioritized actions plan program.

8.4 Distributed Energy Resources (DER) Control Use Case

The connection of DERs can influence the status of the power grids affecting the capacity of the DSO to comply with the contracted terms with the TSO and directly the quality of service of their neighbor grids. This difficulty not only could be transferred into charges to the DSO, but it may also impact on the TSO operation because the scheduled voltages at grid nodes could not be observed and voltage stability problems cannot be managed properly. In order to maintain stable voltages in the distribution grid the Voltage Control function is introduced. The primary aim of this use case is to address the communication needs of a Voltage Control (VC) function for medium voltage grids connecting DERs. The actions derived from the VC function are evaluated with the objective of defining an ICT architecture suitable for security analysis. The full use case template following the IEC TC 8 format [29] is available in [30].

8.4.1 SGAM Mapping

The following figures are showing how the actors and the functions of the Use Case can be mapped over the different layers of the SGAM plane. The actors of the use case are placed into the Transmission, Distribution and DER domains. The zones vary from the Market zone of the Aggregator to the Field zone of the control functions of the OLTC, Capacitor bank, DER and Flexible Load. In the middle we have the Generation and Load Forecast functions placed in the cell Enterprise zone/Distribution domain. The EMS and DMS control functions are in the Operation zone hosting all the active grid operation functions. The Substation Automation System and the Medium Voltage Grid Control functions are located in the Station zone.

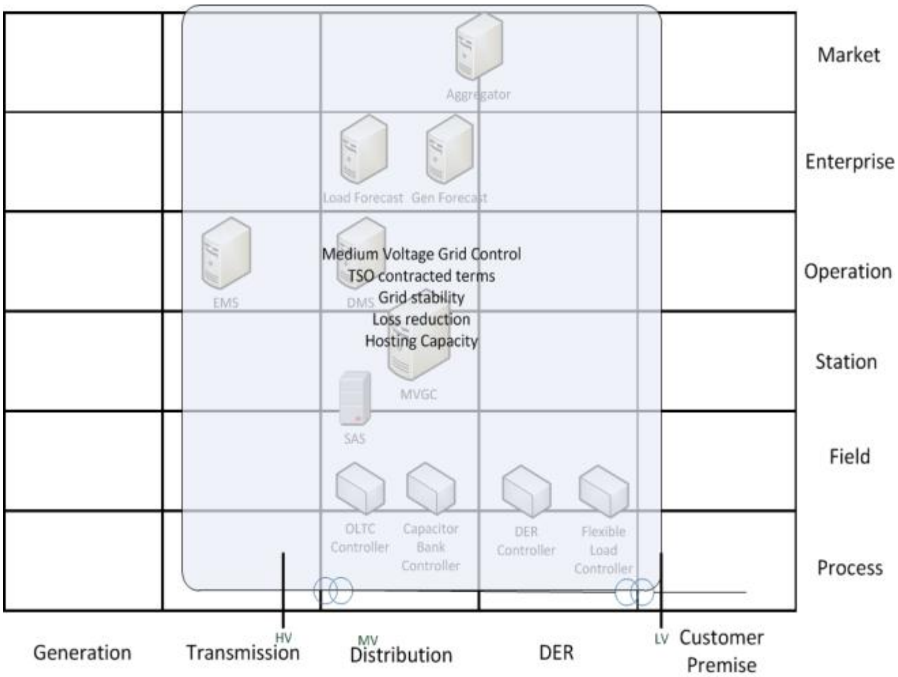


Figure 29: DER control use case – SGAM mapping: Business Layer

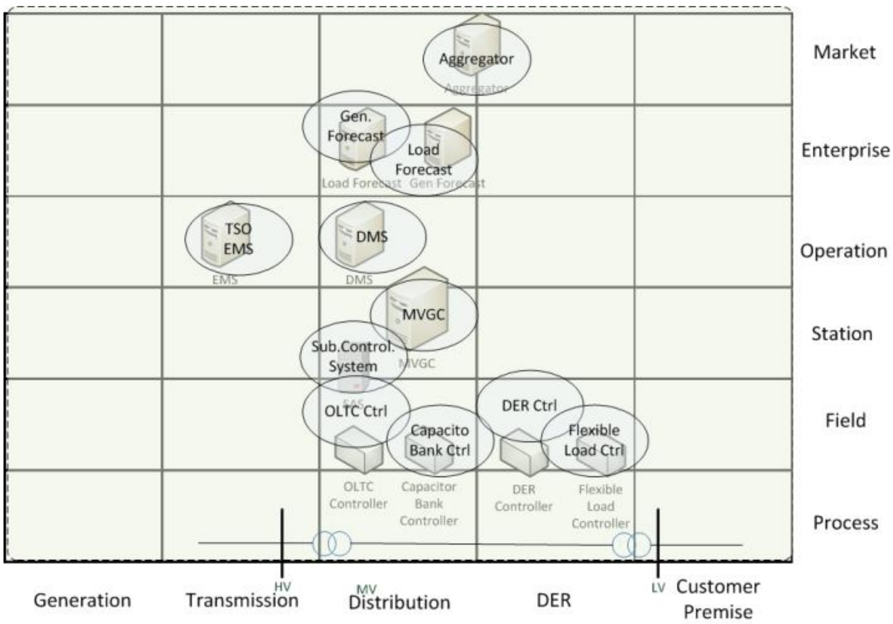


Figure 30: DER control use case - SGAM mapping: Function Layer

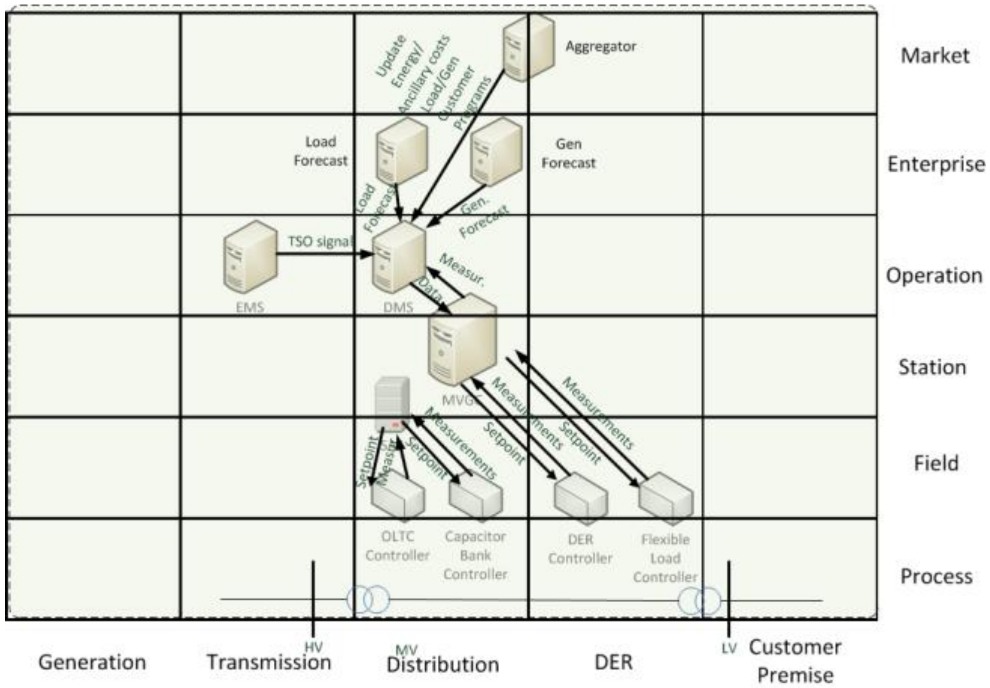


Figure 31: DER control use case - SGAM mapping: Information Layer

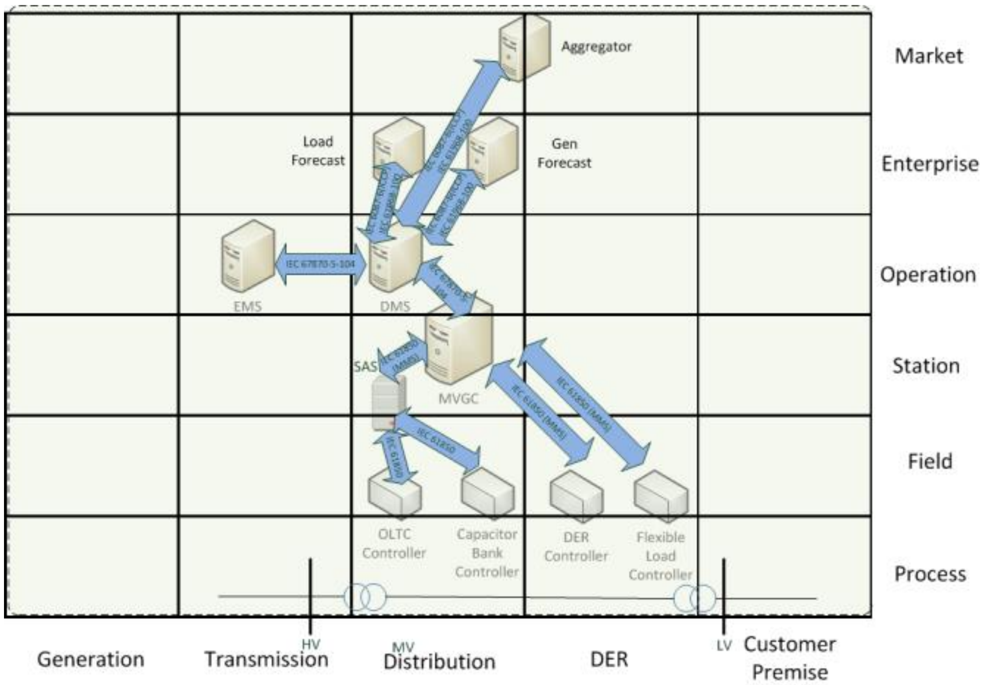


Figure 32: DER control use case - SGAM mapping: Communication Layer

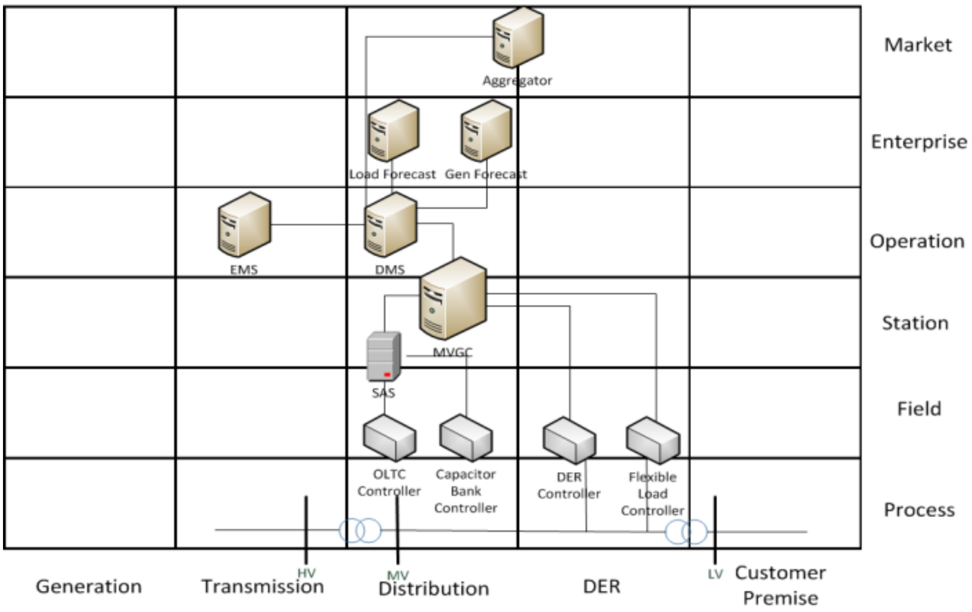


Figure 33: DER control use case - SGAM mapping: Component Layer

More details to the use case can be found in Annex A where the information exchanges among the components at the upper control zones and the communication flows within the substation and with DERs are shown.

8.4.2 Applied Cyber Security

8.4.2.1 Use Case Security Level

For the risk analysis of the DER control use case the SGIS toolbox as presented in [6] has been initially used when starting the work for this use case. Therefore some reference to it can still be found for this use case work continuity reason, acknowledging that SGIS toolbox has now evolved to SGIS Framework, see chapter 10.

The impact of attacks is evaluated through the five-scale impact matrix in Figure 34 defining the levels of operational, financial and additional risks. In order to perform the use case analysis, a benchmark grid has to be defined. A sample realistic 2020 grid scenario has been used for this use case, installing 40 GW of renewable connected to the Italian medium voltage grids. From the application of the SGIS impact levels to the benchmark grid, the operational Risk Impact Levels depicted in Figure 34 can be assigned to the information assets of the DER control use case. By focusing on the extreme case analysis, i.e. on those grids in those regions with maximum DER penetration and highest power demand, the loss of energy supply varies with the attack target: in the case of DER network attacks the loss may be up to 100MW (yellow circle in the picture), in the substation network attacks it may be up to 1 GW (orange circle), in the case of centre network attacks it may be up to 6GW (red circle). As for the impact of such attack effects on the registered population, the use case falls into the Medium level, while the impact on critical infrastructures may be High or Critical, depending on the presence of essential or national infrastructures in the sub-regions under attack.

RISK IMPACT LEVELS	Energy supply (Watt)	Energy flow (Watt/hour)	Population	Infrastructures	Data protection	other laws & regulations	HUMAN	REPUTATION	FINANCIAL
HIGHLY CRITICAL	regional grids from 10GW	from 10 GW/h	from 50% population in a country or from 25% in several countries	international critical infrastructures affected	not defined	company closure or collateral disruptions	direct and collateral deaths in several countries	permanent loss of trust affecting all corporation	Thirth party affected
CRITICAL	national grids from 1 GW to 10GW	from 1 GW/h to 10GW/h	from 25% to 50% population size affected	national critical infrastructures affected	not defined	temporary disruption of activities	direct and collateral deaths in a country	permanent loss of trust in a country	>=50% EBITDA
HIGH	city grids from 100MW to 1GW	from 100MW/h to 1GW/h	from 10% to 25% population size affected	essential infrastructures affected	unauthorized disclosure or modification of sensitive data	prison	direct deaths in a country	temporary loss of trust in a country	<50% EBITDA
MEDIUM	neighborhood grids from 10MW to 100MW	from 10MW/h to 100MW/h	from 2% to 10% population size affected	complimentary infrastructures affected	unauthorized disclosure or modification of personal data	fines	seriously injured or discapacity	temporary and local loss or trust	<33% EBITDA
LOW	home or building networks under 10 MW	under 10MW/h	under 2% population size affected in a country	no complimentary infrastructures	no personal nor sensitive data involved	warnings	minor accidents	short time & scope (warnings)	<1% EBITDA
	OPERATIONAL (availability)				LEGAL				

MEASUREMENT CATEGORIES

Figure 34: DER control use case – Risk Impact Levels

By grouping the use case information assets and attack scenarios considering similarity in their parameters, we identify three main categories of assets according to the attack target interfaces and five most relevant attacker profiles. The likelihood levels are presented in Figure 35.

	substation2DER	substation2centre	centre2substation
Dishonest employee (Admin)	Very High	Very High	Very High
Dishonest employee (normal user)	High	Medium	Medium
Vandal	Very High	High	Low
Hacker	Very High	High	Medium
Terrorist	Medium	Very High	Very High

Figure 35: DER control use case - Likelihood Levels

Combining the Risk Impact Levels with the Likelihood levels as indicated by the SGIS approach in Figure 36 the High (3) and Critical (4) Security Levels are identified for the use case, depending on the information assets/security scenarios under consideration. To be noticed that the combination of the impact with the likelihood analysis has increased the need of security protection of substation-DER communications (from a medium impact level to a high risk).
The details on the security analysis of the use case can be found in [57].

