**CEN-CENELEC-ETSI Smart Grid Coordination Group**

**November 2012**

# CEN-CENELEC-ETSI Smart Grid Coordination Group

# Smart Grid Information Security

# Contents

# 1 Scope

This document is released by the Smart Grid Information Security (SGIS) working group under the European Commission Smart Grid Mandate, M/490 Standardization Mandate to European Standardization Organizations (ESOs), to support European Smart Grid deployment.

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 content presented in this report does not provide a complete and definitive answer to the mandate's objective. Nevertheless it provides a high level guidance on how standards can be used to develop Smart Grid information security. It also presents concepts useful to all Smart Grid stakeholders to integrate information security into their daily activities.

Securing the Smart Grid is a continuous effort. Elements presented here are the first steps of the Smart Grid information security journey to achieve end to end security.

# 2 References

- ISO/IEC 27001:2005
- ISO/IEC 27002:2005
- IEC 62351-X
- NERC CIP V4 (US Standard)
- NISTIR-7628 - 2010 (US Guidelines)

# 3 Terms and definitions

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

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

**Smart Grid Information Security (SGIS)**
As quoted from M/490 mandate, Smart Grid Information Security refers to:*"[…] technical and organisational needs for sustainable "state of the art" Smart Grid Information Security (SGIS), Data protection and privacy*

*(DPP), enabling the collection, utilisation, 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.

**Smart Grid Data Protection Class (SG-DPC)**
SG-DPC objective is to create a bridge between information models and their protection needs. Smart Grid Data Protection Classes are set of recommended classifications for information assets (data models).There are 2 distinct areas to be classified for protection needs: personal data and other information classes that need protection.

**Smart Grid Information Security - Risk Impact Level (SGIS-RIL)**
SG-RIL objective is to assess and evaluate how possible information security compromises may impact on Smart Grid operations or efficiency. SGIS working group defined five SGIS Risk Impact Levels in this report.

**Likelihood**
Classical concepts of likelihood and vulnerability cannot be assessed in a generic sense and in the early stages of a risk assessment may not be known. That's the reason because SG Risk Analysis will determine effective likelihood as a value attributed to the combination of the capability and motivation of a threat source and a threat actor to attack an asset.

**Smart Grid Architecture Model – SGAM**
High level conceptual model of the Smart Grid developed by the M/490 Reference Architecture working group describing the main actors of the Smart Grid and their main interactions.

**SGAM Domains and Zones**
Referring to SGAM, domains reflect Smart Grid related domains of actions (Bulk Generation, Transmission, Distribution, DER, Customer) and zones reflect hierarchical system aspect of each domain (Process, Field, Station, Operation, Enterprise, Market).

**Requirement Standard - Type 1 Standard**
Requirement Standards are high level requirement standards, neutral from technology. Those requirements do not provide technical implementation options. (cf. §8 for details).

**Implementation Standard - Type 2 Standard**
Implementation option standards describe many specific implementation options depending on domain and technologies used. (cf. §8 for details).

**Standard profile for interoperability – Type 3 Standard**
To achieve interoperability – it is often required to limit (profile) the implementation options provided by Type 2 standards. (cf. §8 for details).

**Type 1, Type 2 and Type 3 Standards Example**
One example for a type 1 standard is ISO 27002 providing security requirements on an abstract level. Security standards, which already exist and can be leveraged in smart grid security solutions belong to type 2 standards. An example can be given with TLS (RFC 5746) providing a self contained security solution. Nevertheless, the standard provides several options, which may even be negotiated between the communication peers. Hence, to optimize communication, IEC 62351-3 limits the available configuration options of TLS resulting in a profile, which in turn is a type 3 standard.

# 4 Symbols and abbreviations

- **SGIS** - Smart Grid Information Security
- **SGIS-SL** - Smart Grid Information Security – Security Level

- **SG-DPC** - Smart Grid Data Protection Class
- **SGIS-RIL** - Smart Grid Information Security - Risk Impact Level
- **SGAM** - Smart Grid Architecture Model
- **CIA** – Confidentiality, Integrity, Availability
- **EU** – European Union
- **US** – United States
- **PKI** – Public Key Infrastructure

# 5 Executive Summary

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

SGIS essential requirements presented emphasize the importance of the CIA (Confidentiality, Integrity and Availability) triad for Information Security but also underline the varying weight of the Confidentiality, Integrity and Availability as essential requirements and the issue encountered to address Information Security topics for the Smart Grid as a whole.

Key SGIS elements like the SGAM (Smart Grid Architecture Model), SGIS-SL (SGIS Security Levels), Smart Grid Data Protection Classes (SG-DPC) and the Security View per SGAM layers are introduced and used to provide security requirements and recommendations on their implementations thru a European Electrical Smart Grid stability scenario.

SGIS standards landscape illustrates the role of standards in requirements implementation and establishes a current picture and a target for this landscape.

SGIS Toolbox provides Smart Grid Use Case stakeholders an easy and pragmatic way to identify what might be their use case security needs.

In conclusion, the standards needed to establish the basis of the Smart Grid Information Security are available today. Nevertheless there is a need for enhancement and for additional standards to integrate Smart Grid specific needs.

As a final thought, outside of standardization, the risks of connecting Smart Grid critical infrastructures equipments to public networks should be carefully considered in all implementations, as well as the opportunity to send encrypted and authenticated orders to smart grid components.

# 6 Essential Requirements

Requirements presented in this chapter are relevant for Smart Grid Information Security. All these requirements should not jeopardize Smart Grid development but rather support the interoperability and exchangeability of products and services within the EU.

ISO/IEC 27001:2005, proposes the following definition of information security: "*preservation of confidentiality, integrity and availability of information; in addition, other properties, such as authenticity, accountability, non-repudiation, and reliability can also be involved*". **Confidentiality, Integrity and Availability** (CIA) are thus the key essential requirements of Information Security.

Some stakeholders have pointed out a **CIA vs. AIC paradigm of Smart Grid Information Security**. Confidentiality, Integrity and Availability are usually presented this way without any meaning of ordering. Nevertheless, depending on the context, there may be a prioritization of the required security services. For instance in the electricity transport domain usually availability is most important then comes integrity and last confidentiality. This is the CIA vs. AIC paradigm of Smart Grid Information Security. The weight of the Confidentiality, Integrity and Availability as essential requirements will vary depending to the Smart Grid stakeholder activity.

The CIA vs. AIC paradigm reflects the heterogeneity and complexity of the Smart Grid and illustrates the difficulty to address the information security of the Smart Grid as a whole.  The Smart Grid is a system of systems connected and interacting with each other. Therefore their essential security requirements will vary depending on your role or function in the Smart Grid

# 7 SGIS Key Elements

## *7.1 Smart Grid Architecture Model (SGAM)*

Information presented in this chapter is extract from the Smart Grid Reference Architecture working group report. 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 Reference Architecture work 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

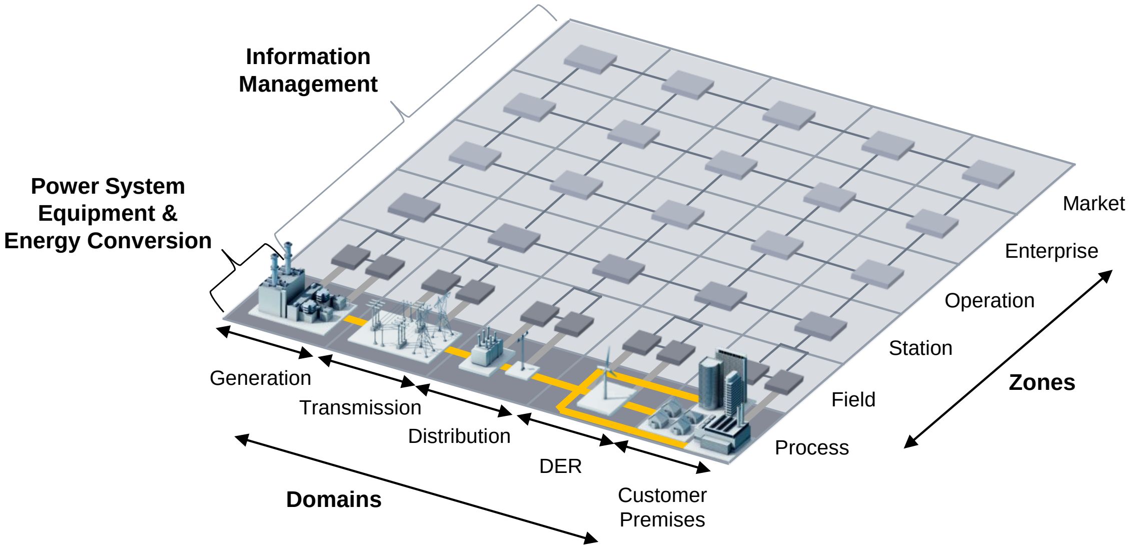


**Figure 1: Smart Grid Plane**

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 …). |
| **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 |

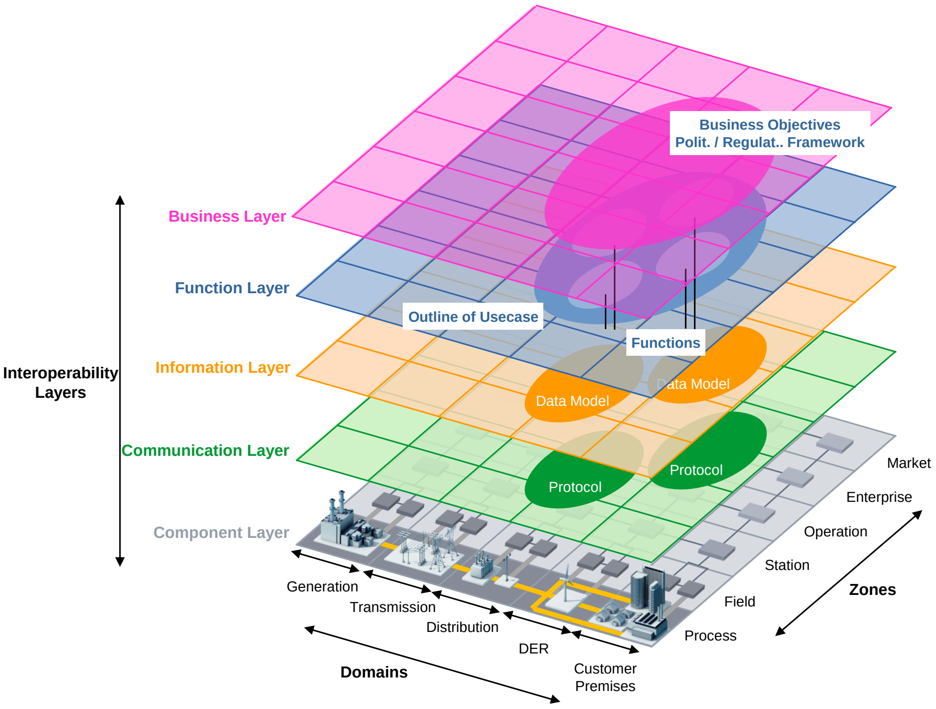


**Figure 2: SGAM Layers**

## *7.2 SGIS Security Levels (SGIS-SL)*

SGIS - Security Levels (SGIS-SL) have been defined with the objective to create a bridge between electrical grid operations and information security. 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 instance we can estimate this amount at around 126 GW for France. 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. All these electrical data have been used to define each SGIS Security Level.

European Electrical Grid stability has been chosen as reference to define SGIS-SL and create a bridge between electrical operations and information security. Thus focus is made on power loss caused by ICT systems failures. Further criteria to asses required security levels are presented in chapter 11.

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

**Figure 3: SGIS-SL Description**

Proposed 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 reflect assets criticality from a global European Electrical Grid stability point of view and their associated different security needs.

As described in Annex A, SGSIS Security Levels correspond to a set of recommended security requirements that may be assigned to each SGAM Domain/Zone cell.

## *7.3 Smart Grid Data Protection classes (SG-DPC)*

Use Cases describe intended usage of all information (received, processed, stored, transmitted or erased) as well as the role/actor (human or technical) that is allowed to do this.

Assessing security risk starts with the information asset involved. Smart Grid Services (i.e. generic use cases) span over several domains/zones – hence data models “travel” through a very diverse information system at different locations and with varying ownerships. Therefore it is recommended to classify and tag the data models. This classification is called SG-Data Protection Classes. It supports the identification of the appropriate SGIS-SL for standards selection for each use case and system component/actor involved.

In the future by performing pre-transmission checks about SGIS-SL abilities of actors to whom the information maybe sent, thru mutual authentication using certificates and PKI for example, SG-DPC may allow state of the art management of Smart Grid Information Security

Both SG-DPC classes, as exposed in the Figure 4 below, apply to any specific information model/asset. Information assets may need protection and “*preservation of confidentiality, integrity and availability of information; in addition, other properties, such as authenticity, accountability, non-repudiation, and reliability can also be involved*”, wherever they are generated, received, processed, sent or erased within the Smart Grid information system.

Two classes are proposed to illustrate the difference between domain independent protection needs for privacy and domain specific protection classifications and protection needs of information assets handled in use cases/service. E.g. Revenue metering data – SG-DPC2 is measurement data (justification metrological laws) at the same time SG-DPC1 is personal data (justification: privacy law). Both protection need to be assessed for the appropriate SGIS-SL independently (as outlined later in this document Figure 7).

| **SG-DPC 1 Personal Information** |
|---|
| Sensitive Personal Information |
| Personal Information |
| De-personalized Pseudonym zed Personal information |
| No Personal information |

| **SG-DPC 2 System Information** |
|---|
| System Data (i.e. Firmware), Configuration Data, Customer Credentials, Private & Public Keys, Roles /Actor IDs |
| Governance & Reporting Information, Logging and Audit Information |
| Audit & Log required information |
| Information to administrate remotely |
| Information to operate remotely (Control signals) |
| Business Information |
| Measurement data |

**Figure 4: SG-DPCs**

## *7.4 Security View per Layer*

European Smart Grid is under construction and still not a physical reality. In order to circumvent this lack of physical reference architecture to analyze the choice has been made to use the SGAM. Analyzing the SGAM, it quickly appeared information security should be considered in all domains, zones, and layers.

Now this needs to be incorporated into the model without denaturing or over sizing it. The choice was made with M/490 Reference Architecture working group to use an additional layer that could be slipped under each layer. This is what we call the **Security View per Layer**.

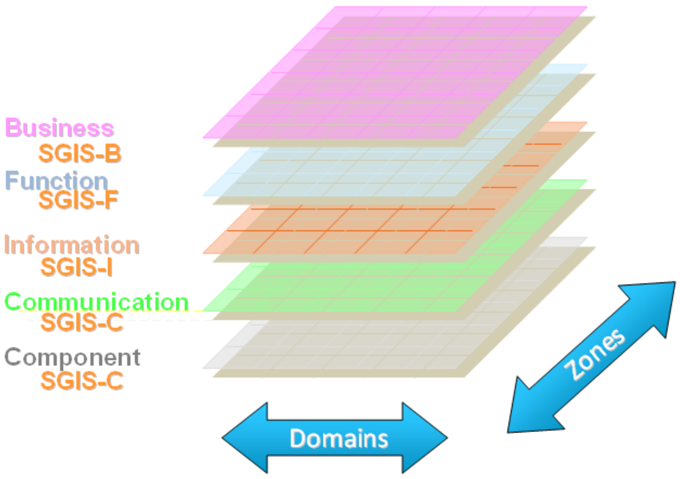


**Figure 5: Security View per Layer**

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 you are located. The Security View per Layer is the conceptual representation used to illustrate this.

# 8 SGIS-SL High Level Recommendations

As exposed previously, European Commission M/490 mandate and Smart Grid stakeholders have required some guidance on Smart Grid information security.

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 in § 7.2, Fig.3.

