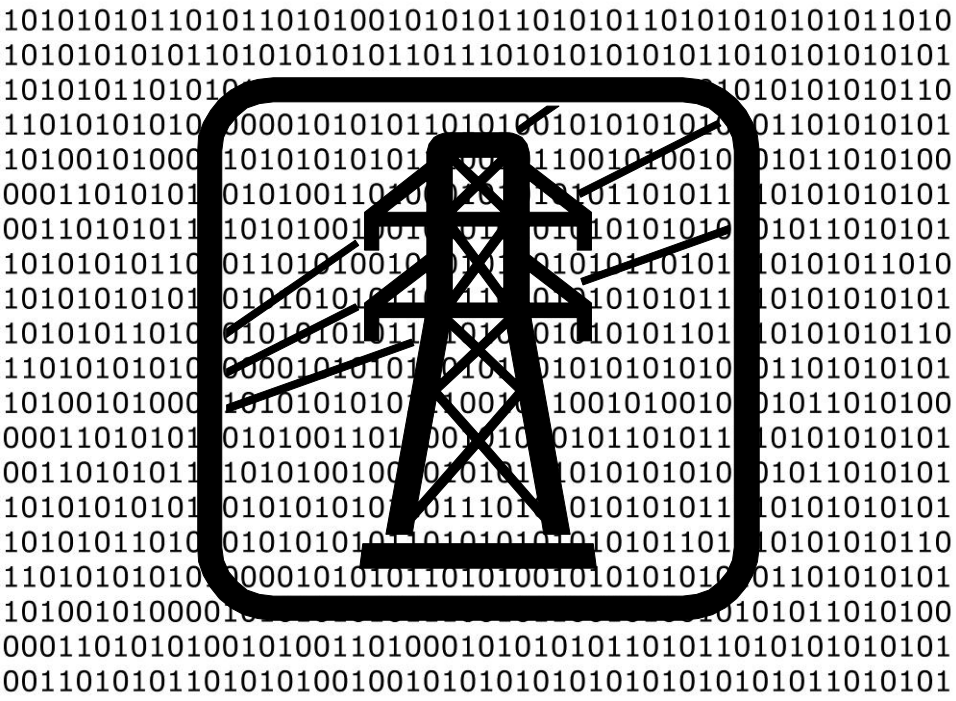

Smart Grid Threat Landscape and Good Practice Guide

9 December 2013

European Union Agency for Network and Information Security www.enisa.europa.eu

About ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its member states, the private sector and Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

Authors

Louis Marinos, ENISA
E-mail: Louis.marinos@enisa.europa.eu

Contact

For contacting the editors please use resilience@enisa.europa.eu.

For media enquires about this paper, please use press@enisa.europa.eu.

Acknowledgements

This study has been carried out in collaboration a group of experts in the area of Smart Grids, namely: Ralph Eckmaier, Independent Advisor, Austria, Michael John, Elster GmbH, Germany and Jean-Pierre Mennella, Alstom Grid, France.

Everis Aerospace and Defence, together with Universidad Politécnica de Madrid has contributed as external contractor in the phase of information collection and analysis. The involved experst within this contract were:

- Everis Aerospace & Defence: María Pilar Torres Bruna, Fernando Sanchez Palencia
- Universidad Politécnica de Madrid: Professor Dr Victor Villagrá González, Professor Dr Carmen Sanchez Ávila, Verónica Mateos Lanchas, Vicente Jara Vera

Executive summary

Smart grids are complex systems. A smart grid is a system of systems delivering energy to consumers. Smart grid stores, transports and manages energy. Smart grid is a de facto Critical Infrastructure[1] as energy is important for the well-functioning of the society and economy. Being the blending of the energy and telecommunication critical infrastructures, smart grids should operate securely and by respecting end users' privacy. Moreover, the protection of the smart grid is the key to energy availability. In this document we elaborate on cyber security issues with regards to smart grid information infrastructure.

The security of a complex system is also a complex matter. In order to cope with this complex environment, this document leverages the following principles for simplifying the problem:

Consider external and internal threats: In cyber-security the external environment are the cyber-threats. This cyber-threat environment originates from threat agents, the adversaries utilizing cyber-threats and launching cyber-attacks. Although dynamically changing, the cyber-threat landscape can be described and has finite elements. An understanding of the cyber-threat landscape is indispensable for the identification of the necessary protection measures. In this document, we provide a threat landscape affecting smart grid components. Internal threats are considered as well: a variety of threats emanating from errors and insider attacks are also taken into account.

Decompose and classify the elements: A decomposition of smart grid components is one of the main tasks to tackle its complexity. This task is currently being performed by various experts around Europe and the World. Within this report, we have adopted the smart grid decomposition provided in the document Smart Grid Reference Architecture[10] of the Smart Grid Standardization Coordination Group of CEN-CENELEC-ETSI. This is because this work is a highly reputed document among the security experts in Europe.

Capture available knowledge: What have others done in the area of smart grid protection? This has been addressed by taking stock of available cyber-security approaches, protection approaches and good practices developed recently.

In response to the urgent question of many stakeholders: *How does this document support me in my work?* this document provides tools to assess risk exposure of smart grid assets and will show what others have done in this respect. It elaborates on the threats smart grid components are exposed to and on the security controls to reduce threat exposure. But the assessment on the living object can be done only by the asset owner, just because asset owners master the complexity of infrastructures and the interdependencies among various assets. This task cannot be done as a generic exercise or it would have low value.

Concluding, one should note that the use of these tools will depend on the capabilities of the expert users. In cyber-security preparedness, however, much depends on the capabilities of the adversary, which are not always known and certain;

"That which depends on me, I can do; that which depends on the enemy cannot be certain. Therefore it is said that one may know how to win, but cannot necessarily do so" (Sun Tzu[2]).

[1] http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/crisis-and-terrorism/critical-infrastructure/index_en.htm, accessed 13 Nov 2013.
[2] http://en.wikipedia.org/wiki/The_Art_of_War, accessed 13 Nov 2013.

Being knowledgeable about what can be achieved is one thing. The other is to reduce the impact. In cyber-security – an environment with asymmetric approaches - this can be achieved through common effort and coordination.

Table of Contents

1 Introduction

This document elaborates on threats related to smart grids. Being an ENISA deliverable in the area of Threat Landscape, it comprises a detailed threat assessment in the area of smart grids, based on input form the generic ENISA Threat Landscape activities[13]. The rationale behind this piece of work is to "deepen" the generic threat assessment by taking into account specificities of smart grids, a vital CIIP sector.

By doing so, the objective is to complement various activities going on both within and outside ENISA, that is:

- To perform a threat assessment on the basis of which smart grid security measures will be based. This activity is in support of related activities of the Commission: DG-ENER, in close cooperation with ENISA and DG CNECT, has decided to task the EG2 working group[29] with the organisation of consultations security requirements with national cyber security authorities and the energy and ICT industry.
- To deliver input to other international activities, in particular in the area of standardisation[3],[4]. In this context, the threat analysis provided in this document will be reused in the definition of security measures for smart grid infrastructure models (scenarios).

The present work is based on information developed within the ENISA Threat Landscape (ETL): relevant information about top threats is included in this document. The threats have been mapped to smart grid assets: this indicates the kind of exposure each asset has. Moreover, threat agents have been identified as originators of these threats. Through the established relationship among threats->assets->threat agents it becomes evident what threats smart grid assets are exposed to. Moreover, the capabilities of possible adversaries are also identified. This information is useful for a variety of security related activities in the area of smart grids, such as risk assessments, formulation of security requirements, identification of protection requirements, etc.

This work is concluded with a good practice guide, consisting of an overview of smart grid security approaches. In particular, it is demonstrated how available smart grid controls from various existing standards protect against the identified threats.

The structure of this report has been agreed with the expert group that has supported this ENISA work. Moreover, a contribution to the ENISA work on security measures for smart grids has been generated.

Policy Context

The Cyber Security Strategy for the EU[5] stresses the importance of threat analysis and emerging trends in cyber security. The ENISA Threat Landscape is an activity towards the achievement of objectives formulated in this regulation, in particular by contributing to the identification of emerging trends in cyber-threats and understanding the evolution of cyber-crime (see 2.4 regarding proposed role of ENISA).

Moreover, the new ENISA regulation[6] mentions the necessity to analyse current and emerging risks (and their components), stating: "*the Agency, in cooperation with Member States and, as*

[3] http://www.cen.eu/cen/Sectors/Sectors/UtilitiesAndEnergy/SmartGrids/Pages/default.aspx#, accessed 11 November 2013.
[4] http://www.cenelec.eu/aboutcenelec/whatwedo/technologysectors/smartgrids.html, accessed 11 November 2013.
[5] http://www.ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security, accessed 28 Nov 2013.
[6] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:165:0041:0058:EN:PDF, accessed 28 Nov 2013.

appropriate, with statistical bodies and others, collects relevant information". In particular, under Art. 3, Tasks, d), iii), the new ENISA regulations states that ENISA should "*enable effective responses to current and emerging network and information security risks and threats*".

From the above points it becomes apparent that the ENISA Threat Landscape is a significant contribution to the EU Cyber Security Strategy by streamlining and consolidating available information on cyber-threats and their evolution.

Detailing the ENISA Threat Landscape for various emerging areas provides valuable contextual information to existing policy measures established by the commission. In the area of smart grids, in particular, this work supports a recommendation of the Commission: the European Commission included a number of data protection, privacy and security measures in the March 2012 Commission Recommendation on preparations for the roll-out of Smart Metering systems[7]. Furthermore, it initiated action under the auspices of the smart grids Task Force with a dedicated Expert Group[29] (EG2) focusing on two key concrete outcomes to be delivered in 2013, namely: 1) a Data Protection Impact Assessment (DPIA) template as a response to consumer concerns related to data protection and privacy; and 2) a cyber-security assessment framework as a response to investor and industry concerns related to system security. The cyber security assessment framework is composed of two sub-deliverables. First, a set of *Best Available Techniques (BATs)* pinpoints the potential cyber security risks inherent to each of the common minimal functional requirements for Smart Metering Systems recommended in the March 2012 Recommendation[8] and identifies optimal controls and Privacy Enhancing Technologies to mitigate each of these risks. Second, a blueprint for a *network* will be elaborated, where information about incidents, threats, vulnerabilities and good practices can be shared for critical infrastructure protection[9].

This work aims to provide a significant contribution towards assessing cyber threat exposure of smart grid infrastructures. As such it will directly contribute to the assessment of cyber security and comes to support investor and industry concerns.

Target Audience

This material is a tool for smart grid asset owners who wish to perform threat analysis and risk assessment according to their particular needs (i.e. asset protection level based on asset impact, vulnerabilities and detail of mitigation measures). While in this document the threat exposure of smart grid assets is being presented, asset owners may deepen their threat analysis and risk assessment by using asset and threat details provided in this document. A deeper analysis will be based on assessed threats, vulnerabilities and impact statements with regard to the concrete assets participating in a smart grid infrastructure scenario (see also specific threats in section 5).

Moreover, the smart grid threat landscape will be of interest for policy makers: current threats and threat trend may be important input in policy actions in the area of cyber-security, critical infrastructure protection and smart grid in particular.

Through the large number of collected reports, the smart grid threat landscape provides a unique collection of information regarding cyber-security threats. Hence, a further target group of this document are individuals who would like to obtain access to these sources in order to use them for their own purposes.

[7] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2012:073:0009:0022:EN:PDF, accessed 3 December 2013.
[8] defined in points 3.f and 18 of the Recommendation 2012/148/EU
[9] "Evaluation of available methodologies for a trustworthy network sharing vulnerabilities and threats analysis of Smart Grid and Smart Metering systems among stakeholders"

Structure of this document

The rest of this document is organised as follows:

- The rationale of the smart grid threat landscape is presented
- A section that presents asset types that are typical for a smart grid environment. Moreover, composite assets are being presented, covering various asset types as they are foreseen within the Smart Grid Reference Architecture Model (SGAM)[10];
- A section on the threat categories smart grid assets are exposed to. In this section, smart grid specific threats are presented as they emerged from the performed information collection and analysis.
- A section showing the smart grid asset types exposure to the threats and
- A section showing which threats emerge from which threat agent groups.
- A chapter with available smart grid security good practices indicating their protection against the identified threats.
- A conclusion summarizes various issues and gives an outlook of activities/open issues and upcoming actions in this area.

It is worth mentioning that in order to keep the size of this text as short as possible and enhance readability, detailed material is being provided by means of Annexes. This information is important for smart grid owners who wish to perform risk assessment and/or adapt the proposed security measures to their particular environment and needs.

[10] http://ec.europa.eu/energy/gas_electricity/smartgrids/doc/xpert_group1_reference_architecture.pdf, accessed 10 Sept 2013.