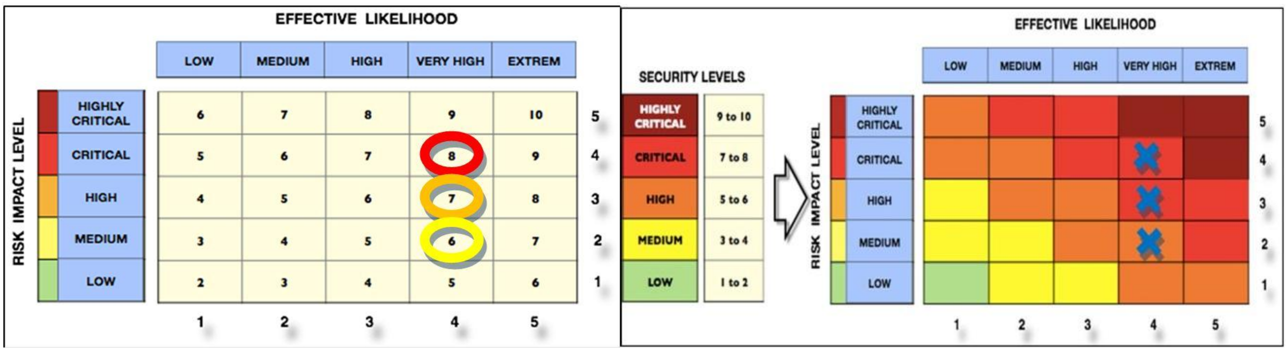


Figure 36: DER control use case - Security Levels

The value of the outcome (Risk Impact Level and Security Level) of the application of the SGIS toolbox (SGIS phase 1 version [6]) to the smart grid use cases highly depends on the amount and quality of the information collected during the analysis steps. The SGIS toolbox application to the DER control use case allowed identifying some complementary information needed for evaluating the risk impact levels related to the operational categories.

8.4.2.2 *Use Case Cyber Security Recommendations*

As a next step the European set of recommendation dashboard from section 7.2 Table 2 can be used for identifying the prioritized domains relevant for the DER control use case. The following action plan can be proposed to secure the DER control scenarios achieving SL 4:

High Priority

- Security governance and risk management
- Secure lifecycle process for smart grid components and operating procedures
- Incident response & information exchange
- Continuity of operations
- Physical security
- Information systems security
- Network security
- Resilient and robust design of critical core functionalities and infrastructures
- Situational Awareness
- Liability

Medium Priority

- Third parties management
- Personnel security, awareness and training
- Audit and accountability

Low Priority

- None

8.4.3 Standards

From the analysis of the DER control ICT architecture and communications, the following groups of security standards has been identified as relevant for the DER control use case:

Requirement standards

- IEC 2700x
- NISTIR 7628

Solution standards (see Figure 37)

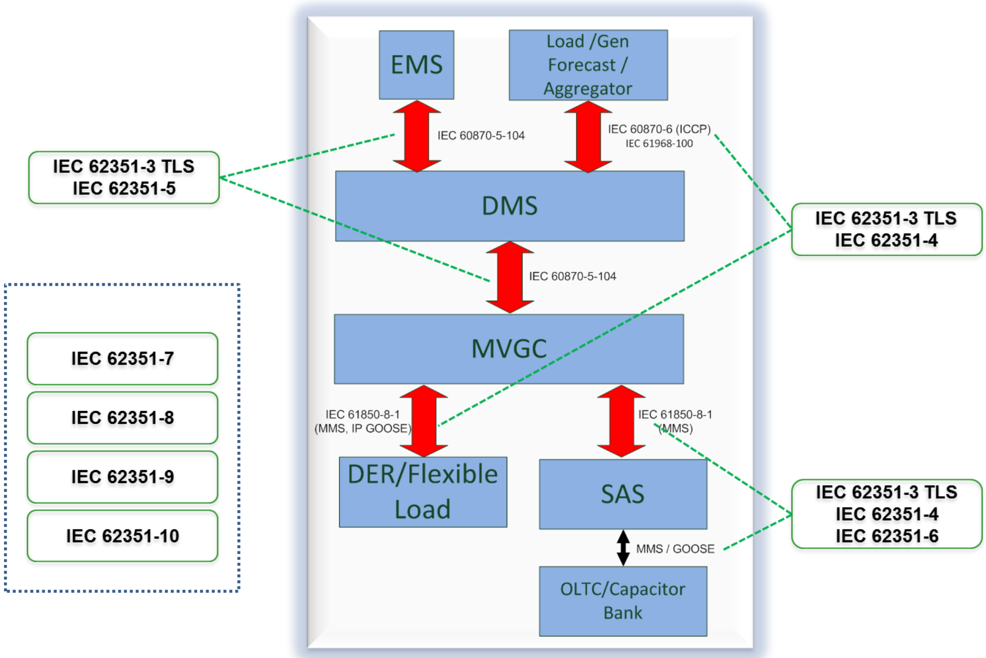
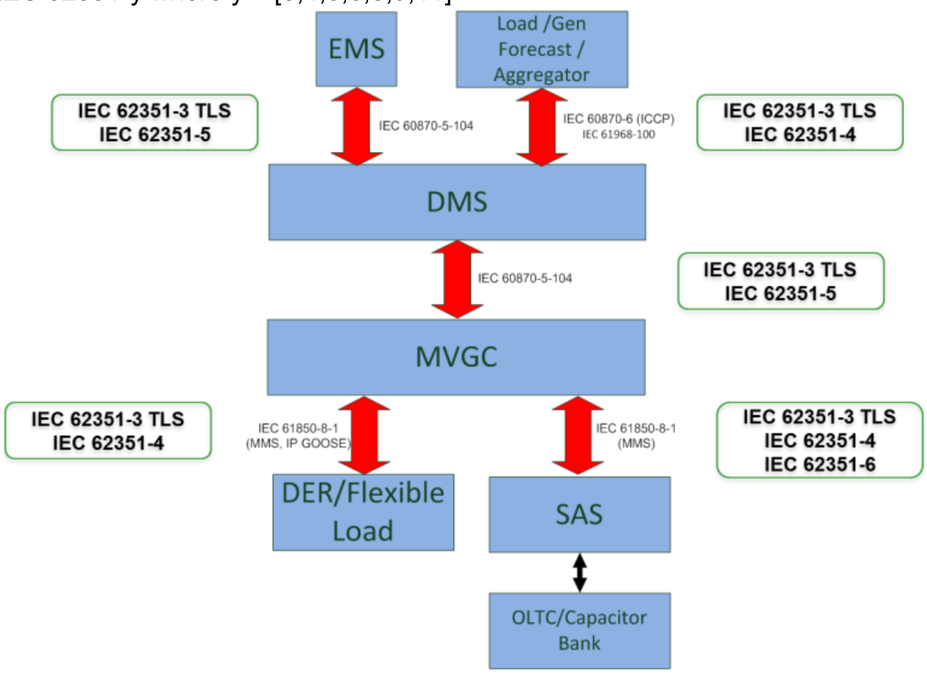


Figure 37: DER control use case – Security standards

- Communication protocol security standards
  - IEC 62351-y where y = [3,4,5,6,8,9,11]



- Network security standards
  - IEC 61351-10, IPSEC
- System and Network monitoring standards
  - IEC 62351-7, SNMP
- Enabling standard IT security protocols
  - TLS, https, ssh

The following dashboard can be used to identify which standards could be used per security recommendations domain:

	European Set of Recommendations Domains	SGAM			Standards
		Domains	Zones	Layers	
ENISA Security Measures Domains	Security governance & risk management	All	All	Business, Function	ISO/IEC 27002, ISO/IEC 27019, ISO/IEC 27005, NISTIR 7628
	Third parties management	All	Station, Operation, Enterprise, Market	Business, Function	ISO/IEC 27002, ISO/IEC 27019, NISTIR 7628
	Secure lifecycle process for smart grid components and operating procedures	All	All	Business, Function, Component	ISO/IEC 27002, ISO/IEC 27019, NISTIR 7628
	Personnel security, awareness and training	All	All	Business, Function	ISO/IEC 27002, ISO/IEC 27019, NISTIR 7628
	Incident response & information exchange	All	Station, Operation, Enterprise, Market	Business, Function	ISO/IEC 27002, ISO/IEC 27019, NISTIR 7628
	Audit and accountability	All	Station, Operation, Enterprise, Market	All	ISO/IEC 27002, ISO/IEC 27019, NISTIR 7628
	Continuity of operations	All	All	All	ISO/IEC 27002, ISO/IEC 27019, NISTIR 7628, IEC 62351-3, IEC 62351-4, IEC 62351-5, IEC 62351-6
	Physical security	All	Process, Field, Station, Operation	Business, Function	ISO/IEC 27002, ISO/IEC 27019, NISTIR 7628
	Information systems security	All	All	All	ISO/IEC 27002, ISO/IEC 27019, NISTIR 7628, IEC 62351-3, IEC 62351-4, IEC 62351-5, IEC 62351-6, IEC 62351-7, IEC 62351-8, IEC 62351-9, IEC 62351-10, IEC 62351-11 HTTPS, SSH, TLS, SNMP
	Network security	All	All	Function, Information, Communication, Component	ISO/IEC 27002, ISO/IEC 27019, NISTIR 7628, IEC 62351-7, IEC 62351-10, IPSEC, SNMP
	Resilient and robust design of critical core functionalities and infrastructures	All	All	All	
New	Situational Awareness	All	All	All	IEC 62351-7, SNMP
	Liability	All	All	Business, Function	

Table 5: DER control use case - Cyber security dashboard

8.4.4 Measure implementation in the DER control use case

This section illustrates how the security standards identified previously may be deployed to get a secure architecture. An overview of a DER control secure architecture is presented in Figure 38, where the IEC 62351 solution standards have been integrated into the DER control component architecture. We see as the main communication channels are protected by means by the encryption mechanisms (IEC 62351 parts 3-4-5-6) represented by a lock. A certificate system is deployed in order to guarantee the authentication of the different parties exchanging information (IEC 62351 part 9). In order to monitor and detect anomalies a structure for capturing and analysing log information is developed where different monitor agents are scattered over the ICT architecture (IEC 62351 part 7). These agents may perform local analysis and create alarms and/or report values to server agents placed at the ICT maintenance centre where a global view of the ICT systems is supervised by operators and correlation functions are performed enabling the application of automatic recovery measures.

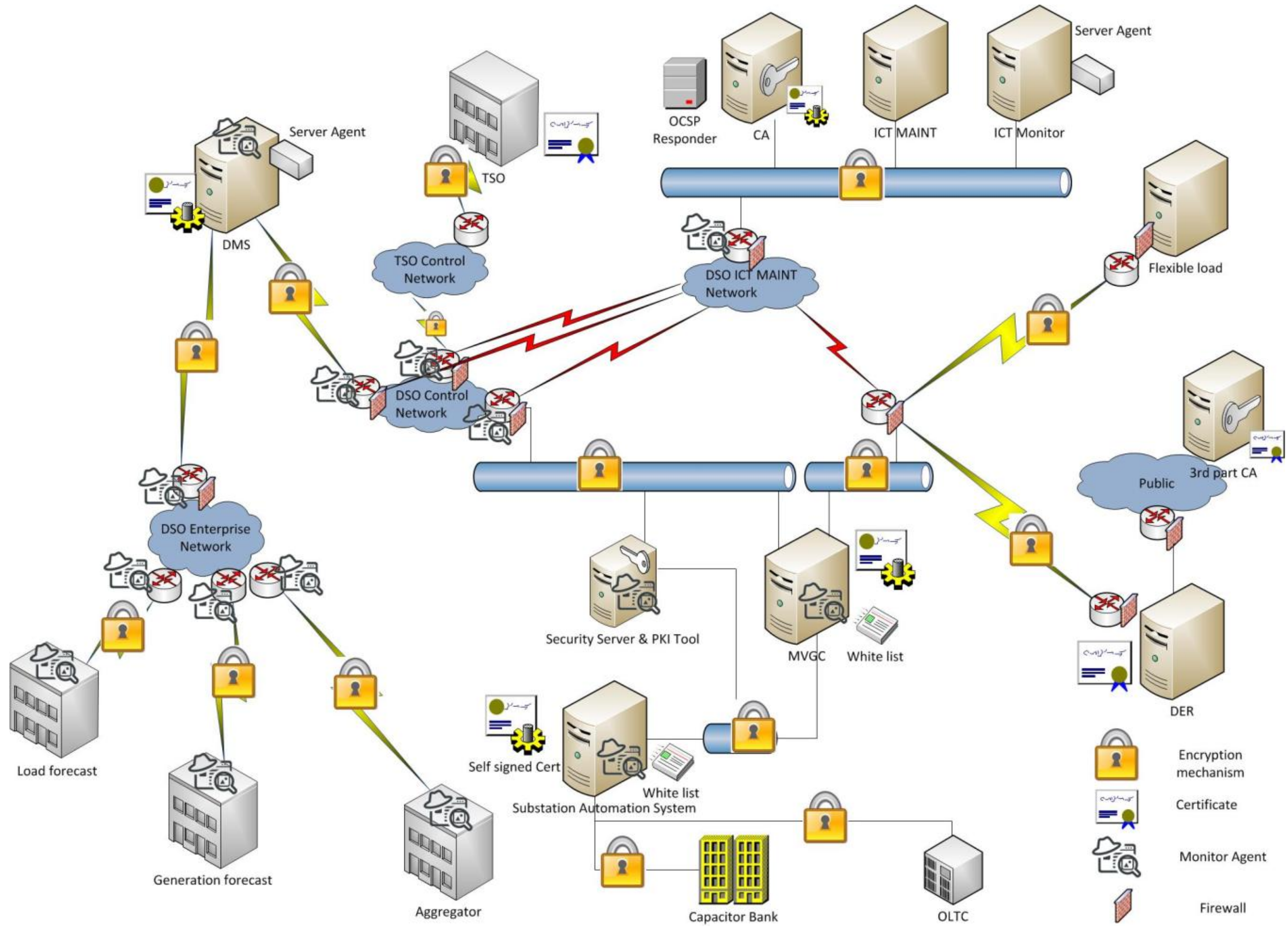


Figure 38: DER control use case – Secure architecture

Some issues related to the implementation of the solution standards are reported in the DER control policies described in [57].

8.4.5 Conclusion

Selected standards are not mandatory for the present use case but have been identified as relevant to cyber security for the DER control use case. Use case stakeholders now have a narrowed set of standards from which to start to put in place cyber security recommendations through their prioritized actions plan program. An example implementation of such measures has been given in section 8.4.4.

9 Privacy Protection

Privacy is a major concern of the European Commission and Member States, and - driven by the deployment of smart meters – is of increasing interest to consumers and society generally. This section on privacy essentially addresses the need to protect consumers from breaches of data protection, while other sections focus on security concerns. In the context of smart grid security, it should be noted that vulnerable customers may be particularly impacted e.g. by security breaches involving the misuse of remote functionality.

This section looks at current and expected data protection regulation with a view to setting a context and base line for further work by Member States and other authorities on the subject.

SGIS has considered privacy from various angles.

First, an analysis of the upcoming European Commission data protection regulation [31] has been performed in order to understand the possible impact on stakeholders.

Second, the 'Data Protection Impact Assessment' (DPIA) template of the Smart Grid Task Force Expert Group 2 and the SGIS toolbox as presented in [6] has been applied on four member states regulation in order to improve the risk assessment of privacy in the SGIS toolbox. The DPIA will be recommended by the European Commission for usage by operators to identify the risk concerning privacy protection.

Third, available and upcoming technologies for privacy protection by design have been evaluated.

It is essential for a successful deployment of smart grids that the technologies involved have the confidence and trust of citizens. Trust will be facilitated by the legislative framework at EU and national level described below, together with the use of the DPIA template and the introduction of the latest privacy enhanced technologies and standards.

9.1 Analysis of expectable Effects of the proposed EU General Data Protection Regulation

An integral aspect of the analysis is the expectable impact of the currently discussed General Data Protection Regulation (GDPR) [31] for the Domain of Smart Grids. If being put into force, this GDPR will be the most important legislative provision with regard to data protection (or, as often referred to, ‘privacy’) across Europe and it will undoubtedly have effects for Smart Grids in a multitude of ways. It is the aim of the following analysis to anticipate these effects as far as possible in order to consciously take them into account in subsequent discussions and suggestions on the future design of European Smart Grids.

If the GDPR will be finally adopted, it will be directly applicable in all member states of the EU. Therefore, all relevant data protection requirements set forth by the final version of the GDPR should be duly taken into consideration while establishing and adapting technical standards for Smart Grids in order to ensure compliance of the resulting standards with the GDPR. This comprises the main principles of data protection (e.g. in Art. 5 GDPR) as well as other planned provisions of possible relevance for Smart Grid standardization, e.g. ‘data protection by design and by default’ (Art. 23 GDPR) or ‘security of processing’ (Art. 30 GDPR).