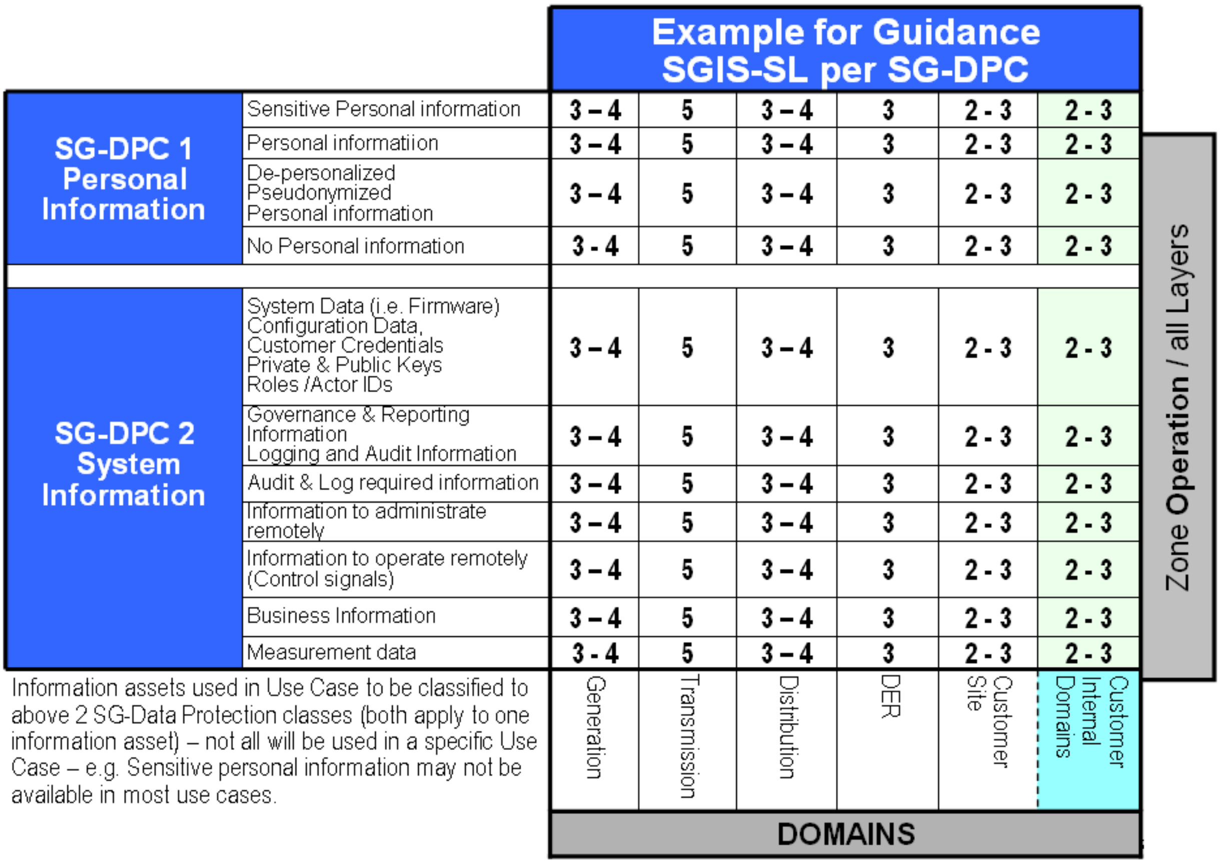
| SGIS-SL HIGH LEVEL GUIDANCE* | | | | | | |
|---|---|---|---|---|---|---|
| 3 – 4 | 3 – 4 | 3 – 4 | 2 – 3 | 2 – 3 | MARKET | ZONES |
| 3 – 4 | 3 – 4 | 3 – 4 | 2 – 3 | 2 – 3 | ENTREPRISE | |
| 3 – 4 | 5 | 3 -4 | 3 | 2 – 3 | OPERATION | |
| 2 – 3 | 4 | 2 | 1 – 2 | 2 | STATION | |
| 2 – 3 | 3 | 2 | 1 –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

**Figure 6: High Level Security View per Layer values recommendations**

** Please note values proposed are guidance examples only*

Values proposed 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 thru more formal exercise as detailed later.

The table hereunder reflects the anticipated ranged values for all use cases / SG-DPC in SGAM cells domains for zone operation. Specific Use Cases may vary. For use cases – the Information assets and its Information security classification (SG-DPC) are known – therefore guidance can be more specific.



Example for Guidance SGIS-SL per SG-DPC

Zone Operation / all Layers

| | | Generation | Transmission | Distribution | DER | Customer Site | Customer Internal Domains |
|---|---|---|---|---|---|---|---|
| SG-DPC 1 Personal Information | Sensitive Personal information | 3 – 4 | 5 | 3 – 4 | 3 | 2 - 3 | 2 - 3 |
| | Personal information | 3 – 4 | 5 | 3 – 4 | 3 | 2 - 3 | 2 - 3 |
| | De-personalized<br>Pseudonymized<br>Personal information | 3 – 4 | 5 | 3 – 4 | 3 | 2 - 3 | 2 - 3 |
| | No Personal information | 3 - 4 | 5 | 3 – 4 | 3 | 2 - 3 | 2 - 3 |
| SG-DPC 2 System Information | System Data (i.e. Firmware)<br>Configuration Data,<br>Customer Credentials<br>Private & Public Keys<br>Roles /Actor IDs | 3 – 4 | 5 | 3 – 4 | 3 | 2 - 3 | 2 - 3 |
| | Governance & Reporting Information<br>Logging and Audit Information | 3 – 4 | 5 | 3 – 4 | 3 | 2 - 3 | 2 - 3 |
| | Audit & Log required information | 3 – 4 | 5 | 3 – 4 | 3 | 2 - 3 | 2 - 3 |
| | Information to administrate remotely | 3 – 4 | 5 | 3 – 4 | 3 | 2 - 3 | 2 - 3 |
| | Information to operate remotely (Control signals) | 3 – 4 | 5 | 3 – 4 | 3 | 2 - 3 | 2 - 3 |
| | Business Information | 3 – 4 | 5 | 3 – 4 | 3 | 2 - 3 | 2 - 3 |
| | Measurement data | 3 - 4 | 5 | 3 – 4 | 3 | 2 - 3 | 2 - 3 |

Information assets used in Use Case to be classified to above 2 SG-Data Protection classes (both apply to one information asset) – not all will be used in a specific Use Case – e.g. Sensitive personal information may not be available in most use cases.

DOMAINS

**Figure 7: High Level Guidance for SGIC-SL per SG-DPC all Domains Zone Operation**

** Please note*

- *Values proposed are examples for guidance in the Zone Operation only*
- *Depending on customer site internal impacts that may be critical for the customer – this may result in customer driven higher end to end SGIS-SL requirements – to achieve interoperability.*

Even if guidance is provided, Smart Grid stakeholders are recommended to perform the exercise by themselves.

The proposed values may also be useful for **interoperability** reasons. In a given SGAM domain and zone a single or several actors having to exchange information using equipments from one or several manufacturers will at least have guidance to start from.

Smart Grid stakeholders are also 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. Then up to them following their risk appetite and business and operational rules to identify the right SGIS-SL to be implemented. They are the ones that know best their risks and how to mitigate them.

# 9 Security Recommendation Implementation

When the work for this report started NISTIR-7628 guidelines (cf. Annex A) were the only Smart Grid dedicated set of security requirements available. They have been used as an input for this work. Further elements like ISO/IEC 2700x sector specific standards will be integrated alongside.

Like the security view per layer values, the distribution of the security requirements per security level are only high level recommendations proposed to support Smart Grid stakeholders' effort in securing the Smart Grid. They will vary depending on Smart Grid stakeholders' roles and responsibilities and are to be challenged by their assessment results. Further work is required and will be performed to best fit all Smart Grid stakeholders' need. Nevertheless they are proposed as a first basis to start the work related to security measures to be implemented to secure the Smart Grid.

Additionally, as for security view per layer SGIS-SL values, the final decision on requirements to be implemented belongs to Smart Grid stakeholders. They should review the requirements proposed for their required security level and assess if they are all relevant and if some are missing. Nevertheless in an ever more inter-connected Smart Grid, interoperability of security measures is seen as an essential condition to the success of the European Smart Grid.

Indeed, the way security measures will be implemented is very critical for interoperability. For example a as simple measure as user authentication mechanisms to access a Smart Grid asset can be implemented in many different ways (user authentication may be done using different means: username and password (whereas the password may be trivial, complex, one-time password), certificate and corresponding private keys, biometrics, etc…). Such a simple security measure could lead to very complex technical challenge in current stage of Smart Grid if interoperability is not part of the problem.

As exposed previously, European Smart Grid is under construction and still not a physical reality and there is not one Smart Grid physical architecture reference. Additionally there are a lot of different technologies interacting with each others. Therefore going into very detailed technical implementation guidance is very difficult not to say nearly impossible right now.

This and the different SGAM cell (domain/zone) specificities reflect the heterogeneity and complexity of the Smart Grid and illustrate the difficulty to address the security of the Smart Grid as a whole. All related technical and organizational aspects have to be investigated for each SGAM cell. Additionally things become even more complex when a use case crosses several SGAM cells. Hence we recommend the application of the SGIS Toolbox (cf. §11) on each use case.

# 10 SGIS Standard Landscape

The study of the current Smart Grid information security standards landscape started establishing an as-is of the existing smart grid relevant documents. This work led us to identify the following documents as relevant for the analysis:

- ISO/IEC 27001
- ISO/IEC 27002
- IEC 62351
- NERC CIP  (US Standard)
- NISTIR-7628  (US Guidelines)

Report from European task force on Smart Grid privacy and security and Joint Working Group have also been used as inputs for this study.

To be chosen, documents had to be already published, widely known by Smart Grid stakeholders and well accepted both in Europe and US. The list is not exhaustive. The objective was to establish an analysis methodology and identify a **first set of standards** that could be used today to secure the Smart Grid. This first set of standards will have to grow and be maintained over time.

Standards were analyzed thru two axes as illustrated in the figure hereunder.  The first one is their relevance for Organizations (Smart Grid operators) and products and services (product manufacturer and service providers). The second one is their relevance from a technical point of view and their relevance from an organizational point of view.

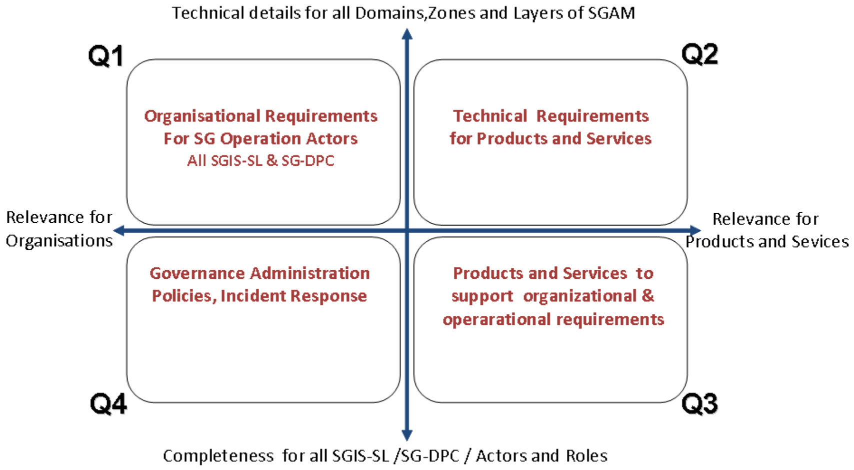

Technical details for all Domains,Zones and Layers of SGAM
Q1
Q2
Organisational Requirements For SG Operation Actors All SGIS-SL & SG-DPC
Technical Requirements for Products and Services
Relevance for Organisations
Relevance for Products and Sevices
Governance Administration Policies, Incident Response
Products and Services to support organizational & operarational requirements
Q4
Q3
Completeness for all SGIS-SL /SG-DPC / Actors and Roles

**Figure 8: SGIS Standards Areas**

Using this representation the current SGIS Standards landscape with the documents analyzed can be established as illustrated in the figure hereunder:

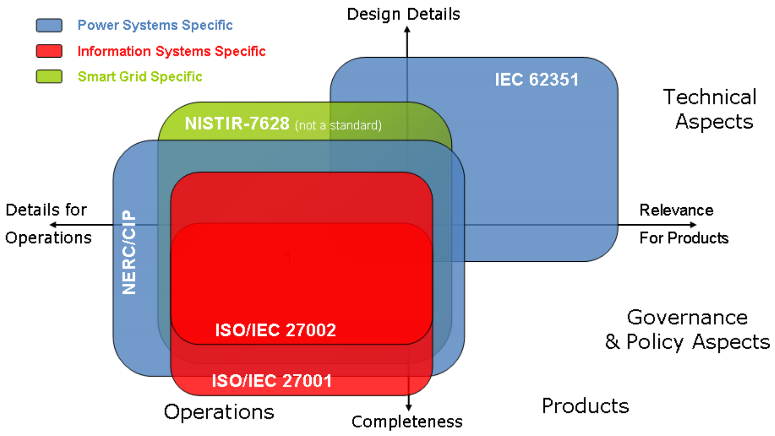


**Figure 9: Current SGIS Standard Landscape Analyzed**

A first target was to have this current SGIS standard landscape “Smart Grid Ready”, i.e. by transforming the zones which are not green yet, into green one as illustrated below.

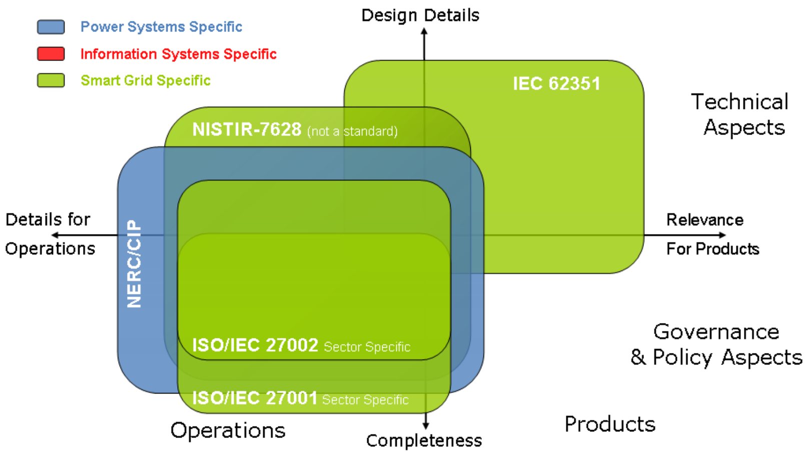


**Figure 10: SGIS Standard Landscape Target**

This target is to be seen as a first step in the Smart Grid Information Security journey. The following picture illustrates the areas and anticipated status for SGIS-SL implementation in Standards at year end 2012.

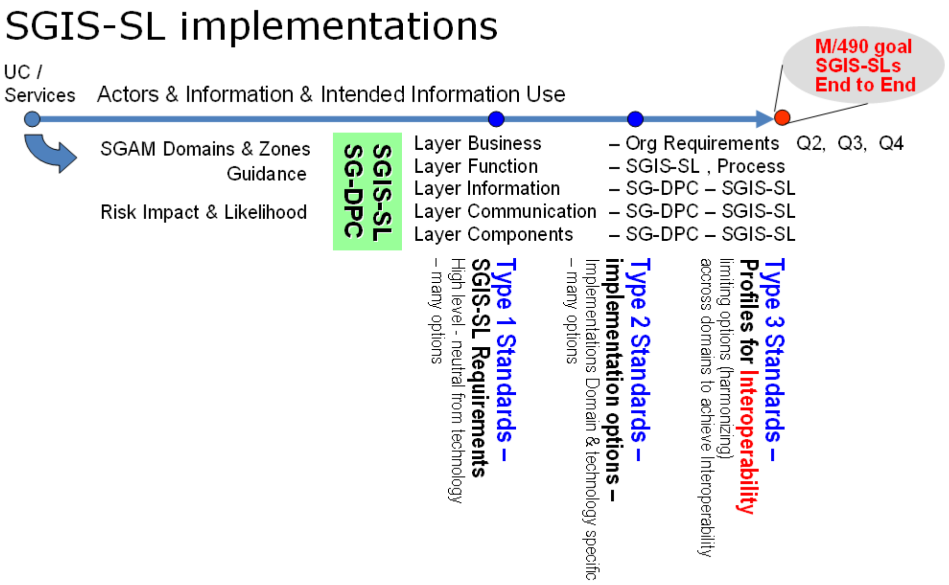

SGIS-SL implementations
UC / Services
Actors & Information & Intended Information Use
M/490 goal SGIS-SLs End to End
SGAM Domains & Zones Guidance
Risk Impact & Likelihood
SGIS-SL SG-DPC
Layer Business – Org Requirements Q2, Q3, Q4
Layer Function – SGIS-SL , Process
Layer Information – SG-DPC – SGIS-SL
Layer Communication – SG-DPC – SGIS-SL
Layer Components – SG-DPC – SGIS-SL
Type 1 Standards – SGIS-SL Requirements
High level - neutral from technology – many options
Type 2 Standards – implementation options –
Implementations Domain & technology specific – many options
Type 3 Standards – Profiles for Interoperability
limiting options (harmonizing) accross domains to achieve Interoperability

**Figure 11: SGIS Standards Landscape Target YE2012 Details**

One item of this first step was to present recommendations related to IEC 62351 to IEC TC57:WG15. Recommendations have been made and target the technological advancement of the current standard to address recent technology advances and also to address further development to support smart grid use cases.

The second item identified was to establish a standard for the Smart Grid sector specific application of ISO/IEC 27002 standard. The DIN (Deutsches Institut für Normung) in the DIN 27009 - “Information security management guidelines for process control systems used in the energy utility industry on the basis of ISO/IEC 27002” document made a first proposal in this sense. Now this need has been recognized (ISO/IEC JTC1 resolution 58:Nov2011). In response to this resolution ISO/IEC JTC1/SC27 launched a study period within working group to asses this need for an ISO/IEC 27002 standard specific for the Smart Grid sector

But as stated this is only a first step. The ultimate goal is to identify SGIS requirement standards in all four quadrants to enforce SGIS-SL security requirements in all SGAM domains, zones and layers. The figure 12 hereunder gives an overview of this ultimate goal.

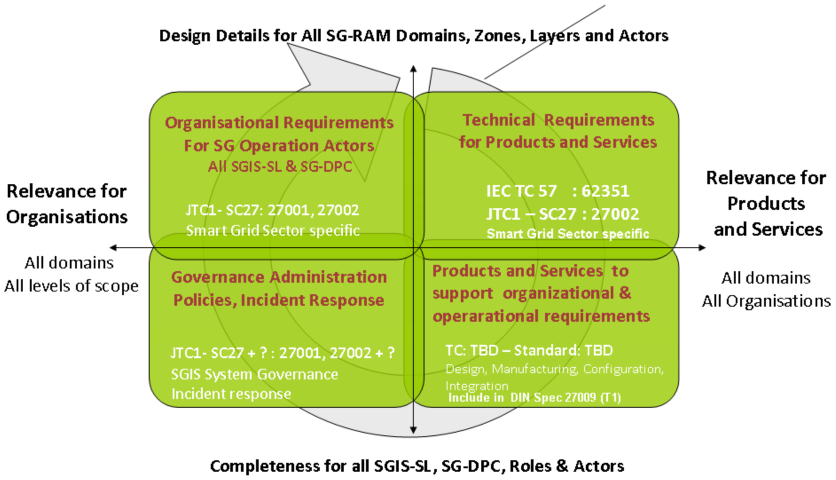

Design Details for All SG-RAM Domains, Zones, Layers and Actors
Organisational Requirements For SG Operation Actors
All SGIS-SL & SG-DPC
JTC1- SC27: 27001, 27002
Smart Grid Sector specific
Technical Requirements for Products and Services
IEC TC 57 : 62351
JTC1 – SC27 : 27002
Smart Grid Sector specific
Relevance for Organisations
All domains
All levels of scope
Relevance for Products and Services
All domains
All Organisations
Governance Administration Policies, Incident Response
JTC1- SC27 + ? : 27001, 27002 + ?
SGIS System Governance
Incident response
Products and Services to support organizational & operarational requirements
TC: TBD – Standard: TBD
Design, Manufacturing, Configuration, Integration
Include in DIN Spec 27009 (T1)
Completeness for all SGIS-SL, SG-DPC, Roles & Actors

**Figure 12: SGIS Standards Ultimate Goal**

The Smart Grid, as a system of systems, is heterogeneous and complex. Covering exhaustively all standards needed to secure the Smart Grid is a long and fastidious task. Smart Grid use cases are so numerous and different as are the technologies used to deliver the identified services that additional existing standards are to be considered. Some more can be found in SG-CG/FSS Report § 9.3 Security.

