24 February 2012

Work Package 1.1

Identification and Categorisation of all relevant Smart Grid Assets

Expert Group on the security and resilience of Communication networks and Information systems for Smart Grids

Version 1.0

Table of contents

1. Introduction

This work package attempts to help categorise the various assets in the smart grids that need to be protected from a cyber perspective.

1.1. Mission, vision and goals

Identify and categorise all relevant communication networks and information systems assets (ICT, SCADA, and other smart grid components like sensors/ controls, phasors, reclosers, voltage regulators, etc.) of smart grids that need to come under the security and resilience mandate of the EU.

1.2. Strategy

The expert group decided to take an indirect view of identifying the critical assets. The first step was to create a classification, identify the magnitude of any impact that should be protected against, and then classifying the assets based on the protection needs.

1.3. Scope

All critical energy assets within the Transmission, Distribution and Generation space which can

1. Cause a International, Cross Border, National or Regional power outage or damage to infrastructure
2. Cause a significant impact to Energy market participants ,
3. Cause a significant impact on Operations and Maintenance of the energy grid
4. Pose a significant risk to Personal Data of citizens (Privacy);
5. Cause significant safety issues for people

1.4. Team

Team leader:

- Rajesh Nair: Bachelor of Technology Applied Electronics and Instrumentation Engineering (Kerala University), M.B.A. Finance and Technology (Vanderbilt University). Heads the Strategy, Architecture and Security Department within Swissgrid.

Team members:

- Simone Riccetti: IBM, Expert in Security. degree in Telecommunication Engineering (Politecnico di Milano University), contract Professor at University of Insubria.
- Meir Shargal, Expert in Utilities, Smart Metering / Grid and US regulations. Part of the leadership team of CSC Global Energy and Utility Vertical leading the strategy, “Smart” Utility, Generation and Transmission & Distribution practices. Bachelor of Science in Applied Mathematics, University of Tel Aviv and Bachelor

of Science in Computer Science, University of Minnesota. Masters of Science in Computer Science and Management Information Systems (MIS), University of Minnesota.

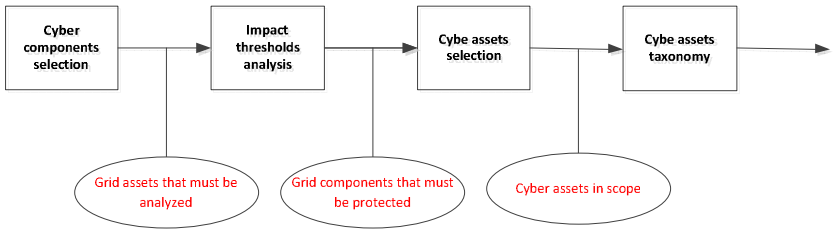
Co-operation with and reviewed by:

- Bernhard M. Haemmerli
- Erik lujif, TNO / CPNI.NL, The Netherlands
- Nisheeth Singh
- Eric V. Aken

2. Methodology

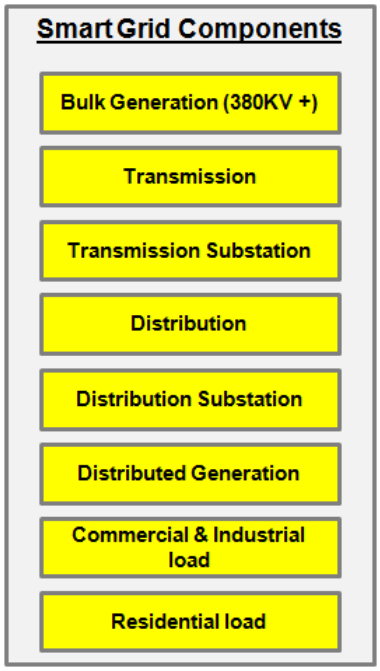
The expert group decided to take an indirect view of identifying the critical assets. The strategy consists in the following steps:

- ***Grid components selection***: establish which critical assets are potentially included in scope
- ***Impact thresholds analysis***: define the impact thresholds and identify which grid components must be protected
- ***Cyber assets selection***. Identify the cyber assets that sustain grid components in scope and that must be considered in scope
- ***Cyber assets taxonomy***: All in scope cyber assets are broken down into their main elements that need to be secured to ensure cyber assets security. Those main elements must be included in threat and risk analysis phases.