An in depth analysis of the effects of the GDPR or specific provisions is, however, neither within the scope of this document nor is a detailed analysis possible by now, since the GDPR is not yet adopted and thus not available in its final version. This document is based on the current draft version of the GDPR [31] and it is assumed, that the GDPR will eventually be put into force.

Besides ensuring that citizens’ fundamental rights are not infringed in the course of establishing Smart Grids, consideration of the GDPR in an early stage could also prevent all stakeholders from running into avoidable conflicts and frictions between the regulatory framework on the one and the developed and employed technologies and processes on the other hand. Last but not least, a non- or insufficient consideration of the GDPR during the ongoing standardization activities would also decrease trust in the respective technologies among citizens (even further) and could thereby impede the overall acceptance of Smart Grid technologies.

In order to provide a sufficiently exhaustive but at the same time well-focused overview of the most important regulatory changes that are to be introduced by the GDPR with particular regard to the Smart Grid domain, the analysis is structured as follows: The most fundamental changes in European data protection legislation that are coming along with the establishment of the GDPR are sketched in brief. In particular, significant changes are to be expected with regard to the fundamental legislative construction of the GDPR as opposed to the current regulatory framework based on the Data Protection Directive and with regard to the role of national sector-specific regulations.

Due to the significantly changed role of national regulations currently governing data protection aspects of (Smart) Grids, the different national approaches and regulatory givens with regard to data protection in (Smart) Grids are then analyzed and juxtaposed using the examples of five member states: France, Germany, The Netherlands, Great Britain and Sweden. As it becomes clear, current national givens are highly diverse in several matters including the general approach to the handling of and the responsibility for personal data, the used processes of market communication on the basis of these data and the employed regulatory instruments governing Smart Grid data protection in general.

Based on these country-specific analyses, foreseeable regulatory uncertainties and conflicts that will conceivably emanate from the significantly changed interplay between GDPR and national regulations are identified. Without being properly addressed soon, these uncertainties and conflicts will in all likelihood give rise to the adverse effects mentioned above. Therefore, some recommendations are developed in order to sketch the way towards a comprehensive and conclusive regulatory framework governing data protection aspects of Smart Grid Communication that properly addresses the societal needs for smarter energy solutions as well as the citizens' individual rights for data protection.

9.1.1 Comparison of Current vs. Potential New Regulatory Regime

At present, the European data protection framework consists of several provisions with different scopes and addressees. Of further relevance for this WP is mainly the European Data Protection Directive 95/46/EC (EDPD) [54] that will in all likelihood be replaced by the planned 'General Data Protection Regulation' [31] (GDPR) in the future. The most substantial and most evident difference between these provisions is the change in the type of legal instrument chosen by the European Commission: the directive currently in force will be replaced by a regulation.

As stated in Art. 288 TFEU [55], directives are '*binding, as to the result to be achieved, upon each member state to which it is addressed, but shall leave to the national authorities the choice of form and methods.*' In other words, directives need to be transposed into national law in order to take (full) effect. Member states are obliged to adopt national laws in accordance with the directive, but have a certain leeway when it comes to details, a fact that may lead to differences between the resulting national provisions. The requirements set forth by directive 95/46/EC were implemented by the member states into more or less detailed country- and sometimes also sector-specific laws on the protection of personal data. Germany, for example, has already adopted detailed sector-specific regulations for the smart metering sector.

A regulation like the planned 'General Data Protection Regulation', in turn, *'shall have general application. It shall be binding in its entirety and directly applicable in all Member States'*, as stated in Art. 288 TFEU [55]. Therefore, the planned GDPR will directly affect all activities within its material and territorial scope and will probably leave little or no room for national data protection laws. National data protection acts like the German 'BDSG' or sector-specific national regulations, for example several provisions of the German 'Energy Industry Act' dealing with data protection especially for smart metering, will widely be overridden by the planned GDPR, see Figure 39.

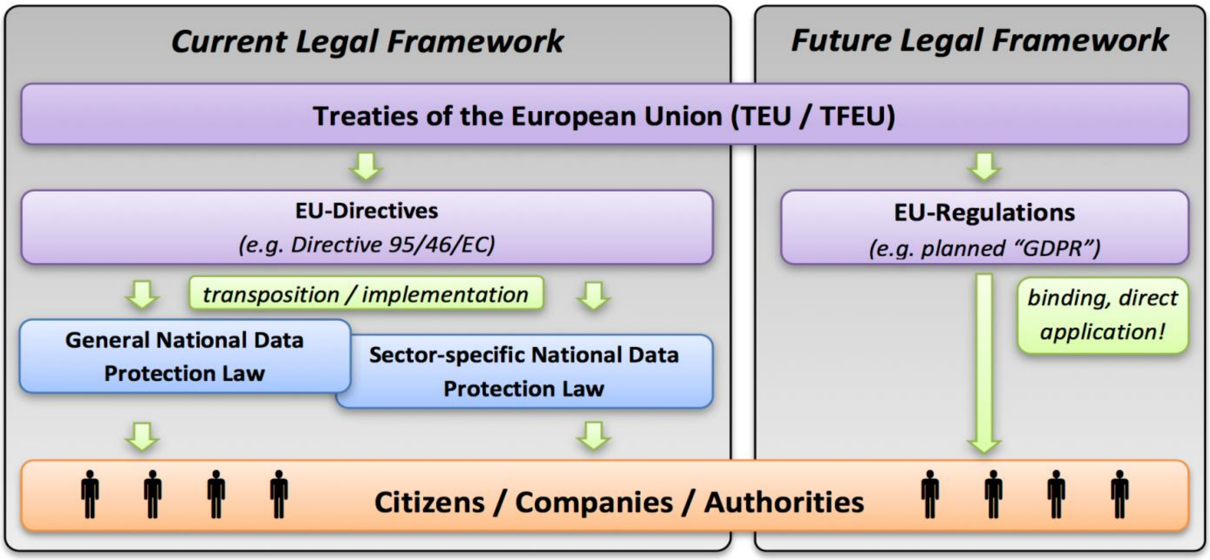


Figure 39: Logical Structure of Data Protection Legislation under Current vs. Upcoming Regime

Because the GDPR is (partially) based on the existing directive, the general principles of data protection remain mostly the same as under the current regulatory framework (e.g. '*data minimization*', '*purpose limitation'*, etc.). But since the regulation will be directly applicable, it has to be more comprehensive and has to regulate more details than the existing directive, which only defines the objectives to be reached by national legislation, while leaving it up to the Member States to regulate the details. Specifications of terms and procedures that are even more detailed than those directly provided within the upcoming regulation may be uniformly determined by the commission through delegated acts and implementing acts according to chapter X of the GDPR draft. To establish common procedures, the European Data Protection Board (composed of national data protection supervisory authorities, Art 64-72 GDPR) will be entrusted with the task of issuing guidelines, recommendations and best practices. The important further differences and similarities between the current data protection directive and the upcoming GDPR are summarized in Table 6.

Topic	Directive 95/46/EC	General Data Protection Regulation
Direct / Indirect Application	Not directly applicable, transposition and implementation into national law necessary.	Union-wide direct application.
Effects on national law	• Member states are obliged to adapt their national legislation to the directive • National laws must be interpreted in accordance with the directive	• National law is overridden by the data protection regulation • Within the scope of the GDPR there is little or no room for national regulations, except the GDPR authorizes national legislation
Main principle	'ban with permit reservation': Data shall not be processed without legitimation (Recital 30 EDPD, Art. 7, Art. 8 EDPD; Recital 31 GDPR, Art. 6, Art. 9 GDPR)	
Other important principles of data protection	Other important principles of data protection like *lawfulness*, *fairness*, *transparency*, *data minimization*, *purpose limitation etc.* remain mostly the same as under the already existing Data Protection Directive (compare Art. 6 EDPD, Art. 5 GDPR).	
Possible legitimation for processing of data (Art. 7 EDPD; Art. 6 GDPR) *[Underlined sentences are the ones especially relevant for carrying out smart metering]*	a) Consent of the data subject. b) Necessity for the performance of a contract to which the data subject is party. c) Necessity for compliance with a legal obligation to which the controller is subject, either according to union law or the respective national law. d) Necessity to protect the vital interest of the data subject e) Necessity to carry out a task in public interest or in exercise of official authority f) Necessity for the purpose of legitimate interest of controller/third party which are not overridden by interests of fundamental rights and freedoms of data subject	
Risk analysis	Member states have to determine, which processing operations present specific risks for the data subject. These processing operations shall be checked in advance by the supervisory authority (Art. 20 EDPD).	Controllers/processors shall carry out and document a risk analysis (Art. 32a GDPR), if processing presents specific risks, further obligations may result (e.g. mandatory conduction of a DPIA or designation of a data protection officer).
Data protection impact assessment (DPIA)		Assessment of the impact of the envisaged processing operations on the rights and freedoms of the data subject (Art. 33 GDPR). Periodically documented compliance review (Art. 33a GDPR).

Topic	Directive 95/46/EC	General Data Protection Regulation
Prior Consultation of supervisory authority / data protection official	Notification of the supervisory authority before carrying out any wholly or partly automatic processing operation (Art. 18, 19 EDPD) Exemptions in Art. 18 (2) EDPD. All processing operations shall be publicized. (Art. 21 EDPD).	Necessary if DPIA indicates a 'high degree of specific risk' or data protection officer / supervisory authority deems prior consultation necessary because of certain high risks for the rights of data subject (Art. 34 GDPR).
Further Notification of the supervisory authority or data subject		Data breach notification: in case of a data breach the data subject and supervisory authority have to be informed (Art. 31, 32 GDPR).
Data Protection by Design and by default **Security of processing**	Data processor is obliged to 'implement appropriate technical and organizational measures to protect personal data'. (Art. 17 EDPD). No detailed specifications of these measures.	Data processor is obliged to implement appropriate technical and organizational measures to protect personal data (Art. 23 GDPR) and to ensure security of processing (Art. 30 GDPR). More detailed specifications of how to fulfill these obligations are given compared to the existing EDPD.
Rights of the data subject	The data subject has the right to get information about the controller and the data processed (Art. 10, 11, 12 EDPD), and the right to obtain from the controller the rectification, erasure or blocking of data if the processing does not comply with the provisions of the directive (Art. 12 (b) EDPD).	The controller has to provide standardized information policies (Art. 13 a GDPR). The data subject has the right to get information about the controller and the data processed (Art. 14, Art. 15 GDPR), and has the right to obtain from the controller rectification of inaccurate data (Art. 16 GDPR) and erasure or restriction of processing in certain cases (Art. 17 GDPR). More detailed specifications of how to fulfill these obligations are provided.
Right to data portability		Depending on the type of data and the way it was obtained, Art. 15 (2a) GDPR grants the data subject the right to obtain a copy or to directly transfer data from one controller to another.

Topic	Directive 95/46/EC	General Data Protection Regulation
Sanctions and liability/damages	Member states are obliged to adopt provisions dealing with liability/damages (Art. 23 EDPD) and other sanctions (Art. 24 EDPD) for cases of data protection infringements.	Liability/damages are regulated (Art. 77 GDPR). Member states shall lay down rules concerning penalties (Art. 78 GDPR). Supervisory authorities will be empowered to impose various sanctions, reaching from warnings to very high fines of up to 100.000.000 EUR or 5% of the worldwide turnover of an enterprise (Art. 79 GDPR).

Table 6: Existing Data Protection Directive vs. Upcoming General Data Protection Regulation

As Table 6 shows, there are only minor differences in matters of the main principles of data protection between the current data protection directive and the upcoming GDPR. The newly introduced provisions and the minor changes of existing ones not specific to smart grids and will – with certain effort – be manageable for the affected parties. They shall therefore not be considered in detail herein. Nonetheless, changes are to be expected with regard to the role of the above-mentioned sector-specific regulations. These sector-specific regulations are, within the boundaries set by the Data Protection Directive, currently of national nature across Europe and shall therefore be exemplarily analyzed for five member states.

9.1.2 Country-specific Analyses

In order to achieve comparability of the different national givens, the following analyses follow a recurring scheme. For each considered member state, some foundational facts (e.g. the ownership or the location of smart meters, the rollout status etc.) are provided, followed by some general remarks necessary to understand the specific national model. On this basis, it is laid out which party gets what data under which circumstances in the respective national model and, finally, which regulatory requirements exist for the customer access to data.

This report summarizes the way in which in some states with the ownership and the data from smart meters is handled. The Member States are responsible for implementation of EU and local law and regulations. This report does not intend to provide any opinion on the smart meter environment implementation in the Member States.

Whenever the concept of ‘data ownership’ is used in the course of this analysis, this shall by no means be understood as ‘ownership’ in the legal sense but rather as an intuitive concept referring to the right to decide and determine – within well defined boundaries – who is granted access to individual meter data.

9.1.2.1 France

Ownership of Smart Meter: Theoretically granted to the DSO (typically ERDF) by local public authorities, but due to cost Smart Meters are claimed as its property by the DSO.
Ownership of Smart Meter Data: Final customer (i.e. Data subject)
Location of majority of Smart Meters: Private meters may be either in private premises or often in public parts of apartment buildings. Some meters for private households may be accessible from the street.
Smart Meter Rollout Status: For electricity, 2 pilot experiments done (300.000 units), plan to deploy 3 Million units by 2016 and to replace the existing 35 million units by 2020. Plans to deploy smart gas and water meters are also in discussion.
Smart Meter Communication capabilities into the home: The possibility to connect an in-home display to the smart meter was not initially planned. There is a serial interface for remote customer information, but the intention is to charge consumers for opening the possibility to monitor daily consumption.
Who has primary control of data: The DSO (ERDF)

General Remarks:

The French data protection authority, the CNIL, has expressed concerns and recommendations for the DSO to ‘bring serious guarantees’ on the privacy and security of the data. ERDF answered that all consumption data are ciphered (according to DLMS/COSEM specifications) to protect the system from external attacks, and that any collected information is considered private and therefore transmitted to other parties in accordance to applicable confidentiality requirements, under CNIL supervision.

Currently, consumer associations complain against a system conceived in the exclusive interest of grid managers and suppliers, even more so as consumers will be charged for accessing their own daily consumption data for monitoring purposes.

Data Protection Regulation in full: Who gets data under what exact circumstances:
Data from the meter are transmitted to the contracted energy supplier by the DSO. The French smart metering system is intended to serve for asset management (e.g. fault detection), administration of metering data and automatic service delivery to customers and suppliers alike (e.g. when subscribing a new contract after moving in).

Regulatory requirements for consumer access to data (i.e. informative bills, website, ...) and steps taken to achieve:
Access to metering data is subject to the following articles of sector-specific French law:

- Art. 79 of Law 2010-788 from 12 July 2010, called ‘Grenelle II’ on national engagement for the environment. It implies a state decree superseding Art. L 224-1 of the ‘Code de l’Environnement’ to require utilities suppliers to periodically communicate a statement of energy consumption to final consumers, including comparison data, recommendations to reduce consumption and a financial assessment of potential savings.

- Art. 18 of Law 2010-1488 from 7 December 2010, code of consumption organizing the new electricity market and entitling consumers with free access to their consumption data. A decree following advice from the CRE (French Energy Regulator) and a consumption instance clarifies the methods for accessing such data. In 2011 the CRE recommended to enable access via a website financed by fares charged by the DSO, using a personal access code.

9.1.2.2 Germany

Ownership of Smart Meter: Metering Point Operator (see below)
Ownership of Smart Meter Data: ‘Data sovereignty’ is primarily attributed to the customer and will be technically enforced through ‘Smart Meter Gateways’ (see below)
Location of majority of Smart Meters: Either inside single houses or flats or in a central place (e.g. in the basement) of multi-family houses.
Smart Meter Rollout Status: At the moment primarily bulk consumers. Currently established legislation will, however, prescribe smart meters and ‘Smart Meter Gateways’ (SMGWs, see below) at least for customers above 6.000 kWh/year as well as for new buildings and in case of substantial renovations. The limitation to households above 6.000 kWh/year instead of an 80%-rollout was just confirmed by a cost-benefit analysis following Annex I, No. 2 of the EU-Directive 2009/72/EC.
Smart Meter Communication capabilities into the home: SMGWs must provide interfaces to the ‘home area network’ (HAN) for: 1) In-home-displays; 2) Service technicians; 3) proxy functionality for ‘controllable local systems’.