The conclusion of this study is key information for the Smart Grid Information Security Landscape. As shown above (Fig. 10 about IEC-62351 and ISO/IEC 27002), the standards needed to establish the basis of the Smart Grid Information Security are available today. Nevertheless there is a need for additional standards to integrate Smart Grid specific needs.

But this exercise (standards gap analysis) can not be one shot only. This should be a continuous exercise integrating the evolution of the Smart Grid information security needs. The remaining relevant question and challenge is to know if standards will be able to adapt to the pace of these evolutions.

The SGIS Toolbox will help identifying which standards can be used in Europe today and in future and systematically identifying gaps in existing SGIS standards.

# 11 Going Further – The SGIS Toolbox

## *11.1 Toolbox Overview*

The SGIS Toolbox is the answer to the following question: How to integrate security in the General Smart Grid Use Case Analysis Framework?

To answer this question, the SGIS toolbox will have to be part of this framework as illustrated hereunder and will help identifying which standards can be used in Europe today and in future and systematically identifying gaps in existing SGIS standards.

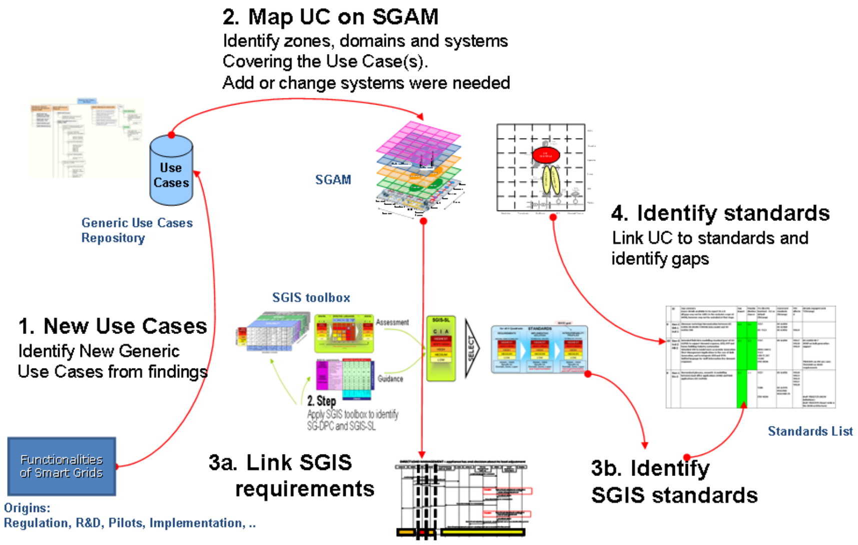

2. Map UC on SGAM
Identify zones, domains and systems
Covering the Use Case(s).
Add or change systems were needed
Use Cases
Generic Use Cases Repository
SGAM
4. Identify standards
Link UC to standards and identify gaps
SGIS toolbox
Assessment
Guidance
SGIS-SL
SELECT
2. Step
Apply SGIS toolbox to identify SG-DPC and SGIS-SL
1. New Use Cases
Identify New Generic Use Cases from findings
Standards List
Functionalities of Smart Grids
Origins:
Regulation, R&D, Pilots, Implementation, ..
3a. Link SGIS requirements
3b. Identify SGIS standards

**Figure 13: SGIS Toolbox in Smart Grid Use Case General Framework**

The SGIS Toolbox objective is to provide Smart Grid Use Case stakeholders an easy and pragmatic way to identify what might be their use case security needs. It can be used as exposed hereunder:

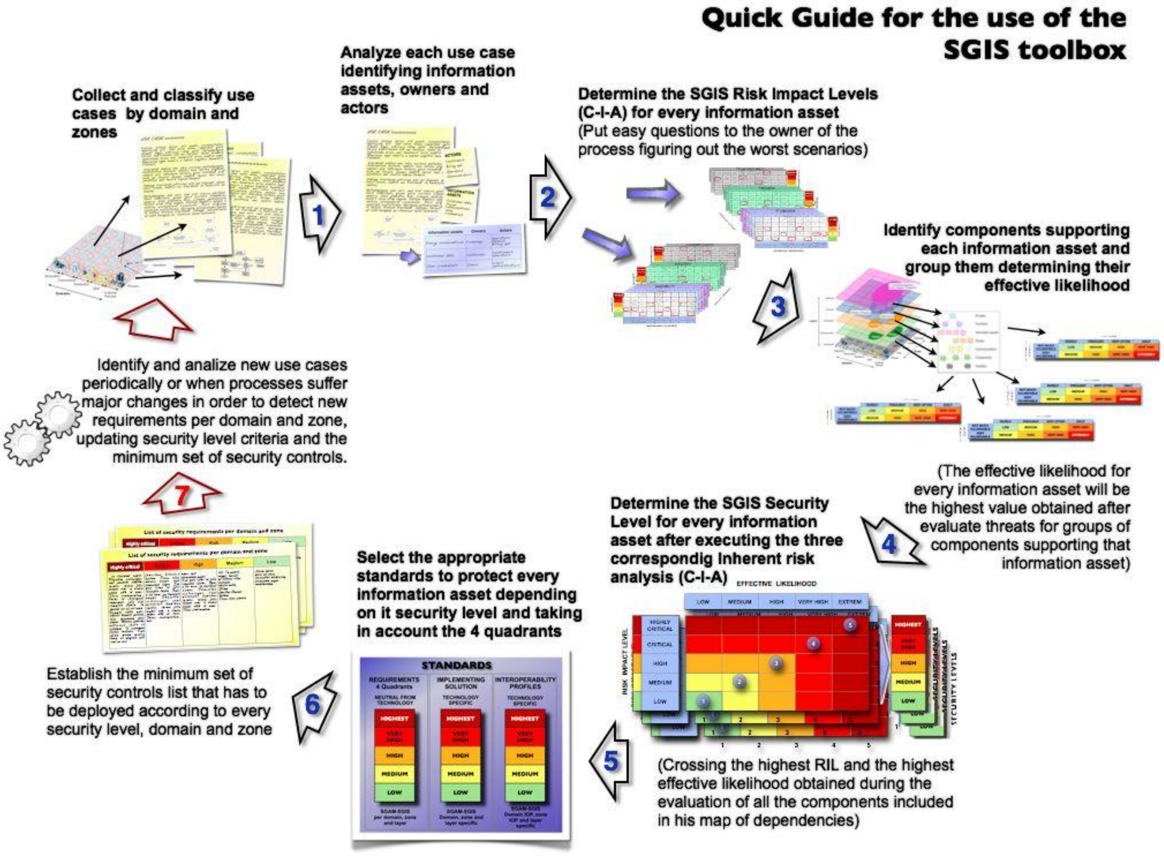
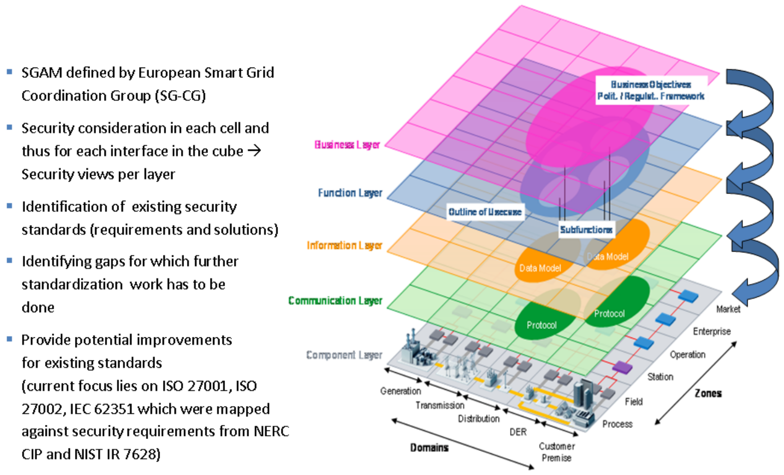

Quick Guide for the use of the SGIS toolbox
Collect and classify use cases by domain and zones
1
Analyze each use case identifying information assets, owners and actors
2
Determine the SGIS Risk Impact Levels (C-I-A) for every information asset (Put easy questions to the owner of the process figuring out the worst scenarios)
3
Identify components supporting each information asset and group them determining their effective likelihood
(The effective likelihood for every information asset will be the highest value obtained after evaluate threats for groups of components supporting that information asset)
4
Determine the SGIS Security Level for every information asset after executing the three correspondig inherent risk analysis (C-I-A)
(Crossing the highest RIL and the highest effective likelihood obtained during the evaluation of all the components included in his map of dependencies)
5
Select the appropriate standards to protect every information asset depending on it security level and taking in account the 4 quadrants
STANDARDS
6
Establish the minimum set of security controls list that has to be deployed according to every security level, domain and zone
7
Identify and analize new use cases periodically or when processes suffer major changes in order to detect new requirements per domain and zone, updating security level criteria and the minimum set of security controls.

**Figure 14: Quick Guide for the use of the SGIS Toolbox**

The details of the proposed SGIS Risk Assessment methodology can be found in Annex B - SGIS Risk Impact Level Assessment Methodology.

## 11.2 How to use the Toolbox

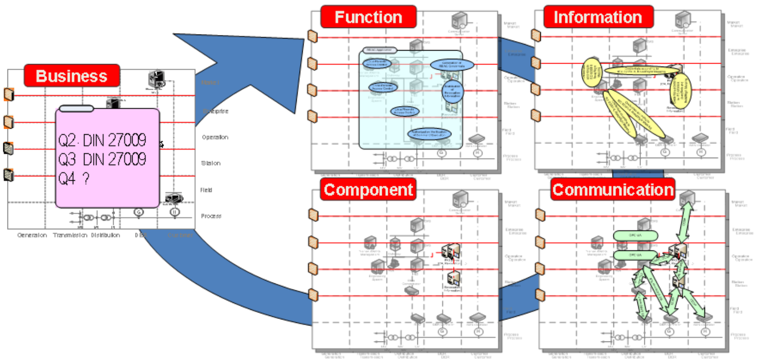
For a use case, by drilling down the SGAM in regard of the use case function and the information used to deliver the function, you identify the Domains, Zones and Layers crossed by the use case.



- SGAM defined by European Smart Grid Coordination Group (SG-CG)
- Security consideration in each cell and thus for each interface in the cube → Security views per layer
- Identification of existing security standards (requirements and solutions)
- Identifying gaps for which further standardization work has to be done
- Provide potential improvements for existing standards (current focus lies on ISO 27001, ISO 27002, IEC 62351 which were mapped against security requirements from NERC CIP and NIST IR 7628)

**Figure 15: Use case mapping using SGAM**

An example of security use case mapping has been defined jointly by SG-CG/FSS and SG-CG/SGIS team. It is about Authentication, Authorization and Accounting systems and can be found in SG-CG/FSS report, §8.9.4.



example of IEC 62351–8 RBAC

**Figure 16: Use Case SGAM Layers coverage example**

Business layer includes Q2 organizational requirements, Q3 purchasing requirements and Q4 Governance requirements (cf. §10). It is binding actor credentials to roles, access rights management and role management (human and technical). The business layer is also where legal or company policies essential requirements related to the use case are given (i.e. key anchors, time synchronicity).

Function layer includes commercial, functional and SGIS use cases. Use cases describe the role/actor usage of data (capture, reception, processing, storage, sending and erase), data-models (information assets) including its access control to components but also command execution, authentication and authorization control. Please note use cases describe the intention of usage of information assets. Use cases do NOT describe foreseeable non intentional usage or illegal usage of information assets – this is addressed by the risk assessment.

Information layer defines the information assets and its data Protection classes (SG-DPC), the Role Based Access Control (RBAC) credential specification (includes mapping of access rights of certain roles held by human or technical actors) to data-models (rights on specific information assets) or to Smart Grid Data Protection Classes (SG-DPC). Please note that IEC TC57 WG15 already provides an approach for RBAC in power system environments with IEC 62351-8.

Communication layer include all technical requirements for all data-models or SG-DPC that are sent or received for all SGIS-SL.

Component layer includes all technical SGIS requirements for the system components. The System component is utilizing role information to grant access (remote or local) utilizing build in sub-components for credential handling like certificate generation or revocation. It also includes requirements about attacks at component level depending on the organizational requirement for physical protection to be applied for the System component

Using either the security view per layer or your risk assessment results you now have identified your required SGIS Security Levels for each domain/zone cell crossed.

Knowing the required SGIS Security Level, you are able to identify security requirements and standards that could be used to implement the requirements using Annex A and SG-CG/FSS §9.3 Security standards list.

Annex C - SGIS Toolbox experience feedback presents some examples of SGIS Toolbox usage on use case by Smart Grid stakeholders.

# 12 Next Steps

The list hereunder presents additional works to be further elaborated by SG-CG/SGIS:

- Analysis of IEC/62443-X-Y and other relevant standards
- Analysis of ISO/IEC 19790:2012 and ISO/IEC 15408 and other relevant standards
- Review of current SGIS-SL scale to reflect sizing evolution of the electrical grid network
- Update of SGIS Toolbox (Risk Assessment and Security Levels vs. requirements)
- Review of NISTIR-7628 and new Security requirements per SGIS-SL to be defined
- Bridge between SGIS security levels and NISTIR-7628 security levels
- Collect SGIS Toolbox Usage examples
- Develop SGIS specific use cases
- Develop collaboration on security topics with other task forces and organisations (M/441, ESMIG, M/468, ISO, IEC, ENISA, EC SGTF-EG2, SGIP-CSWG…)

# 13 Conclusion

As exposed all over this report, European Smart Grid is under construction and still not a physical reality. Additionally the Smart Grid is heterogeneous and complex as reflected by the varying weight of the Confidentiality, Integrity and Availability as essential requirements and the issue encountered to address Information Security topics for the Smart Grid as a whole.

The conclusion of this report is that the standards needed to establish the basis of the Smart Grid Information Security are available today. Nevertheless there is a need for enhancement and for additional standards to integrate Smart Grid specific needs with a particular attention paid implementing them at organizations and in system components (inherently secure by design and default configuration when brought to market or into operation – as well as while in operation) to guarantee interoperability and ensure on-going respect of good practices. Both functional and implementation security aspects should be addressed.

This can not be a one shot only. This will require a continuous effort. The real challenge will be to maintain this effort and to have standards evolving as fast as the Smart Grid Information Security needs. This is the only way to reach end to end security to ensure appropriate SGIS-SL are reaching to the final nodes (Sensors/Actors) i.e. also in Customer site domain and its property internal domains and zones. The SGIS Toolbox is a valuable tool to be further developed and maintained that can be used to reach this objective.

As a final thought, outside of standardization, the risks of connecting Smart Grid critical infrastructures equipments to public networks should be carefully considered in all implementations, as well as the opportunity to send encrypted and authenticated orders to smart grid components. Additionally, the need for a European Organization for the Smart Grid sector similar to US ICS-CERT has been identified. This organization should be mandated to support incident management and provide information on Smart Grid systems and information security incidents and the required response to those.