2 Method

In order to identify required protection levels of valuable assets it is common to perform a risk assessment. Subsequently, security measures have to be introduced to achieve the target level of protection by mitigating (part of) the assessed risks. As discussed below, threats are an important element in risk assessment.

In this chapter we present the rationale and method followed within the *Smart Grid Threat Landscape (SGTL)*. It consists of a number of threats to which smart grid assets are exposed. Hence, the presented SGTL is an important tool for those who want to assess the risks within a smart grid environment. Based on these risks, appropriate security measures can be selected to achieve risk mitigation.

The role of threats in the risk assessment activity becomes evident when looking at the components of risks. According to the widely accepted ISO 27005 definition risks emerge when: "Threats abuse vulnerabilities of assets to generate harm for the organization". In more detailed terms, we consider risk as taking into account the following elements:

Asset *(Vulnerabilities, Controls),* ***Threat*** *(Threat Agent Profile, Likelihood) and* ***Impact***

The elements of risks are graphically depicted in the figure below:

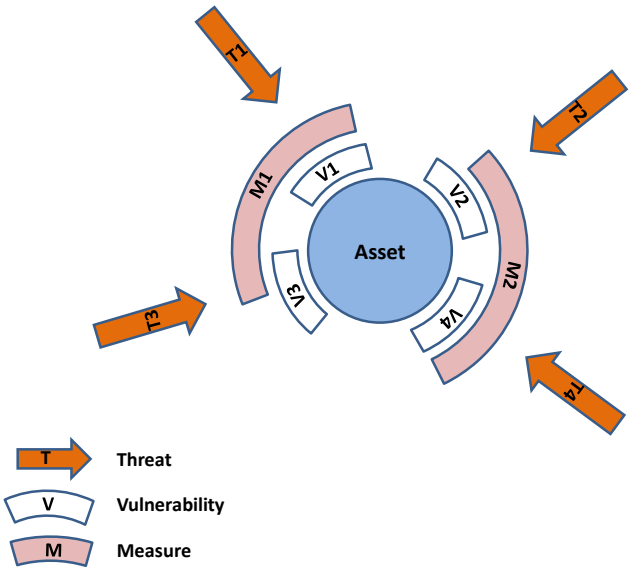

Figure 1: Threats targeting an asset by trying to exploit its vulnerabilities.

This figure has been adopted from ISO 13335-4 and shows how threats try to exploit asset vulnerabilities in order to harm/take over the asset. The asset owner has implemented security measures to protect the asset, that is, to eliminate its vulnerabilities. The impact achieved by the potential materialization of a threat is the final element to evaluate the risk of an asset (see also risk definition above).

While the definition of risks for an asset is a quite straight forward task, in complex environments it is often a challenge to assess risks. This is in particular the case in smart grids due to their technical complexity, interdependencies among components, multiplicity in operational responsibilities and

complex supply processes. The present document is generic, hence it does not assume any particular smart grid environment and/or the processes implemented through it. As such, it is impossible to make any valid assumptions about impact and vulnerabilities of assets. These are activities that can solely be performed by the asset owner. Hence, the need for supporting tools for the performance of risk assessments becomes obvious and essential for the asset owner in this complex environment.

In this document, we provide information on threats and threat exposure of typical smart grid assets, independently of any infrastructure scenarios. In other words, the smart grid Threat Landscape consists of a list of assets, and the threats applying to these assets.

Further, by means of the presented good practices, we identify various security measures found in smart grid security approaches. By mapping these measures against threats we show how security measures are the used to avoid the assumed threat exposure.

Given this information, the asset owner will need to assess vulnerabilities and impact in order to assess the risk and find risk mitigation measures (eventually among the ones from the processed good practices).

3 Smart Grid Assets

A smart grid may consist of a plethora of asset types. For the sake of information security, we consider assets that are mainly related to information and communication technology. Due to the massive deployment of IT-based components in the area of electricity and transport network, some assets that are characteristic for smart grids have been added. These assets generate or process data and as such are exposed to cyber-security threats. In addition to the IT-assets, some non-IT assets have been included that are tightly related to the proper operation of IT assets. Examples hereto are: some electrical assets such as cables and relays, facilities, human resources, non-IT media, etc.

The figure bellow gives an overview of the smart grid assets structure into relevant categories according to their use (see Figure 2). A more detailed description of these assets is given in Annex A.

Besides these smart grid assets, some composite, more complex assets have been identified. These assets have been taken from the Smart Grid Architecture Model (SGAM)[10]. By considering these assets, our intention is to take into account this standard, while at the same time showing the decomposition of the SGAM[10] assets by means of the assets of Figure 2. This will allow interested individuals to find threats applying to such complex assets by cumulating the threats of their counterparts.

Given the relatively young age of smart grid, it has to be taken as given that smart grid environments might grow over what is today being considered to be part of a smart grid infrastructure. Examples of such assets might be elements currently considered as part of Smart Cities[11] and Smart Mobility[12]. Indicatively for this type of assets, we have included a relevant part of e-Mobility in the smart grid asset types. Hence, the asset taxonomy presented should be considered as a snapshot of the current state-of-play and as such non-exhaustive.

[11] http://www.smart-cities.eu/press-ressources.html, accessed 5 September 2013.
[12] http://www.mobincity.eu/, accessed 5 September 2013.

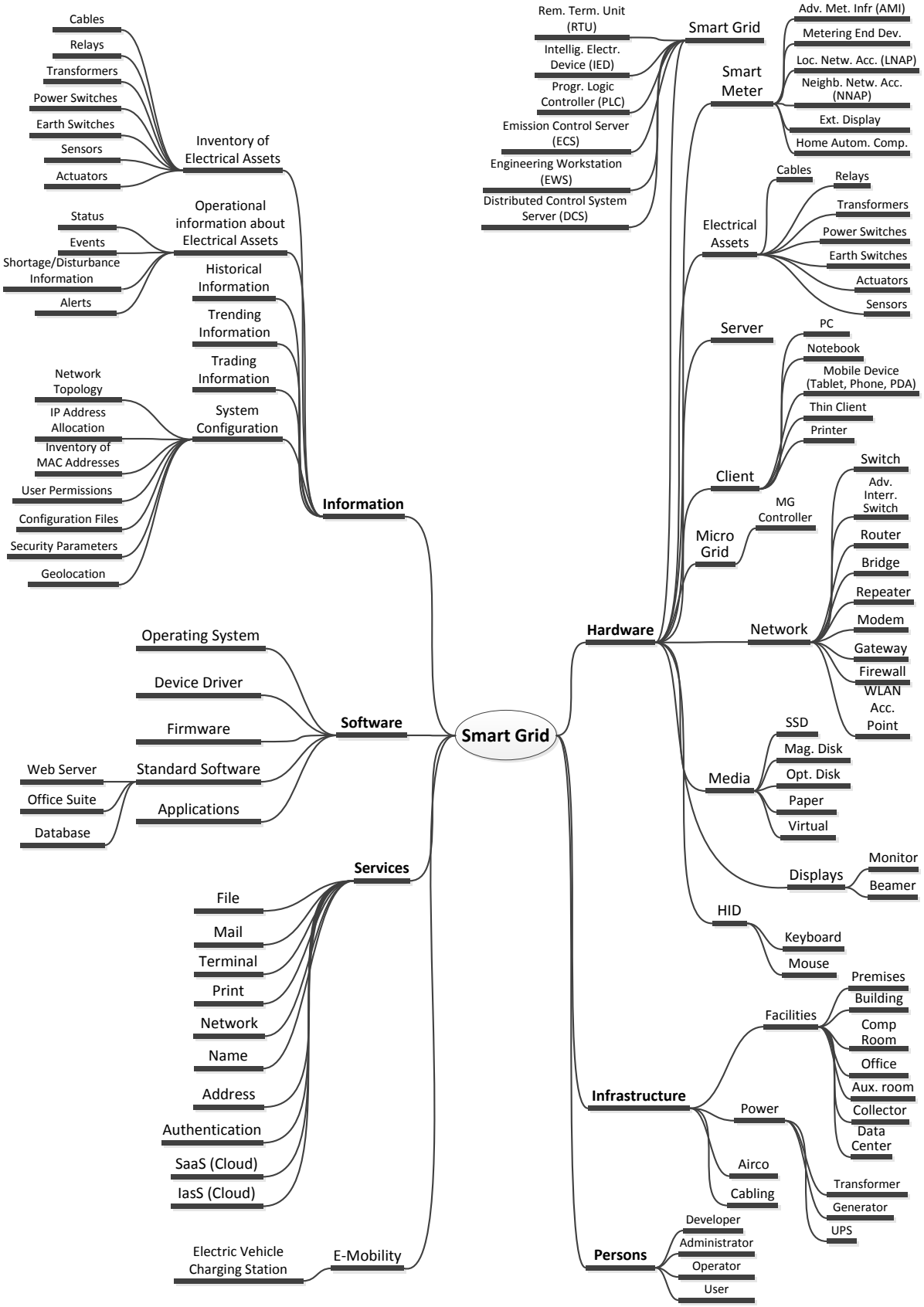

Figure 2: Overview of smart grid assets

The SGAM composite assets are decomposed by means of the asset groups shown in Figure 2. The decomposition of SGAM assets is presented in Table 1 below. It is worth mentioning that the terminology used, in particular zones and domains, has been taken as-is from the SGAM standard. Interested individuals might visit the SGAM document[10] to find more explanations about zones, domains and their counterparts.

ZONES	**Market**	Routers, Switches, Firewalls, Servers, Workstations	Routers, Switches, Firewalls, Servers, Workstations	Routers, Switches, Firewalls, Servers, Workstations	Routers, Switches, Firewalls, Servers, Workstations	Routers, Switches, Firewalls, Servers, Workstations
	Enterprise	Routers, Switches, Firewalls, Servers, Workstations	Routers, Switches, Firewalls, Servers, Workstations	Routers, Switches, Firewalls, Servers, Workstations	Routers, Switches, Firewalls, Servers, Workstations	Routers, Switches, Firewalls, Servers, Workstations
	Operation	Routers, Switches, Firewalls, Servers, Workstations	Routers, Switches, Firewalls, Servers, Workstations	Routers, Switches, Firewalls, Servers, Workstations	Routers, Switches, Firewalls, Servers, Workstations	Routers, Switches, Firewalls, Servers, Workstations
	Station	Routers, Switches, Firewalls, Servers, Workstations	Routers, Switches, Firewalls, Servers, Workstations	Routers, Switches, Firewalls, Servers, Workstations	Routers, Switches, Firewalls, Servers, Workstations	Routers, Switches, Firewalls, Servers, Workstations
	Field	RTUs, IEDs	RTUs, IEDs	RTUs, IEDs	RTUs, IEDs	IEDs, Router, Servers, Workstations, Firewalls
	Process	Actuators and Sensors (local communication line wired with RTUs or IEDs at Field level)	Actuators and Sensors (local communication line wired with RTUs or IEDs at Field level)	Actuators and Sensors (local communication line wired with RTUs or IEDs at Field level)	Actuators and Sensors (local communication line wired with RTUs or IEDs at Field level)	Actuators and Sensors (local communication line wired with IEDs or Customer Energy Management Systems at Field level)
		Generation	**Transmission**	**Distribution**	**DER**	**Customer Premises**
		DOMAINS				

Table 1: List of SGAM assets and their decomposition

4 Threats

For the purpose of the SGTL, a threat-taxonomy has been developed. The threats included in this collection of threats are all applicable to the smart grid assets presented in the previous section. The presented threat taxonomy covers mainly cyber-security threats, that is, threats applying to information and communication technology assets. Some additional non-IT threats have been assumed in order to cover threats to physical assets that are necessary to operate the considered ICT-assets. It is worth mentioning that the presented threats are a consolidation of threats from the ENISA Threat Landscape[13] and threats used within a smart grid assessment performed by DG CONNECT[14]. Moreover, the threats presented reflect the experience made within the ENISA Annual Incident Report 2012 regarding incidents in the telecommunication sector[15]. This report is considered relevant, as attack methods and threats in smart grid and the telecommunication sector are considered to be very similar (i.e. as applying to similar IT-assets).

The threats presented in Figure 3 are an overview. A detailed listing of these threats can be found in Annex B. This material contains additional information on threats such as:

- Threat details: this field explains further details of a threat as they have been found in analysed material on cyber-threats.
- Threat Agent: This field explains which threat agent group is considered to deploy attacks based on this threat.
- Trend: This field indicates assessed trends for each particular threat. Such trends have been assessed by analysing publicly available threat reports. Threats that do not have a value in the trend field are not subject of ENISA Threat Landscape. They are mentioned because they might be potentially useful for risk assessments.