General Remarks:
First of all, Germany is currently establishing regulations that will make the installation of an additional technical device, the ‘Smart Meter Gateway’ (SMGW), between MID-conformant meters and wide area communication networks mandatory. Furthermore, Germany introduced the additional market role of the ‘Metering Point Operator (MPO)’ who is responsible for installing, operating and (in all likelihood) administrating meters and the newly introduced SMGWs. By default, the DSO assumes this role but customers can freely choose other MPOs from the market.

Data Protection Regulation in full: Who gets what exact data under what exact circumstances:
The German Energy Industry Act (‘EnWG’) sets forth several sector-specific provisions dealing with the protection of metering data. More general provisions contained in the German ‘Federal Data Protection Act’

are replaced/overwritten by these specific rules. § 21g EnWG entitles MPOs, DSOs, TSOs and suppliers to collect, process and use personal data originating from smart meters. All other third parties need the written consent of the consumer. Additionally, §21g provides an exhaustive list of purposes metering data may legally be used for by these parties (measuring energy consumption, implementing variable tariffs, preventing fraud, etc.). Personal metering data may only be collected and processed if actually *'necessary'* for achieving one of the purposes mentioned in this list, depending on the customer's contract and other factors (*'principle of data minimization'*). Currently, customers may, however, not even at their own free will give their consent to the collection or use of 'their' data for purposes not explicitly covered by the above-mentioned list of legitimate purposes (e.g. future efficiency services, unforeseen innovations).

Anonymization and pseudonymization are required if feasible at reasonable effort given the respective use case and protective purpose. Further regulations ensuring data protection within the common and mandatory backend processes of the liberalized energy market (as defined by the Federal Network Agency) are not provided.

Currently, data is collected by the MPO, who transmits it to the local DSO who, in turn, transmits personal measurement data to the respective supplier and aggregated data to the TSO ('chained communication'). Future legislation may, however, lead to different market processes with any market actor collecting data directly from the SMGW ('star-shaped communication').

Regulatory requirements for consumer access to data (i.e. informative bills, website, ...) and steps taken to achieve:
Customers have a right for access to 'their' metering data, which may be granted via local or web-based interfaces. Suppliers have to provide customers with monthly usage and billing information.

9.1.2.3 Netherlands

Ownership of Smart Meter: DSO
Ownership of Smart Meter Data: The consumer is the owner of the smart meter data.
Location of majority of Smart Meters: Always inside a house or apartment.[2]
Smart Meter Rollout Status: At the moment primarily bulk consumers. The grid operators are installing smart meters at households. However this is still in project phases. The definitive roll out of smart meters is planned from 2015 and further.
Smart Meter Communication capabilities into the home: On the smart meter a 'P-1 port' exists which is intended for display purposes in home. The P-1 port can also be used for connection to an external facility (e.g. external provider/web interface) to show the metering values.

General Remarks:
The most important rules in the Netherlands for recording and using personal data have been set forth in the Wet bescherming persoonsgegevens (Wbp; Dutch Personal Data Protection Act). This act was unanimously adopted by the Dutch Senate on 23 November 1999 and accepted by the Dutch Congress on 3 July 2000. The act came into force on 1 September 2001.

The Wbp relates to every use – 'processing' – of personal data, from the collection of these data up to and including the destruction of personal data.

Data Protection Regulation in full: Who gets what exact data under what exact circumstances?
In the Netherlands the consumer is the owner of the (personal) data. This means in the context of smart energy and smart meter data, the grid operator is the data controller and collects the (personal) data on behalf of the consumer. In the Netherlands every household, every building has a unique European Article Number (EAN-code) for its water, gas and electricity meter. In principle the DSO knows the address and the EAN-code. The smart meter ID is connected to the EAN-code.

Following an approach of self-regulation, sector-specific concretions of the general data protection law with regard to the handling of smart meter data are laid out in the *'Code of Conduct for the Processing of Personal*

[2] In the Dutch situation the house (flat, apartment etc.) is an independent unit which has a meter. In some cases such as a shop and a semi-separated house in one building might have 1 meter for the entire building or 2 meters for the shop and the house separated.

Data by Grid Operators in the context of installation and management of Smart Meters with private customers'. According to this code, smart meter data is first sent to the DSO. The DSO then sends the meter data to the service provider that the customer has a contract with.

Regulatory requirements for consumer access to data (i.e. informative bills, website, ...) and steps taken to achieve:
Customers have a right for access to 'their' metering data, which may be granted via local or web-based interfaces. Suppliers have to provide customers with monthly usage and billing information. The customer:

- Gets the smart meter in his or her home, which the grid operator can read remotely.
- Can (whether or not the meter allows remotely readings) readout the meter to get insight in detailed information, which gives a reflection of energy consumption and energy production.
- Can resist the smart meter (opt-out):
- May refuse initial placement.
- Or may (if the meter is already installed) make the smart meter witless (when no measurement data can be readout remotely).
- Gives permission for the smart meter (opt-in).
- Gives permission to the energy supplier or Independent Service Provider (ISP), and then the energy supplier or ISP is authorized to retrieve the measurement data.
- Can ask for priority placement of the smart meter.

Can use smart meter information for an understanding of the energy consumption and energy production, for instance for energy saving purposes.

9.1.2.4 United Kingdom

Ownership of Smart Meter: The most common model is for meters to be owned by investment banks and then leased to the relevant energy supplier.
Ownership of Smart Meter Data: Smart meter data is owned by the customer.
Location of majority of Smart Meters: There is no standard location for meters. Around 30% of gas and 16% of electricity meters are housed in external meter boxes. The remainders are mostly in entrance halls, adjoining garages, under stairs, etc.
Smart Meter Rollout Status: There is no formal 'start date' for the roll-out but the Government has the power to introduce one if necessary, by requiring all new and replacement meters to comply with the smart specification from a specified date. There is, however, an end date of 31^{st} December 2020. The roll-out is supplier-led and is being progressed at different speeds by the various suppliers. Most suppliers are installing trial volumes only and are expected to increase steadily over the next two years, with a rapid acceleration in late 2015. In Q4 2015 the central Data and Communications Company (DCC) will become operational, delivering full interoperability between suppliers and, through the Communication Service Providers, supplying the communications hubs that link metering equipment via the HAN and provide communications over the WAN.
Smart Meter Communication capabilities into the home: Three regional Communications Service Providers (CSPs) are responsible for the network that carries messages between the suppliers and the meters. The CSPs also provide the communications hub to energy suppliers. The hub provides connectivity between the gas and electricity meters, the in-home energy monitor and the optional Consumer Access Device; the consumer access device can provide metering data direct to the consumer and may also support smart appliances and home automation. Communications between devices will be based on ZigBee and DLMS open standards, initially at 2.4GHz and later at 868MHz for devices located at greater distance from the communications hub.
Who has primary control of data: Smart meter data is owned by the customer but controlled by the energy supplier. The DCC is the data processor.

General Remarks:
Without prejudice to general legislative provisions contained in the Electricity Act, the Data Protection Act and the Energy Licences & associated Energy Codes, the Smart Energy Code will establish sector-specific obligations on code users regarding data protection and access to consumption & personal data**.**

Data Protection Regulation in full: Who gets data under what exact circumstances:
Meters will record consumption data every 30 minutes but customers must give their explicit consent for suppliers to be able to access data at this level of detail. Suppliers are unable to access more than one

reading per month unless they explain to customers what the consumption data is used for, the frequency of reading that they propose to collect, and how the customer can express their preferences. If the customer does not express a preference within 7 days, the supplier can obtain one reading per day. Each year, suppliers must remind customers how much consumption data they are accessing and the customers can change that level of access at any time.

Regulatory requirements for consumer access to data (i.e. informative bills, website, ...) and steps taken to achieve:
There is an expectation that smart meter readings will be used to support accurate billing. This is a clear area of benefit for all parties and is being monitored by the Department for Energy & Climate Change (in terms of the number of estimates sent). Information on bills must include a comparison with consumption for the same period in the previous year, a summary of the energy used for the preceding 12 months, and a projection of costs for the forthcoming year.

Currently, there is a consultation in progress over the implementation in the UK of Articles 9 and 10 (2) of the EED (2012/27/EC) on smart metering. This is expected to result in an obligation on suppliers to advise customers that they are entitled to daily consumption data for a period of up to two years, which can be accessed via the internet or through a meter interface device.

9.1.2.5 Sweden

Ownership of Smart Meter: Network owner
Ownership of Smart Meter Data: Smart Meter Data in Sweden is not explicitly regulated. Presumably, customers own the data, however network owners and electricity suppliers have control over the data.
Location of majority of Smart Meters: On the outside wall in a meter cabinet or in the basement of the apartment building.
Smart Meter Rollout Status: 100% completed as of 2009. Rollout was completed in order to provide consumers accurate bills. Therefore communication capabilities or other program types were not taken into account. At the beginning of 2012 a new regulation was released. It allows customers to have smart meter which can communicate into the home, if they want or in the case of new build.
Smart Meter Communication capabilities into the home: This will depend on the region, and when the meters were rolled out. However there is no standardized level of communication into the home. As of today the consumer can request a meter change and ask for feedback capabilities. How many consumers know of this right is another question.
Who has primary control of data: The network owners and electricity supplier

General Remarks:
Explicit smart meter data protection regulation does not really exist in Sweden so far. Issues related to meter data have not as yet been inspected in matters of data protection.

Data Protection Regulation in full: Who gets data under what exact circumstances:
The general regulatory provisions for data protection are stated in the law on personal data (personuppgiftslagen, PUL). According to this law, suppliers and network owners can process customers' data for regular operation activities, for example, for invoicing. If they gather more data than those which are needed for regular operation activities or need/want to perform unusual activities (for example, to sell data) they would need additional customer consent. Furthermore, the PUL states that the customer has the right to know at least once a year what data the company has related to the customer. If monthly and/or hourly measurement data is to be considered as personal data, which seems plausible, this data is subject to PUL and requires a certain treatment like customer consent and possibility to withdraw consent.

Regulatory requirements for consumer access to data (i.e. informative bills, website...) and steps taken to achieve:
Sometimes customers have the option view their own consumption, but it is not obligatory for suppliers to present or provide this kind of information.

9.1.3 Expectable Effects of the New Data Protection Regulation on Smart Grids

As it can be seen from the above analysis, national sector-specific regulations with regard to data handling and, in particular, data protection within the energy domain currently differ significantly across Europe, ranging from smart metering being conducted on the basis of general data protection laws alone, over self-regulatory 'Codes of Conduct' being agreed upon by the various stakeholders (like in the Netherlands), to explicit and exhaustive legal regulations (like in Germany). Given this fact and the more general findings on the fundamental change in legal 'construction' outlined at the beginning of this chapter, the expectable effects of the forthcoming General Data Protection Regulation for the Smart Grid domain shall now be identified and discussed. In particular, this refers a) to the legitimation that is necessary for any collection, processing and use of personal data, b) to the future role of sector-specific procedural and technical safeguards laid out in the respective sector-specific regulations and their interplay with the GDPR, and c) to the interrelations between the GDPR and the overall aim of establishing a single European market in the energy / Smart Grid sector.

9.1.3.1 Legitimation of Data Processing

As outlined in Table 6, possible legitimation for processing[3] personal data are basically the same under the existing Data Protection Directive and in the upcoming General Data Protection Regulation: Processing of personal data (to which at least individual meter readings will belong in most cases) is legitimate only if at least one of the following conditions (set forth in Article 6(1) GDPR) is fulfilled:

a) <u>Consent of the data subject</u>.
b) <u>Necessity for the performance of a contract to which the data subject is party</u>.
c) <u>Necessity for compliance with a legal obligation to which the controller is subject, either according to union law or the respective national law</u>.
d) Necessity to protect the vital interest of the data subject
e) Necessity to carry out a task in public interest or in exercise of official authority
f) Necessity for the purpose of legitimate interest of controller/third party which are not overridden by interests of fundamental rights and freedoms of data subject

Of these, the first three general options (underlined above) can be identified as being of significant relevance for the field of Smart Grids. Besides individual consent by the data subject (that is, the person that the personal data relates to, i.e. the energy customer), processing of smart meter data is legitimate (even without individual consent being given) if the data is unquestionably necessary for carrying out a contract with the data subject[4]. An energy contract based on highly variable tariffs, for example, might therefore legitimate the collection of meter data in comparably high resolution. The option of processing meter data being legitimated by the necessity for compliance with a legal obligation could, for instance, gain relevance when a national regulation obligates an actor within the energy market to process meter data in short intervals and forward them to other actors on the market or when certain national legal obligations (e.g. of network management or balancing in the liberalized market) can only be fulfilled with the respective actor having such personal data at hand.

Under the current regulatory regime, this third option (and, to a certain extent, the second one) is filled with live by the national sector-specific regulations. As different models of responsibility sharing among the different market roles, different technical approaches and different processes of data handling for market communication necessarily lead to different kinds of meter data being needed by the respective actors for fulfilling their legal duties, for example, this leads to different national legitimacy situations across member states. While it might, due to legal obligations, be legitimate for the DSO to collect personal meter data in high

[3] In line with the definition from Art. 4(3) of the current GDPR proposal, 'processing' shall herein be understood as 'any operation or set of operations which is performed upon personal data or sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, erasure or destruction'.

[4] Even in these cases, the Directive 95/46/EC provides for transparency of the consumer data that has been collected. As mentioned in 10.1.1, the data subject has the right to get information about the controller and the data processed (Art. 10, 11, 12 EPDP), and the right to obtain from the controller the rectification, erasure or blocking of data if the processing does not comply with the provisions of the directive (Art. 12 (b) EPDP). The upcoming 'General Data Protection Regulation' that will most likely replace the Directive 95/46/EC EPDP, also provides for requirements for transparency of consumer data that has been collected. As mentioned in table 5, the data subject has the right to get information about the controller and the data processed (Art. 14, Art. 15 GDPR), and has the right to obtain from the controller rectification of inaccurate data (Art. 16 GDPR) and erasure or restriction of processing in certain cases (Art. 17 GDPR). Depending on the type of data and the way it was obtained, Art. 15 (2a) GDPR grants the data subject the right to obtain a copy or to directly transfer data from one controller to another.

resolution in one member state, this might be unnecessary and thus primarily illegitimate in another one. In the end, this leads to a non-uniform set of ultimately effective legitimacy provisions even under a strictly uniform General Data Protection Regulation – something that should originally be counteracted with a uniform and directly applicable General Data Protection Regulation. This thwarting of the original aim behind establishing a uniform General Data Protection Regulation across Europe notwithstanding, the upcoming regulation would thus at first sight have no ground-breaking implications with regard to the legitimacy of the processing of personal smart meter data as opposed to the current status quo.

9.1.3.2 Sector-Specific Procedural and Technical Safeguards

Beyond the mechanism of legitimation, however, a multitude of sources for legal uncertainty, conflicts and frictions can be identified for the development of Smart Grids in the light of the upcoming GDPR. In particular, this refers to sector-specific provisions on procedural as well as technical safeguards. As it can be seen from the country-specific analyses above, member states have established different kinds of sometimes highly sophisticated regulatory frameworks (including self-regulatory ones like in the Netherlands and strictly legalistic ones like in Germany) to achieve the best possible balance between citizens' data protection rights and the highly specific requirements of Smart Grids under the regime of a liberalized energy market. The procedural and technical safeguards provided within such frameworks take sector-specific data protection risks and functional necessities into account and typically (partially) replace/overwrite the default mechanisms provided by general data protection laws. In accordance with the legal model of the current Data Protection Directive, the current national, sector-specific regimes are thus different sector-specific transpositions and implementations of the rather generic requirements for procedural and technical safeguards defined by the current Data Protection Directive. National sector-specific data protection regulations do thus, at least to a certain extent, stand 'in parallel' to the respective general national data protection laws (see also Figure 39 above).