# Annex A - NISTIR-7628 Security Guidelines per Security Level

There are several security measures that can be applied on different SL. The difference in the application on different SL can be the strength of the security measure. An example can be given by authentication, which could be user name password combinations for SL1, while it could be certificate based authentication on SL3. This may lead at the end to a catalogue of security measures, comprising cryptographically based measures but also local measures like plausibility checks or contingency analysis. Further work is required and will be performed to best fit all Smart Grid stakeholders' need.

| LEGEND | |
|---|---|
| Recommended | 🟩 |
| Stakeholder Decision | 🟪 |

| NISTIR-7628 | | | SGIS - SL | | | | |
|---|---|---|---|---|---|---|---|
| Security Guidelines | Reference | Category | Low<br>1 | Medium<br>2 | High<br>3 | Critical<br>4 | Highest<br>5 |
| ACCESS CONTROL | SG.AC | | | | | | |
| Access Control Policy and Procedures | SG.AC.1 | Governance | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Remote Access Policy and Procedures | SG.AC.2 | Governance | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Account Management | SG.AC.3 | Governance | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Access Enforcement | SG.AC.4 | Governance | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Information Flow Enforcement | SG.AC.5 | Technical | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Separation of Duties | SG.AC.6 | Technical | 🟪 | 🟩 | 🟩 | 🟩 | 🟩 |
| Least Privilege | SG.AC.7 | Technical | 🟪 | 🟩 | 🟩 | 🟩 | 🟩 |
| Unsuccessful Login Attempts | SG.AC.8 | Technical | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Smart Grid Information System Use Notification | SG.AC.9 | Technical | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Previous Logon Notification | SG.AC.10 | Technical | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Concurrent Session Control | SG.AC.11 | Technical | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Session Lock | SG.AC.12 | Technical | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Remote Session Termination | SG.AC.13 | Technical | 🟪 | 🟩 | 🟩 | 🟩 | 🟩 |
| Permitted Actions without Identification or Authentication | SG.AC-14 | Technical | 🟪 | 🟩 | 🟩 | 🟩 | 🟩 |
| Remote Access | SG.AC-15 | Technical | 🟪 | 🟪 | 🟩 | 🟩 | 🟩 |
| Wireless Access Restrictions | SG.AC-16 | Technical | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Access Control for Portable and Mobile Devices | SG.AC-17 | Technical | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Use of External Information Control Systems | SG.AC-18 | Governance | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Control System Access Restrictions | SG.AC-19 | Governance | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Publicly Accessible Content | SG.AC-20 | Governance | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Passwords | SG.AC-21 | Governance | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| AWARENESS AND TRAINING | SG.AT | | | | | | |
| Awareness and Training Policy and Procedures | SG.AT-1 | Governance | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Security Awareness | SG.AT-2 | Governance | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Security Training | SG.AT-3 | Governance | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Security Awareness and Training Records | SG.AT-4 | Governance | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Contact with Security Groups and Associations | SG.AT-5 | Governance | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Security Responsibility Testing | SG.AT-6 | Governance | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Planning Process Training | SG.AT-7 | Governance | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| AUDIT AND ACCOUNTABILITY | SG.AU | | | | | | |
| Audit and Accountability Policy and Procedures | SG.AU-1 | Governance | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Auditable Events | SG.AU-2 | Technical | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Content of Audit Records | SG.AU-3 | Technical | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Audit Storage Capacity | SG.AU-4 | Technical | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Response to Audit Processing Failures | SG.AU-5 | Governance | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Audit Monitoring, Analysis, and Reporting | SG.AU-6 | Governance | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Audit Reduction and Report Generation | SG.AU-7 | Governance | 🟪 | 🟩 | 🟩 | 🟩 | 🟩 |
| Time Stamps | SG.AU-8 | Governance | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Protection of Audit Information | SG.AU-9 | Governance | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Audit Record Retention | SG.AU-10 | Governance | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Conduct and Frequency of Audits | SG.AU-11 | Governance | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Auditor Qualification | SG.AU-12 | Governance | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Audit Tools | SG.AU-13 | Governance | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Security Policy Compliance | SG.AU-14 | Governance | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Audit Generation | SG.AU-15 | Technical | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Non-Repudiation | SG.AU-16 | Technical | 🟪 | 🟩 | 🟩 | 🟩 | 🟩 |

| NISTIR-7628 | | | SGIS - SL | | | | |
|---|---|---|---|---|---|---|---|
| Security Guidelines | Reference | Category | Low<br>1 | Medium<br>2 | High<br>3 | Critical<br>4 | Highest<br>5 |
| **SECURITY ASSESSMENT AND AUTHORIZATION** | **SG.CA** | | | | | | |
| Security Assessment and Authorization Policy and Procedures | SG.CA-1 | Governance | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Security Assessments | SG.CA-2 | Governance | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Continuous Improvement | SG.CA-3 | Governance | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Smart Grid Information System Connections | SG.CA-4 | Governance | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Security Authorization to Operate | SG.CA-5 | Governance | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Continuous Monitoring | SG.CA-6 | Governance | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| **CONFIGURATION MANAGEMENT** | **SG.CM** | | | | | | |
| Configuration Management Policy and Procedures | SG.CM-1 | Governance | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Baseline Configuration | SG.CM-2 | Governance | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Configuration Change Control | SG.CM-3 | Governance | 🟪 | 🟩 | 🟩 | 🟩 | 🟩 |
| Monitoring Configuration Changes | SG.CM-4 | Governance | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Access Restrictions for Configuration Change | SG.CM-5 | Governance | 🟪 | 🟩 | 🟩 | 🟩 | 🟩 |
| Configuration Settings | SG.CM-6 | Governance | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Configuration for Least Functionality | SG.CM-7 | Technical | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Component Inventory | SG.CM-8 | Technical | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Addition, Removal, and Disposal of Equipment | SG.CM-9 | Governance | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Factory Default Settings Management | SG.CM-10 | Governance | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Configuration Management Plan | SG.CM-11 | Governance | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| **CONTINUITY OF OPERATIONS** | **SG.CP** | | | | | | |
| Continuity of Operations Policy and Procedures | SG.CP-1 | Governance | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Continuity of Operations Plan | SG.CP-2 | Governance | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Continuity of Operations Roles and Responsibilities | SG.CP-3 | Governance | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Continuity of Operations Training | SG.CP-4 | Governance | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Continuity of Operations Plan Testing | SG.CP-5 | Governance | 🟪 | 🟩 | 🟩 | 🟩 | 🟩 |
| Continuity of Operations Plan Update | SG.CP-6 | Governance | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Alternate Storage Sites | SG.CP-7 | Governance | 🟪 | 🟩 | 🟩 | 🟩 | 🟩 |
| Alternate Telecommunication Services | SG.CP-8 | Governance | 🟪 | 🟩 | 🟩 | 🟩 | 🟩 |
| Alternate Control Center | SG.CP-9 | Governance | 🟪 | 🟩 | 🟩 | 🟩 | 🟩 |
| Smart Grid Information System Recovery and Reconstitution | SG.CP-10 | Governance | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Fail-Safe Response | SG.CP-11 | Governance | 🟪 | 🟪 | 🟩 | 🟩 | 🟩 |
| **IDENTIFICATION AND AUTHENTICATION** | **SG.IA** | | | | | | |
| Identification and Authentication Policy and Procedures | SG.IA-1 | Governance | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Identifier Management | SG.IA-2 | Governance | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Authenticator Management | SG.IA-3 | Governance | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| User Identification and Authentication | SG.IA-4 | Technical | 🟪 | 🟩 | 🟩 | 🟩 | 🟩 |
| Device Identification and Authentication | SG.IA-5 | Technical | 🟪 | 🟩 | 🟩 | 🟩 | 🟩 |
| Authenticator Feedback | SG.IA-6 | Technical | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| **INFORMATION AND DOCUMENT MANAGEMENT** | **SG.ID** | | | | | | |
| Information and Document Management Policy and Procedures | SG.ID-1 | Governance | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Information and Document Retention | SG.ID-2 | Governance | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Information Handling | SG.ID-3 | Governance | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Information Exchange | SG.ID-4 | Governance | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Automated Labeling | SG.ID-5 | Governance | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| **INCIDENT RESPONSE** | **SG.IR** | | | | | | |
| Incident Response Policy and Procedures | SG.IR-1 | Governance | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Incident Response Roles and Responsibilities | SG.IR-2 | Governance | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Incident Response Training | SG.IR-3 | Governance | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Incident Response Testing and Exercises | SG.IR-4 | Governance | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Incident Handling | SG.IR-5 | Governance | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Incident Monitoring | SG.IR-6 | Governance | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Incident Reporting | SG.IR-7 | Governance | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Incident Response Investigation and Analysis | SG.IR-8 | Governance | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Corrective Action | SG.IR-9 | Governance | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Smart Grid Information System Backup | SG.IR-10 | Governance | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Coordination of Emergency Response | SG.IR-11 | Governance | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| **SMART GRID INFORMATION SYSTEM DEVELOPMENT AND MAINTENANCE** | **SG.MA** | | | | | | |
| Smart Grid Information System Maintenance Policy | SG.MA-1 | Governance | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Legacy Smart Grid Information System Upgrades | SG.MA-2 | Governance | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Smart Grid Information System Maintenance | SG.MA-3 | Governance | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Maintenance Tools | SG.MA-4 | Governance | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Maintenance Personnel | SG.MA-5 | Governance | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Remote Maintenance | SG.MA-6 | Governance | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Timely Maintenance | SG.MA-7 | Governance | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |

| NISTIR-7628 | | | SGIS - SL | | | | |
|---|---|---|---|---|---|---|---|
| Security Guidelines | Reference | Category | Low<br>1 | Medium<br>2 | High<br>3 | Critical<br>4 | Highest<br>5 |
| **MEDIA PROTECTION** | **SG.MP** | | | | | | |
| Media Protection Policy and Procedures | SG.MP-1 | Governance | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Media Sensitivity Level | SG.MP-2 | Governance | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Media Marking | SG.MP-3 | Governance | 🟪 | 🟩 | 🟩 | 🟩 | 🟩 |
| Media Storage | SG.MP-4 | Governance | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Media Transport | SG.MP-5 | Governance | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Media Sanitization and Disposal | SG.MP-6 | Governance | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| **PHYSICAL AND ENVIRONMENTAL SECURITY** | **SG.PE** | | | | | | |
| Physical and Environmental Security Policy and | SG.PE-1 | Governance | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Physical Access Authorizations | SG.PE-2 | Governance | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Physical Access | SG.PE-3 | Governance | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Monitoring Physical Access | SG.PE-4 | Governance | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Visitor Control | SG.PE-5 | Governance | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Visitor Records | SG.PE-6 | Governance | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Physical Access Log Retention | SG.PE-7 | Governance | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Emergency Shutoff Protection | SG.PE-8 | Governance | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Emergency Power | SG.PE-9 | Governance | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Delivery and Removal | SG.PE-10 | Governance | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Alternate Work Site | SG.PE-11 | Governance | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Location of Smart Grid Information System Assets | SG.PE-12 | Governance | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| **PLANNING** | **SG.PL** | | | | | | |
| Strategic Planning Policy and Procedures | SG.PL-1 | Governance | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Smart Grid Information System Security Plan | SG.PL-2 | Governance | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Rules of Behavior | SG.PL-3 | Governance | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Privacy Impact Assessment | SG.PL-4 | Governance | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Security-Related Activity Planning | SG.PL-5 | Governance | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| **SECURITY PROGRAM MANAGEMENT** | **SG.PM** | | | | | | |
| Security Policy and Procedures | SG.PM-1 | Governance | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Security Program Plan | SG.PM-2 | Governance | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Senior Management Authority | SG.PM-3 | Governance | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Security Architecture | SG.PM-4 | Governance | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Risk Management Strategy | SG.PM-5 | Governance | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Security Authorization to Operate Process | SG.PM-6 | Governance | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Mission/Business Process Definition | SG.PM-7 | Governance | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Management Accountability | SG.PM-8 | Governance | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| **PERSONNEL SECURITY** | **SG.PS** | | | | | | |
| Personnel Security Policy and Procedures | SG.PS-1 | Governance | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Position Categorization | SG.PS-2 | Governance | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Personnel Screening | SG.PS-3 | Governance | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Personnel Termination | SG.PS-4 | Governance | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Personnel Transfer | SG.PS-5 | Governance | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Access Agreements | SG.PS-6 | Governance | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Contractor and Third-Party Personnel Security | SG.PS-7 | Governance | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Personnel Accountability | SG.PS-8 | Governance | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Personnel Roles | SG.PS-9 | Governance | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| **RISK MANAGEMENT AND ASSESSMENT** | **SG.RA** | | | | | | |
| Risk Assessment Policy and Procedures | SG.RA-1 | Governance | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Risk Management Plan | SG.RA-2 | Governance | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Security Impact Level | SG.RA-3 | Governance | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Risk Assessment | SG.RA-4 | Governance | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Risk Assessment Update | SG.RA-5 | Governance | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Vulnerability Assessment and Awareness | SG.RA-6 | Governance | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| **SMART GRID INFORMATION SYSTEM AND SERVICES ACQUISITION** | **SG.SA** | | | | | | |
| Smart Grid Information System and Services Acquisition Policy and Procedures | SG.SA-1 | Governance | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Security Policies for Contractors and Third Parties | SG.SA-2 | Governance | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Life-Cycle Support | SG.SA-3 | Governance | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Acquisitions | SG.SA-4 | Governance | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Smart Grid Information System Documentation | SG.SA-5 | Governance | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Software License Usage Restrictions | SG.SA-6 | Governance | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| User-Installed Software | SG.SA-7 | Governance | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Security Engineering Principles | SG.SA-8 | Governance | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Developer Configuration Management | SG.SA-9 | Governance | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Developer Security Testing | SG.SA-10 | Technical | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Supply Chain Protection | SG.SA-11 | Technical | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |

| NISTIR-7628 | | | SGIS - SL | | | | |
|---|---|---|---|---|---|---|---|
| Security Guidelines | Reference | Category | Low<br>1 | Medium<br>2 | High<br>3 | Critical<br>4 | Highest<br>5 |
| **SMART GRID INFORMATION SYSTEM AND COMMUNICATION PROTECTION** | **SG.SC** | | | | | | |
| Smart Grid Information System and Communication Protection Policy and Procedures | SG.SC-1 | Governance | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Communications Partitioning | SG.SC-2 | Technical | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Security Function Isolation | SG.SC-3 | Technical | 🟪 | 🟩 | 🟩 | 🟩 | 🟩 |
| Information Remnants | SG.SC-4 | Technical | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Denial-of-Service Protection | SG.SC-5 | Technical | 🟪 | 🟩 | 🟩 | 🟩 | 🟩 |
| Resource Priority | SG.SC-6 | Technical | 🟪 | 🟪 | 🟩 | 🟩 | 🟩 |
| Boundary Protection | SG.SC-7 | Technical | 🟪 | 🟩 | 🟩 | 🟩 | 🟩 |
| Communication Integrity | SG.SC-8 | Technical | 🟪 | 🟩 | 🟩 | 🟩 | 🟩 |
| Communication Confidentiality | SG.SC-9 | Technical | 🟪 | 🟪 | 🟩 | 🟩 | 🟩 |
| Trusted Path | SG.SC-10 | Technical | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Cryptographic Key Establishment and Management | SG.SC-11 | Technical | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Use of Validated Cryptography | SG.SC-12 | Technical | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Collaborative Computing | SG.SC-13 | Governance | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Transmission of Security Parameters | SG.SC-14 | Technical | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Public Key Infrastructure Certificates | SG.SC-15 | Technical | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Mobile Code | SG.SC-16 | Technical | 🟪 | 🟩 | 🟩 | 🟩 | 🟩 |
| Voice-Over Internet Protocol | SG.SC-17 | Technical | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| System Connections | SG.SC-18 | Technical | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Security Roles | SG.SC-19 | Technical | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Message Authenticity | SG.SC-20 | Technical | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Secure Name/Address Resolution Service | SG.SC-21 | Technical | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Fail in Known State | SG.SC-22 | Technical | 🟪 | 🟩 | 🟩 | 🟩 | 🟩 |
| Thin Nodes | SG.SC-23 | Technical | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Honeypots | SG.SC-24 | Technical | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Operating System-Independent Applications | SG.SC-25 | Technical | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Confidentiality of Information at Rest | SG.SC-26 | Technical | 🟪 | 🟪 | 🟩 | 🟩 | 🟩 |
| Heterogeneity | SG.SC-27 | Technical | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Virtualization Techniques | SG.SC-28 | Technical | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Application Partitioning | SG.SC-29 | Technical | 🟪 | 🟪 | 🟩 | 🟩 | 🟩 |
| Smart Grid Information System Partitioning | SG.SC-30 | Technical | 🟪 | 🟩 | 🟩 | 🟩 | 🟩 |
| **SMART GRID INFORMATION SYSTEM AND INFORMATION INTEGRITY** | **SG.SI** | | | | | | |
| Smart Grid Information System and Information Integrity Policy and Procedures | SG.SI-1 | Governance | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Flaw Remediation | SG.SI-2 | Technical | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Malicious Code and Spam Protection | SG.SI-3 | Technical | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Smart Grid Information System Monitoring Tools and Techniques | SG.SI-4 | Governance | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Security Alerts and Advisories | SG.SI-5 | Governance | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Security Functionality Verification | SG.SI-6 | Governance | 🟪 | 🟩 | 🟩 | 🟩 | 🟩 |
| Software and Information Integrity | SG.SI-7 | Technical | 🟪 | 🟩 | 🟩 | 🟩 | 🟩 |
| Information Input Validation | SG.SI-8 | Technical | 🟪 | 🟩 | 🟩 | 🟩 | 🟩 |
| Error Handling | SG.SI-9 | Technical | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |

# Annex B - SGIS Risk Impact Assessment Methodology

## 1. Considerations and assumptions

- Risk impact is by definition the impact that a possible information security compromise has on the operations or efficiency of the organization or even on customers or citizens.

- The risk impact analysis is the first stage for the risk assessment. It describes the consequences that may happen in case of smart grids were compromised for any method by a threat actor affecting confidentiality, integrity or availability of information assets.

- For the scope of the analysis consider an **information asset** as a type of information stored and managed for a particular purpose. i.e. billing data, personal data, etc. Each information asset belongs to a single owner (individual or organization), is valuable for him and could be managed by different actors as part of the process or use case where it’s involved.

- A risk impact analysis starts evaluating the processes and subprocesses involved in all the smart grid domains and zones and finishes determining the maximum possible impact for involved stakeholders (e.g., customers or citizens).

- SG-RIL evaluates **inherent risks** (that means, processes, information assets and supporting components without security measures in place) as the only way to determine how important is every information asset for the organization. Collected uses cases shouldn’t include or describe security controls in place. If they are depicted, both SG risk impact assessment and SG risk analysis should avoid them.