2.1. Grid components selection

These are the traditional components except for the Distributed generation part. Traditionally the top-down impact is significant and calls for very high resilience in the top layers, decreasing down the chain. Historically the electric grids have been built taking this into consideration. In the figure below, have been selected all critical components that are fundamental to sustain the grid value chain. All these components have to be analysed to establish under which conditions they must be considered in scope.



2.2. *Impact thresholds analysis*

The traditional core components of the smart grid like Bulk Generation, Transmission and Distribution are built already in a componentised manner which can island and protect itself very quickly to prevent any damage. They need to be strengthened against the new cyber threats based on the new risks. The Smart Assets and Grid Assets have another protection requirement. These needs have been defined below:

1. Top down volume threshold based categorisation: Usually any asset or group of assets that can impact more than 2 GW. (900 GW total ENTSO-E generations x 0.8 %*), so that 3 concurrent events can be managed with a reserve of 1.2 GW is considered in scope for the cyber protection.

   All core components which cross this threshold will need to be considered as critical assets for protection.

2. Horizontal or collective impact threshold based categorization: Can impact more end points (as Intelligent devices massive attack) which collectively can have an impact over 2 GW. This will include all Grid assets (like SCADA and communication systems) and Smart assets (smart meters which cover over 2 GW collective connected load) which cross the threshold.

3. Critical asset protection based categorization: Each national entity or the EU can define specific assets like military, police, hospitals etc.

4. The Transmission system and Distribution system operators are also free to identify any other asset which they consider to be critical in the case of transient or non stable conditions (low or high Frequency / voltage) .

5. Data privacy: Each national entity or the EU can define specific privacy data protection rules to comply with the national entity regulation

Smart Grid Component	Impact Level
Bulk Generation	National/EU
Transmission	National/EU
Transmission substation	National/city (>2 GW)
Distribution	Area (>2 GW)
Distribution substation	Part of Area (>2GW)
Distributed Generation	Few consumers to be defined by CA
Commercial & Industrial	Few consumers to be defined by CA
Residential	Few generators to be defined by CA