It should be noted, that the details presented reflect the current state of play within the ENISA Threat Landscape[16] and are subject to changes according to new developments in that area and emerging threat issues (i.e. being a living document reflecting dynamic changes in the cyber-threat environment).

[13] http://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/ENISA_Threat_Landscape, accessed 5 September 2013.
[14] http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?action=display&doc_id=1763, accessed 5 September 2013.
[15] http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/annual-reports/annual-incident-reports-2012/at_download/fullReport, accessed 5 September 2013.

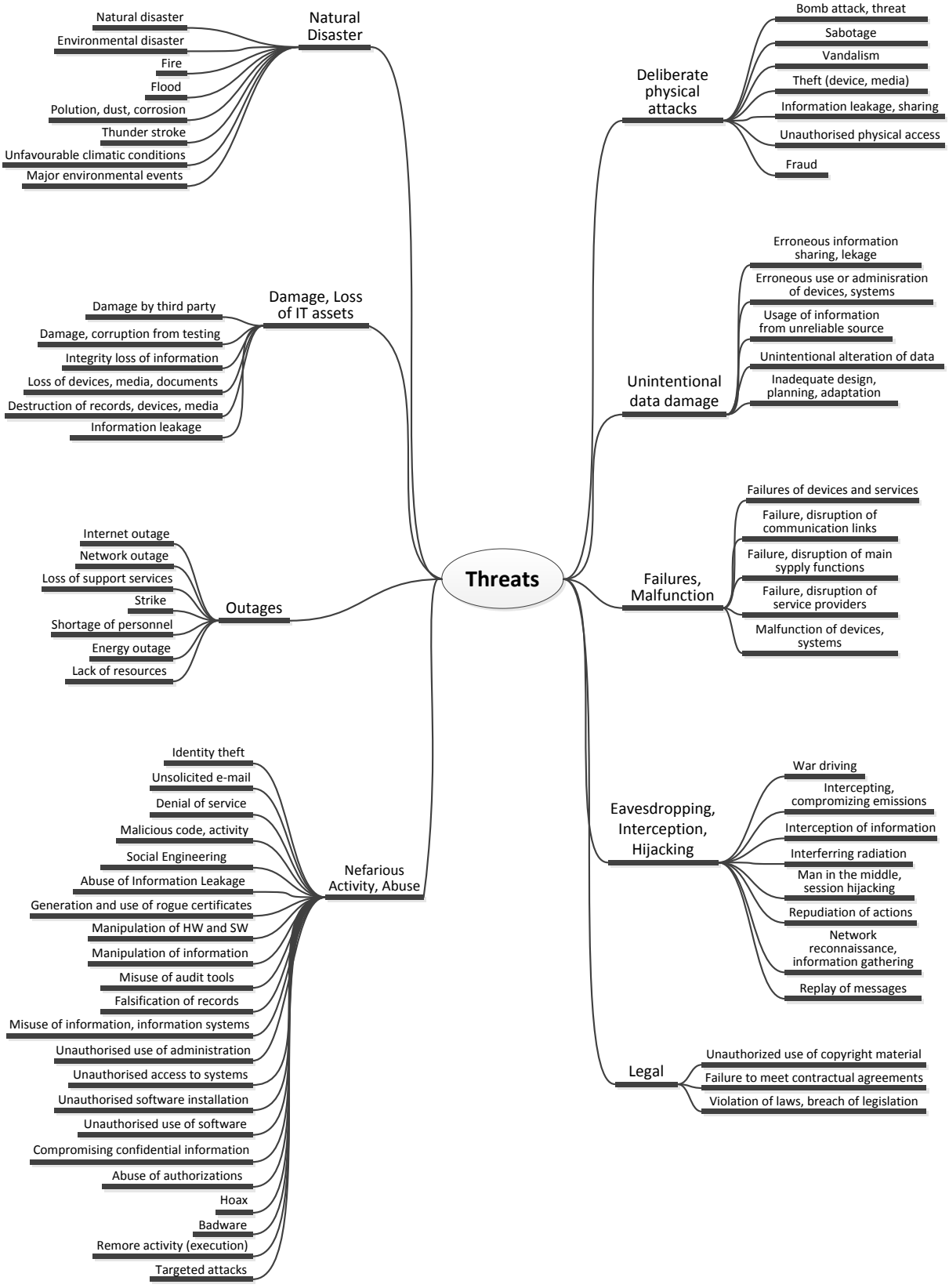

Figure 3: Overview of threats assumed for smart grid assets

5 Specific Smart Grid Threats

By analysing existing literature on smart grid security (see references and collected information in Annex D), we have identified specific threats that have been taken into account in existing assessments. The analysed material covers parts of smart grid infrastructure, in particular smart meters and some generic smart grid infrastructures within research projects. Thus, the specific smart grid threats presented in this section reflect the state-of-play in relevant available documents and, as such, are not exhaustive. Due to the complexity of smart grid infrastructures, one should argue that the set of threats presented in this chapter still have relevance for prospective infrastructure configurations and should be considered within risk assessments when relevant assets are part of the scenario at hand.

The specific smart grids encountered in the analysed literature are structured according to the categories mentioned in Figure 3. They are presented by means of threat details of particular threats and threat groups. It should be noted that the sequence of the specific smart grid threats presented below is not prioritized. This is because the analysed material has not provided any information that would allow prioritizing threats. Given the fact that no significant experience exists in this domain from existing implementations (i.e. through incident statistics in this area), no attempt has been undertaken to introduce any priorities for these threats. For obtaining a priority list of current cyber-threats, we suggest interested readers to visit the ENISA Threat Landscape report[16,17,18].

In the presentation of specific smart grid threats below, we use the same threat classification as the one used in Figure 3.

Threat Group: **Damage/Loss**

Threat: *Loss of devices, media and documents*

In smart grid environments this threat involves rummaging through disposed magnetic media for retrieving sensitive data that is left behind on it. In particular, it is assumed that unauthorized people might come to possession of data related to Advanced Metering Infrastructure (AMI) communication[19].

Threat: *Information leakage*

Attacks of this type target various smart grid components and their main aim is to acquire private sensitive information (energy consumption, credit cards, session data, access control data)[19,20].

Threat Group: **Eavesdropping/Interception/Hijacking**

Threat: *Interfering radiation*

Electro -Magnetic/ Radio Frequency interception is a threat that aims at performing unauthorized interception of private communication. In particular, it is assumed that unauthorized people might come to possession of data related to Advanced Metering Infrastructure (AMI) communication[19].

[16] http://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/ENISA_Threat_Landscape/at_download/fullReport, accessed 11 Nov 2013.
[17] http://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape-mid-year-2013/at_download/fullReport, accessed 11 Nov 2103.
[18] http://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape-2013-overview-of-current-and-emerging-cyber-threats/at_download/fullReport, accessed 11 Dec 2013.
[19] http://www.energy.ca.gov/2013publications/CEC-500-2013-056/CEC-500-2013-056.pdf, accessed 11 Nov 2013.

This threat materialises when threat agents are trying to interfere with the physical transmission and reception of wireless communications. It is one of the most efficient ways to launch physical-layer DoS attacks, especially targeting wireless communications. This can severely impact smart grid operations as they use wireless communication for various tasks[20].

Another threat of this type in smart grid regards the extraction of data by analysis of various types of electromagnetic radiation emitted by a CPU, display, keyboard, etc. In case of smart grids, these attacks are viable because equipment is installed in the field, geographically distributed and they are accessible[19].

Threat: *Man in the middle, session hijacking*

In smart grid environments, interactions of AMI components with the infrastructure can be compromised. That could lead to unauthorized access to AMI communication information, modification of AMI data, denial of service to authorized users, and repudiation of actions[19].

Threat: *Interception of information*

Through interception of information several networks of different natures can be affected, such as WIFI, Zegbee and fixed networks. Particular variations of this threat may include:

- Hijacking of the meter connection though a kind of unauthorized devices / messages to communicate with the DR system[19].
- Intercepting information by side-channel attacks. Such attacks are based on physical accessibility (Substation, smart meters, collectors, etc.) to gain information from the physical implementation of a cryptosystem as the components of the smart grid are geographically distributed.
- Intercepting and examining messages in order to deduce information from patterns in communication[20].
- Sniffer attacks whereby an attacker with the appropriate access captures and analyses the messages transmitted over the network[19,20,21].
- Use of External Traffic with the aim to intercepting and examining messages in order to deduce information from patterns in communication[19].

Threat: *Network reconnaissance and information gathering*

Information gathering attacks of mobile communication (in particular 802.16e) may target the Advanced Encryption Standard (AES) cipher providing strong confidentiality on user data[19].

Threat: *Replay of messages*

Acknowledges forgery is a threat where an attacker knows the DNS value and can send a false acknowledgement messages to the sender saying that the receiver has received the message when, in fact, it hasn't[19].

Threat Group: **Failures/Malfunction**

Threat: Failure of devices and systems

Given the complexity of smart grids and the multiplicity of devices and systems, it should be taken as given that a significant amount of incidents will be attributed to failures, misconfiguration and

[20] http://csrc.nist.gov/publications/nistir/ir7628/introduction-to-nistir-7628.pdf, accessed 11 Nov 2013.
[21] http://www.ece.ncsu.edu/netwis/papers/13wl-comnet.pdf, accessed 11 Von 2013.

errors. This has been confirmed by incidents communicated to ENISA in the area of telecommunications[22], a sector with equally complex infrastructure.

Threat: *Failure or disruption of communication links (communication networks)*
Attacks abusing implementations of standards are based on missing or weak implementations of security mechanisms, in particular when standards used have not been developed with security in mind[23].

Threat Group: **Nefarious Activity/Abuse**

Threat: *Unsolicited e-mail*

Personnel engaged by various players in smart grid can be victims of anonymous, unsolicited e-mail attacks. This might be part of a targeted campaign[20].

Threat: *Denial of Service attacks*

These attacks attempt to make smart grid resources unavailable to its intended users (internal and external). They can target to different layers of network and applications (physical / data-link)[20,21]. Such attacks can be also performed by jamming the power-line[24].

Threat: *Manipulation of hard- and software*

Through manipulation, an attacker may manipulate scheduling by disabling antenna and changing Programmable Communicating Thermostat (PCT) Time locally[19]. In particular:

- Break into EWS, use engineering software to access field controllers and change their logic[24].
- Get access to the operator station and perform targeted operator actions to stop all machines[24].
- Manipulation of firmware of smart e-meters. This may include manipulated firmware that is sent from Central System to E-meter of manipulated firmware that is sent from Central system (via Data Concentrator)[24].
- Compromise Central Systems to (1) switch off homes with E-meters; (2) delete all keys for the E-meters; and (3) distribute malicious firmware[24].

Threat: *Malicious code /Activity*

These threats affect smart grid as all the functioning of all involved IT components depends on the installed software. In detail, this threat consists of:

- Exploit kits are a widely deployed form attack. Through exploit kits virus and malware infections are performed. Infected devices may be manipulated by the attacker. Malware infected operator stations may send targeted commands to DCS Server to disturb or manipulate they operation[24].
- In smart grid, worms may be distributed by using the network to send copies to other nodes (computers on the network)[19]. Worms may affect the operation of all smart grid components connected to the network.
- Trojans are pieces of malware that facilitate unauthorized access to a computer system[19]. Worms may affect the operation of all smart grid components connected to the network.

[22] http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/annual-reports/annual-incident-reports-2012/at_download/fullReport, accessed 11 Nov 2013.
[23] http://www.etsi.org/WebSite/document/0905_RA%20smart%20grids-Bdef.pdf, accessed 11 Nov 2013.
[24] Crisalis Project EU (http://www.crisalis-project.eu/), Deliverable D2.2 Final Requirement Definition.

- Backdoor / trapdoor is an undocumented entry point into a computer program, which is generally inserted by a programmer to allow access to the program[19]. Vendors of smart meters, for example, may have installed firmware with backdoors or some hidden functionality[24] to facilitate access to the device.
- Service Spoofing is an attack in which the adversary successfully masquerades as another by falsifying data and thereby gaining an illegitimate advantage[19]. A concrete example of spoofing is ARP spoofing in the MAC layer: the management frames are not authenticated in 802.11. Every frame has a source address. The attackers take advantage of the spoofed frame to redirect the traffic and corrupt the ARP tables[19].
- With an ICMP-flooding attack, an adversary can flood a gateway with ICMP packets, thereby creating difficulties in the operation of clients associated to the same IP to send and receive packet.

A special case of a malicious activity that is leading to numerous incidents in all environments is that of "insider threat". With this approach, adversaries would take advantage of access to systems at the operator's end of the AMI system. The systems that the insider may be able to access include multiple appliances of a smart grid environment, including AMI, the system containing pricing information (either EMS or ICCP server to an ISO or generation entity), as well as the network infrastructure supporting those systems. Which malicious activity an insider uses, depends on their access to the various smart grid systems[19].