- Next diagram depicts how the SGIS-RIL fits in the SGIS toolbox:

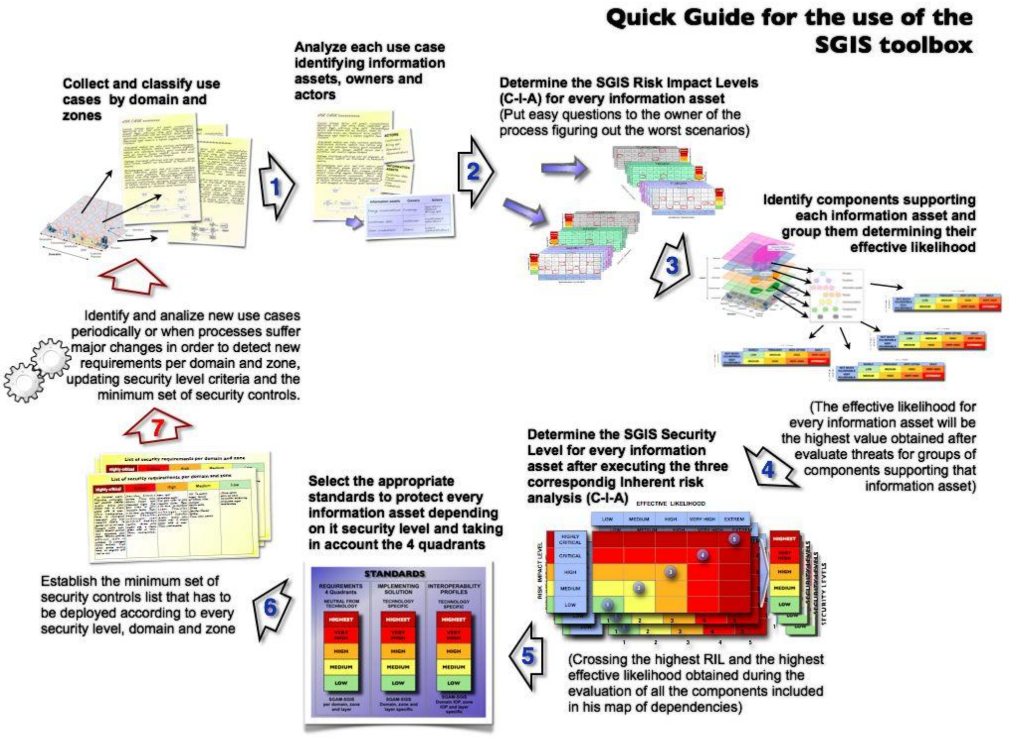

Quick Guide for the use of the SGIS toolbox
Collect and classify use cases by domain and zones
1
Analyze each use case identifying information assets, owners and actors
2
Determine the SGIS Risk Impact Levels (C-I-A) for every information asset (Put easy questions to the owner of the process figuring out the worst scenarios)
3
Identify components supporting each information asset and group them determining their effective likelihood
4
(The effective likelihood for every information asset will be the highest value obtained after evaluate threats for groups of components supporting that information asset)
Determine the SGIS Security Level for every information asset after executing the three correspondig Inherent risk analysis (C-I-A)
EFFECTIVE LIKELIHOOD
LOW
MEDIUM
HIGH
VERY HIGH
EXTREM
RISK IMPACT LEVEL
HIGHEST
CRITICAL
HIGH
MEDIUM
LOW
SECURITY LEVELS
5
(Crossing the highest RIL and the highest effective likelihood obtained during the evaluation of all the components included in his map of dependencies)
Select the appropriate standards to protect every information asset depending on it security level and taking in account the 4 quadrants
STANDARDS
REQUIREMENTS 4 Quadrants
IMPLEMENTING SOLUTION
INTEROPERABILITY PROFILES
NEUTRAL FROM TECHNOLOGY
TECHNOLOGY SPECIFIC
TECHNOLOGY SPECIFIC
HIGHEST
VERY HIGH
HIGH
MEDIUM
LOW
6
Establish the minimum set of security controls list that has to be deployed according to every security level, domain and zone
List of security requirements per domain and zone
7
Identify and analize new use cases periodically or when processes suffer major changes in order to detect new requirements per domain and zone, updating security level criteria and the minimum set of security controls.

**Figure 1 — A simple step by step guide for the inherent risk analysis process**

- As the above diagram describes, SG-Risk Impact Assessment is part of a continuous process. Even although technical equipment could stay in field 10 or 20 years, smart grid processes evolve dramatically and new threats appear every day. This changing scenario requires

**periodical reviews** of the executed risk levels analysis as well as the entire criteria and categories defined in the SGIS toolbox. The SGIS-RIL shall be executed:

  - Periodically (once a year)
  - When processes suffer major changes
  - When new actors are involved

- The result of any iteration implies a review of pre-established security levels and security requirements identifying GAPS and checking the need for update existent standards and regulations or for create new ones.

- Organizations shall execute periodical GAP analysis identifying deviations or lacks from the mandatory SG security requirements and their particular implementations.

- In order to assure accurate and reliable results, the smart grid risk impact assessment and the smart grid risk analysis as well, shall be executed by smart grid experts (people with a high degree of knowledge about the involved smart grid processes) and shall be driven by information security professionals familiarized with the proposed methodology and terminology.

- Use cases are the start point for the assessment. They describe processes related to each smart grid domain and zone, helping to identify information assets, their owners and supporting components, as well as other involved actors and process interoperability.

- Information assets are the unit of work when analyzing the risk associated to use cases. Every information asset has one owner, it could be involved in several use cases and It has several supporting components to take in account during the assessment (actors, systems, facilities, etc.). After the assessment, every information asset should have a particular risk impact level so, when a particular information asset appears in different use cases it will be necessary to group those use cases obtaining a global view of the process (if it take sense) or just consider the highest risk impact level for that asset, obtained from the analysis of every use case where it is involved.

- SG Risk Impact assessment considers risks associated with interconnected components, systems and layers in order to assess interoperability security risks and requirements.

## 2. Collecting use cases

- In order to assure the best and reliable results executing the SGIS security risk analysis, it is critical to gather detailed and complete use cases identifying clearly the domain and zone (one or more) whose belongs.

- Each domain covers a set of particular processes and has different actors and owners. Drilling down in domains, zones are subprocesses within each domain representing hierarchical levels of power system management where different actors, technologies and specific activities are involved.

- The risk assessment of specific use cases, crossing over domains and zones, will allow to determine consolidated risk levels and security requirements for all involved SGAM cells.

- Basically, a use case is a document describing a process or subprocess where different elements or assets are involved.

- Following the form template defined by Sustainable Process Group, for the risk assessment process, each use case should at least:

- Describe the related process in terms of goals, main activities, expected times for the execution of the whole process and activities if it makes sense, involved regulations or laws determining how it has to be executed.

- Identify the owner of the process as its maximum responsible (It would be very useful if the owner of the process or use case could participate in the risk impact assessment).

- Identify and explain the purpose of its information assets.

- Identify the owner of every information asset and the rest of actors involved in its processing (administrators, operators, developers, users, ...) explaining briefly their capabilities processing every information asset.

- Who enters the information (people or devices)? Who processes it (one or more actors)? How is it processed (manually, automatically?) Is any other actor processing or accessing the data? Are there any systems administrators who could view or alter the data? Is the whole process executed by one single company or are there more companies usually involved? In that case, does all that companies need to access to the information asset? Who is the final owner of the information data (customers, organizations, …)?

- Enumerate another elements involved in processing every information asset from the business and functional point of view.

- Does it needs a network to transfer the information? Does it needs servers, computers or any other devices to store the data or applications to visualize and manage it? Any other devices to get and process the information, like smart meters, industrial readers, sensors, Scada systems ...? all the process is executed from the same site or place with controlled computers? Are they executed from different facilities? May be a part of the process executed from the field with mobile devices of from customer houses with their own devices?.

- Avoid to include in the use case mentions or references to security controls or identify them clearly in order to avoid them during the Risk Analysis process (it has to be an inherent risk analysis).

- Use cases should describe just the business process where collecting, processing and generating data are part of the goal of the process. If security elements in place are described, it will be important to identify them clearly and to avoid them during the inherent risk analysis process.

- If use cases don't provide enough information then assumptions have to be taken and documented during the risk impact analysis.

- Take in mind that collecting and executing risk analysis from poor or incomplete use cases could derive in wrong classifications and other mistakes impacting in the final results.

- Finally, there is another type of specific use cases related to SG information security (i.e. user credentials management).

## 3. SGIS-RIL classification criteria

- The risk impact analysis covers ALL SGIS essential requirements as defined in Section 4 of the main report. Therefore a classification criteria is needed for group and evaluate each of those essential requirements.

- All classification criteria are evaluated for the inherent situation, meaning that all use cases shall be assessed under the assumption that no controls (aka security measures or countermeasures) are implemented at all.

- Determining the adequate risk impact level is a complex process where different aspects have to be taken in account when analyzing how incidents affect to every information asset.

- Classical Information Security Risk Analysis evaluates the three main aspects of information security, enumerated as the first three essential requirements presented in section 4 of the main report (confidentiality, integrity and availability).

- This three essential requirements and the rest of essential requirements defined in this document as well are taken in account in the SGIS risk impact analysis methodology. Some of them will be considered measurement categories, others will determine scenarios for the evaluation.

### 3.1. Risk Impact Scale

- The Risk Impact is established analyzing how incidents into a particular information asset affects to the process where it is involved. Different incidents produce different impacts. So the highest impact identified in all the possible scenarios determines the Risk impact level for the analyzed information asset.

- The result is expressed in a scale from 1 to 5 where level 1 is the lowest possible and 5 the highest risk impact level. Below is the notation used to express these levels:

| | |
|---|---|
| RIL 5: Highly Critical Impact | 🟫 |
| RIL 4: Critical Impact | 🟥 |
| RIL 3: High Impact | 🟧 |
| RIL 2: Medium Impact | 🟨 |
| RIL 1: Low Impact | 🟨 |

### 3.2. Risk Impact Categories

- Security incidents against information assets affect to their involved processes in different ways. SGIS Impact Analysis methodology identifies six different types of affectation or categories. Categories should be evaluated independently. Every one assesses the impact with a particular criteria using the scale defined above (from 1 to 5).

- This section describes six categories that must be evaluated during this process for identifying the risk impact produced by security incidents. Two of these categories are subdivided in subcategories as indicated in next list:

-

| CATEGORIES | SUBCATEGORIES |
|---|---|
| OPERATIONAL | ENERGY SUPPLY |
| | ENERGY FLOW |
| | POPULATION |
| | INFRASTRUCTURES |
| LEGAL | DATA PROTECTION |
| | OTHER LAWS AND REGULATIONS |
| HUMAN | |
| REPUTATION | |
| ENVIRONMENTAL | |
| FINANCIAL | |

- More categories and/or subcategories could be added here in order to get a deeper and more specific risk impact analysis in smart grids.

- It is a requirement when adding categories or subcategories to evaluate measurable aspects and scales where identified information assets could be easily classified and fitted in. The same principle applies to the proposed categories so the user should select the categories that are relevant for the analysis of his specific use case.

#### 3.2.1. Operational category

- Operational category measures how security incidents impacts in service availability. This category starts offering four different aspects to assess service availability. Other measurable subcategories could be added here if they demonstrate to be useful when analyzing use cases.

- Stakeholders doing this assessment could not always determine RIL for each particular subcategory due to their limited knowledge or even due to particular considerations of the involved information asset and use case. As much subcategories could be assessed, results will be more accurate and reliable.

- Particular thresholds for each proposed scale shall be reviewed by the SGIS group and approved in first instance before to be presented just as a first proposal to the SGCG committee.

- **Energy supply.** Determines the risk impact level based on the size and type of grid affected by an information security incident:

  - RIL1: Networks under 1MW
  - RIL2: Grids from 1MW to 100MW
  - RIL3: Grids from 100MW to **1GW**
  - RIL4: Grids from **1GW** to 10GW
  - RIL5: Grids over 10GW

- **Energy flow.** Determines the risk impact level based on the flow (Watts/hour) affected:

  - RIL1: Under 1MW/h
  - RIL2: From 1MW/h to 100MW/h
  - RIL3: From 100MW/h to **1GW/h**
  - RIL4: From **1GW/h** to 10GW/h
  - RIL5: More than 10GW/h

- **Population**. Determines the risk impact level based on the percentage of people affected in one or more countries (population size and population density were discarded because their variability from one country to another). This scale measures scenarios producing power or access disruptions to critical consumer oriented Smart Grid services:

  - RIL1: Below 2% population size affected by power services disruption in a country
  - RIL2: From 2% to 10% of population size affected by power services disruption in a country
  - RIL3: From 10% to 25% of population size affected by power services disruption in a country
  - RIL4: From 25% to 50% of population size affected by power services disruption in a country
  - RIL5: More than 50% of population size affected by power services disruption in one country or more than 25% in several countries

- **Infrastructures**. Determines the risk impact level based on how many critical, essential or complimentary infrastructures could be affected by a security incident. Usually, at every country, Ministry of Defense defines and determines three types of infrastructures depending of their impact for a nation in case of disruption. The resultant catalog is secret and it's only communicated to the affected companies who operate the mentioned infrastructures. Critical Infrastructures scope determines the risk impact level based on the type of infrastructures affected in case of unavailability.

  - RIL1: Incident doesn't affect any infrastructure included in the catalog (No complimentary, essential nor critical infrastructures affected)
  - RIL2: complimentary infrastructures affected
  - RIL3: Essential infrastructures affected

- RIL4: National critical infrastructures affected
- RIL5: Critical infrastructures affected in more than one country

### 3.2.2. Legal category

- Legal category measures the impact of security incidents deriving in both, legal or regulatory non-fulfillments. Because the tight relation between smart grid and citizens, this category is divided in two subcategories, allowing analyze the privacy impact in an independent manner.

- In terms of information security, legal or regulatory non-fulfillments could derive from several reasons like unavailability of services or inadequate quality of services due to insufficient data protection, disclosure of private information, lack of tracking or accounting, lack of due diligence, etc.

- **Data protection.** Determines the risk impact level in accordance to the definitions to Directive 95/46/EC. Following that, there are two levels of relevant data related to privacy:
  Personal data (cf art. 2): Shall mean any information relating to an identified or identifiable natural person. Considering an identifiable person as one who can be identified directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.
  Sensitive data (cf art. 8): Particular risky personal data what includes: revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, the processing of data concerning health or sex life, biometric and genetic data (judicial interpretation).

  - RIL1: No personal or sensitive data involved
  - RIL2: Unauthorized disclosure or modification of personal data
  - RIL3: Unauthorized disclosure or modification of sensitive data
  - RIL4: not defined yet
  - RIL5: not defined yet

- Last two levels are not defined yet but could be established following the new european privacy criteria.

- **Other laws and regulations.** Determines the risk impact level based on legal and regulation punishments. Every country has different laws and regulations in addition to European directives. All of them have to be taken in account for this assessment. Actors (companies and organizations involved in use cases and processes have to participate during this assessment).

  - RIL1: Only Warnings derived from non-fulfillments
  - RIL2: Fines up to 10% EBITDA as result of legal or regulatory non-fulfillments
  - RIL3: Fines of >10% EBITDA as result of legal or regulatory non-fulfillments
  - RIL4: Temporary disruption as result of legal or regulatory non-fulfillments
  - RIL5: Company closure or collateral disruptions if service providers or third parties were involved in the punishment.

### 3.2.3. Human category

- Human category measures how security incidents impact directly or indirectly on people's health.

  - RIL1: Minor accidents
  - RIL2: People serious injures or incapacity
  - RIL3: Direct deaths

- RIL4: Collateral deaths
- RIL5: Direct and collateral deaths

### 3.2.4. Reputation category

- Reputation category is one of the most difficult aspects to measure when security incidents affect information assets and processes because people reactions are always unpredictable, but it has to be evaluated. Security Incidents damaging an organization's reputation for confidentiality, safety or availability may cause serious damage to finances.

  - RIL1: Short time and scope. Very punctual loss of trust considered as a warning
  - RIL2: Temporary loss of trust in a reduced area or to a specific service/department
  - RIL3: Temporary loss of trust in one country
  - RIL4: Permanent loss of trust in one country
  - RIL5: All corporation affected (international)

### 3.2.5. Environmental category

- Environmental category measures how a security incident on a particular information asset could produce negative changes to the land or ecosystem.

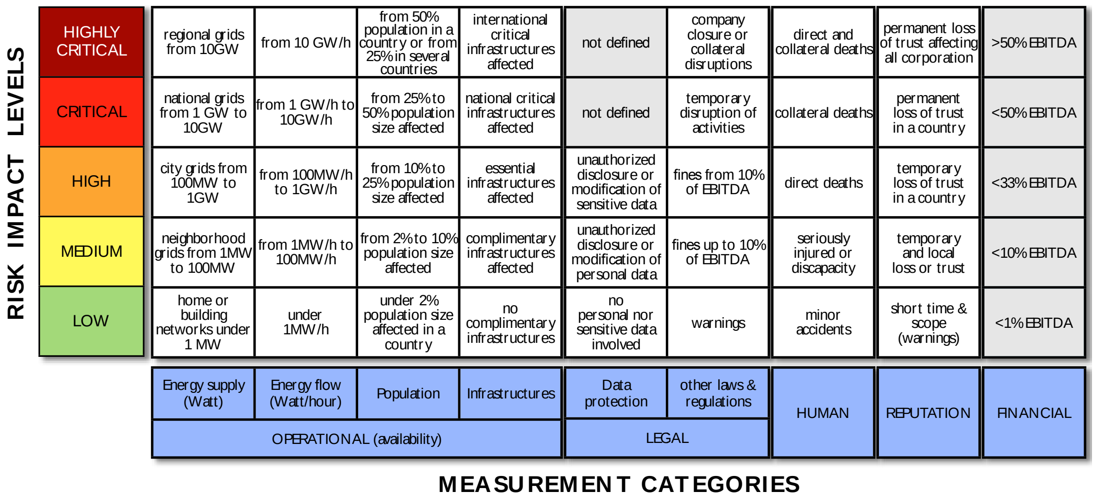
- This category is not filled yet. It was just identified during the last SGIS toolbox application exercise workshop.

### 3.2.6. Financial category

- Financial category measures risk impact based on direct monetary loss derived from information security incidents. This category is **quantitative** and not necessary applies to all use cases so involved people in use cases has to collaborate in the assessment of this category. It's important distinguishing between direct monetary loss and other impact categories what involves indirect or potential monetary loss (i.e. reputation) This scale uses as criteria the annual organization's EBITDA (acronym for Earning Before Interest, Taxes, Depreciation and Amortization).