Under the model promoted with the forthcoming General Data Protection Regulation, such 'parallel' implementations will only be possible to a very limited extent. Indeed, Art. 6(3) of the current GDPR proposal allows for separate and specific national specifications on 'processing measures and procedures, recipients' etc. for the case of processing being legitimated by a legal obligation the controller is subject to – albeit only '[w]ithin the limits of [the GDPR]'. Given this confinement, it is at least unclear to what extent such national laws may actually specify procedural and technical safeguards that are to be employed *instead* of the ones prescribed in the GDPR. In the best case, this yet unanswered question will only lead to uncertainties, frictions and delays in the broad establishment of Smart Grids. In the worst, it will prescribe largely inappropriate or even impedimental procedural and technical obligations to be applied to the highly specific domain of Smart Grids.

Even more important, however, is the confinement of this opportunity for defining specific 'processing measures and procedures, recipients', etc. to those cases where the processing of personal data is necessary for fulfilling a legal *obligation*.[5] This does, however, not cover alternative legitimations like the necessity for the performance of a contract or the individual consent, which will presumably form the basis for most processes involving personal meter data in future Smart Grids. In these cases, only the rather generic requirements for procedural and technical safeguards defined by the current Data Protection Directive apply. This stands in stark contrast to the fact laid out above that the energy market and, in particular, the upcoming establishment of Smart Grids call for more specific regulations on procedural and technical safeguards that pay regard to the specific circumstances, risks and requirements of this field. Up to now, these have been accounted for and brought into balance within the different national sector-specific regulations. Giving up this well-established mechanism of sector-specific provisions therefore seems highly disputable and should only be done after due consideration.

9.1.3.3 Overall Aim of a Single European Market in the Energy / Smart Grid Sector

Finally, there is an overarching argument that will in all likelihood gain significant relevance for the Smart Grid domain in the foreseeable future: Generally speaking, the establishment of Smart Grids and the striving towards a single European market in this area require trans-European interoperability – in matters of technologies as well as regulatory frameworks for market communication to facilitate innovative products and

[5] To be exact, it also applies to cases legitimated by a necessity 'for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller', but this option is of less relevance here.

services. Only with traditional as well as yet unforeseeable innovative energy services being marketable across national boundaries, with energy suppliers not being factually confined to territorial boundaries and with extensive interoperability of devices and facilities throughout Europe will we be able to establish a single European energy market on the level of end-customers and to unlock the full potential of Smart Grids.

In line with CEN/CENELEC/ETSI's striving towards technological standardization and interoperability, this also necessitates interoperability in matters of data protection regulations. From this perspective, it is therefore consequent and highly welcome that currently existing national data protection regulations are to be replaced by unified European provisions. Without such a unified regulatory framework for smart grid communication, a single internal energy market would be illusive. Given the above discussions on the importance of sector-specific regulations, it does, however, become obvious that similar mechanisms are also required in the context of a European General Data Protection Regulation.

The GDPR should therefore be augmented by at least basic sector-specific regulations on data protection within the Smart Grid domain which basically serve the same purpose as the respective national regulations do today: take the particular preconditions of Smart Grids into account and employ tailored regulatory provisions that ensure a better and more appropriate balance of circumstances, risks and requirements than general data protection regulations do. Besides technical specifications and the sector-specific adaption of procedural questions already covered by the GDPR itself, such a sector-specific augmentation could, in particular, also include harmonized provisions on the necessary market communication and thereby extend the concept of 'data protection by design and by default' from the level of devices and protocols to the level of processes.

In any case, lifting the well-established instrument of sector-specific data protection regulations from the national to the European level would allow to combine the best of both worlds: A single European Smart Grid market on the one hand and an appropriate comprehension of sector-specific givens, risks and requirements on the other.

9.2 Impact Assessment of Use Cases in Four Member States

An impact assessment analysis has been carried out on use cases in four member states: France, Germany, Netherland and United Kingdom. The approach has been via the DPIA tool-set and via the SGIS methodology. Findings are reported in this chapter.

Data protection includes both data security and data privacy. Breaches of data security threaten the operation of the smart grid, and where they also involve personal data, they may also compromise the privacy of individuals.

9.2.1 SGIS Toolbox Methodology

The SGIS Risk Impact Assessment Methodology ('toolbox') as set out in Annex B of the SGIS report from last year [6] considers SGIS risks under a number of categories and sub-categories, one of which is data protection. These subcategories have been defined according to the type of impact e.g. energy supply, energy flow, population and each is linked to five risk impact levels ranging from low to highly critical (e.g. networks under 1MW, grids from 1MW to 100MW, 100MW to 1GW, 1GW to 10GW and over 10GW). This approach is primarily of value in considering the risk and impact of security breaches threatening the operation or integrity of the smart grid infrastructure.

9.2.2 Data Protection Impact Assessment Template

A similar risk/impact philosophy is adopted in the Data Protection Impact Assessment template[6], which considers personal data as an asset and seeks to quantify risks to that data in terms of those risks with a high severity and likelihood, risks with a high severity and low likelihood, risks with a low severity and high likelihood and risks with a low severity and likelihood. An extensive list of data protection threats is given together with examples on how these may apply to the smart grid situation.

[6] The Data Protection Impact Assessment (DPIA) template can be found on request by the SGTF EG2.

9.2.3 Data Security and Data Privacy

There are difficulties in assessing the risks associated with data protection as a whole – an approach that works for data security does not work so well for data privacy. Data privacy breaches only indirectly threaten the smart grid infrastructure/operation; their primary impact is on the individual whose privacy has been infringed. The potential loss of consumer confidence in smart grids which may result if breaches are widespread or not addressed, and the consequent risks to smart grid benefits e.g. to consumer participation in demand response measures. Thus, while it is possible to consider the smart grid infrastructure as the responsibility of the network operator concerned, privacy is the responsibility of all actors involved in the control or processing of personal data. Moreover privacy has so far been considered only in terms of three impact levels – no personal or sensitive data, involved unauthorized disclosure or modification of personal data, unauthorized disclosure or modification of sensitive data. The scale/severity of the breach has not been further quantified as yet, except possibly in terms of the potential financial penalty.

To reflect the differences in data security and data privacy and to facilitate the use of the SGIS toolbox, it is suggested that data protection is separated into its security and privacy aspects in the toolbox, i.e. the categorization cannot be applied for data privacy, see Figure 40.

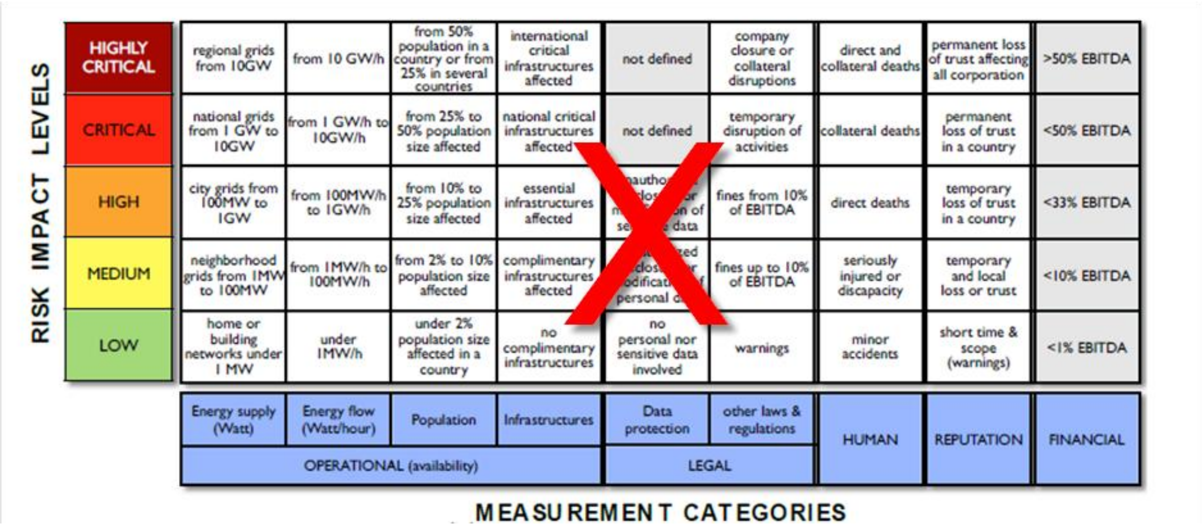


Figure 40: Risk impact levels are not applicable for data privacy

In the view angle of **data security**, there would be no change from the current toolbox approach. Security can be seen in terms of the effect of breaches on the integrity and operation of the overall smart grid, and therefore can be viewed from the perspective of the stakeholders concerned. Cyber-security threats and weaknesses can be considered, drawing on the questions in the relevant sections of the DPIA template. These external threats can then be analyzed and the results captured using the current risk assessment matrix, which considers the likelihood and extent of impact on a five-point scale, and computes an overall risk assessment for the smart grid system as a whole, based on 'likelihood x impact'.

In the view angle of **privacy protection**, privacy breaches mainly threaten the interests of the individuals whose data is involved, rather than critical infrastructure. However the extent of a breach is not always easily quantified in terms of e.g. the number of customers affected. Moreover the financial impact is likely to be dependent on the financial penalties considered appropriate by the regulatory body, and this in turn may depend on the nature of the breach, whether reasonable internal controls were in place and whether there have been previous breaches. Depending on the actor concerned, the consequences may largely be reputational for the organization found to have been in breach. Thus applying the 'likelihood x impact' approach in the SGIS toolbox is much less appropriate for privacy.

It should also be noted that privacy is likely to be of concern to many more actors than just the TNO/DNO and each actor will need to do its own DPIA, whereas typically only the network operator will use the SGIS toolbox.

9.2.4 Generic Data Privacy Threats

Looking more closely into the DPIA template, the generic data protection threats in the DPIA template often relate to the possible vulnerability of the smart grid to security breaches and fears about data integrity. The main elements of the DPIA template relevant specifically to individual privacy are found in sections 3.4.1.2 and 3.4.1.4 of the DPIA template, where detailed explanations can be found. These DPIA privacy elements are:

- Unlimited purpose
- Collection exceeding purpose
- Incomplete information
- Combination exceeding purpose
- Missing erasure policies or mechanisms; excessive retention periods
- Invalidation of explicit consent
- Undeclared data collection
- Lack of granting access to personal data
- Inability to respond to requests for subject access, correction or deletion of data in a timely and satisfying manner.
- Prevention of objections
- Lack of transparency
- Insufficient access control procedures
- Insufficient information security controls
- Non legally based personal data processing
- Insufficient logging mechanism
- Breach in security implementation
- Access to data that was not intended (not necessary for the purpose of collection)
- Unjustified data access after Change of Tenancy (CoT) or Change of Supply (CoS).
- The protection of data is compromised outside the European Economic Area (EEA).
- Smart Grid data is processed by Government Departments, Local Authorities and Law Enforcement Agencies without a legal basis.
- Inability to execute individual rights (inspection rights)
- Individuals should be provided with easy means to get insight in the data collected (e.g. by a unified user access rights).
- Lack of quality of data for the purpose of use

Rather than considering each in terms of likelihood and impact, the above DPIA privacy elements would be used as a checklist, to allow the organization concerned to carry out a periodic DPIA self-assessment (e.g. with a red/amber/green rating) of the extent to which the organization was already compliant or appropriate safeguards were in place to minimize the risk of each potential breach.

For both security and privacy, a key actor is the DSO (or whoever is the main data processor), who will be a major user of the SGIS toolbox [6] as it affects the security of the smart grid infrastructure. For privacy, it is similarly proposed that the DSO takes the main elements of the DPIA template relevant to privacy and regularly carries out a self-assessment of its compliance in each area, as described above, instead of the 'likelihood x impact' analysis of security risks.

This self-assessment (which could be expressed in some form of red/amber/green summary table) would provide the DSO with a picture of the extent to which the organization had appropriate controls in place.

Since the elements of the checklist are of varying significance, no single overall rating is appropriate, whether calculated mechanistically e.g. from considering 'likelihood x risk' or from averaging the elements, nor would it simply reflect the worst-ranked area. The purpose of the self-assessment is to provide a broad indication of where weaknesses may exist which could affect the organization's risk of infringing the privacy rights of the individual. It would sit alongside the security evaluation using the SGIS toolbox [6].

9.3 Analysis of Emerging Privacy Technologies

This chapter provides an overview of modern privacy preserving technologies that can benefit smart grid use cases which require the use of personal data. The primary focus is on emerging technologies that may not necessarily be available on the market today, but are practical and developed enough to have a realistic perspective to be used in the field in the future.

For any meaningful analysis, it is necessary to get a precise definition of the use cases; only then is it possible to identify technological approaches and determine the required adaption to fit into use case requirements. We identify two main sources for privacy sensitive data for the smart grid, smart meters and electric vehicles. In the case of electric vehicles, the end use case is fairly clearly defined – intelligently manage the charging of a fleet of electric vehicles and provide accurate billing. It is, however, not very well defined how the final architecture will look like, and what level of data is required to support the use cases. Nevertheless, we can identify existing technologies, such as ‘*anonymous attestation’*, that have well proven their practicality in related areas.

In the case of smart metering, the situation is vice-versa; while the smart metering architecture is reasonably well defined, while the data generated by a smart meter might be used for a large number of different use cases. Here, some technologies have evolved – such as ‘*verifiable private computation’* and ‘*homomorphic aggregation’* – that can address a large number of use cases, especially load balancing, benchmarking, fraud detection, and billing.

9.3.1 Privacy by Design

Privacy by Design is a concept developed by Ontario’s Information and Privacy Commissioner, Dr. Ann Cavoukian. In the 1990s she began to address the ever-growing and systemic effects of Information and Communication Technologies and large–scale networked data systems concerns. The Privacy by Design framework states that companies should promote consumer privacy throughout their organizations and at every stage of the development of their products and services in an effort to better protect consumers.

- Proactive not reactive; preventative not remedial
  - The Privacy by Design approach is characterized by proactive rather than reactive measures. It anticipates and prevents privacy-invasive events before they happen. PbD does not wait for privacy risks to materialize, nor does it offer remedies for resolving privacy infractions once they have occurred – it aims to prevent them from occurring. In short, Privacy by Design comes before-the-fact, not after.

- Privacy as the default setting
  - We can all be certain of one thing – the default rules! Privacy by Design seeks to deliver the maximum degree of privacy by ensuring that personal data are automatically protected in any given IT system or business practice. If an individual does nothing, their privacy still remains intact. No action is required on the part of the individual to protect their privacy – it is built into the system, by default.

- Privacy embedded into design
  - Privacy is embedded into the design and architecture of IT systems and business practices. It is not bolted on as an add-on, after the fact. The result is that it becomes an essential component of the core functionality being delivered. Privacy is integral to the system, without diminishing functionality.

- Full functionality – positive-sum, not zero-sum
  - Privacy by Design seeks to accommodate all legitimate interests and objectives in a positive-sum “win-win” manner, not through a dated, zero-sum approach, where unnecessary trade-offs are made. Privacy by Design avoids the pretence of false dichotomies, such as privacy vs. security, demonstrating that it is possible to have both.

- End-to-End Security – full lifecycle protection
  - Privacy by Design, having been embedded into the system prior to the first element of information being collected, extends throughout the entire lifecycle of the data involved, from start to finish. This ensures that at the end of the process, all data are securely destroyed, in a

timely fashion. Thus, Privacy by Design ensures cradle to grave, lifecycle management of information, end-to-end.

- Visibility and transparency – keep it open
    - Privacy by Design seeks to assure all stakeholders that whatever the business practice or technology involved, it is in fact, operating according to the stated promises and objectives, subject to independent verification. Its component parts and operations remain visible and transparent, to users and providers alike. Remember, trust but verify.

- Respect for user privacy – keep it user-centric
    - Above all, Privacy by Design requires architects and operators to keep the interests of the individual uppermost by offering such measures as strong privacy defaults, appropriate notice, and empowering user-friendly options. Keep it user-centric.

Privacy by Design continues to gain traction as the recommended solution for companies releasing new products or services. Many (energy) companies often struggle with transforming these high-level principles into an actionable system of confirming that their practices adequately protect consumer privacy. By adopting the data protection impact analysis (DPIA) of Expert group 2, energy companies get the necessary help to comply with privacy legislation and to protect their customers. A draft EU mandate on the management of Privacy by Design from the European Commission has been issued.

9.3.2 Privacy in a Smart Grid

There are two major sources of privacy relevant data in the future Smart Grid; the data generate by smart meters and the data generated in the context of electric vehicles. In the future, the introduction of smart homes will generate an additional source of private data, though the data flows and use cases for this concept are still under development.