Threat: *Unauthorized access to information system / network*

External disclosure of information is an attack occurring when information is being disclosed to unauthorized entities. Smart grids manage privacy data, hence this threat is relevant in this environment.

Regarding the unauthorized access to systems/network, the attacker may gain unauthorized access to the information system / network from different locations[19,21,25] of the smart grid such as:

- Customer endpoint: There is a potential for AMI to allow access to the bulk electric grid from the residential or small business customer endpoint. The adversary can suborn the customer endpoint, intervene in wireless communication between the AMI meter and other endpoint equipment, or from the AMI meter to the local concentrator. These attacks will expose the head end equipment and systems to which the head end are connected. The exact details of this attack are greatly dependent on the implementation of AMI, particularly at the head end. Certain configurations would allow an attacker to affect the bulk electric grid.

  Through violation of the privacy of the consumer (1) disclose meter data or configuration data (Meter, Gateway or CLS configuration) or parts of it when transmitted between gateway and external entities in the WAN; (2) disclose meter data transmitted between the TOE and the meter. This threat is of specific importance if meters of more than one consumer are served by one gateway[27].
- Remote access: Unauthorized remote access to SCADA systems via remote access from outside the smart grid network.
- Remote access or physical access to the network: compromise DCS Server and disturb / disable communication with controllers in the field network[24]. Compromise DCS Server and send commands to control and manipulate the configuration (parameters) of controllers. Compromise

[25] http://www.ijsgce.com/uploadfile/2012/1011/20121011121836539.pdf, accessed 11 Nov 2013.

DCS Server and stop communication with Operator Station (stop delivery of data to Operator Station)[24]. Compromise RTU and send commands directly to controller[24].

Threat: *Manipulation of information*

This threat includes all kinds of manipulative activity regarding smart grid information, in particular AMI data and repudiation related information (e.g. AMI data, pricing information, invoicing information, etc.). This threat relates to information of all software used, but also certificates[19,20]. This threat might be deployed by means of the following methods:

- Through buffer overflow attacks by inserting an incorrect value in the message fields, thus affecting message processing or sets the DFC flag. This might cause, for example, an outstation device to appear busy to the master. These attacks can result in data corruption, unexpected actions and device crashes[21].
- Load redistribution attack is an injection of realistic false data with limited access to specific measurement data[26].
- Delivery of wrong data to operator station that looks valid and harmless[24].
- Manipulation of data received from TSO plant will cause working with wrong values, thus affecting the operation of RTU[24].
- Manipulation of data sent to TSO and Energy Management Center, thus affecting the operation of RTU[24].
- Attacker compromises an existing data concentrator and causes sending wrong data to the central system[24].
- Attacker alters meter data when transmitted between meter and Gateway, Gateway and consumer or Gateway and external entities. The objective can be to alter billing-relevant information or grid status information; the attack may be performed via any interface (e.g. LMN, HAN or WAN)[27].
- Attacker alters meter data, gateway configuration data, meter configuration data, CLS configuration data or a firmware update when transmitted between the gateway and an external entity in the Wan[27].
- False data are injected by an attacker in the smart grid traffic. The attacker injects false or malicious DR events in DRAS (Demand Response Automation Server), causing blackouts and instability of the grid. Attacker modifies configuration data in the DRAS such as DR program data, customer list and shed event information, affecting the DR program behavior[19].
- Through time modification of the Gateway time attackers aim at changing the relation between date / time measured consumption or production values in the meter data records[27].

Threat: *Misuse of information/Information Systems*

In the absence of end-to-end encryption, a compromised data concentrator can be misused to monitor data of other customers[24].

[26] http://www.iitmicrogrid.net/event/greatlake2012/publication/PPTs/32-Smart%20Grid%20Monitoring%20and%20Cyber%20Security/32-ZuyiLi-Load%20Redistribution%20Attacks%20and%20Protection%20Strategy%20in%20Electric%20Power%20Systems.pdf, accessed 11 Nov 2013.

[27] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/SmartMeter/PP-SmartMeter.pdf?__blob=publicationFile, accessed 11 Nov 2013.

Threat Group: **Physical attack**

Threat: *Fraud*

Within a reverse engineering attack, the customer at an endpoint would achieve reduction of cost of electric and/or natural gas use. They would use information freely available from the AMI meter vendor or the standard used within AMI meters to reset the meter and reprogram it to report false information. If the information is not freely available, the attacker would reverse-engineer a meter to develop a way to modify it. This is very similar to the many cable modem attacks that are openly available. Either the configuration settings from the utility or the actual firmware controlling the operation of the meter would be modified in this attack[24]. With the same objective, AMI meters can be removed from one home and placed to another[24].

6 Smart Grid assets exposure to cyber threats

In this section the threat exposure of smart grid assets is presented. The association between assumed threats from Figure 3 and assets from Figure 2 is established through Table 2 below. As such, this table shows the threat exposure of assets and can be used as guidance in identification of security needs. This table has been used within the document "*Appropriate Security Measures*"[28] that have been developed by ENISA on behalf of EG2 working group of the Commission[29].

Threat Group	Threat	Asset Group	Asset/Detail	Comment
Physical attack (deliberate/ intentional)		**Infrastructure Hardware E-Mobility Persons**		
	Bomb attack / threat	*Ditto*		
	Fraud	*Ditto*		
	Sabotage	*Ditto*		
	Vandalism	*Ditto*		
	Theft (of devices, storage media and documents)	*Ditto*		
	Information leakage/sharing	*Ditto*		
	Unauthorized physical access / Unauthorised entry to premises	*Ditto*		
	Coercion, extortion or corruption	*Ditto*		
Unintentional damage (accidental)		**Hardware Software Information Services**		
	Information leakage/sharing due to user error	*Ditto*		

[28] This ENISA contribution to Commission's EG2 working group is going to be published in short. Upon availability, the URL is going to be referenced.

[29] http://di.dk/SiteCollectionDocuments/Virksomhed/Sikkerhed/Presentations/05-Moulinos.pdf, accessed 3 Dec 2013

Threat Group	Threat	Asset Group	Asset/Detail	Comment
	Erroneous use or administration of devices and systems	*Ditto*		
	Using information from an unreliable source	*Ditto*		
	Unintentional change of data in an information system	*Ditto*		
	Inadequate design and planning or lack of adaptation	*Ditto*		
Disaster (natural, environmental)		**Infrastructure Hardware E-Mobility Persons**		
	Disaster (natural earthquakes, floods, landslides, tsunamis)	*Ditto*		
	Disaster (environmental - fire, explosion, dangerous radiation leak)	*Ditto*		
	Fire	*Ditto*		
	Flood	*Ditto*		
	Pollution, dust, corrosion	*Ditto*		
	Thunder stroke	*Ditto*		
	Water	*Ditto*		
	Unfavourable climatic conditions	*Ditto*		
	Major events in the environment	*Ditto*		
Damage/Loss (IT Assets)		**Hardware Software Information Services**		
	Damage caused by a third party	*Ditto*		
	Damages resulting from penetration testing		**Software Information Services**	
	Loss of (integrity of) sensitive information		**Software Information Services**	
	Loss of devices, storage media and documents		**Hardware Facilities**	
	Destruction of records, devices or storage media		**Software Information Services**	
	Information Leakage	*Ditto*		
Failures/ Malfunction		**Hardware Software Information Services**		
	Failure of devices or systems		**Hardware Software Services**	

Threat Group	Threat	Asset Group	Asset/Detail	Comment
	Failure or disruption of communication links (communication networks)		**Network Services**	
	Failure or disruption of main supply		**Facilities Power Airco**	
	Failure or disruption of service providers (supply chain)	*Ditto*		
	Malfunction of equipment (devices or systems)		**Hardware Software Services**	
	Insecure Interfaces (APIs)		**Hardware Software Services**	
Outages		**Infrastructure Hardware Software Services E-Mobility**		
	Lack of resources	*Ditto*	**Persons**	
	Loss of electricity	*Ditto*		
	Absence of personnel	*Ditto*		
	Strike	*Ditto*	**Persons**	
	Loss of support services	*Ditto*		
	Internet outage	*Ditto*		
	Network outage	*Ditto*		
Eavesdropping/Interception/ Hijacking		**Network Hardware Software Services Information**		
	War driving		**Network Services**	
	Intercepting compromising emissions		**Network Services**	
	Interception of information		**Information Network**	
	Interfering radiation		**Media HID Displays Electrical Assets**	
	Replay of messages		**Network Services Software**	
	Network Reconnaissance and Information gathering		**Network Information Persons**	
	Man in the middle/ Session hijacking		**Network Services Hardware Software**	
	Repudiation of actions		**Network Services Hardware Software Persons**	

Threat Group	Threat	Asset Group	Asset/Detail	Comment
Nefarious Activity/ Abuse		**Network Services Hardware Software Person**		
	Identity theft		**Network Services Software Person**	
	Unsolicited E-mail		**Person**	
	Denial of service		**Network Service Software**	
	Malicious code/ software/ activity		**Software Service**	
	Social Engineering		**Person**	
	Abuse of Information Leakage	*Ditto*		
	Generation and use of rogue certificates		**Network Service Software**	
	Manipulation of hardware and software		**Hardware Software Service**	
	Manipulation of information		**Information Service Software**	
	Misuse of audit tools		**Software Information**	
	Falsification of records		**Information Software**	
	Misuse of information/ information systems		**Information Software**	
	Unauthorised use or administration of devices and systems	*Ditto*		
	Unauthorized access to the information system / network	*Ditto*		
	Unauthorized changes of records		**Information Software**	
	Unauthorized installation of software		**Software**	
	Unauthorized use of software		**Software**	
	Compromising confidential information (data breaches)		**Network Information Service Software**	
	Abuse of authorizations	*Ditto*		
	Abuse of personal data	*Ditto*		
	Hoax	*Ditto*		
	Badware		**Network Information Service Software**	
	Remote activity (execution)		**Network Information Software**	

Threat Group	Threat	Asset Group	Asset/Detail	Comment
	Targeted attacks (APTs etc.)	*Ditto*	**Information**	
Legal		**Information** **Software** **People**		
	Violation of laws or regulations / Breach of legislation	*Ditto*		
	Failure to meet contractual requirements	*Ditto*		
	Unauthorized use of copyrighted material	*Ditto*		

Table 2: Association between Threats and smart grid Assets

7 Threat agents

Threats emerge from groups of threat agents. For smart grid asset owners it is considered important to know which threats emerge from which threat agent group. This information is significant to decide on the kind of risks that should be mitigated: threat agent groups are indicative of the determination behind launched attacks and capability level. Given the importance of smart grids and the potential impact of attacks, smart grid asset owners will need to spend some thoughts on which protection might be appropriate in order to avoid exposure to attacks from a certain type of threat agent. The threat agents considered within this document are as follows:

- **Corporations**: This kind of threat refers to corporations/organizations/enterprises that adopt and/or are engaged in offensive tactics. In this context, corporations are considered as hostile threat agents and their motivation is to build competitive advantage over competitors, who also make up their main target. Depending on their size and sector, corporations usually possess significant capabilities, ranging from technology up to human engineering intelligence, especially in their area of expertise.
- **Cybercriminals**: Cybercriminals are hostile by nature. Moreover, their motivation is usually financial gain and their skill level is, nowadays, quite high. Cybercriminals can be organised on a local, national or even international level. It should be taken as given, that a certain degree of networking between cybercriminals is being maintained.
- **Employees**: This category refers to the staff, contractors, operational staff or security guards of a company. They can have insider access to company's resources and they are considered as both non-hostile threat agents (i.e. distracted employees) as well as hostile ones (i.e. disgruntled employees). This kind of threat agents possesses a significant amount of knowledge that allows them to place effective attacks against assets of their organization.
- **Hacktivists**: Hacktivists are politically and socially motivated individuals that use computer systems in order to protest and promote their cause. Moreover, they are usually targeting high profile websites, corporations, intelligence agencies and military institutions.
- **Nation States**: Nation states can have offensive cyber capabilities and use them against an adversary. Nation states have recently become a prominent threat agent due to the deployment of sophisticated attacks that are considered as cyber weapons. From the sophistication of these malware it can be confirmed that nation states have a plethora of resources and they have a high level of skills and expertise.
- **Natural disasters**: Natural disasters are also threat agents and organizations are influenced by them, as they can cause potential physical damage. Natural disasters include lightning, fires, floods, earthquakes, windstorms etc. Although not a human threat agent, natural disasters are considered as such, as they can cause severe physical damage and impact the availability of information systems.
- **Terrorists**: Terrorists have expanded their activities and engage also in cyber-attacks. Their motivation can be political or religious and their capability varies from low to high. Preferred targets of cyber terrorists are mostly critical infrastructures (e.g. public health, energy production, telecommunication etc.), as their failures causes severe impact in society and government. It has to be noted, that in the public material analyses, the profile of cyber terrorists still seems to be blurry.