  - RIL1: Below 1% of EBITDA
  - RIL2: From 1% to 10% of EBITDA
  - RIL3: From 10% to 33% of EBITDA
  - RIL4: From 33% to 50% of EBITDA
  - RIL5: Above 50% of EBITDA

- The table below shows the described categories criteria and its risk impact levels:



| RISK IMPACT LEVELS | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 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 | permanent loss of trust affecting all corporation | >50% EBITDA |
| 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 | collateral deaths | 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 | fines from 10% of EBITDA | direct deaths | temporary loss of trust in a country | <33% EBITDA |
| MEDIUM | neighborhood grids from 1MW to 100MW | from 1MW/h to 100MW/h | from 2% to 10% population size affected | complimentary infrastructures affected | unauthorized disclosure or modification of personal data | fines up to 10% of EBITDA | seriously injured or discapacity | temporary and local loss or trust | <10% EBITDA |
| LOW | home or building networks under 1 MW | under 1MW/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 |
| | Energy supply (Watt) | Energy flow (Watt/hour) | Population | Infrastructures | Data protection | other laws & regulations | HUMAN | REPUTATION | FINANCIAL |
| | OPERATIONAL (availability) | | | | LEGAL | | | | |

MEASUREMENT CATEGORIES

**Figure 2 — The risk impact evaluation table measures impact levels on SG process for one specific asset**

**Current criteria for categories described above are not yet normalized. They should be further discussed and they have to be established based on the existing use cases in the Pan-European context.**

## 3.3. Risk Impact Scenarios

- It's important to understand how **different types of incidents** have different effects over an information asset and over the all process belonging to. I.e. *the financial risk impact level for an asset if a loss of availability occurs wont be the same if the disruption takes one hour than if it takes 3 days.*

- Enumerating and analyzing all the possible threats and incidents for a given information asset and fulfilling as many tables of risk impact levels as the one above, is a hard, long and complex task.

- SGIS risk impact methodology defines a reduced set of scenarios grouping all possible security incidents to make easier and faster the risk impact analysis process without loss reliability. These scenarios are grouped following the three essential requirements presented in section 5 (confidentiality, integrity, availability) and a couple of additional requirements grouped under the term of accounting and assessed within the legal category.

- Evaluating scenarios one level deeper than just confidentiality, Integrity and availability gives a valuable information to guide and identify specific groups of countermeasures for the mitigation plan matching with the compliance of the rest of essential requirements.

- Additionally, the assessment of those scenarios allows to determine specific parameters for defining disaster recovery plans (i.e. Recovery Time Objectives and Recovery Point Objectives; aka RTO and RPO) and to determine specific countermeasures when defining mitigation plans.

- Below are the details for the defined scenarios to take in account during the process of impact assessment.

### 3.3.1. Confidentiality scenarios

- Confidentiality scenarios summarize all security incidents and vector attacks what could be exploited gaining access to internal information and disclosing it to unauthorized people. The lack of legitimacy and authenticity or access of all actors and roles, the lack of encryption and authentication when transmitting control information to smart grid devices and the existence of pathways from outside to smart grid energy transport control systems usually derive in confidentiality scenarios:

- SGIS proposes two security incident scenarios related to confidentiality:

- **Internal disclosure scenario.** It summarizes security incidents where the analyzed information asset would be disclosed to unauthorized but internal people. This scenario doesn't consider unauthorized external people gaining access to information. The main questions to put in place during the evaluation process of Risk impact assessment for this scenario will be:

  *What if an unauthorized insider (employee or hired third party) could get access to 'this' particular information asset for a short or long period of time? Could this information be used to gain access to more relevant or sensitive information assets or to take control or alter systems or processes? How it would impact on the different measurement categories? (operational, legal, human, reputation or financial)*

- **External disclosure scenario.** It includes security incidents where the analyzed information asset would be disclosed to unauthorized external people. This scenario considers explicitly disclosing information to outsiders (i.e. competitors, other customers, providers, ...). The start point for the evaluation of this scenario could be the next questions:

> *What if an outsider (customer, competitor, terrorist, …) could get access to 'this' particular information asset for a short or long period of time? Could this information be used to gain access to more relevant or sensitive information assets or to take control or alter systems or processes? How it would impact from the point of view from the different measurement categories? (operational, legal, human, reputation or financial)*

### 3.3.2. Integrity scenarios

- Integrity scenarios include all security incidents, accidents and vector attacks what could be exploited with the intermediate goal of altering information for multiple malicious purposes (*i.e. altering consumptions to reduce bills, or causing incorrect decisions for the generation and distribution of energy, ...*).

- Information has to be authentic, legitimate, valid, resistant to being interfered with or altered (tamper proof), and actors cannot repudiate what they send or process and when every action is done. Any incident affecting these essential requirements shall to be included within the integrity scenarios.

- SGIS risk impact analysis defines three integrity scenarios:

- **Data loss or alteration by error.** It summarizes security incidents where the analyzed information asset would be accidentally altered or lost during the process. This scenario doesn't consider malicious intentions. The main questions to put in place evaluating this scenario would be:

  > *What if 'this' information asset was accidentally altered or lost? Could we continue working properly? How it could impact to the affected use case and to the whole process or services as well? Could this alteration or loss affect to different processes, systems or information assets?*

- **Manipulation.** It includes all possible incidents where authorized actors could alter information assets with malicious purposes producing different results from what was expected for the defined process. In this scenario, the assessment could start answering next questions:

  > *What if authorized users (administrators, operators, other users …) could alter 'this' information asset? How it could impact to the affected use case and to the whole process or services as well? Could this alteration or loss affect to different processes, systems or information assets?*

- **Authenticity.** Similar to the above scenario (manipulation) but it takes in account when unauthorized users or agents alters information or inject fake information producing different results from what was expected for the defined process. Some questions to cover the impact assessment in that particular scenario could be:

  > *Is this information asset processed in accordance to the origin or owner? What if the information asset were altered with malicious purposes applying data forgery or identity theft? What would be the impact in terms of every defined category (operational, legal, human, reputation or financial)?*

### 3.3.3. Availability scenarios

- These scenarios refer to unavailability of required information for particular services due information security incidents against any component supporting the analyzed information asset or even directly to the asset (i.e. Distributed Denial of Service Attacks).

- SGIS defines a set of scenarios with different recovery times helping to determine the maximum acceptable time to restore information and services. Different Domains, zones and information assets have different needs so it's important to analyze how time of disruption due to information security incidents, affecting data assets, impacts on people, processes and services.

- Robustness in situations of crisis, resiliency in/after blackouts and in respect to system components interdependence are three of the SGSI essential requirements for Smart Grid infrastructures where availability is involved. Interoperability in the Smart Grid Information system and exchangeability of products & services in the EU as well.

- Below are the defined security incident scenarios related to availability from the point of view of smart grid services (not just the supply of electricity). The term disruption refers to unavailability of power supply. Next scenarios are just a proposal and they should be defined taking in account member state regulations requirements:

- Disruption of information for less than 4 msec.

- Disruption of information for less than 3 min.

- Disruption of information from 3 min to 10 hours.

- Disruption of information from 10 hours to 1 day.

- Disruption of information longer than 1 day.

- Usually, there aren't availability scenarios longer than a week because nowadays a disruption of two weeks is considered as a business closure.

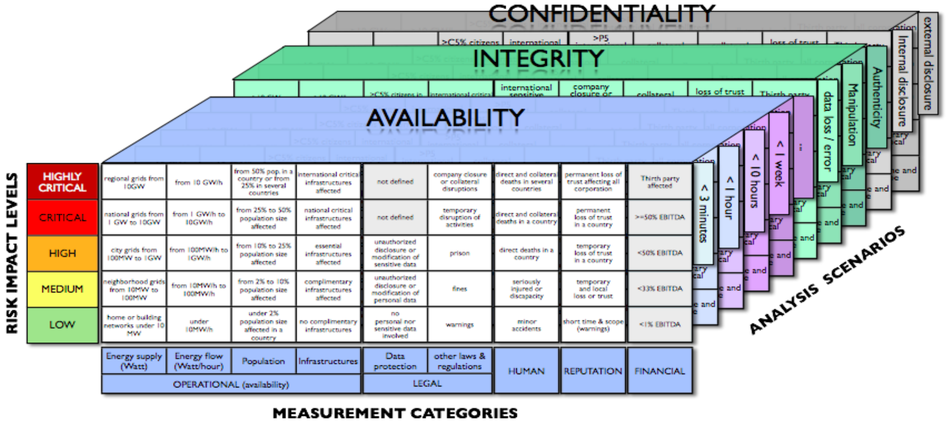
- The first questions to put in place for the evaluation of the availability scenarios would be:

  *What if an incident occurred affecting to the availability of the information asset and/or the involved process or service? What if the disruption is longer than n min/hours?*

## 3.4 Combining risk impact level assessments

- To determine the risk impact level for a specific information asset implies to evaluate every category and subcategory risk impact level at every SGIS predefined incident scenario affecting the involved process (use case).

- Putting easy questions about the worst possible scenarios of lost, alteration, or disclosure of the analyzed information to the owner of the process depicted in each use case and thinking about how it will affect the process, actors and society (impacts) will help to determine the risk impact levels (one by category) for a particular information asset.



| | OPERATIONAL (availability) | | | | LEGAL | | HUMAN | REPUTATION | FINANCIAL |
|---|---|---|---|---|---|---|---|---|---|
| | Energy supply (Watt) | Energy flow (Watt/hour) | Population | Infrastructures | Data protection | other laws & regulations | | | |
| HIGHLY CRITICAL | regional grids from 10GW | from 10 GWh | from 50% pop. 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 GWh to 10GWh | 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 100MWh to 1GWh | 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 10MWh to 100MWh | 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 10MWh | 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 |

-

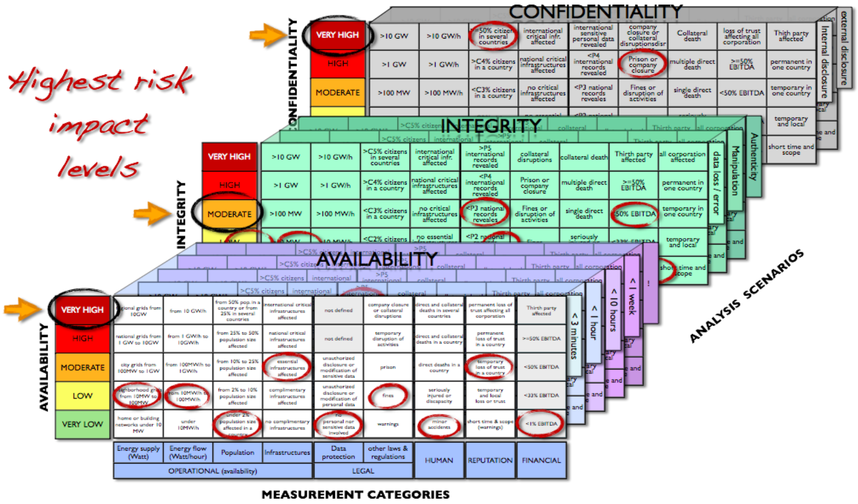
**Figure 3 — The Risk impact analysis cube includes so many tables as scenarios were defined**

- At the end of this process, grouping the results of each type of scenario (availability, integrity and confidentiality) will determine three different risk impact level for the analyzed asset.

- The highest risk impact level obtained evaluating all categories within the availability subscenarios will determine the risk impact level for availability. Applying that method with integrity and confidentiality scenarios will establish their correspondent risk impact levels

USE CASE (PROCESS): Energy supplier change

INFORMATION ASSET: User credentials



| AVAILABILITY | Energy supply (Watt) | Energy flow (Watt/hour) | Population | Infrastructures | Data protection | other laws & regulations | HUMAN | REPUTATION | FINANCIAL |
|---|---|---|---|---|---|---|---|---|---|
| VERY HIGH | gional grids from 10GW | from 10 GW/h | from 50% pop. 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 |
| HIGH | 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 |
| MODERATE | 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 |
| LOW | ighborhood grids from 10MW to 100MW | om 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 |
| VERY LOW | home or building networks under 10 MW | under 10MW/h | under 2% population size affected in a country | no complimentary infrastructures | personal nor sensitive data involved | warnings | minor accidents | short time & scope (warnings) | <1% EBITDA |
|  | OPERATIONAL (availability) |  |  |  | LEGAL |  |  |  |  |

**Figure 4 — Example of a full risk impact assessment for a particular information asset**

- At the end of the Risk Impact analysis, every information asset will get three risk impact levels (C-I-A). Every specific sector has different interests and prioritize confidentiality, integrity and availability in a different way. In the particular case of Smart Grids, service availability is the main concern. Although the origin of a disruption of the service could be originated from different threats and scenarios of information assets availability, integrity or confidentiality.

- The combination of these three values prioritized in the right way will determine the security level what will fit better.

- Don’t forget to compare different risk impact analysis cubes when one single information asset appears in different use cases. Then, the highest risk impact analysis level obtained from all use cases analyzed will be the right RIL for that asset.

## 4. Building the dependencies map

- In a mature scenario where business processes were totally deployed, after determining the risk impact level for an information asset and in order to determine its inherent information security risk, the next step is to identify all the assets (elements) involved in its life cycle and build a map of dependencies where every element would be represented.

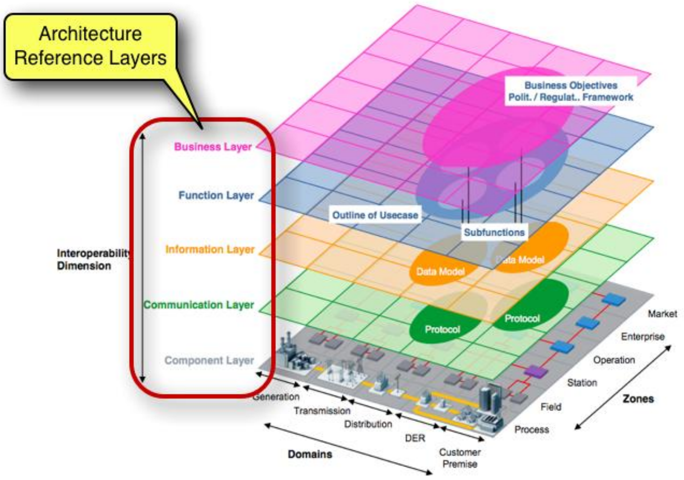
- The goal for this part of the risk analysis process is to identify all the vulnerabilities, threats and exposure frequencies for every element what supports the analyzed information asset allowing to determine the likelihood of success for those threats.

- All the elements included within the dependency map are affected by different vulnerabilities and threats and they should be analyzed separately establishing their particular effective likelihood in their inherent state. That means without any kind of security controls in place.

- The map of dependencies allows identify every relevant element involved in the management process for each information asset showing their relations. Those components are categorized following the layers established and described in the architecture reference model.

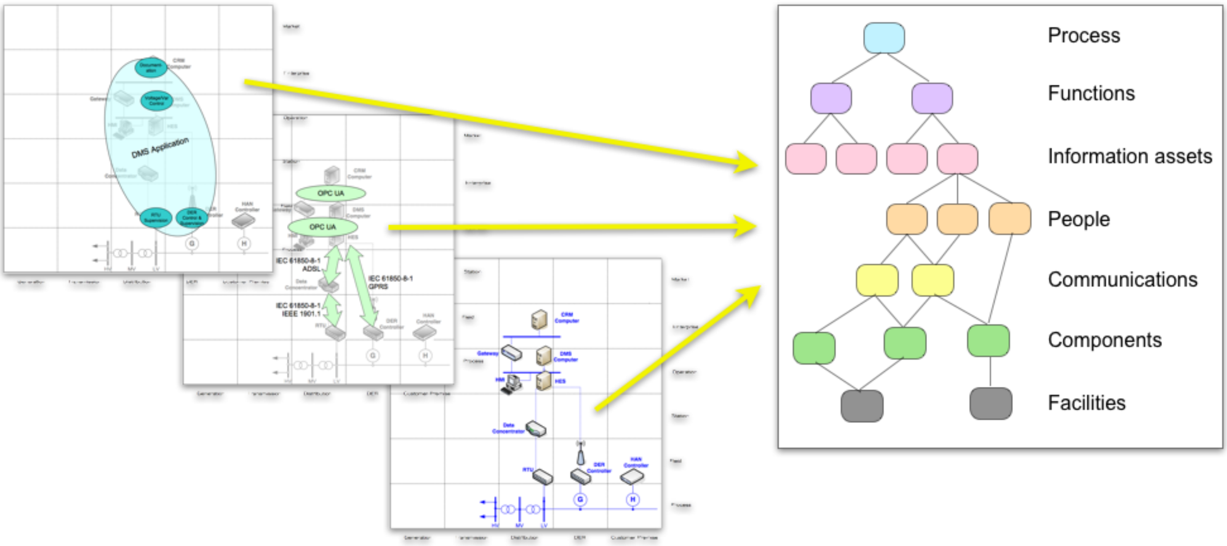
- Use cases have to include enough information to identify, at least at a top level what elements (assets/components) exist and support the analyzed information asset and which layer fits better for every one.

- The next list shows what ISO 27005 names “supporting-assets”. A dependency map should include next six types of elements:



- Personnel (owners, users, operators and maintenance, developers, …)
- Hardware (transportable and fixed equipment, industrial devices, passive data processing, data medium, …)
- Software (operating systems, maintenance, administration, …)
- Business application (standard or ad-hoc)
- Network (medium, relays, communication interfaces
- Sites and locations.
- At the end of the whole evaluation, the resultant effective likelihood for every information asset will be the highest level value of all their analyzed elements (supporting assets).
- Next diagram depicts an approach for mapping the SGIS layers from a use case to several information assets and its dependencies map.