The collection of this fine-grained data has led to privacy concerns [32][33]. Lisovich and Wicker [33] reported results of collaboration between researchers from law and engineering. They argue that there ‘exist strong motivations for entities involved in law enforcement, advertising, and criminal enterprises to collect and repurpose power consumption data’ [2, p. 1]. For example, burglars could use the data to determine occupancy patterns of houses to time break-ins. Marketing agencies could identify specific brands of used appliances, which could then be used for targeted advertising, and employers and insurances can identify unwanted behavior patterns. In summary, while there are many useful applications of smart meter data, such as energy saving, network monitoring and tailor-made energy rates, the privacy of this kind of data needs to be ensured.

It has been argued, that approaches relying on policy alone, may prove inadequate to provide a sufficient level privacy and that technological methods that enforce privacy by virtue of ‘strength of mechanism’ need to be employed [34]. Indeed, a number of such technological approaches, so-called privacy-enhancing technologies, have been suggested to remedy the (perceived) loss in privacy and still enable functionality on a broad basis. In this, such mechanism are more business-friendly than a pure policy approach – while policy can only set constraints in data usage, modern privacy enhancing technologies can enable functionality that otherwise would not be possible from a legal or a consumer acceptance point of view.

9.3.3 Privacy Enhancing Technologies

Privacy Enhancing Technologies (PETs) is a term for a group of technologies to enable using data for a specific business case, without requiring using privacy critical data. The technologies most interesting for our cases are the technologies that can be used to handle data in a privacy preserving ways (as opposed to, for example, anonymous communication networks). A number of basic approaches have been taken to this end in the past:

Anonymization/Pseudonymization: A classical approach to privacy is to strip the data of all personally identifiable information, and process the anonymous (and thus no longer privacy critical) data. While this approach has been widely used in the past, it also has shown its limits; several academic papers have demonstrated that smart-grid data can be de-anonymized relatively easily.

Trusted Computation: Using Trusted Computation it is possible to give the data owner some assurance that the data handler can use the data only for the authorized use cases, and will not be able to access the data for unauthorized use cases or accidentally reveal privacy sensitive user data**.** In this approach, a trusted service provider or hardware module receives the data, performs the computation in question, and returns the result to the data handler. Trust can be obtained in different ways; the device may be a specially certified hardware device, it might be remotely verifiable, or it can be locally in the possession of the consumer and thus be under their control.

Encrypted Computation: There are different technologies available to perform some computations on encrypted data, and only decrypt the result of the computation. This way, data only needs to leave the consumer's domain in encrypted form, and never may be decrypted as an individual data item; only the results of the computation are available. While generic schemes to allow encrypted computations are prohibitively expensive in terms of computation and communication resources, specialized schemes (e.g., to aggregate data, or to prove that a user performed a payment without revealing their identity) can be done extremely efficiently.

Perturbation: By adding small errors to the data, it is possible to allow the data handler to get roughly correct results (which increase in quality if more data is added, either by aggregating over more input sources or over time), while masking the details of the data. A special case of this is to use extra energy consumption (e.g., the battery of an electric vehicle) to not only add noise to the data, but to the actual consumption.

Zero Knowledge Proofs: A zero knowledge proof is a cryptographic construct that allows the checker to demonstrate knowledge of a secret without revealing the secret itself; in the more advanced forms, it allows the checker to demonstrate that they performed a computation correctly, without needing to reveal the details of the computation. In the smart grid context, this approach is mostly used for billing. In smart metering, the main use case would be to compute a bill on the users' side, and then demonstrate that the boll was computed correctly without revealing the inputs (i.e., detailed consumption values); in the electric vehicle scenario, this can be used to implement a form of anonymous credits the consumer can buy wherever they want, and then use to recharge their cards without revealing their identity. A special form of zero knowledge proofs are anonymous credentials, which allow a user or a system to prove that they have a certain property (e.g., a car has a certified meter on board), without revealing any additional information.

In general, it is helpful for an advanced Privacy Enhancing Technology if the use cases are clearly defined; once it is known what data the data handler really needs, it is often possible to find a way to provide that data without requiring privacy sensitive data in the first place (for example, to bill an electric vehicle, one does not need the vehicles' identity; what one does need is assurance that the money has been paid, and a way to identify the vehicle in case of dispute at a later state). In those cases, PETs can provide a positive sum result – the data quality increases (as data can be used that would otherwise not be legally available, and consumers have no incentive to fight the scheme), and consumers are assured of their privacy to be protected.

9.3.4 Privacy Enhanced Technologies in Smart Metering

A smart meter is a device usually installed on the premises of individual households, which can measure electricity consumption as well as other data related to energy quality and report it to the head-end. A smart meter usually also can receive commands such as price updates, and may actively interfere with electricity delivery (e.g., through the 'remote off switch', which is installed in some countries and one of the minimum functionalities as defined by the EU). Smart meters also can act as a gateway, both to other meters (e.g., gas and water) and to household appliances. Use cases for smart metering data vary widely; however, some main use cases have evolved already that seem to get some general agreement: billing, consumer engagement, demand response, benchmarking, load monitoring and forecasting, fraud and failure detection, dispute handling and settlement, line monitoring and power quality.

To protect the privacy in a smart meter environment privacy enhanced technologies in combination with Privacy by Design is important. The next version of the Toolbox, now called SGIS Framework, gives direction how to assess privacy risks and refers to the data protection impact assessment of Expert group 2.

An overview of privacy enhanced technologies for smart metering is given in the Annex B. Here an evaluation of these technologies:

- De- anonymization: Through advances in statistical methods as well as increasing availability of additional data sources, anonymization is becoming increasingly vulnerable to de- anonymization techniques. This does create a legal challenge, as it is also increasingly unclear when data can be considered truly anonymous, and when it does fall under data protection regulation. While anonymization will likely remain an important tool, it needs to be used with great care, and should be replaced if better approaches are made available.

- Data expansion: If data is encrypted way that allows for advanced techniques, such as homomorphic encryption, most schemes require an encryption that increases the message size. In few cases, this can cause a bandwidth issue. Even if that is not the case, larger data packets can cause issues in integrating into existing communication stacks, which often are not prepared to handle dynamic data length. In some cases – such as aggregating through masking – it is possible to keep the data length constant, which greatly eases integration.
- Resource complexity: Cryptographic schemes tend to create a computational, communication and memory overhead, which the smart meters and head end system need to be able to absorb. While some meters may be so close to their limit that this poses a serious problem, implementation tests [43] have shown that the effort required by resource optimized protocols is well inside the possible limit
- Scalability: The privacy enhancing technologies must be able to scale to a system of millions of meters, without significantly adding potential for failure. In most cases, however, it is straightforward to partition the smart metering chain into fairly small units that can then – from the point of view of the privacy enhancing technology – operate independently of each other. A challenge for smart device owners is management of cryptographic keys. Encryption systems in the past were not developed to support millions of devices. Hundreds, sometimes a few thousands were the maximal amounts of devices. Driven by smart device owners, suppliers are now developing systems that can handle large numbers of devices the energy sector uses. Pilots have been successfully implemented. However it is a new market for the cryptographic industry. There will still be plenty of challenges available to good systems before a large scale roll-out of smart devices will be possible.
- Number of required participants: In the case of aggregation protocols, it is not clear what group size is needed to protect individual data; estimates start at 7, and have no upper limit. While protocols can be designed to be configurable in this respect, it is important to get some solid guidance of the protocols are to be used in practice.
- Fault tolerance: As with most security technologies, an increase of security can make error handling harder. Extra measures may be required to perform advanced error handling in case of communication- or device errors, though those measures seem to be quite manageable.
- Realistic adversary model: As argued above, the adversary model has a significant impact on the complexity of the solution. It is important to provide a model that covers all realistic failure cases, without requiring an unreasonable level of protection that renders the system unusable.
- Economic feasibility: Finally, a privacy enhancing technology must be economically feasible, i.e., integrate well with legacy hardware, cause minimal overhead, and avoid causing additional risks. Ideally, they can even add economic value, by enabling new use cases or increasing the data quality for existing ones, e.g. through allowing for higher-frequent measurements than would be possible under normal circumstances.

In summary, there are a number of approaches that can strike a balance between required functionality and privacy requirements in smart metering. However, as discussed above, other requirements need to be addressed before the start of standardization efforts. The most important requirements include low resource complexity, economic feasibility and scalability and the conformance with existing protocols. Primarily, approaches that have already been subjected to thorough real-world testing should be considered for standardization in the near future. For example, aggregation protocols based on masking have been shown to fulfill the abovementioned requirements and real-world tests have been conducted [43]. Other approaches, for which the fulfillment of some requirements still needs to be determined, are worth to be observed further. Still another class of approaches, where it is clear at this point in time that important requirements cannot be fulfilled, can be disregarded for standardization purposes.

9.3.5 Privacy Enhanced Technologies in Electric Vehicles

The other primary source for private data in the smart grid is the use of electric vehicles. Electric vehicles will pose a substantial challenge to grid management, as they can add a load to the grid that it cannot handle – both in terms of total energy available (e.g., when all cars start charging simultaneously after work), and in terms of line capacity. To mitigate this problem, some intelligent charging system is required than can schedule charging times in a way to meet all users' demands and optimize the load on the grid. In addition to load balancing, electric vehicles also need additional billing functionality, to ensure that the electricity bill is paid by the person owning the car, rather than the owner of the socket.

The main privacy concerns here are:

- Location Privacy: Where did a car recharge, how long did it stay there, how much did it drive between charges
- Behavior Privacy: Does the owner of the car frequently come home at late hours, does she drive the distance from home to work in a time that requires speeding, etc.
- Planning Algorithms: It is unlikely that the grid is able to support charging of all cars at the same time; therefore, some scheduling needs to be done. Ideally, the schedule would take into account the users behavior – a person who regularly gets up at 10 a.m. can get different schedules than one who repeatedly uses the car at 3 a.m. The input needed for those plans (and thus indirectly the plans themselves, too) should be considered highly private information.

There are several different models for billing on electric vehicles, each of which requiring a slightly different approach. If the meter is build into the vehicle, privacy can be achieved using *anonymous credentials* – the vehicle proves to the socket that it is a properly metered device, and the socket the delivers energy trusting the device to take care of all billing issues. There are some details here – e.g., the socket may need to know which retailer a vehicle belongs to to do its own billing, and some revocation mechanism needs to be in place to identify corrupted devices. All this is already readily available [UProof, TCG, IRMa]. If metering is done outside the car, anonymous credentials are not enough; rather, it is necessary to bill the owner of the vehicle, or provide enough information to the owner of the charging station to forward the bill. The most obvious technologies to this end would be variations of anonymous payment systems, which allow a user to buy credits which can then be spent in an anonymous way.

In the case of scheduling, the situation is somewhat more complicated. As opposed to most other use cases, there is no clear definition on what data – there is an unlimited number of factors that influence an owners user charging requirements, and it is not clear what is needed to provide predictions with a sufficient accuracy. One pragmatic solution is to ask the owners themselves to provide times at which they need their cars charged, and use only those schedules to derive a charging schedule. While it is possible to compute such a schedule in a privacy preserving way under encryption, it is probably sufficient to simply leave the computation locally, and never store individual schedules; some information will leak through the resulting schedule, though that is probably impossible to prevent.

Another option is group signatures for the metering device. In this scenario the location of the metering device remains unknown while the signature can still be verified. For disputes such schemes include a trusted third party which can trace the location only in those cases.

Given that the requirements depend strongly on the way the charging is implemented, it is hard to pin down specific PETs for the electric vehicle use case; in the end, the privacy enhancing technologies will have to be developed in parallel with the smart vehicle architectures. Independent of the final architecture, however, we can identify some of the technologies described above that can be used to address privacy in charging of electronic vehicles:

Anonymous credentials (a special form of the zero-knowledge proof) can allow a vehicle to authenticate to a charging station as a genuine vehicle. This way, a trust relationship between the vehicle and the charging station can be established without revealing the identity of the vehicle in question unless a dispute needs to be resolved. In addition, this allows for a vehicle to prove that it has an internal meter that properly handles billing, which would no longer require the charging station to store data for billing purposes.

More advanced versions *of zero-knowledge proofs* can be used for anonymous payment; a vehicle can proof that it did pay the proper amount to the charging station, without revealing who at this point.

Using a *trusted third party* for payment processing and/or scheduling allows to easier anonymise data for example, the entity computing the schedule does not need to know the identities of the vehicles involved, and a separate billing entity can translate pseudonymous payment data into real payments. While this approach is the pragmatically easiest, it is also the most vulnerable one to accidental data leaks if not implemented carefully. De-pseudominization might be possible using metadata (the vehicle charging in front of my house most evenings is likely linked to me), and all relevant data is available in some database, though in a distributed form.

Trusted computing platforms in the home and the charging stations allows to execute planning algorithms that rely on personal data, while assuring the users that the raw data will not be used for different purposes. There are different proposals on how this can be implemented in practice, primarily use of multi-party computation or hardware security modules.

10 SGIS Framework (Former SGIS Toolbox)

During the SGIS Toolbox update discussions an improved approach has been defined which is more focused on the necessity to perform risk analysis than to have a general framework for risk analysis.

What is the goal of a risk analysis? Who will use the results? Security measures were chosen during the risk analysis. What was the motivation behind the choice of these security measures and why did the risk analyst choose these specific security measures?

The new approach changes the SGIS Toolbox into a methodology that could be used to create “Awareness” for management and/or decisions makers. Management is responsible for funding the implementation of security measures. To be able to make the correct decisions, management needs a clear view of the risks and consequences of incidents.

The factors transparency and traceability are then very important to perform the new risk analysis method. Based on these factors the following steps of the new approach have been developed:

0. **Preliminary Assessment**
    a. Define scope
    b. If it appears that personal related data is used in the use case, in a separate step Data Protection Impact Assessment (DPIA) has to be performed.
1. **SGAM Mapping**
    a. The use case has to be mapped on the Smart Grid Architecture Model
2. **Threats Mapping to the Use Case Assets**
    a. Identify threats, risks and vulnerabilities and compare these to the ENISA threat landscape (Threat catalogue) in ENISA/EG2 “Proposal for a list of security measures for smart grids” report [8].
3. **Define a Risk Mitigation Plan**
    a. Identify mitigating measures and link these to the risks
4. **Define Traceability**
    a. Be able to explain why a specific security measure is chosen to mitigate a defined risk
5. **Define a Mitigation Plan.**
    a. Compare incident costs to budget and costs of mitigation measures.
6. **Define an Action Plan**
    a. Define actions to be taken
    b. Classify on priority and budget.

It appeared that the ‘SGIS Toolbox’ name was creating expectations regarding a ready to use tool that would have identified security levels and which calculated ad hoc security measures to mitigate threats and risks.

The new approach defines the steps to be taken to perform a smart-grid related risk analysis. This new approach can be perceived as a framework. Therefore choice was made to rename it ‘SGIS Framework’.

More details on SGIS Framework steps can be found in Annex D.

11 Conclusion

The dimension of Smart Grids and variety of technologies used reflect the heterogeneity and complexity to be considered to secure Smart Grids. Smart Grid security and standards evolve at the same pace as Smart Grids develop.

Smart Grid as a critical infrastructure needs varying weights of confidentiality, integrity and availability as essential requirements. To support the development of Smart Grid in Europe, the SGIS has considered various levels to address the need for a sustainable deployment.

Security standards are widely available today. Enhancements are needed to support Smart Grid deployment in particular in the direction of interoperability. Additionally, with increased awareness such as in the area of privacy protection, there are mandatory needs to address gaps in security who haven’t been considered before. As a conclusion, security standards are available and can be applied, but it needs continuous effort to incorporate existing and new technologies, architectures, use cases, policies, best practice or other forms of security diligence

For the daily use, the complexity of Smart Grids requires a more simplified approach by having recommendations and guidelines at hand which are mapped to standards for implementation guidance on cyber security for related stakeholders. This report is striving into this direction and took the first steps by providing standardization landscapes, recommendations and guidance for security implementation.

Smart Grid stakeholders can use proposed guidance and/or SGIS Framework risk assessment approach to identify how to implement proposed European set of recommendations for their related use cases. Both approaches can be valuable depending on their objectives or cyber security maturity level.