- **Cyber fighters**: an emerging phenomenon is that of patriotic motivated groups of citizens with the potential to launch cyber-attacks[30]. Such groups might have strong feelings when their political, national or religious values seem to be threatened by another group and are capable of launching cyber-attacks[31]. Having said that, one can argue that such groups are special cases (maybe an evolution or yet another instance) of hacktivism. To an extent, such groups may be supporters of totalitarian regimes and, rightly or wrongly, act on behalf of their supporting parties (i.e. governments) by contributing to national activities in the cyber-space[32]. Their activities may include conflicts with other groups (i.e. hacktivists)[33].

Based on these short threat agent profiles, the threats presented in this document can be assigned to relevant groups. This assignment is based on the threat agent group profile and in particular on assumed motives. Table 3 below presents the potential involvement of threat agent groups in the threats considered for smart grid assets.

	Corporation	Cyber-criminals	Employees	Hackti-vists	Nation States	Natural Disasters	Terrorists	Cyber fighters
Physical attacks					√		√	
Unintentional damage			√					
Failures / Malfunction		√	√	√	√			√
Eavesdropping / Interception / Hacking	√	√	√	√	√		√	√
Legal			√					
Nefarious activity / abuse	√	√	√	√	√		√	√
Outages			√		√	√		
Damage / Loss (IT-Assets)	√	√	√	√	√		√	√
Disaster						√	√	

Table 3: Involvement of Threat Agents in the threats

[30] http://krebsonsecurity.com/2013/06/iranian-elections-bring-lull-in-bank-attacks/ , accessed 13 Nov 2013.
[31] http://www.dailymail.co.uk/news/article-2313652/AP-Twitter-hackers-break-news-White-House-explosions-injured-Obama.html
[32] http://www.mcafee.com/us/resources/white-papers/wp-hacktivism.pdf
[33] http://mashable.com/2012/08/10/syrian-electronic-army/

8 Vulnerabilities and Risks in Smart Grid

In this section some reflections are provided on smart grid vulnerabilities and risks. Before going into the findings, one should note that both developments of smart grid infrastructures and smart grid security are at an early stage of maturity. This is mainly because not very many such infrastructures are operational for a sufficient period such that experiences have been gained, analysed and shared. On the other hand, smart grid developments and security assessments are in many cases managed confidentially, either for reasons of competitiveness or for security reasons. Hence, publicly available information on smart grid security issues originates from research and standardisation activities and is based on requirements and generic assumptions. The validation of this material through real-life experience/examples is currently not feasible, at least at European level.

Due to the immense investments that are necessary to set up a smart grid environment, standardisation activities are an important issue towards security of investments. Hence, a big amount of effort is currently invested in standardisation activities. Such activities are based on generic assumptions (i.e. infrastructure components, scenarios, security requirements, etc.) and are aiming at establishing a context that will serve as basis for industrial developments.

Having said that, some interesting information on vulnerabilities and risk has been found in the collected documents[20,24,25]. Given the general situation in smart grids the following vulnerabilities and risks were assessed:

- **Smart grid vulnerabilities**: Currently, vulnerabilities assumed within smart grid environments related to some areas that are not differentiated from other IT systems. In particular we have seen vulnerabilities related to the areas[25]: of customer security, physical security (in particular of publicly accessible devices), implicit trust between used components, teams with different skills and competences, involvement of multiple stakeholders (supply chain issues).

  Further, through to the utilization of wireless communication, relevant components might be vulnerable to threats targeting such components. Besides typical vulnerabilities in the area of wireless communication[34], some relevant material can be found in[20]. In the same document a number of generic non-smart grid related vulnerabilities can also be found.

  Concluding, one should mention that in the public domain there is a lack of information of vulnerabilities related to smart grid specific infrastructures, scenarios and components. There are some European projects that would cover this gap[24]. Also the analysis has identified a Spanish Centre[35] that is currently working in two European projects related with vulnerabilities in smart grids: n-SHIELD (www.newshield.eu/) and RISC (DG-HOME CIPS call).
- **Smart grid risks**: Regarding smart grid risks, only one document has been found that provides a comprehensive assessment of risks[24]. The risks assessed are related to the unavailability of some key smart grid components such as DCS and RTU; and AMI related components such as data concentrators, smart meters and central system to control and manage smart meters. The risks related to key smart grid components are mainly impact the stability and availability of the smart grid through manipulations in hard- and software (see nefarious activity, eavesdropping, and physical attack threat groups in Figure 3).

  Risks assessed for AMI are related to manipulation of components by users in order to perform fraud (i.e. primarily manipulating billing information and secondary affect operations of multiple meters). (see nefarious activity, eavesdropping, and physical attack threat groups in Figure 3).

[34] Vast amount of material does exist in this area. The reference give is just an example: http://www.ijarcce.com/upload/2013/july/49-h-marigowda-security%20vulnerability%20issues%20in%20wireless.pdf accessed 11 Nov 2013.

[35] http://www.tecnalia.com/, accessed 11 Nov 2013.

Although thoroughly done, this assessment covers only a part of the smart grid infrastructure and takes into account a reduced number of vulnerabilities. As already stated, more assessments will be necessary, ideally based on real infrastructures (even at the level of a laboratory) in order to achieve a better maturity in the implementation of smart grid cyber security measures.

Concluding, one should note that due to the fact that a smart grid is a system of systems, it is important to understand the dependencies among involved components. Certainly, work that has been done in the area of SCADA is highly relevant to smart grid environments. Moreover, with increasing proliferation of mobile devices in industrial systems work on mobile security is another important part of such a complex system. Hence, vulnerability and risk assessment will depend on the particular mix of components, processes and human infrastructure involved in a particular scenario.

9 Good Practice of Smart Grid Security Measures

In order to elaborate on good practices we took stock of publicly available smart grid security approaches. In doing so, existing literature has been analysed and security measures/controls proposed by these approaches have been identified. The security measures have been categorised in:

- *Security measures related to IT Systems and Logical Networks used within smart grid infrastructures*: Such measures are related to assets such as Wide Area Networks, Gateways, Home Area Network (HAN) and Zigbee (IEEE 802.15.4) protocol, Advanced Metering Infrastructure (AMI), Master Terminal Unit (MTU) and Remote Terminal Unit (RTU)
- *Security measures related to Supply Chain of smart grid*: Such measures are related to Providers, Distribution and Logistics and Customers.

In the following sections, the identified security measures are presented with indication of their origin.

In summary it is noticeable that three existing good practices provide a comprehensive set of security measures[19,20,36]. The majority of other documents analysed cover only a relatively small part of security measures[21,37,38,39,40,41,42]. This is quite natural thought, as this material is dedicated to some specific portions of smart grid infrastructure.

ENISA has also performed some work on security measures for smart grid. A report has been published on the minimum security measures for smart grids in 2012[43]. Based on this report, ENISA, in collaboration with the Commission, has initiated a number of consultations with both private and public sector stakeholders, under the umbrella of EG2[29], aiming at delivering a report with a set of smart grid appropriate cyber security measures which might end up to a Commission Recommendation on minimum cyber security requirements for smart grids in 2014. Both the ENISA report on minimum security measures and the contribution to EG2 are not covered within this good practice guide. The coverage of security measures proposed by ENISA with regard to threats mentioned in the present document can be found in the ENISA contribution to EG2 and are not repeated in this report.

The identified security measures are then mapped to the threats, completing thus the picture between threat exposure and proposed security measure. This information can be found in Annex C.

[36] http://www-304.ibm.com/jct03001c/procurement/proweb.nsf/objectdocswebview/filesupply+chain+security+white+paper+and+assessment+guide+april+2004/$file/supply+chain+security+white+paper+and+assessment+guide+april+2004.pdf, accessed 12 Nov 2013.

[37] http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5452993, *accessed 12 Nov 2013.*

[38] http://ieeexplore.ieee.org/xpl/articleDetails.jsp?reload=true&arnumber=6309314, accessed 12 Nov 2013.

[39] http://s3.amazonaws.com/sdieee/207-SG-Threats_Vulns_Countermeasure.pdf, accessed 12 Nov 2013.

[40] http://www.smartgrid.gov/sites/default/files/doc/files/2012_Cybersecurity_Information_Exchange.pdf, accessed 12 Nov 2013.

[41] http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/14-AMI_System_Security_Requirements_updated.pdf, accessed 12 Nov 2013.

[42] http://www.navigantresearch.com/wp-assets/uploads/2013/03/WP-SG10T-13-Navigant-Research.pdf, accessed 12 Nov 2013.

[43] http://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/smart-grids-and-smart-metering/appropriate-security-measures-for-smart-grids, accessed 2 Dec 2013.

9.1 IT Systems and Logical Networks

This group of security measures relates to information and communication systems, nodes and links, transmission systems, control and management. Best practices related to security measures for protection of IT systems and logical networks are:

1. Align cyber-security to the organization's overall IT strategy based on the defined risk profile[19,20].
2. Establish a rigorous, on-going risk management process[19,20].
3. Establish effective configuration management process[19].
4. Utilities to formally publish internal security program (policies, guidelines, procedures) and ensure compliance[19,20].
5. Develop cyber-security around IEC 62351[19,20].
6. Adopt the security measures regarding the defined SGIS Security Levels (SGIS-SL)[19].
7. Adopt the defined smart grid Data Protection classes (SG-DPC) [19].
8. Document network architecture and identify systems that serve critical functions or contain sensitive information that require additional levels of protection[19,20].
9. Conduct routine self-assessments[19].
10. Ensure Interoperability and Testing/Certification[19,20].
11. Implement a Security View per Layer, that is, establish a network protection strategy based on the principle of defence-in-depth[19,20].
12. Establish 24-hour-a-day incident monitoring and logging and audit systems[20,37].
13. Implement attack mitigation mechanisms and network security proactive measures: prevention, detection and analysis of vulnerabilities, correlation of events, etc[19,20,21].
14. Implement internal and external Intrusion Detection Systems (IDS) and Attack detection tools[20,21,37].
15. Establish incident response mechanisms: a breach is inevitable since no system can be 100% secure. Incident response procedures must be developed so that it is used in the event of an incident. Incident response includes disaster-recovery and business-continuity plans[19,20].
16. Maintain safe start, stop and fail modes for smart grid components: systems shall be capable of operating in an operational or non-operational state according to some policies. These may include activities allowed during initialization state, management functions necessary for element configuration, policy establishment and security domain establishment. The system shall transition into the operational state only upon completion of the critical initialization activities. The system shall transition into the non-operational state upon detection of a critical failure and transition into the operational state when the critical failure has been solved. At this point, the system shall be able to operating in a degraded mode while in an operational state. Also, supporting activities pertaining to the health of the system (e.g., diagnostics, maintenance, training, etc.) shall only be allowed during the operational state[19,20].
17. Establish system backups and disaster recovery plans[19,20].
18. Apply regular updates: applying software patches on a regular basis to the SCADA operation system, applications and components in the smart grid[19,20].
19. Removing or disabling unnecessary services[37,20].

20. Perform technical audits of SCADA devices and networks, and any other connected networks, to identify security concerns: analyse identified vulnerabilities to determine their significance, and take corrective actions as appropriate. Track corrective actions and analyse this information to identify trends. Additionally, retest systems after corrective actions have been taken to ensure that vulnerabilities were actually eliminated. Scan non-production environments actively to identify and address potential problems[37].
21. Conduct physical security surveys and assess all remote sites connected to the SCADA network to evaluate their security[37].
22. Identify and develop a comprehensive understanding of all connections to SCADA networks and evaluate and strengthen the security of these connections in order to protect them: internal local area and wide area networks, including business networks, Internet, wireless network devices, including satellite uplinks, modem or dial-up connections, connections to business partners, vendors or regulatory agencies, etc[37,19]. Some security measures can be adopted to protect these connections, such as, conduct penetration testing or vulnerability analysis, use of firewalls, Intrusion Detection Systems (IDSs), and other appropriate security measures at each point of entry[37,20].
23. Disconnect unnecessary connections to the SCADA network or isolate the SCADA network from other network connections: isolate the SCADA network from other networks as possible using "Demilitarized Zones" (DMZs) and data warehousing[19,37].
24. Establish strong controls over any medium that is used as a backdoor into the SCADA network[19,37].
25. Do not rely on proprietary protocols to protect your system: additionally, demand that vendors disclose any backdoors or vendor interfaces to your SCADA systems, and expect them to provide systems that are capable of being secured[37].
26. Implant Identification, Authentication and Access Control to all network devices, systems and users[19,20,21].
27. Support of biometric authentication for user access to critical components [19,20].
28. Establish a Role-based Access Control (RBAC): roles or responsibilities that a subject or a user has within the organization and on rules which determine what access rights are permitted for the subject in a given role. Clearly define cyber security roles, responsibilities, and authorities for managers, system administrators, and users[19,20].
29. Establish an Access Control List (ACL) and a Discretionary Access Control (DAC): list of permissions associated with an object that is used to specify which subjects, users, process, components or systems are allowed to access that particular object as well as which operations the subject can perform on that particular object[19,20].
30. Establish the necessary Capability Lists (CL): list of objects associated with the permission to it[19].
31. Establish a Mandatory Access Control (MAC): access policy used in multiple-level systems that require highly sensitive data[19,20].
32. Data Classification and Retention: data classification refers to classifying data according their security (confidentiality, integrity, or availability) level. Retention refers to how long data is kept before destroyed[19].
33. Define a strong Password Requirements and Guidelines and follow them[19,20].
34. Follow a correct policy of Control Key Management: all cryptographic keys, load control commands and network management commands must be encrypted before being shared on the network and only the intended recipients must possess the decryption keys[19,20].