*Use case: DMS System controls reactive power of DER unit*



-

**Figure 5 — Example: building the map of dependencies from an use case**

## 5. Determining SGIS Risk Likelihood

- A risk exists if a cyber-attack can be executed against a particular system by exploiting some vulnerability leading to a negative consequence against the system and the information asset processed by it.
- Estimating risk level, therefore, depends on two factors:
- The severity of consequence of that attack.

- The likelihood of success of an attack (effective likelihood),
- Combining those two factors will establish the inherent SGIS security level and the corresponding essential requirements for every information asset.
- The severity of consequence of that attack is measured via the risk impact level (aka business impact level) following the methodology already explained in early chapters.
- The likelihood of success of an attack is typically determined by a combination of different variables (particular vulnerabilities by each supporting element, exposure time to threats and likelihood of successful threats) and this part of the process has to be iterated so many times as supporting assets appear in the map of dependencies for each information asset.
- Sadly, we are still in the early stages of smart grids definition and a detailed technical architecture determining every supporting element is still pending so a typical risk assessment evaluating both vulnerabilities and likelihood (related to technical assets) cannot be assessed.
- Attending to those limitations, SGIS risk methodology proposes to follow the HMG IS1 standard. This methodology groups generic supporting assets, features and facilities reducing the amount of elements to analyze.
- Once the generic supporting elements of a particular information asset are identified and grouped, IS1 risk methodology proposes to determine the likelihood of success of an attack for every group of supporting assets (aka Focus of Interest) instead of determine it once by every particular supporting asset. This approach reduces such significantly the amount of iterations but increases the risk of mistakes.
- People involved in the risk assessment process require a thorough understanding of use cases and about potential threats and vulnerabilities that may be exploited causing incidents that may result in harm of smart grid services, organizations or citizens.
- A lack of understanding or an wrong criteria grouping too much assets could derive in miss risks in the analysis or even determine wrong security levels for a particular information asset.
- The likelihood of success of an attack is determined by the **threat level**. This factor is defined as a value attributed to the combination of the capability and motivation of a threat source and a threat actor to attack an asset.
- Therefore, likelihood criteria will be determined based on a combination of three factors:
- Threat sources. A person or group of people who are assumed to wish to compromise a property (C,I or A) of an Asset. They may or may not perform an attack themselves but every threat source has its particular interests.
- Threat actors. A person or group of people who are in a position to attempt to exploit a particular set of compromise methods.
- Compromise methods (attack vectors). The means available to a Threat Actor to compromise the Confidentiality, Integrity or Availability of an Asset.
- As more is known about the architecture and design defined for smart grids, more will be known about how threat actors might be able to exercise particular compromise methods.
- In order to simplify the analysis and following the proposed IS1 methodology, supporting assets and threat actors should be grouped and classified based on their interest, opportunity, ability to mount attacks (capability) and compromise methods available.
-

An easy criteria for grouping is consolidate supporting assets what share common Threat Actors, Business Impact Levels or Compromise Methods.

- IS1 methodology establishes a set of tables enumerating and defining threat sources, threat actors, possible interests and capability levels in order to help determining the effective likelihood:

| **Threat sources list** (not limited) |
|---|
| Disaffected or dishonest employees |
| Foreign intelligence services |
| Amateur or professional hackers |
| Virus and other malware writers |
| Terrorists |
| Investigative journalists |
| Commercial competitors |
| Political pressure groups /activists |
| Organized criminal groups |
| … |
| |
| |

| **Threat actor types** |
|---|
| Bystander |
| Handler |
| Indirectly connected |
| Information exchange partner |
| normal user |
| Person within range |
| Physical intruder |
| Privileged user |
| Service consumer |
| Service provider |
| Shared service subscriber |
| Supplier |

-

| **Threat capabilities criteria** |
|---|
| Very little: The threat source has almost no capabilities or resources |
| Little: The threat source has very modest capabilities and resources |
| Limited: The threat source has modest capabilities and resources |
| Significant: The threat source is capable and has significant resources |
| Formidable: The threat source is extremely capable and well-resourced |

| **Threat interest (priority)** |
|---|
| Very low – Indifferent |
| Low – Curious |
| Medium – Interested |
| High – Committed |
| Very high – Focused |

- In addition IS1 provides a set of forms for the risk assessment process guiding the likelihood assessment as well as a detailed list of threat capabilities (vector attacks).
- At the end of the likelihood analysis, the combination of threat sources, threat actors, interest, capabilities and possible compromise methods of attack will determine the level of likelihood for every information asset.
- Every combination of those elements will get an effective likelihood within a scale from 1 to 5:
- L1: Low – The likelihood of success of an attack is low
- L2: Medium – The likelihood of success of an attack is medium
- L3: High – The likelihood of success of an attack is high
- L4: Very high – The likelihood of success of an attack is very high
- L5: Extremely – The likelihood of success of an attack is extremely high.
- Next update of this document will provide a table depicting the translation from the three threat factors and the final five level effective likelihood scale.

## 6. Inherent Risk

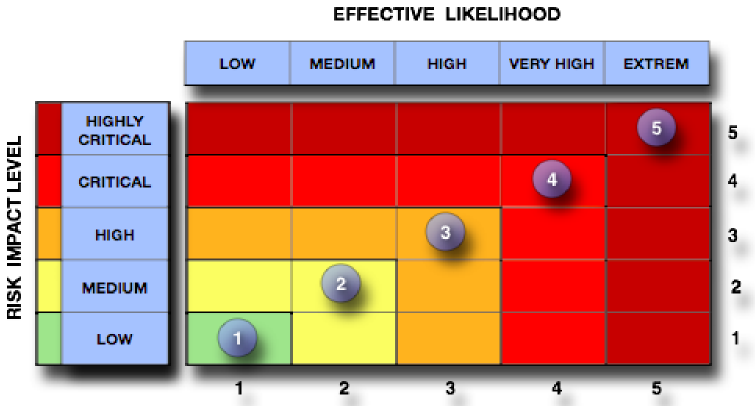
- After determining the SGIS-Risk impact level and the effective likelihood for every component what supports every information asset, the next step is determining the inherent risk for that asset.

- The inherent risk assessment evaluates processes and assets always in an inherent situation. It means that all use cases shall be assessed under the assumption that no controls were implemented at all. That's the reason for no including security controls during the process of identifying components and systems what support every information asset.

- The Inherent risk scale is established crossing the five risk impact levels determined for Confidentiality, Availability and Integrity separately, and the five effective likelihood levels. The result will bring three grids (C-I-A), each one of them composed by 25 cells grouped in five levels. Each group fits in one of the five security levels.

- After analyze several mathematical models SGIS concludes that high criticality low likelihood incidents are not properly addressed therefore developed the following graphical matrix-based scale.

- The grouping criteria join cells from the lowest level (low likelihood and low impact) increasing the security level at every step when either RIL or likelihood scales increase.



-

**Figure 6 — first approach to risk assessment.**

- It considers all cells with highly critical risk impact level as Security Level 5 ignoring lower likelihood levels.

- Fukushima and Twin Towers disasters demonstrated how a low or even a very low likelihood cannot justify low security levels because the impacts are high.

- Following this principle, effective likelihood scale combined in this way with the risk impact assessment could increase the resultant risk level for information assets with lower risk impact levels.

- Alternative Risk calculus methods can be found in §8.

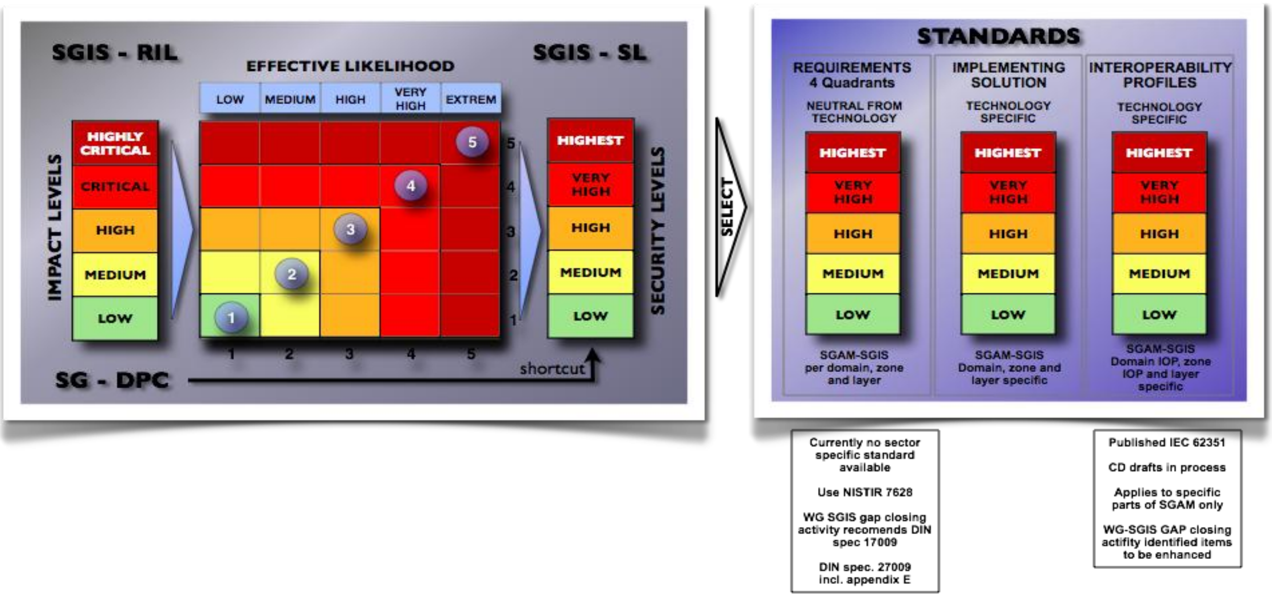
## 7. Establishing appropriate countermeasures for SGIS-SL

- Once the inherent risk analysis results are obtained, the assigned security level will determine the appropriate set of mandatory measures and their maturity level.

- Different security levels will establish different degrees of security requirements from three different points of view:

- Essential requirements

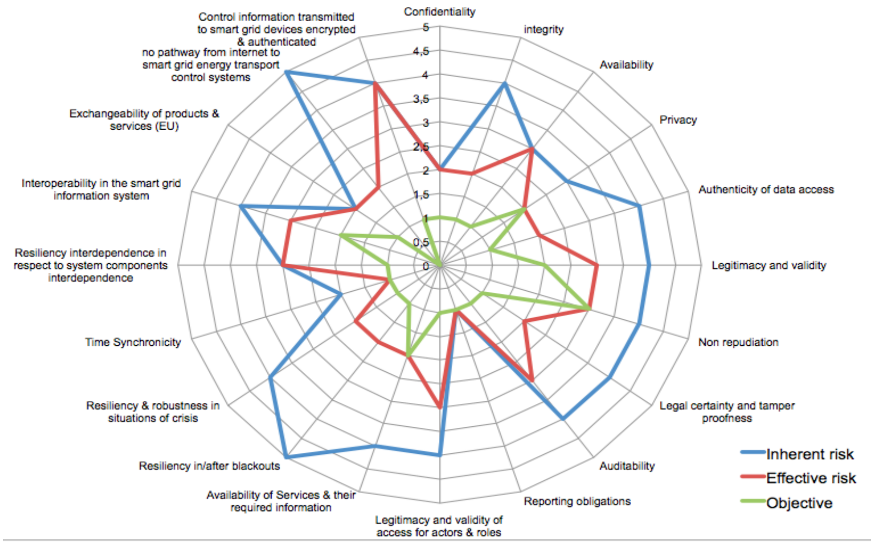
- Technology
- Interoperability process
- These three points of view should be covered by standards establishing the appropriate protective measures for all four quadrants.



-

**Figure 7 — Determining standards for security levels**

- Establishing the adequate set of countermeasures/requirements as standards covering those three aspects will allow determine security baselines and identify gaps between smart grid implementations and their adequate deployments.
- As the protective measures are defined in the SGIS requirement standards listed in Annex A, the implementation of those standards varies for specific products, services and organizations. Therefore all specific implementation also needs to assure that the remaining risk is acceptable for all participating actors in the smart grid – and society at all times.
- The execution of an inherent risk analysis covering all use cases for a specific cell (particular Domain and zone) will determine the security level for every information asset on this cell and those values will establish the security baselines or minimum requirements for that particular cell.
- Knowing the inherent risks and the appropriate minimal security requirements defined by standards, the execution of a gap analysis will determine the real state of the art.
- Next graph measures the inherent risk level for one particular cell (in blue), the required controls (in green) what have to be deployed and the real state taking in account countermeasures already deployed (in red) for every security essential requirement.



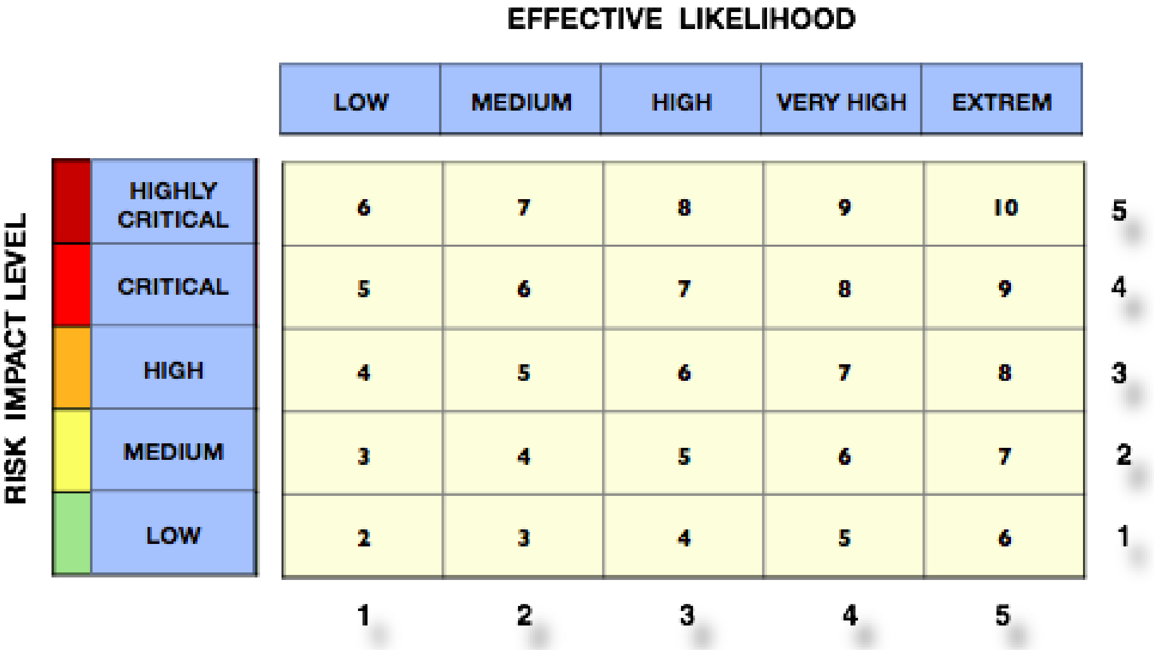
-

**Figure 8 — Example Visualizing SGIS Impact Analysis result – substation time sync**

## 7. Establishing appropriate countermeasures for SGIS-SL

**Alt. 1** – A different approach in order to prioritize those 25 scenarios consists in giving a different value or weight to every cell depending on its position in the grid. SGIS methodology assigns the value 1 to the lowest scenario (low effective likelihood and very low risk impact) increasing values as risk impact or effective likelihood level raises. The next two proposals calculate the value for every cell in two different ways:

- Next approach weights cells using a linear distribution after adding the column position and row position values:



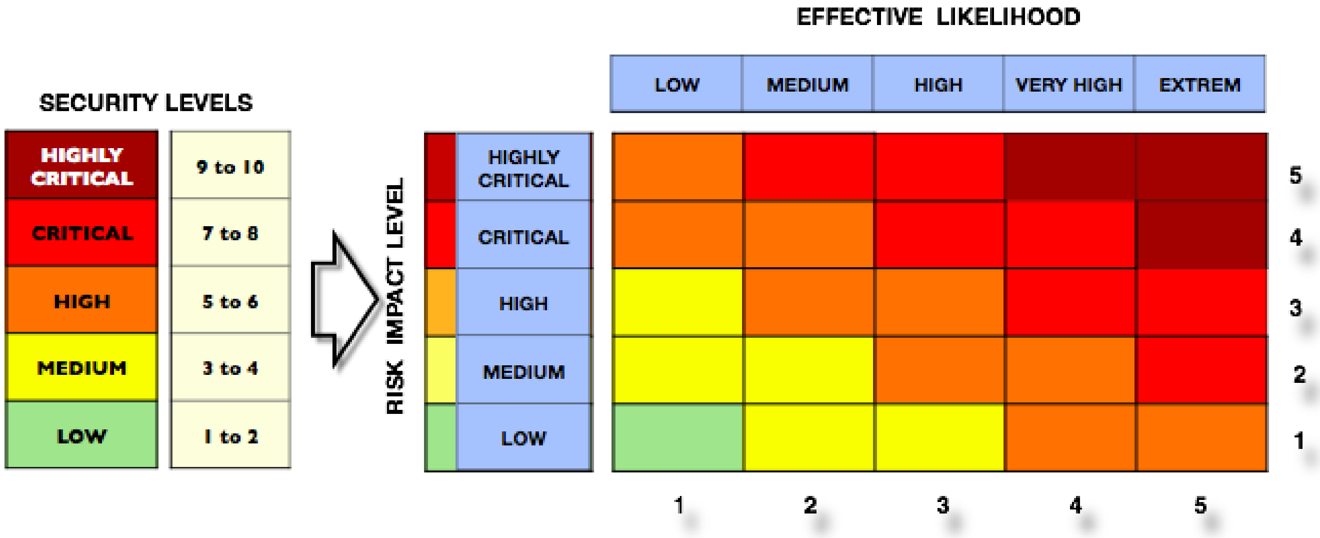
| | | EFFECTIVE LIKELIHOOD | | | | | |
|---|---|---|---|---|---|---|---|
| | | LOW | MEDIUM | HIGH | VERY HIGH | EXTREM | |
| RISK IMPACT LEVEL | HIGHLY CRITICAL | 6 | 7 | 8 | 9 | 10 | 5 |
| | CRITICAL | 5 | 6 | 7 | 8 | 9 | 4 |
| | HIGH | 4 | 5 | 6 | 7 | 8 | 3 |
| | MEDIUM | 3 | 4 | 5 | 6 | 7 | 2 |
| | LOW | 2 | 3 | 4 | 5 | 6 | 1 |
| | | 1 | 2 | 3 | 4 | 5 | |