It should be noted, that cyber security is a continuous effort and cannot be handled in one shot only. Neither can be a 100 % security achieved.

Cyber Security is a continuous process, as both, cyber security measures and forms of attacks are constantly evolving.

Annex A – Additional Information on DER control use case

Figure 41 provides the information exchanges among the components at the upper control zones, while Figure 42 reports the communication flows within the substation and with DERs.

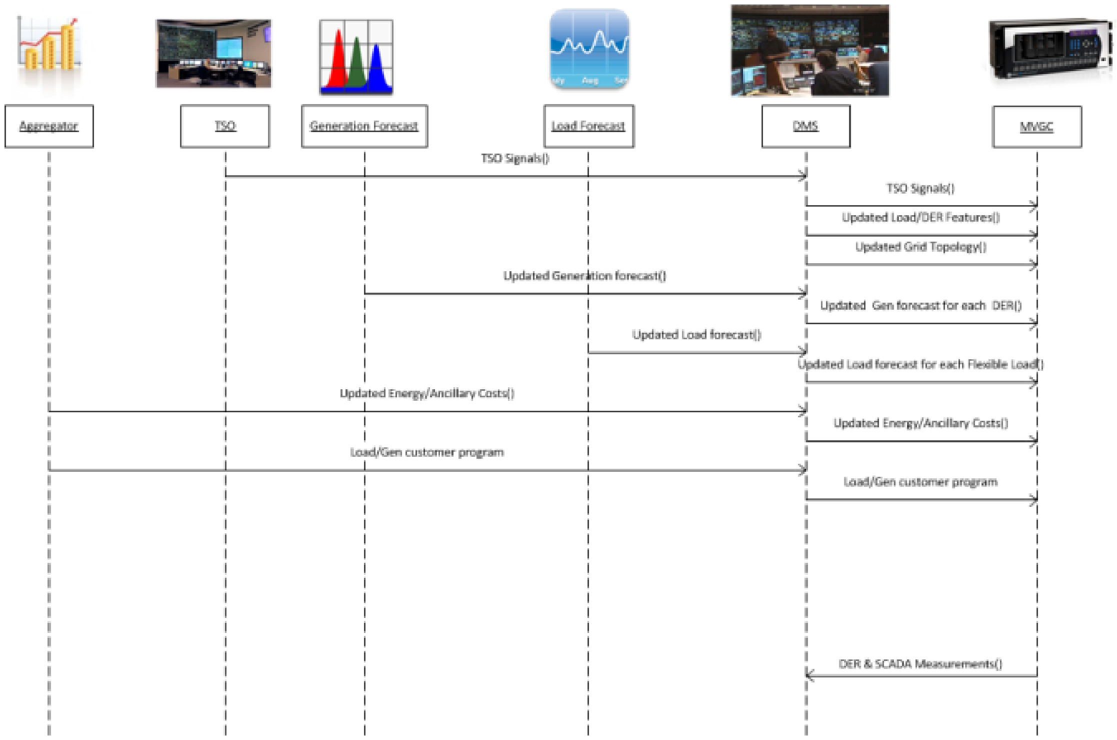


Figure 41: DER control use case - Sequence Diagram

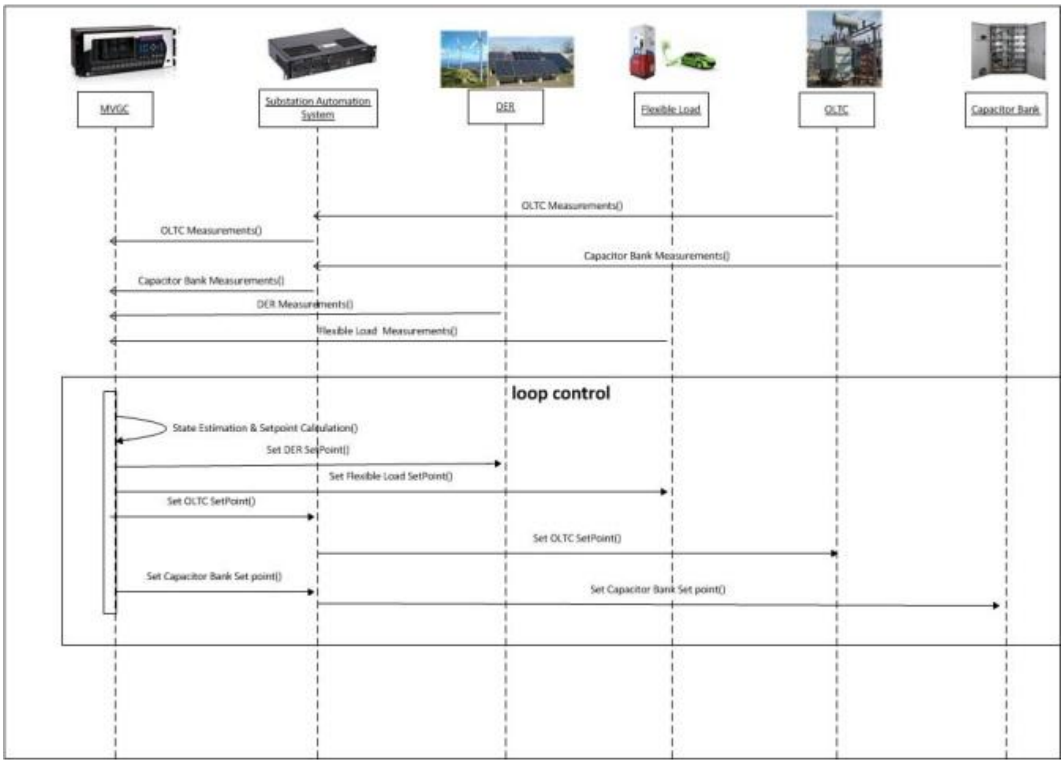


Figure 42: DER control use case – Inter & Intra substation information flows

Annex B – Overview on Privacy Enhanced Technologies for Smart Metering

A number of technological privacy-enhancing technologies (PET) have been proposed for smart metering. Recent surveys have been conducted by Jawurek et al. [34] and Erkin et al. [35]. In the following, we give an overview of the types of approaches, without aiming at listing or detailing all existing approaches, and point out properties that may prevent real-world use or at least prove a challenge should these approaches be deployed in the real world.

In general, there is a close relation between the resolution in which the load data is available and the extractable information. As not all extractable information is necessarily privacy-sensitive, a comprehensive and formal account on how extractable information, such as type or brand of appliance, relates to personal information, and how such data items could be combined by a potential attacker. To date there is no formal investigation on what information can be extracted by which method at what resolution, and what kind of threat this may represent to an individual's privacy.

One important aspect to consider is the trust model. In an extreme case, all systems not under full control of the user are considered to be malicious, and the system is to assure that privacy is preserved under all circumstances. In a more pragmatic way, one can assume that data handlers may be flawed, careless, and subject to insider attacks, but do not behave outright criminal. Even then, though, it is crucial to minimize the incentive to cheat – a system that intrinsically prevents data from being collected in the first place is preferable to a system that generates large amount of data that need to be protected by internal policy, as the later system is substantially more vulnerable to loss of data through manipulation or carelessness.

Anonymization/Pseudonymization

The classic approach, and the only approach that is widely used in the real world at this point in time, is anonymization or pseudonymization of smart metering data. The consumption data and the personal data are split and stored separately.

Methods for de-anonymization are a major threat for these types of approaches. It has been shown that even after anonymization or pseudonymization, data items can still be attributed to the individual that originated them. For example, in the area of social networks, it has been shown by Backstrom et al. [36] that anonymization is somewhat difficult, because individual users can be traced based on structural cues evident in the network even after anonymization. Jawurek et al. [37] show that de-anonymization can also be done in the smart grid user domain. This structural traceability is a problem for schemes that rely on anonymization or pseudonymization only without the use of additional encryption.

Simple Aggregation

Simple aggregation tries to hide data related to individuals by aggregating over a number of households, e.g., all households in a neighborhood are networking (NAN). For example, Bohli et al. [38] propose a privacy scheme in which high resolution smart meter readings are aggregated at NAN level and only the aggregate is sent to the utility. They introduce two solutions both with and without involvement of trusted third parties.

A possible issue with this kind of approaches is the number of households required. If a NAN only has a small number of households, traces of individual data can still be identified in the aggregate. Furthermore, these approaches often assume complete trust between the households in a NAN, as the data is aggregated in a hop-by-hop manner. If one participant should start an attack, the schemes can be easily compromised. Introducing a dedicated aggregator in each NAN only moves the issue to a different part of the system, as in this case, the aggregator needs to be afforded complete trust by all parties. In general, the adversary models which are used to analyze PET in smart grids often exclude malicious attackers. Most authors evaluate their approaches in honest-but-curious adversary models.

Multiple Resolutions

Due to the inherent link between load data resolution and privacy, splitting the load data into a variety of different resolutions, each associated with different authorization levels, has been proposed by a number of contributions.

For example, the anonymization scheme proposed by Efthymiou and Kalogridis [39] is based on two different resolutions: a low resolution that can be used for billing purposes, and a high resolution that allows further investigation. This scheme employs a trusted third party escrow service. Engel [40][41] proposes the use of the wavelet transform to generate a whole cascade of different resolutions. The approach is combined with a conditional access scheme: each wavelet resolution is encrypted with a different key, allowing differentiated access management. By using a suitable wavelet filter, it is ensured that the sum of the original data is preserved over all resolutions.

For application in the real world, the requirements of use cases with respect to data resolution need to be clarified. It could turn out that most of the more interesting use cases (except for billing), such as distribution system monitoring, may require high resolution data, rendering a cascade of lower and medium resolutions useless. Furthermore, many of these use cases may require the data in (near) real-time. Using the wavelet transform to create a number of resolutions is at odds with this requirement, as a sufficient amount of data needs to be available for transformation.

Masking

Masking relates to approaches which add numerical artifacts, e.g., random sequences to the original load data to obfuscate individual contribution. The added artifacts are constructed in such a way that they cancel each other out upon aggregation. The aggregator can therefore combine the data of all participants to create an accurate aggregation, but cannot gain access to individual contribution. For example, Kursawe et al.[42] propose such an aggregation protocol, which compared to other approaches has the advantage of relatively low computational complexity.

For real-world use, the issue of creating the random secret shares among each group of participants needs to be addressed. In [42] this is achieved by either selecting a leader among the participants, or by relying on a trusted third party to create the final shares (which exhibit the property of cancelling each other out) from the individually generated random shares. Again, this relates to the assumed underlying adversary and trust models; in reality, it is likely that the meter operator will take the role to manage groups, with some form of assurance and certification to protect against abuse. Another issue, as Jawurek et al. [34] point out, is fault tolerance: if a single participant fails (e.g., due to a hardware error), the whole aggregate is affected. As pointed out in [43], this can be handled by minimizing the group sizes covered by the protocol, and by recovery protocols on the head end side.

Differential Privacy

As Dwork [44] puts it, differential privacy, roughly speaking, ‘ensures that (almost, and quantifiably) no risk is incurred by joining a statistical database’. Adding or removing an item from the database will not (or only to a very limited degree) affect the result of statistical computations. This is commonly achieved by the distributed generation of noise which is added to the individual data contribution.

Shi et al. [45] propose a scheme for adding random noise to time series data using a symmetric geometric distribution. An advantage of this scheme is that the participants need not trust each other, nor rely on a trusted aggregator. As another example, Acs and Castelluccia [46] obscure individual data sets by adding Laplacian noise, which is jointly generated by the participants.

As Shi et al. [45] point out themselves, the issue of data pollution, i.e., a malicious participant or a group of malicious participants injecting false data. Furthermore, although keeping the contribution of each participant private, the protocols exhibit little to no fault tolerance of participants [34]. Finally, in order to achieve a high level of (differential) privacy, the number of participants needs to be large.

Secure Signal Processing

Secure Signal Processing (SSP) refers to the possibility to perform certain computations, such as aggregation in the encrypted domain. A commonly employed mechanism in SSP is *homomorphic encryption*, which allows some specific manipulations of the ciphertext to be reflected in the plaintext domain.

For example, Li et al. [47] propose an overlay network in a tree-like topology and the use of a Paillier cryptosystem [48]. Garcia and Jacobs [49] combine *secret sharing* with a Paillier cryptosystem to add flexibility in the aggregation (at the expense of additional computational complexity). Erkin and Tsudik [50] extend the idea of homomorphic encryption of smart meter readings by splitting the module into random shares, which, in combination with a modified Pailler cryptosystem, allows flexible spatial and temporal aggregation for different use cases, such as billing or network monitoring. The complexity of this approach is lower than that presented in [49]. Engel and Eibl [51] show that SSP can be combined with multi-resolution signal processing, increasing the degrees of freedom.

For real-world applicability, a number of factors need to be taken into account. For most schemes, homomorphic additivity comes at the cost of data expansion. For example, when a Paillier cryptosystem is used, a plaintext of size n is encrypted to a cipher text modulo n^2, thus doubling the number of bits needed for data representation in the encrypted domain. The ensuing data expansion, which grows with the number of participating nodes, may prove a challenge, especially if communication is done over low-bandwidth power line carrier. Computational complexity is another issue to be considered. Compared to other ciphers, homomorphic encryption systems are often more demanding. Furthermore, unlike standardized cryptographic ciphers, such as AES and RSA, homomorphic encryption schemes are not commonly supported by standard crypto hardware (this of course may change if a standard for homomorphic encryption is brought forward). For a smart meter roll-out to be successful, the required computational complexity may prove to be too high to allow manufacturing devices that satisfy economic feasibility. Furthermore, high computational demands may lead to energy demands that are significantly higher than traditional meters, and low energy efficiency for smart meters may negatively impact consumer acceptance.

Another issue, as with previously discussed approaches, lies with the number of required participants and the underlying trust model, i.e., what level of mutual trust needs to be afforded among the participants. For real-world use both need to be carefully investigated. In many homomorphic encryption schemes, participants are required to use the same key, which implies that they need to trust each other with their meter readings.

Multiparty computation

Similar to computing on encrypted data, it is also possible to compute on distributed data; in this case, the data is split and given to a set of parties, which then jointly perform the computation. All (or, respectively, a defined subset) of those parties need to collaborate in order to reconstruct data, allowing for individual parties to behave faulty without endangering privacy.

Rechargeable batteries

There are a number approaches that propose to install rechargeable batteries at the end-user home to mask the real profile. In the approach presented by Kalogridis et al. [52], a flat load curve is produced by constant charging of a battery as far as possible, matching the household consumption over time. Varodayan and Khisti [53] argue that with this best-effort approach, privacy may still leak through lower frequencies. They propose the use of a ‘stochastic battery’ which instead of constant charging employs a randomized model to decrease information leakage.

While in theory this is an effective approach, the practical applicability remains questionable due to the high costs of installing batteries. Furthermore, the energy loss introduced by using a battery buffer leads to low energy efficiency of this approach, which, as mentioned above, is not desirable in general, but specifically detrimental in the context of smart grids.