35. Protect sensitive information using cryptographic functions to avoid external or not authorized access to it[19,20,21]. Sensitive information should be assessed by means of proper risk assessment.
36. Encrypt consumer usage data: only entities that are authorized to view the data possess the decryption keys[19,20].
37. Keep personally identifiable information in a minimum number of systems from which it may be securely accessed[19,20].
38. Encrypt the application level load control commands with the trust centre link key: Replay protection will be provided for this command by using a monotonically increasing sequence number[19].
39. Use Smart Energy Profile 2 (SEP 2) protocol: end-to-end Network Authentication and Authorization. Application Authentication (ACL). Authorization context (HTTPS, TLS). Digital Signatures ECDSA-SHA256 and X.509v3 Certificates. Cryptography: ECDHE, ECDSA, AES128[20,38].
40. The network key will be exchanged only with devices that successfully complete the join procedure: the join procedure requires the joining devices to establish a shared secret with the trust centre and use that to initiate communications. The shared key must be derived from the device installation code and shared with the trust centre using a secure out-of-band mechanism. Once the device joins the network successfully, the trust centre sends it the network key encrypted with the shared secret[19].
41. Avoid any unnecessary trade-offs between privacy and legitimate objectives of smart grid projects[19].
42. Visible and transparent to consumers — engaging in accountable business practices — to ensure that new smart grid systems operate according to stated objectives[19,20].
43. Make privacy a core functionality in the design and architecture of smart grid systems and practices[19,20].
44. Build in privacy end-to-end, throughout the entire life cycle of any personal information collected[19,20].
45. The trust centre must ensure availability: the centre must implement mechanisms for high availability including protection from denial of service attacks, resource starvation, or network congestion[19,20].

Some best practices are related to specific asset type, such as Wireless Neighbourhood Area Network (WNAN), Demand Response (DR) systems, Gateway, Home Area Network (HAN), Advanced Metering Infrastructure (AMI), or Master Terminal Unit (MTU).

9.1.1 WAN

This group of security measures covers all wireless communication that is necessary within smart grids. It covers WNAN (Wireless Neighbourhood Area Network, Wireless Local Area Network (WLAN) and Wireless Wide Area Network (WWAN).

1. IEEE 802.11: Use Media Access Control (MAC) address filtering; Wi-Fi Protected Access (WPA); IEEE 802.11w-2009 (an approved amendment to IEEE 802.11 to increase security of the management frames. The objective of this protocol is to increase the security by providing data confidentiality of management frames, mechanisms that enable data integrity, data origin authenticity, and replay protection) [19,20].
2. IEEE 802.15.4: Use MAC address filtering; Flash memories; AES encryption; Source Node Authentication[19,20].

3. IEEE 802.16: Use Message Authentication Code (MAC) techniques; Protection against masquerading parties, AES-CCM5[19].

9.1.2 Gateway

1. Low Power Encryption techniques (power consumption[19,20].
2. Central Authority for Public Key Infrastructure[19,20].
3. Trusted Platform Module[19,20].
4. MAC address filtering[19,20].
5. Virtual Home Command Exec. Execute all the commands received from the outside world on itself (Virtual Home Command Exec.) before deploying it on the real environment[19].

9.1.3 Home Area Network (HAN) and Zigbee (IEEE 802.15.4) protocol

1. Use Flash memory[19].
2. Avoiding Counter Mode (not secure Mode) in AES encryption[19].
3. Use MAC Address Filtering and Access Control List (ACL[19,20].
4. Source node authentication[19,20].
5. Restrict node connectivity using a pre-assigned PAN Identifier[19].
6. Secure Network Admission Control[19].
7. Out-of-band key loading method[19].
8. Trust Center address to be preconfigured in all nodes[19].
9. Establish an interference control (adequate band of frequency, increase, transmit power, mesh topology, frequency hopping[19,20].
10. Secure the Demand Response (DR) system. Proper data handling practices must be carried out in order to protect the security and privacy of customer information[19,20].

9.1.4 Advanced Metering Infrastructure (AMI)

1. Adopt an open reference standard for security of advanced meters[19,20].
2. Enforce full implementation of the security standard by advanced meter vendors[19].
3. Implement strong separation between the AMI network and the electronic security perimeters of other systems[19,20].
4. Implement network separation, strong firewalls, and limited router access control lists in the AMI network[19,20].
5. Traffic Control. Session control and mechanisms of detection and halting of rapid market fluctuations[19].
6. Ensure the existence of audit log maintenance[19,20].
7. Cryptographically authenticate metering assets to the network to ensure that only known and approved devices participate in the network[19,20].
8. Authenticate and integrity check system commands, at the meter, to ensure they are authorized and haven't been tampered[19,20].
9. Guard against replay attacks to prevent denial of service attacks or load shedding and ensure availability of system resources[19,20].

10. Encrypt meter data to protect consumer privacy[19,20].
11. Provide integrity protection and origin authentication of meter data[19,20].
12. Provide a means of non-repudiation for consumer demand response programs[19].
13. Physical protection security and tamper-protection[19,20].
14. Authenticate and integrity check meter firmware and configuration images when updates are provisioned. It is when firmware is being reprogrammed that devices can be most vulnerable[19,20].
15. Code Signing. It is a mechanism whereby publishers of software and content can use a certificate-based digital signature to verify their identities to users of the code, thus allowing users to decide whether or not to install it based on whether they trust the publisher[19].
16. Virtual Home Command Exec. Execute all the commands received from the outside world on itself (Virtual Home Command Exec.) before deploying it on the real environment[19].
17. Authenticate all commands from the head-end to the customer endpoint. The Head-End manages the information exchanges between external systems, such as the Meter Data Management (MDM) system and the AMI network[19,20].`
18. Authenticate all reporting from the customer endpoint to the head-end[19,20].
19. Protect Head-End systems as if they were critical cyber assets[19,20].
20. Implement host-based Intrusion Detection with software integrity checking of the Head-End systems[19,20].
21. Perform frequent, irregularly scheduled audits of Head-End outputs to ensure they reflect inputs[19].
22. Use strong user authentication on all Head-End systems and log all user actions[19,20].
23. Implement safety logic to prevent rapid changes in pricing information sent from the Head-End to the customer endpoint[19,20].

9.1.5 Master Terminal Unit (MTU) and Remote Terminal Unit (RTU)'

1. Security Architecture Design[19].
2. Security features provided by device and system vendors[19].
3. Check regularly and see if there is an abnormal operations taking place[19,20].
4. Conducting physical security surveys and assessing all remote sites connected to SCADA Network[19].
5. Use of firewalls and Demilitarized Zones (DMZs[19,20].
6. Implement electronic Perimeter Control[19,20 by means of a more rigorous scheme to implement network protection beyond IDS and Firewall.
7. Use of Intrusion Detection Systems (external and internal), including Domain-Specific IDS[19].
8. Proper implementation of IEC-60870 101, IEC-60870 104, DNP 3.0 and Modbus protocols[19,20].

9.2 Supply Chain

9.2.1 Providers

1. Recommend/enforce implementation of security standards[20,36,39].

2. Build a common understanding in security with vendors: standards, testing, checking, audits… (Work collaboratively with suppliers to refine security requirements.)[36,40].
3. Evaluation of vendors[39,36].
4. Provide strong contractual language in Request for Proposals (RFPs[36,40].
5. Implement the security features provided by device and system vendors. Many SCADA systems (old) in use have no security features whatsoever. SCADA system owners must insist that their system vendor implement security features in the form of product patches or upgrades. Some newer SCADA devices are shipped with basic security features, but these are usually disabled to ensure ease of installation. Analyse each SCADA device to determine whether security features are present[36,37].
6. To ensure the secure device design[36,40].
7. Develop database of components and too with all the discrete components, though this can be difficult to maintain with thousands of components[36].
8. To make available to vendors devices to track end of life of their products[36,39].
9. Provide regular feedback for terminal/port operator regarding supply chain security requirements and performance[36].
10. Test proactively terminal operators' supply chain security capabilities[36].
11. Control access to order and shipment information[36].
12. Inform the consumers of how information collected from them will be used[36].
13. Provide the consumers with clear instructions on how to use the privacy safeguards offered, such as a secure login and password, as well as how to de-enrol or delete personally identifiable information relating to them[36].
14. Require verification of carrier and driver prior to allowing entry[36].
15. Use Radio Frequency (RFDC) to track storage and retrieval of product and movement by employee[36].
16. Have backup power for key operational areas and high-value cargo areas[36].
17. Establish alternative source as part of contracting process[36].
18. Require contractually electronic seals for monitoring access to containers[36].
19. Employ closed-circuit monitoring of cargo loading process with recordings to be maintained for a specified period[36].

9.2.2 Distribution and Logistics

1. Include specific supply chain security requirements in contracts as a condition for acceptance[36].
2. Mandate that suppliers adhere to established standards, help them to do it and supervise periodically[36].
3. Include appropriate language in contractual agreements to safeguard consumers[36].
4. Have information regarding customer supply chain security concerns and to develop implications[36].
5. Work collaboratively with suppliers to refine security requirements[36].
6. Replicate best practices and results among trading partners[36].
7. Pre-screen potential suppliers with security capabilities as a major consideration[36].

8. Demand transparency and visibility across the supply chain[36].
9. Adequate control in all the points: Supplier, Terminal/Port Operator, Carrier, Customer[36].
10. Require use of closed-circuit video monitoring of facilities, docks, and cargo[36].
11. Monitor the process closely during the cargo loading process and transportation journey and record it for a specific period of time[36].
12. Automate the chain of custody[36].
13. Record and reports detected deviations from approved transport routes[36].
14. Secure the cross-border supply chains[36].
15. Inspect products and containers at the points of origin and maintain cargo integrity[36].
16. Require Supply Chain Event Management (SCEM) capability to proactively manage transport movements[36].
17. Use Radio Frequency (RFDC) to track storage and retrieval of product and movement by employee[36].
18. Have extensive policies such as two drivers, use of GPS, escorted service, driver security training, and route varying for high-risk shipments[36].
19. Require verification of carrier and driver prior to allowing entry[36].
20. Require approval by firm security of any deviation from approved transport routes[36].
21. Require satellite tracking of trucks and containers as a condition of contract[36].
22. Use tracking and protocols to allow real-time notification of diversion to security and law enforcement[36].
23. Check systematically containers prior to release for re-use[36].
24. Have a mode-shifting protocol to accommodate unexpected delays, interruptions and disasters[36].
25. Plan to guarantee continuous supply of critical components to the customers[36].
26. Employ backup power supply for operations and security systems[36].
27. Establish comprehensive metrics for evaluating supply chain security performance and makes them available[36].
28. Test and review regularly, objectively and proactively carrier supply chain security capabilities and response plans[36].
29. Perform unannounced inspections/assessments or validation by third party[36].
30. Acquire comprehensive education regarding the role in enhancing supply chain security[36].
31. Have a comprehensive “code of ethics” regarding supply chain security practices[36].
32. Train personnel to observe for signs of employees who might respond to coercion[36].
33. Require contractually international carriers to transmit electronic crew and cargo manifests[36].
34. Identify supply chain security education initiatives and have a formal plan for moving employees through the program[36].
35. Participate actively in cross-organizational initiatives to develop and influence governmental supply chain security policies[36].