Security guidelines from EU

Security guidelines from Control areas

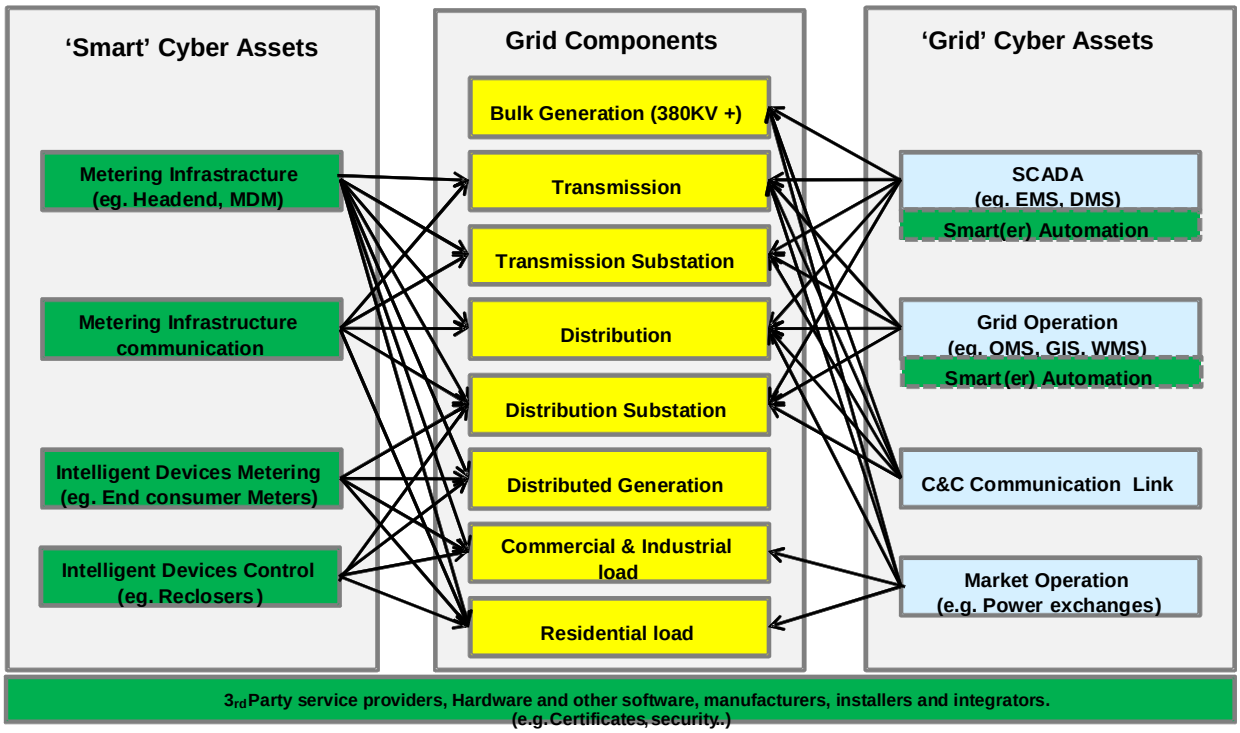
* (50.2 hz – 49.8 Hz)/50 Hz %= 0.8%

2.3. *Cyber assets selection*

Smart grid architecture involved many cyber assets some have been part of the grid for a while and others are new "smarter" assets. To better distinguish the "smart" assets (i.e. AMI, Intelligent device control) from the "traditional" cyber assets (ie SCADA), we have spitted assets into two categories (see picture):

- Smart Cyber assets (green)
- Grid Cyber assets

This split help in the identification of the impact that each cyber assets have on "core components" and that drives the cyber assets that must be considered in scope.



Smart grid is an evolutionary theme. It is built on the existing (core components) and introduce various new functions and capabilities (in green) to the core components.

2.3.1. Smart Cyber Assets

A new Smart Asset category which includes new monitoring and control devices, communication infrastructures, etc. which add a whole new set of capabilities for the Grid Assets to utilise. The smart movement open the grid to vulnerabilities that already exist in the ICT world, now those vulnerabilities pose threat to the Smart Grid (and SCADA) communications and applications also.

This is a new category, which has influence mostly on all core component layers. They contribute in automation of processes and increased controllability of the grid. Consequently they increase the risk in the overall grid considerably due to the large numbers of the devices, and their collective impact. Their impact can be in any or multiple layers hence the security mechanisms need address other vectors as well.

2.3.2. Grid Cyber Assets

Grid Assets historically developed along with the core components and exist in a very mature fashion in today's infrastructure. The traditional grid assets are now being upgraded with the capability to address the needs of the smart Assets and the new Distributed Generation aspects of the core components. Additional functionalities in the Grid Assets which help automate, improve control capabilities and increase the efficiency of grid operations or the energy markets are now being implemented due to smart grids.

The span of control of the Grid assets is also considerably high. This means that their impact is also similar to those of the Smart Assets, but the numbers of assets are very few. These then form the high value targets that have a different protection need.

2.4. Cyber assets taxonomy

The cyber security of individual assets in the scope depends on the security of the various sub-elements that constitute them and for that reason should be considered for a correct assessment of threats and countermeasures to be applied to cyber assets.The sub elements that must be analyzed in protecting the cyber assets in scope are the following:

- Hardware (IT, Grid Operations)
- Software (including SCADA)
- Communications networks and protocols (including Smart Metering /Grid networks)
- Data
- Operations processes

3. Definitions

The first step is to define in detail the various main assumptions that have been considered while writing this paper.

3.1. "CYBER"

Includes all subjects for normal and emergency operations:

- Communication (control, measurement and coordination)
- Applications (control and monitoring systems)
- Databases and Operating Systems
- Hardware (Computing, Sensing or measurement devices, controlling (actuating) devices, networking and security)
- Infrastructure (Data centers, control centers etc.)
- Network (LAN and WAN)
- Security processes and procedures
- Identity and access management services
- Information medium (memory, USB sticks, Harddisks)
- Personnel developing , operating, maintaining and governing above topics
- Power autonomy
- Physical security of the cyber assets themselves (data centers and Power Plants, and communication network end points)

It does not include

- Physical security of transmission, distribution lines, transformers, meters, buildings, and any end consumer devices
- Office and back office automation

3.2. "Energy Market"

Includes the following players

- Traders

- Exchanges
- Grid operators
- Shippers
- Producers and Consumers
- Prosumers
- Critical services providers (Financial and billing)

4. Conclusion

The Working group suggests a classification to classify the relevant smart grid assets into the three major classifications (Smart cyber assets, Grid components and Grid Cyber assets. The criticality of the asset types are defined and a minimum measurable impact is also defined.

The risk management processes are expected to be dovetailed into this defined classification and the defined impact thresholds.