Annex C – Overview on Document Status of Investigated Standards

Standard	Description	Standardization Status
ISO/IEC 15408 Part 1	Introduction and General Model (Principles)	IS (2009)
ISO/IEC 15408 Part 2	Security Functional Requirements	IS (2008)
ISO/IEC 15408 Part 3	Security Assurance Requirements	IS (2008)
ISO/IEC 18045	Methodology for IT security evaluation	IS (2008)
ISO 24759	Test requirements for cryptographic modules	Published 2008 – under first revision. Now DIS ballot Publication Q2 2014
ISO 18367	Algorithm and security mechanisms conformance testing	First release Text for 2nd WD
ISO 17825	Testing methods for the mitigation of non-invasive attack classes against crypto modules	First release Text for 4th WD (first CD to be decided)
ISO 30104 Technical Specification	Physical security attacks, mitigation techniques and security requirements	First release Text for 3rd Preliminary Draft Technical Specification
ISO/IEC 27001	Information technology — Security techniques — Information security management systems — Requirements	New release in 2013
ISO/IEC TR 27002	Information technology — Security techniques — Code of practice for information security controls	New release in 2013
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	Published. ISO/IEC TR 27019 is aligned to the previous version of ISO/IEC 27002:2005
IEC 62443-2-4	Requirements for Security Programs for IACS Integration and Maintenance Service Providers	Committee Draft for Vote (CDV) expected end August 2013
IEC 62443-3-3	System security requirements and security levels	IS (July 2013)
IEC 62443-4-2	Technical Security Requirements for IACS Components	Working Draft (WD) (July 2013)
IEEE 1686	Substation Intelligent Electronic Devices (IED) Cyber Security Standards	Working Draft
IEEE C37.240	Cyber Security Requirements for Substation Automation, Protection and Control Systems	Working Draft
IETF RFC 7030	Enrollment over Secure Transport	Published (11/2013)
draft-weis-gdoi-iec62351-9	IEC 62351 Security Protocol Support for GDOI	Working Draft (07/2014)
RFC 7252	CoAP Constrained Application Protocol	Published (06/2014)
ISO/IEC 15118 Part 2	Network and application protocol requirements	International Standard
IEC 62351 Part 1	Introduction and overview	Technical Specification (TS)
IEC 62351 Part 2	Glossary of terms	TS, Edition 2 is currently prepared
IEC 62351 Part 3	Profiles including TCP/IP	TS,

Standard	Description	Standardization Status
		FDIS Edition 2 available in 08/2014 , IS expected in 06/2015
IEC 62351 Part 4	Profiles including MMS	TS, work on edition 2 has started (CD in 06/2015)
IEC 62351 Part 5	Security for IEC 60870-5 and Derivatives	TS in edition 2
IEC 62351 Part 6	Security for IEC 61850	TS, edition 2 will align with IEC 61850-90-5 TR
IEC 62351 Part 7	Network and system management (NSM) data object models	TS, edition 2 work started to enhance MIBs and provide mapping to protocols like SNMP, CD in 08/2014
IEC 62351 Part 8	Role-Based Access Control for Power systems management	TS, Amendment planned explaining usage as TR IEC 62351-90-1
IEC 62351 Part 9	Credential Management	Work in Progress, CD (2) in 08/2014
IEC 62351 Part 10	Security Architecture Guidelines	Technical Report (TR), Amendment planned for dedicated use cases like DER as separate TR
IEC 62351 Part 11	XML Security	Work in Progress, CD in 07/2014
IEC 62056-5-3	The DLMS/COSEM suite - Part 5-3: DLMS/COSEM application layer	FDIS

Annex D – Detailed Description of the SGIS Framework Steps

SGIS FRAMEWORK DETAILS

0. Preliminary Assessment

If a risk analysis (RA) is performed, the respective risk analysis team to follow the process successfully should include:

- A security expert to roll out and facilitate the process
- A Use Case owner, or on behalf of the owner a person who has all knowledge about the use case

PERSONAL DATA IS PART OF THE USE CASE

The SGIS guidance itself does not take personal data privacy into account. If it appears that personal data is used in the use case, in a separate step a Data Protection Impact Assessment has to be performed, using the template delivered by EG2.

The results of the DPIA should be combined with the outcomes of the SGIS risk analysis.

1. SGAM Mapping

One of the first actions to take is an evaluation of the use case. This means a SGAM mapping has to take place and a study on information (data) to be used in the use case.

For details on how to perform use cases SGAM mapping you can refer to present SGIS report and SG-CG/Methodology report.

Then according to SGIS-SL guidance provided in this SGIS report (Figure 4), SGIS-SL can be identified.

Identified SGIS-SL will be used as reference

2. Threats Mapping to the Use Case Assets

2.1 Use existing threat classification

- Threats and Assets classification can be taken from the ENISA/EG2 report “Proposal for a list of security measures for smart grids”, released April 2014 [8].

Threat	Asset	SGAM Cell

2.2 Threats classification

Most companies use for years a chosen risk analysis method that best suits their particular situation. There is no reason to change that if a smart grid use case is the subject of study. The company can - taking this guidance into account - perform the logical steps of their preferred risk analysis methodology.

- Identify most critical threats
- If not available, define critical and not-critical assets
- Use expertise in the company
- Use your own (companies) existing model

3. Define a Risk Mitigation Plan

Map recognised threats to ENISA/EG2 report “Proposal for a list of security measures for smart grids”, released April 2014 [8].

Take the Matrix which you get in Step 2 and then add the fields shown below to create a complete overview of threats, assets, risks and security measures to be taken (cf. p.17 to p.27 and p.38 to p.40 of ENISA/EG2 report [8]).

Output should the look like:

RANK	THREAT	ASSET	RISK	Critical Y/N?	Measures

4. Define Traceability

The Concept of traceability is that there is no hidden logic in any part of the used risk analysis method. Traceability is used to identify the factors that led to particular conclusions or recommendations. Traceability allows the risk analyst and involved management to identify the reasons for a particular countermeasure being recommended.

To prevent discussion on the choices made to mitigate security threats and risks it is important to proof the path or trail followed from the very first step in risk analysis, modeling of the studied environment, until the security plan, covering the recognized risks and mitigating security measures.

4.1 How can you implement traceability in your risk analysis?

Depending of the use of automated tools, manual analysis methods or a combination, the analyst has to document all steps taken.

When collecting documents for a desktop study, always document which documents are used, which document versions, are used and who was the owner respectively the sender of the documents.

During all next steps taken, it is necessary to document who are the participants of interviews and/or workshops. Document who they are and what their roles in the organization are. Document any answers which were given. Let all participants review the interview minutes and be sure they agree with the results.

The outcome of the agreed interview results during the business impact analysis and the threat and vulnerability assessments can be used to define the security measures needed to protect the smart energy system in scope.

Using an automated risk analysis system, especially when the system has an automated calculation function to define security measures, the system must be able to create a ‘back-track’ report which shows why a certain security measure is calculated. This is necessary to keep the results transparent.

The method described above looks very similar to a chain of custody or an audit trail.

5. Define a Mitigation Plan

Starting from table created in step 3, it is easy to move to following table:

SGIS Framework Action Plan Preparation				
Implementation Measures	Threats	Risk	Risk Critical? Yes/no	Costs of an incident

6. Define an Action Plan

6.1 Define an action plan

Source references:

- Use case
- Use Case reference SGIS-SL
- Dashboard
- Measures threat catalogue

Security Measures	Priority	risk	Incident cost	Mitigation cost
Measure 1				
Measure 2				
etc.				

- Star for priority in dashboard
- Identify if critical risk per measure exist

Sometimes you may have to re-assess the chosen star classification. Then use expertise from the use case owner/representative and/or security expert.

Please note expertise is to be used to revisit proposed SGIS-SL priorities in the light of the present exercise. Proposed priorities can then be increased or decreased. Keeping in mind the reference proposed.

6.2 Aggregating ENISA security recommendations and DPIA recommendations

At the end of step 3 you will have security recommendation from ENISA and controls from DPIA. The controls should be merged into a logical set of measures to secure the use case.

The next steps are to review the outcome of the DPIA and SGIS study with the security team and finally the board to approve the chosen security measures and action plan.

Annex E – 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/A_ Framework for Smart Grid Standardization ftp://ftp.cen.eu/EN/EuropeanStandardization/HotTopics/SmartGrids/Framework%20Document.pdf

[3] SG-CG/M490/C_ Smart Grid Reference Architecture ftp://ftp.cen.eu/EN/EuropeanStandardization/HotTopics/SmartGrids/Reference_Architecture_final.pdf

[4] SG-CG/M490/E_ Smart Grid Use Case Management Process ftp://ftp.cen.eu/EN/EuropeanStandardization/HotTopics/SmartGrids/Sustainable%20Processes.pdf

[5] SG-CG/M490/B_ First Set of Standards ftp://ftp.cen.eu/EN/EuropeanStandardization/HotTopics/SmartGrids/First%20Set%20of%20Standards.pdf

[6] SG-CG/M490/D_ Smart Grid Information Security ftp://ftp.cen.eu/EN/EuropeanStandardization/HotTopics/SmartGrids/Security.pdf

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

[8] ENISA, Proposal for a list of security measures for smart grids: http://ec.europa.eu/energy/gas_electricity/smartgrids/doc/20140409_enisa.pdf

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

[10] SM-CG, Functional reference architecture for communications in smart metering systems ftp://ftp.cen.eu/cen/Sectors/List/Measurement/Smartmeters/CENCLCETSI_TR50572.pdf

[11] CMMI-SVC: CMMI for Services, http://cmmiinstitute.com/cmmi-solutions/cmmi-for-services/

[12] ISO/IEC 15408: Information technology — Security techniques — Evaluation Criteria for IT security

[13] ISO/IEC 18045: Information technology — Security techniques — Methodology for IT Security Evaluation

[14] ISO/IEC 19790: Information technology — Security techniques — Security requirements for cryptographic modules

[15] 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

[16] 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

[17] 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

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

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

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

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

[22] ISO /IEC 15118-2 Road vehicles – Vehicle-to-Grid Communication Interface, Part 2: Technical protocol description and Open Systems Interconnections (OSI) layer requirements

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

[24] IEC 62056-5-3 DLMS/COSEM Security

[25] IETF RFC 6960 Online Certificate Status Protocol

[26] IETF draft-ietf-core-coap: CoAP Constrained Application Protocol

[27] IETF draft-weis-gdoi-iec62351-9: IEC 62351 Security Protocol support for GDOI

[28] IETF RFC 7030: Enrollment over Secure Transport

[29] IEC TC8 New Work Item Proposal 'Use Case Approach Part 2 - Definition of Use Case Template, Actor list and Requirement List for Energy Systems' June 2012

[30] SmartC2Net European Project, WP1, Deliverable D1.1 'SmartC2Net Use Cases, Preliminary Architecture and Business Drivers', www.smartc2net.eu

[31] REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data ('General Data Protection Regulation'); This document is based on the latest (inofficial) Version of the GDPR: INOFFICIAL CONSOLIDATED VERSION AFTER LIBE COMMITTEE VOTE, PROVIDED BY THE RAPPORTEUR, 22 October 2013, accessible at http://www.janalbrecht.eu/fileadmin/material/Dokumente/DPR-Regulation-inofficial-consolidated-LIBE.pdf [last access 2013/12/12].

[32] P. McDaniel and S. McLaughlin, 'Security and privacy challenges in the smart grid', *IEEE Security Privacy Magazine*, vol. 7, no. 3, pp. 75–77, 2009

[33] M. A. Lisovich and S. B. Wicker, 'Privacy concerns in upcoming residential and commercial demand-response systems', *IEEE Proceedings on Power Systems*, vol. 1, no. 1, 2008.

[34] M. Jawurek, F. Kerschbaum, and G. Danezis, 'Privacy technologies for smart grids - a survey of options', Microsoft Research, Tech. Rep., 2012.

[35] Z. Erkin, J. Troncoso-Pastoriza, R. Lagendijk, and F. Perez-Gonzalez, 'Privacy-preserving data aggregation in smart metering systems: An overview', *Signal Processing Magazine, IEEE*, vol. 30, no. 2, pp. 75–86, March.

[36] L. Backstrom, C. Dwork, and J. Kleinberg, 'Wherefore art thou R3579X? : anonymized social networks, hidden patterns, and structural steganography', in *Proceedings of the 16th international conference on World Wide Web*, ser. WWW '07. New York, NY, USA: ACM, 2007, pp. 181–190.

[37] M. Jawurek, M. Johns, and K. Rieck, 'Smart metering de-pseudonymization', in *Proceedings of the 27th Annual Computer Security Applications Conference*, ser. ACSAC, New York, NY, USA: ACM, 2011, pp. 227–236. [Online]. Available: http://doi.acm.org/10.1145/2076732.2076764

[38] J.-M. Bohli, C. Sorge, and O. Ugus, 'A privacy model for smart metering', in *Proc. IEEE Int Communications Workshops (ICC) Conf*, 2010, pp. 1–5.

[39] C. Efthymiou and G. Kalogridis, 'Smart grid privacy via anonymization of smart metering data', in *Proceedings of First IEEE International Conference on Smart Grid Communications*, Gaithersburg, Maryland, USA, Oct. 2010, pp. 238–243.

[40] D. Engel, 'Conditional access smart meter privacy based on multi-resolution wavelet analysis', in *Proceedings of the 4th International Symposium on Applied Sciences in Biomedical and Communication Technologies*. New York, NY, USA: ACM, 2011, pp. 45:1–45:5.

[41] D. Engel, 'Wavelet-based load profile representation for smart meter privacy', in *Proc. IEEE PES Innovative Smart Grid Technologies (ISGT'13)*, Washington, D.C., USA, Feb. 2013, pp. 1–6. [Online]. Available: http://dx.doi.org/10.1109/ISGT.2013.6497835

[42] K. Kursawe, G. Danezis, and M. Kohlweiss, 'Privacy-friendly aggregation for the smart grid', in *Privacy Enhanced Technology Symposium*, 2011, pp. 175–191.

[43] B. Defend and K. Kursawe, 'Implementation of Privacy Friendly Aggregation for the Smart Grid', in *Proc. Smart Energy Grid Security Workshop (SEGS 2013),* Berlin, Germany, November 2013.

[44] C. Dwork, ‘Differential privacy: A survey of results’, in *Theory and Applications of Models of Computation*, ser. Lecture Notes in Computer Science, M. Agrawal, D. Du, Z. Duan, and A. Li, Eds. Springer Berlin Heidelberg, 2008, vol. 4978, pp. 1–19. [Online]. Available: http://dx.doi.org/10.1007/978-3-540-79228-4_1

[45] E. Shi, R. Chow, T. h. Hubert Chan, D. Song, and E. Rieffel, ‘Privacy-preserving aggregation of time-series data’, in *Proc. NDSS Symposium*, February 2011.

[46] G. Acs and C. Castelluccia, ‘I have a dream! (differentially private smart metering)’, in *Proc. Information Giding Conference*, 2011, pp. 118–132.

[47] F. Li, B. Luo, and P. Liu, ‘Secure information aggregation for smart grids using homomorphic encryption,’ in *Proceedings of First IEEE International Conference on Smart Grid Communications*, Gaithersburg, Maryland, USA, Oct. 2010, pp. 327–332.

[48] P. Paillier, ‘Public-key cryptosystems based on composite degree residuosity classes’, in *Proceedings of Eurocrypt ’99, Advances in Cryptology*, ser. Lecture Notes in Computer Science, J. Stern, Ed., vol. 1592. Prague, Czech Republic: Springer, May 1999, pp. 223–238.

[49] F. Garcia and B. Jacobs, ‘Privacy-friendly energy-metering via homomorphic encryption’, in *Security and Trust Management*, ser. Lecture Notes in Computer Science, J. Cuellar, J. Lopez, G. Barthe, and A. Pretschner, Eds. Springer Berlin / Heidelberg, 2011, vol. 6710, pp. 226–238. [Online]. Available: http://dx.doi.org/10.1007/978-3-642-22444-7_15

[50] Z. Erkin and G. Tsudik, ‘Private computation of spatial and temporal power consumption with smart meters’, in *Proceedings of the 10th international conference on Applied Cryptography and Network Security*, ser. ACNS’12. Berlin, Heidelberg: Springer-Verlag, 2012, pp. 561–577. [Online]. Available: http://dx.doi.org/10.1007/978-3-642-31284-7_33

[51] D. Engel and G. Eibl, ‘Multi-resolution load profile representation with privacy-preserving aggregation’, in *Proceedings of IEEE Innovative Smart Grid Technologies (ISGT) 2013*. Copenhagen, Denmark: IEEE, Oct. 2013, to appear.

[52] G. Kalogridis, C. Efthymiou, S. Z. Denic, T. A. Lewis, and C. R., ‘Privacy for smart meters: Towards undetectable applicance load signatures’, in Proceedings of First IEEE International Conference on Smart Grid Communications, Gaithersburg, Maryland, USA, Oct. 2010, pp. 232–237.

[53] D. Varodayan and A. Khisti, ‘Smart meter privacy using a rechargeable battery: minimizing the rate of information leakage’, in Proc. IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP 2011), Prague, Czech Republic, May 2011.

[54] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

[55] ‘Treaty on the Functioning of the European Union’.

[56] For a more exhaustive overview of the German approach to smart metering, see F. Pallas, ‘Beyond Gut Level’, http://dx.doi.org/10.1007/978-94-007-5170-5_14

[57] SoES European Project, A.3, Deliverable D3 “Vulnerabilities, Threats, Measures”, www.soes-project.eu