36. Take active role in initiatives to educate and exchange information with government officials responsible for enhancing supply chain security[36].
37. Take active role in guiding and providing feedback for government initiatives to enhance supply chain security initiatives[36].
38. Provide carrier drivers with comprehensive education regarding their role in enhancing supply chain security[36].
39. Adjust processes based on government security levels[36].
40. Provide facility security using a combination of passive and active measures including fences, locks, video, and human inspections[36].
41. Establish an Internet supply-chain-theft report that contains all the information to be reported to law enforcement[36].
42. Employ redundant communications system for critical incident management[36].
43. Define procedures and conditions for notifying customs and other law enforcement agencies regarding shortages, overages, anomalies, or illegal activities[36].
44. Centralize responsibility for supply chain security management with a high-visibility cross-functional team[36].
45. Keep the integrity and confidentiality of system data[36,41].
46. Keep the confidentiality (and access control) of customer equipment, the integrity of control messaging and message information and the availability of customer devices[36,41].
47. Keep the confidentiality (privacy) and integrity of customer data and payments. Integrity of control messaging and message information containing prepayment data, and also the availability of customer payment data and usage balances[36,41].
48. Ensure that any personally identifiable information retained is securely destroyed at the end of its lifecycle[36].
49. Implement and use a Disaster Recovery System[36,42].
50. Establish alternative providers on major lanes[36].
51. Separate break areas from storage and staging areas[36].
52. Require contractually electronic seals for monitoring access to containers[36].
53. Maintain proper storage of empty and full containers in a protected environment to prevent unauthorized access, including use of seals[36].
54. Segregate and mark international, domestic, high-value, and dangerous goods cargo within the warehouse by a safe, vault, caged, or otherwise fenced-in area[36].
55. Prohibits private passenger vehicles from parking in cargo areas or immediately adjacent to cargo storage buildings[36].

9.2.3 Customers

1. Provide information regarding security concerns[36].
2. Include appropriate language in contractual agreements to safeguard consumers[36].
3. Keep the confidentiality (privacy) and integrity of customer data and payments[36,41,20].
4. Keep the confidentiality (access control) of customer equipment, the integrity of control messaging and message information and the availability of customer devices[20,41].

5. Requires verification of carrier and driver prior to allowing entry[36].
6. Document receiving discrepancies using electronic and video means[36].
7. Require matches for production and inventory receipt quantities[36].
8. Require proper weighing, counting, and documenting of cargo equipment verified against manifest documents[36].

10 Conclusions

Based on the experience gained within this activity, a number of issues have been identified that are worth further elaboration and/or action from relevant stakeholders. In particular:

- Develop attack scenarios for smart grid components. The next step towards facilitating risk assessments for smart grid infrastructures would be to develop some kind of threat intelligence in the form of attack scenarios.
- Elaborate on criticality assessment. Stakeholders have expressed the necessity to develop criteria that allow assessing criticality of smart grid components. This would facilitate impact identification and necessary protection levels.
- Develop assessments for various scenarios. It seems to be very advantageous to come up with some smart grid scenarios. Risk assessments would contribute to the specification of appropriate security measures for these scenarios.
- Elaborate on levels of impact for smart grid incidents. Discussions with stakeholders have shown the need to define impact thresholds for incidents in the area of smart grids. Such thresholds would be important parameters for the definition of security levels, identification and management of critical situations, etc.
- As in all CIIP areas, words matter: develop and maintain smart grid security terms and definitions.
- Establish better coordination of European/International activities in the area of smart grids, including standardisation. Currently, various activities are on-going in this area, involving multiple organisations and stakeholders. It is important to identify common areas and coordinate the agendas. This will enable coherence and exploitation of synergies.
- Elaborate on the overlapping issues of safety vs. security: smart grid is a traditional engineering sector in which safety standards are implemented. Cyber security overlaps with safety as it concerns the operation of parts of the grid. These overlaps need to be identified and interfaces need to be established.
- Establish a platform for information exchange on smart grid security. Following the coordination of activities, it is important to establish the platform for information flow. This will enable coherence and exploitation of synergies.
- Initiate a debate on need/importance maturity/compliance/certification approaches for (areas of) smart grid security. As in any industrial area, and in particular in CIIP, it is important to discuss the importance in setting criteria for measuring security maturity in smart grids.
- Track developments in smart grid security and update relevant material. Both smart grid and cyber security are in a dynamic phase of change/development. This will make updates important in order to maintain their usability.
- Link smart grid activities with other related emerging areas such as smart cities, smart (home) environments, eMobility, Future Internet, and liaise with related stakeholders. As the scope of all these areas is quite wide and overlapping, it will be important to identify interfaces and coordinate common topics.
- Create circles of trust to share information about smart grid security. Smart grid security is falls into CIIP and as such parts of the work need to be kept in confidentiality. For this purpose, circles of trust among relevant stakeholders need to be developed and modalities need to be developed for managing this information.

Annex A: Description of Smart Grid assets

Information

Information is a valuable asset as, depending on it, machines and staff will make decisions. It can travel by different supports or represent different meanings. Information assets identified are:

- Inventory of electrical assets: physical components that storage the information while it is travelling or it is being converted: cables, relays, transformers, power switches, earth switches, controllable/regulating inverter, distribution automation, sensors, equipment health sensor, fault current limiter, FACTS devices.
- Operational information about electrical assets: status indicators, alerts, events and shortage - disturbance information.
- Historical information: information related to the past that must be storage by law or due to its value / nature.
- Trending information: information related to the past that can be used to predict future behaviour, and so, to be prepared for it.
- Trading information: information related with commercial issues.
- System Configuration: information related with the network itself: network topology, IP addresses Allocation, inventory of MAC addresses, user credentials, user permissions, configuration files, geolocation.

Different information may be susceptible to the security principles: confidentiality, integrity, availability.

Software

The Software of an infrastructure will let us manage the information (access it, modify it and store new information). No availability of the required software will mean any access to information. Main software in a smart grid is:

- Applications: we will find different types of applications with different connectivity: connected with the Internet but only accessed by the staff of the company; application oriented to end users, to access its own information; real time applications (utility IT information system capable of integrating, organizing, displaying and analysing real-time or near real-time electric distribution data to offer a wide range of operational benefits; SCADA systems: the application that will control industrial processes, in general no connected with Internet.
- Standard Software: software needed to make the applications work.
    - Database.
    - Web server.
- Operating System.
- Device Driver: software installed in the different used drivers as USBs, CDs, DVDs, printers, scanners.
- Firmware.

When we analyse this asset, we will need to think about: the origin of the software (is this origin trustworthy? Do we know the source code?); access to it (who is able to access it and with what kind of permissions? What procedures of access does it have?); real location of the software (where is the server that holds is located?).

Services

The services are activities between a client and a provider. They are considered as valuable assets because its correct functioning is needed to the correct functioning of the smart grid.

Services oriented to the staff of the smart grid:

- Mail Service.
- Terminal Service.
- Print Service.
- Authentication Service.

Services oriented to the network itself and to make possible the necessary communications:

- File Service.
- Network Service.
- Name Service.
- Address Service.

Cloud services:

- Software as a service.
- Infrastructure as a service.

Hardware

The hardware components considered as main assets of a smart grids are:

- Smart grid:
    - Remote Terminal Unit (RTU): microprocessor-controlled electronic device that interfaces objects in the physical world to a distributed control system or SCADA (supervisory control and data acquisition) system by transmitting telemetry data to a master system, and by using messages from the master supervisory system to control connected objects.
    - Intelligent Electronic Device (IED): term used in the electric power industry to describe microprocessor-based controllers of power system equipment, such as circuit breakers, transformers, and capacitor banks.
    - Programmable Logic Controller (PLC): digital computer used for automation of electromechanical processes, such as control of machinery on factory assembly lines, amusement rides, or light fixtures.
    - Distributed Control System (DCS): is a system used in manufacturing to control set of devices in a distributed environment.
- Micro grid: electrical systems that include multiple loads and distributed energy resources that can be operated in parallel with the grid or as an electrical island; Micro grid Controller: devices that control and enable the establishment of micro grids.
- Smart Meter: electrical meter that records consumption of electric energy in intervals of an hour or less and communicates that information at least daily back to the utility for monitoring and billing purposes. The components of smart meters to take into account are:
    - Metering End Device, which let us read date at the end points: Electricity; Gas; Water; Heat.

- Local Network Access Point (LNAP).
- Neighbourhood Network Access Point (NNAP).
- External Display.
- Home Automation Components.
- AMI Head End (Advanced Metering Infrastructure).

- Servers: related with hardware, computer hardware that holds the necessary software to run an infrastructure.
- Clients: devices from which personal staff, end users and potential clients will connect with available applications:
  - PC.
  - Notebook.
  - Tablet.
  - ThinClient.
  - PDA.
  - (Mobil-)Phone.
  - Printer.
  - Smart Appliances and Equipment (Customer): home appliances and devices (i.e., thermostats, pool pumps, clothes washers/dryers, water heaters, etc.) that use wireless technology to receive real-time data from the AMI system to control or modulate their operation.
- Network Components: physical devices needed for the correct functioning of the network:
  - Advanced Interrupting Switch: switches or technologies that can detect and clear faults more quickly or without a traditional reclosing sequence.
  - Switch.
  - Router.
  - Bridge.
  - Repeater.
  - Modem.
  - Gateway.
  - Firewall.
  - WLAN Access Point.
- Media: physical support to storage the information:
  - Semiconductor Storage.
  - Magnetic Storage.
  - Optical Storage
  - Paper

  - Human
- Displays: devices to present the information to the user:
  - Monitor
  - Beamer
- Human Interaction Devices (HID): devices to let the user introduce information to the system.
  - Keyboard
  - Mouse

A main issue talking about hardware is the supply chain. For the critical hardware, the supply chain should be controlled by the owner of the infrastructure.

Infrastructure
Infrastructures are also main assets to protect. There are several types of infrastructures:

- Facilities:
  - Premises
  - Building
  - Server Room
  - Office
  - Auxiliary Room
  - Collector
  - Data centre
- Power:
  - Transformer
  - Emergency Generator
  - UPS
- Air Conditioning
- Cabling

Personnel
Personnel are now considered a main asset in all the organizations, due to its knowledge and experience. The existing profiles of personnel in a smart grid are:

- User
- Operator
- Administrator
- Developer

Every profile has different access to the rest of the assets.

eMobility
EMobility represents the concept of using electric powertrain technologies, in-vehicle information, and communication technologies and connected infrastructures to enable the electric propulsion of

vehicles and fleets. Powertrain technologies include full electric vehicles and plug-in hybrids, as well as hydrogen fuel cell vehicles that convert hydrogen into electricity. The main assets are:

- Electric Vehicle Charging Station.
- Vehicles

Annex B: Threats assumed for Smart Grid assets

Threat Group	Threat	Threat details	Threat Agent	Trend[44]	Comments
Physical attack (deliberate/ intentional)					
	Bomb attack / threat				
	Fraud				
		Fraud by employees	Employees	Increasing	
	Sabotage		Corporations Cybercriminals Employees Hacktivists Nation States Terrorists[45]		
	Vandalism		Employees Terrorists Rioter		
	Theft (of devices, storage media and documents)				
		Theft of mobile devices (smartphones/ tablets)	Corporations Employees Nation States Terrorists	Increasing Stable (theft internal staff)	
		Theft of other hardware	Corporations Employees Nation States Terrorists	Stable	
	Information leakage/sharing		Corporations Cybercriminals Employees Hacktivists Nation States Terrorists	Increasing	
	Unauthorized physical access / Unauthorised entry to premises		Employees Hacktivists Terrorists		
	Coercion, extortion or corruption		Corporations Cybercriminals Employees Hacktivists Nation States Terrorists		

[44] Threats that have been assigned a trend are the ones that have been encountered within the ENISA Threat Landscape 2012.

[45] Terrorists as a Threat Agent: Based on the publicly available information resources, the profile of cyber terrorists still seems to be blurry due to lack of concrete evidence. There are opinions in the literature that cyber criminals and cyber terrorists are involved in similar activities with the difference being solely in their content. On the other hand, it is reported that terrorists are involved mostly in sabotage attacks against high impact targets and their capability resources vary from low to average. Finally, it is often reported that cybercriminals can be engaged by individuals with terroristic motive to perform an attack on their behalf.