-

**Figure 9 — Second approach to risk assessment (weights)**

-

- Resultant values go from 2 to 10 so if we group these values into the five security levels in a distributed way, the result will be:

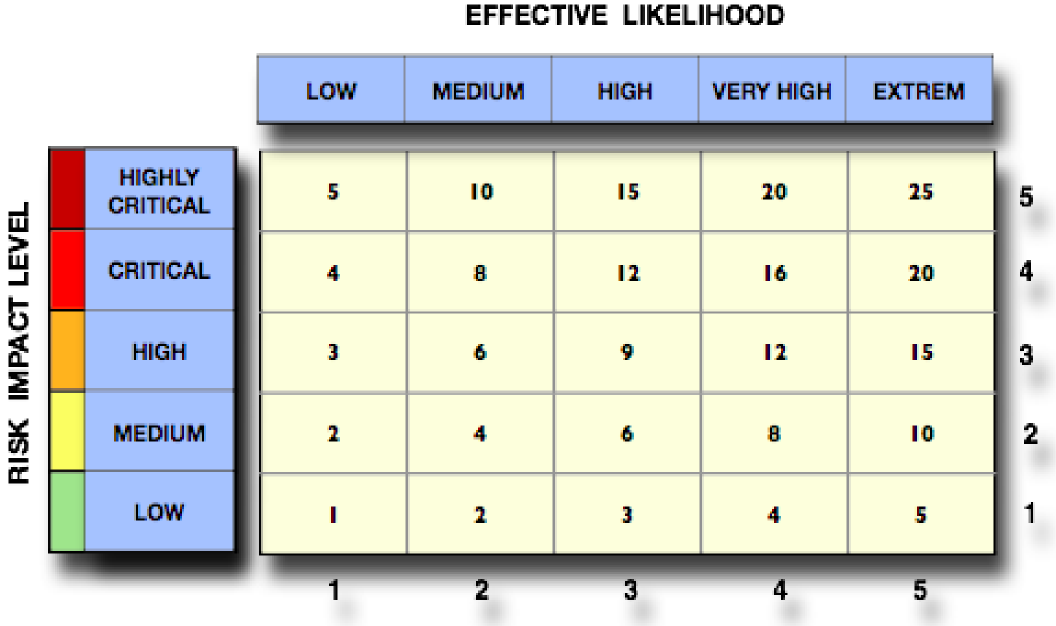


| SECURITY LEVELS | |
|---|---|
| HIGHLY CRITICAL | 9 to 10 |
| CRITICAL | 7 to 8 |
| HIGH | 5 to 6 |
| MEDIUM | 3 to 4 |
| LOW | 1 to 2 |

**Figure 10 — Second approach to risk assessment (resultant distribution)**

-

**Alt. 2** – Below case proposes an exponential distribution obtaining weights for every cell after multiplying the row and column numbers what it belongs.
This methodology distributes the values or weight of cells in an unequal way.


EFFECTIVE LIKELIHOOD
RISK IMPACT LEVEL

| | | LOW | MEDIUM | HIGH | VERY HIGH | EXTREM | |
|---|---|---|---|---|---|---|---|
| HIGHLY CRITICAL | | 5 | 10 | 15 | 20 | 25 | 5 |
| CRITICAL | | 4 | 8 | 12 | 16 | 20 | 4 |
| HIGH | | 3 | 6 | 9 | 12 | 15 | 3 |
| MEDIUM | | 2 | 4 | 6 | 8 | 10 | 2 |
| LOW | | 1 | 2 | 3 | 4 | 5 | 1 |
| | | 1 | 2 | 3 | 4 | 5 | |

-

**Figure 11 — Third approach to risk assessment (weights)**

Grouping those cells in categories allows identifying gaps and defining a strategic plan for risk management where different risk levels will be prioritized and managed in different ways.

The next table (below on the left) establishes a new criteria for grouping the 25 cells of the risk analysis table within the five SGIS information security levels.

The resultant distribution looks like this:

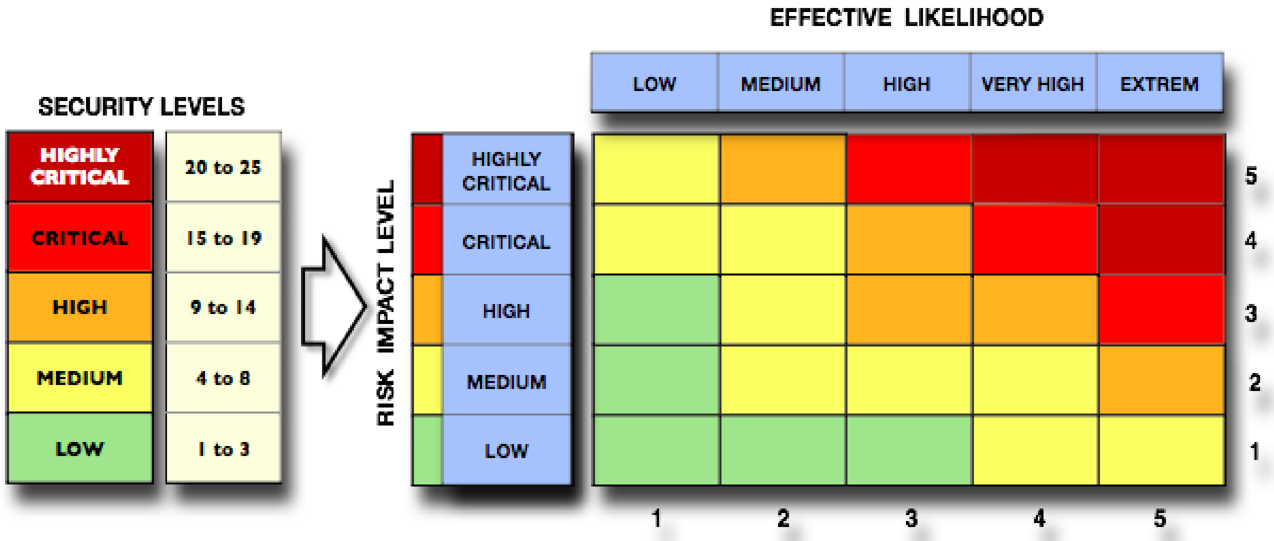


**Figure 12 — Third approach to risk assessment (resultant distribution)**

# Annex C – SGIS Toolbox Experience Feedback

## 1. Summary

The value of the toolbox needs be emphasized –it connects Smart Grid functional use cases well with information security requirements – in a detailed but still to be enhanced way. The methodology the SGIS toolbox together with the results of the other working groups (SGAM and SP/UCMR) as a whole offer a good starting point for the risk impact analysis exercise. It provides a general framework for risk analysis that can be used as a solid basis, from which deviation is possible following user and standardization needs. As generic use cases are on a high level at this stage, it's important to document how and where specific assessments path have deviated from the toolbox, along with any assumptions made. Through the assessment enhancements to the methodology

The outcome of the toolbox methodology is a SGIS-security level for Confidentiality, Integrity and Availability – each may vary on the scale provided for a specific use case.
The outcome of this method will be used to select appropriate standards that define security requirements , implementation options and profiles for interoperability.

The documentation of the risk impact assessment (rather than only looking to the resulting SGIS-SL – (for Confidentiality for Integrity and for Availability), is equally important to review the underlying methodology. It is suggested to elaborate a set of high-level requirements resulting from the identified Security Levels. The requirements should be specific to zones or domains.

The coherence of individual risk impact assessment "scenarios & categories" of the Toolbox, it is important that the risks i.e. for an SGIS-SL 4 are equally importantly. This needs enhancements as the current tables for commercial impacts and the reflected as the risk to the electrical system may not be aligned in the toolbox version distributed with this report.

## 2. ESMIG

In March 2012 ESMIG created its Security and Privacy Group (SPG) which consists of security experts from ESMIG's membership with origin in diverse industries (meter manufacturers, software vendors, integrator, telecoms, etc.).

The main objective of the SPG is to support the different stakeholders in an advanced Smart Metering infrastructure in integrating appropriate countermeasures on the level of system security and privacy for the use cases being relevant for Smart Metering systems.

SPG has had two face-to-face workshops and several phone conferences focused on the deployment and assessment of the SGIS toolbox. More than 20 experts have contributed to this work.

The SPG applied the toolbox on a number of generic use cases. These have been developed by the 'Task Force Use Cases' of the Smart Meter Coordination Group and the 'Working Group Sustainable Processes' of the Smart Grid Coordination Group. Both groups are supported by ESMIG. The table below gives the overview of the use cases on which the toolbox was applied

| Use case name | Information exchanged | Zones | Related to |
|---|---|---|---|
| Reading a smart meter | Measurement data | Operation to Field | SM-CG |
| Disconnect supply | Disconnect command | Operation to Field | SM-CG |
| Sending price and environmental information (Demand Response) | Price and environmental information | Enterprise to Field | SG-CG |

The SGIS risk assessment was performed in the following steps:

1. Selection: define a use case on which to apply the toolbox.
2. Mapping: apply use case steps to the zones and domains of the Smart Grid Reference Architecture.
3. Setting assumptions - When performing risk analysis, even with a detailed model like the one presented in the toolbox, assumptions always need to be made. These have to be captured along with the analysis results, so that conclusions and security levels may be interpreted in the light of earlier made assumptions.
4. Risk Assessment: following the model of measurement categories and analysis scenarios for each piece of information exchanged over a zone/domain, a risk impact assessment was done. A general likelihood assessment, based on experience and insights of SPG members, was performed.
5. Definition of Security Levels by combining risk impact and likelihood.

SPG wants to highlight the following aspects it was confronted during its work:

- SPG appreciates that the risk impact level assessment model is “open”, in the sense that the document mentions explicitly that the user may change, add or remove measurement categories and analysis scenario’s as required by the user’s needs. SPG made use of this flexibility in a way that depending on the use case, especially the availability scenarios were defined in a suitable manner.
- The group found that the “population” category had too high an influence on the risk impact at the enterprise and operation zones and thus chose not to make extensive use of this category.
- The group would suggest to review the balance of RIL criteria with other stakeholders and to have the experts to re-assess the necessity of the elements given in the measurement categories
- The toolbox included a detailed likelihood assessment model which could not easily be leveraged for assessing risk likelihood based on generic use cases. The analysis is based on a dependencies model including facilities, components, communications, organizational roles, etc.…
    - Since this model requires an actual implementation to provide input to it, this model offers great added value for industry players with dedicated/fixed/specific use cases.
    - A more promising method to assess likelihood would be based on a threat analysis. Within the SPG work this was not feasible due to resource constraints. Finally, the SPG made a general assessment of likelihood, based on the experience and insights of its members.
    - Based on this comment, the SGIS proposed an alternative way to perform likelihood assessment, which is now included in the toolbox.
- Finally, risk impact and likelihood were combined to obtain a security level. Again, SPG appreciates the “openness” of the toolbox, presenting several models to make this combination. While a model is recommended in which the highest of either impact or likelihood determines the security level, for several reasons the SPG prefers to make the multiplication of both and translate this score into a security level. This method is also recognized in the toolbox.

Conclusion:

ESMIGs SPG would like to conclude emphasizing the value this toolbox method is providing due to its well, detailed but still open nature.

It provides a general framework for risk analysis that can be used as a solid basis, from which deviation is possible following user needs. It’s important to document how and where one had deviated from the basic models, along with any assumptions made.

The outcome of the toolbox methodology is a security level for Confidentiality, Integrity and Availability. When using the outcome of this method to define security measures, rather than only looking to the resulting security levels, it is equally important to review the underlying risk analysis since measures will likely be taken based on the detailed exercise. It is suggested to elaborate a set of high-level requirements resulting from the identified Security Levels. The requirements should be specific to zones or domains. ESMIG would suggest this as a future work item of SGIS.

In terms of scope of the SGIS toolbox, it is important that the commercial risks are not as importantly reflected as the risk the electrical system is facing when being attacked. Every use-case shall also be assessed according to the commercial impact an actor in the market might experience while the electricity supply is not affected when these risks become reality (e.g. fraud).

Proposed next steps

ESMIG's SPG proposes that the SGIS toolbox would be further refined in 2013 based on the suggestions raised by ESMIG (see above) and other stakeholders.

Furthermore, ESMIG suggests that the toolbox would be expanded with a stakeholder analysis. Preceding the risk assessment with a stakeholder analysis will bring the added value that resulting security requirements can always be traced back to the stakeholder analysis, the main objective of which is that one can make the link between a security requirement and specific stakeholder needs.

ESMIG strongly support an iteration of the Smart Grid Coordination Group Mandate until the end of 2014. In this timeframe, SG-CG/SGIS should work on a European Set of Smart Grid Security Standards. A close cooperation/alignment with a similar initiative in the Smart Meters Coordination Group (the ad hoc Task Force Security) is very important.

ESMIG wants to start working on a first set of privacy and security requirements for Smart Metering (possibly a combination of a few member states' requirements) and use this as a basis for a European-wide set of requirements. Furthermore, a certification approach based on these requirements will be defined and tested. ESMIG would welcome the support and input of the SGIS or its successor in this project.

## 3. Two days security workshop by Netbeheer Nederland to apply the SG-IS toolbox on real life DSO / TSO related use cases

On the 3rd and 4th of July a security workshop was hosted by Netbeheer Nederland in the Netherlands. The main goal was to apply the SG-IS toolbox on a real life use case within the domains of the DSO and /or the TSO. For this purpose one of the Electrical Mobility / Electrical Vehicle (EV) use cases of the Sustainable Processes group was used: WGSP-1300 Generic use case Smart Charging. The ins and outs of this generic use case were presented by the EV representative of the Sustainable Processes group. Afterwards, the workshop representatives (European security experts from NL, SG-CG/SGIS and ENISA) applied the Risk Impact Level Assessment methodology from the SG-IS toolbox to the use case. It led to an intense and fruitful discussion where both the use case and the methodology were challenged.

The main outcome of the workshop:

- The methodology and the SG-IS toolbox as a whole offer a good starting point for the risk analysis exercise and at the same time they are not fully ready at the moment. More workshops need to be planned to challenge the methodology and enhance its content. This needs to be an ongoing activity where interaction between SG-CG/SGIS, SG-CG/RA and SG-CG/SP is needed.
- There was discussion if the risk analysis should be done by looking from the European perspective or just from the perspective of the use case. Furthermore the EV related use cases are not yet rolled out fully. Should the impact be calculated based on a full roll out of the use case? Or should a scale be considered? If Smart Charging is done for 20% of all cars, or just 2% or the full 100% it will result in a different impact if for example the crucial information assets are unavailable.
- The current version of the generic EV Smart Charging use case template of SG-CG/SP doesn't describe the information assets. It focuses on the information exchange between the actors but not the information that is used by actors internally. A full set of information assets that are used in the use case (both by actors and between them) is needed to conduct the risk analysis. We recommend adding a section to the use case template where the information assets will be enlisted. This feedback will be given to the SG-SP workgroup.
- The current Reference Architecture doesn't give clear example of what is on e.g. Field, Operation, Enterprise level. Where should we for example position the Charge Spot of EV's? And the controller on MV-LV transformer level?
- It is not always clear which zone from the SGAM is associated to a given use case step. This feedback will be given to SG-CG/RA. It is recommended that when the next risk analysis is realized representatives from SG-CG/RA participate in this exercise.
- Some participants find a detailed (ICT) architecture of the ICT systems used in the use case of crucial importance where others think it is not necessary to do a risk analysis for Smart Grid use cases.

Furthermore the following feedback can be given related to the risk analysis methodology:

- The generic EV Smart Charging use case (referring to a pilot project) makes use of different communication media and means: GPRS, PLC, Internet, e-mails. The risk analysis has been performed without referring to the characteristics of the specific communication technologies deployed by the use case. The proposed methodology does not require that level of detail.
- During the workshop the participant from SG-CG/SP Electro Mobility proposed to add the Environmental Impact category. This has been accepted by SG-IS and the toolbox has been adapted accordingly.
- Not all the information security properties (CIA) have the same relevance for the different information assets of a given use case. The participant concluded that only relevant properties shall be addressed during the risk analysis.
- Regarding the likelihood analysis it is important to mention that the method proposed by SG-IS for performing this part of the risk analysis was presented and discussed during the workshop. No application of this method and of the combination of risk factors was possible at that time during to time restrictions.
- The results of the performed risk analysis should be reflected in the Use Case description. The participants of the workshop recommend that the Use Case template is extended with sections describing threat scenarios, security requirements and controls.

Conclusion:

Based on the positive experience of applying the use case to the WGSP-1300 Generic use case Smart Charging, future exercises are to be expected. From Netbeheer Nederland perspective we want to continue our efforts in helping improving the SG-IS toolbox. We believe that this will help to increase the maturity and usability of the latter and at the same time it will help grid operators and other stakeholders involved to challenge their use cases on privacy and security issues from the start. The SG-IS toolbox should be an ongoing effort (just like the work on the generic use cases) and therefore we recommend to keep applying it to the use cases. From Netbeheer Nederland we will do this in 2013 (and further) to address the issues that we found during our first exercise.