Threat Group	Threat	Threat details	Threat Agent	Trend[44]	Comments
Unintentional damage (accidental)					
	Information leakage/sharing due to user error				
		Accidental leaks/sharing of data by staff	Employees	Increasing	
		Mobile privacy and mobile applications	Employees	Increasing	
		Web applications	Employees	Increasing	
		Network	Employees	Increasing	
	Erroneous use or administration of devices and systems			Overall increasing (additional mobile devices) Decreasing (as Internal threat)	
		Errors in maintenance	Employees		
		Configuration/ installation error	Employees		
		Technological obsolescence	Employees		
		Increasing recover time	Employees		
		Unpatched software (delayed patching processes)	Employees		
	Using information from an unreliable source		Employees		
	Unintentional change of data in an information system		Employees		
	Inadequate design and planning or lack of adaptation		Employees		
Disaster (natural, environmental)					
	Disaster (natural earthquakes, floods, landslides, tsunamis)		NA		
	Disaster (environmental - fire, explosion, dangerous radiation leak)		NA		
	Fire		NA		
	Flood		NA		
	Pollution, dust, corrosion		NA		

Threat Group	Threat	Threat details	Threat Agent	Trend[44]	Comments
	Thunder stroke		NA		
	Water		NA		
	Unfavourable climatic conditions		NA		
	Major events in the environment		NA		
Damage/Loss (IT Assets)					
	Damage caused by a third party	Security failure by third party	Third party provider	Increasing	
	Damages resulting from penetration testing		Third party provider		
	Loss of (integrity of) sensitive information	Loss of integrity of certificates	Corporations Cybercriminals Employees Hacktivists Nation States Terrorists	Increasing	
	Loss of devices, storage media and documents				
		Mobile devices	Corporations Cybercriminals Employees Hacktivists Nation States Terrorists	Increasing	
		Storage media	Corporations Cybercriminals Employees Hacktivists Nation States Terrorists	Increasing	
		Documentation of IT Infrastructure	Corporations Cybercriminals Employees Hacktivists Nation States Terrorists		
	Destruction of records, devices or storage media				
		Infection of removable media	Corporations Cybercriminals Employees Hacktivists Nation States	Increasing	
		Abuse of storage	Corporations Cybercriminals Employees Hacktivists Nation States	Increasing	
	Information Leakage				
		Mobile data and data of mobile	Corporations Cybercriminals Employees	increasing	

Threat Group	Threat	Threat details	Threat Agent	Trend[44]	Comments
		applications	Hacktivists Nation States Terrorists		
		Web privacy and web applications	Corporations Cybercriminals Employees Hacktivists Nation States Terrorists		
		Network traffic	Corporations Cybercriminals Employees Hacktivists Nation States Terrorists	increasing	
Failures/ Malfunction					
	Failure of devices or systems				
		Defective data media	NA		
		Hardware failure	NA		
		Failure of applications and services	NA		
	Failure or disruption of communication links (communication networks)				
		Failure of cable networks	NA		
		Failure of wireless networks	NA		
		Failure of mobile networks	NA		
	Failure or disruption of main supply		NA		
	Failure or disruption of service providers (supply chain)		NA		
	Malfunction of equipment (devices or systems)		NA		
	Insecure Interfaces (APIs)				
Outages					
	Lack of resources		NA		
	Loss of electricity		NA		
	Absence of personnel		NA		
	Strike		NA		
	Loss of support		NA		

Threat Group	Threat	Threat details	Threat Agent	Trend[44]	Comments
	services				
	Internet outage		NA		
	Network outage				
		Outage of cable networks	NA		
		Outage of wireless networks	NA		
		Outages of mobile networks	NA		
Eavesdropping/Interception/ Hijacking	***War driving***	Search and cartography of free Wi-Fi networks with the objective to abuse them.			
	Intercepting compromising emissions	Numerous devices use air-interfaces (Wi-Fi, Bluetooth, Infrared, etc.). These can be abused.	Corporations Cybercriminals Employees Hacktivists Nation States Terrorists		
	Interception of information				
		Corporate Espionage	Corporations Employees Nation States	Decreasing	
		Unsecured Wi-Fi, rogue access points	Corporations Cybercriminals Employees Hacktivists Nation States Terrorists		
	Interfering radiation	High frequency devices (e.g. displays) radiate. This information can be misused.	Corporations Nation States Terrorists		
	Replay of messages		Cybercriminals Employees		
	Network Reconnaissan-ce and Information gathering	The activity to collect sufficient information from legitimate channels about the structure of a network.	Corporations Cybercriminals Employees Hacktivists Nation States Terrorists	To be taken seriously in the middle term.	
	Man in the middle/ Session hijacking		Corporations Cybercriminals Employees Hacktivists	Increasing	

Threat Group	Threat	Threat details	Threat Agent	Trend[44]	Comments
			Nation States Terrorists		
	Repudiation of actions		Corporations Cybercriminals Employees Hacktivists Nation States Terrorists		
Nefarious Activity/ Abuse	***Identity theft***	Credentials stealing trojans	Corporations Cybercriminals Employees Hacktivists Nation States Terrorists	Overall increasing (with some stability/ decrease in reported cases)	Identity theft, achieved by exploiting existing vulnerabilities via threats, especially Trojans over private PCs.
	Unsolicited E-mail				
		SPAM	Cybercriminals	Decreasing/ Stable	
		Unsolicited infected e-mails	Cybercriminals	Stable/ Increasing	
	Denial of service				
		Plain denial of service (DoS) (e.g. against application services of critical infrastructure)	Cybercriminals Hacktivists	Increasing	
		Distributed DoS (DDoS)	Cybercriminals Hacktivists	Increasing	
	Malicious code/ software/ activity				
		Search Engine Poisoning	Cybercriminals	Increasing	
		Exploitation of fake trust of social media	Cybercriminals	Increasing	
		Worms/Trojans	Corporations Cybercriminals Nation States	Increasing (strongly for mobile devices)	
		Mobile malware	Cybercriminals Hacktivists Nation States	Increasing strongly	
		Alternation of software	Corporations Cybercriminals Employees Hacktivists Nation States	Increasing	
		Infected trusted mobile apps	Corporations Cybercriminals Employees Hacktivists Nation States		

Threat Group	Threat	Threat details	Threat Agent	Trend[44]	Comments
		Elevation of privileges	Corporations Cybercriminals Hacktivists Nation States		
		Phishing attacks	Corporations Cybercriminals Employees Hacktivists Nation States Terrorists	Stable/ Decreasing	
		Web injection attacks (Code injection: SQL, XSS)	Corporations Cybercriminals Hacktivists Nation States	Increasing	
		Exploit Kits	Corporations Cybercriminals Hacktivists Nation States	Increasing	
	Social Engineering				
		Rogue security software/ Rogueware/ Scareware	Cybercriminals Hacktivists	Increasing	
		Ransomware	Cybercriminals	Increasing	
	Abuse of Information Leakage				
		Leakage affecting mobile privacy and mobile applications	Corporations Cybercriminals Employees Hacktivists Nation States		
		Leakage affecting web privacy and web applications	Corporations Cybercriminals Employees Hacktivists Nation States		
		Leakage affecting network traffic	Corporations Cybercriminals Employees Hacktivists Nation States		
	Generation and use of rogue certificates				
		Loss of (integrity of) sensitive information	Corporations Cybercriminals Hacktivists Nation States	Increasing	
		Man in the middle/ Session hijacking	Cybercriminals Hacktivists Nation States	Increasing	
		Social Engineering (e.g. install	Corporations Cybercriminals Employees	Increasing	

Threat Group	Threat	Threat details	Threat Agent	Trend[44]	Comments
		fake trust OS updates)	Hacktivists Nation States		
	Manipulation of hardware and software				
		Anonymous proxies	Corporations Cybercriminals Hacktivists Nation States	Increasing	
		Abuse of computing power of cloud to launch attacks (cybercrime as a service)	Corporations Cybercriminals Hacktivists Nation States		
		Abuse of 0-day vulnerabilities	Corporations Cybercriminals Employees Hacktivists Nation States		
		Access of web sites through chains of HTTP Proxies (**Obfuscation**)	Cybercriminals		
	Manipulation of information				
	Misuse of audit tools		Corporations Cybercriminals Employees Hacktivists Nation States		
	Falsification of records				
	Misuse of information/ information systems		Corporations Cybercriminals Employees Hacktivists Nation States	Increasing	
	Unauthorised use or administration of devices and systems		Corporations Cybercriminals Employees Hacktivists Nation States		
	Unauthorized access to the information system / network	Network Intrusion	Corporations Cybercriminals Employees Hacktivists Nation States	Stable/ Decreasing	
	Unauthorized changes of records		Cybercriminals		
	Unauthorized installation of software	Drive-by download / malicious URLs	Corporations Cybercriminals Employees Hacktivists Nation States	Increasing	

Threat Group	Threat	Threat details	Threat Agent	Trend[44]	Comments
	Unauthorized use of software		Corporations Cybercriminals Employees Hacktivists Nation States		
	Compromising confidential information (data breaches)		Corporations Cybercriminals Employees Hacktivists Nation States	Increasing	
	Abuse of authorizations		Corporations Cybercriminals Employees Hacktivists Nation States	Stable/Decreasing	
	Abuse of personal data				
	Hoax	False rumour and/or a fake warning	Corporations Cybercriminals Employees Hacktivists Nation States Terrorists		
	Badware	Spyware or deceptive adware	Corporations Cybercriminals Nation States		
	Remote activity (execution)				
		Remote Command Execution	Corporations Cybercriminals Employees Hacktivists Nation States Terrorists	Increasing slowly and steadily	
		Botnets / Remote activity	Corporations Cybercriminals Employees Hacktivists Nation States Terrorists	Increasing	
	Targeted attacks (APTs etc.)				
		Spear phishing attacks	Corporations Cybercriminals Nation States	Increasing	
		Installation of sophisticated and targeted malware	Corporations Cybercriminals Nation States	Stable/ Increasing	
Legal	***Violation of laws or regulations / Breach of legislation***		Corporations Cybercriminals Employees Nation States	Increasing	
	Failure to meet contractual requirements		Employees		

Threat Group	Threat	Threat details	Threat Agent	Trend[44]	Comments
	Unauthorized use of copyrighted material	File Sharing services	Corporations Cybercriminals Employees Nation States	Increasing	

Annex C: Good Practices: protection against the Threats

In this annex, various security measures used within the analysed good practices are referenced in the table through the number of the section their section and thir sequence number within each section.

			SOURCES			
Threat Group	Threat	Threat details	NIST[20]	Enhancing Security Throughout the Supply Chain (IBM Center)[36]	Smart grid Information Assurance and Security Technology Assessment (Sacramento State)[19]	Other[21,37,38,39,40,41,42]
Physical attack (deliberate/ intentional)	Bomb attack / threat		[9.1].1-2 // [9.1].4 // [9.1].8 // [9.1].10-17 // [9.1].22 // [9.1].26-29 // [9.1].31 // [9.1].33-35 // [9.1.4].13 // [9.2.1].1	[9.2.1].1 // [9.2.1].7-19 // [9.2.2] // [9.2.3].1 // [9.2.3].5-8	[9.1].1-4 // [9.1].6-11 // [9.1].13 // [9.1].15 // [9.1].16 // [9.1].17 // [2.1.].22-24 // [9.1].26-35 // [9.1.4].13 // [9.1.5].4 //	[9.1].12 // [9.1].14 // [9.1].20-22 // [9.1].23 // [9.1].24 // [9.1].26 // [9.1].28 // [9.1].35 // [9.2.1].1 // [9.2.2].45-47 // [9.2.2].49
	Fraud	Cheating customer (Reverse engineering)	[9.1].1-2 // [9.1].4 // [9.1].8 // [9.1].10-15 // [9.1].22 // [9.1].26-29 // [9.1].31 // [9.1].33-35 // [9.1.4].13 // [9.2.1].1 // [9.2.3].3-4	[9.2.1].1 // [9.2.1].7-19 // [9.2.2] // [9.2.3].1 // [9.2.3].3 // [9.2.3].5-8	[9.1].1-4 // [9.1].6-11 // [9.1].13 // [9.1].15 // [2.1.].22 // [9.1].24 // [9.1].26-35 // [9.1.4].13 // [9.1.5].4 //	[9.1].12 // [9.1].14 // [9.1].20-22 // [9.1].24 // [9.1].26 // [9.1].28 // [9.1].35 // [9.2.1].1 // [9.2.2].45-47 // [9.2.2].49 // [9.2.3].3-4
		Cheating companies	[9.1].1-2 // [9.1].4 // [9.1].8 // [9.1].10-17 // [9.1].22 // [9.1].26-29 // [9.1].31 // [9.1].33-35 // [9.1.4].13 // [9.2.1].1	[9.2.1].1 // [9.2.1].7-19 // [9.2.2] // [9.2.3].1 // [9.2.3].5-8	[9.1].1-4 // [9.1].6-11 // [9.1].13 // [9.1].15 // [9.1].16 // [9.1].17 // [2.1.].22 // [9.1].24 // [9.1].26-35 // [9.1.4].13 // [9.1.5].4 //	[9.1].12 // [9.1].14 // [9.1].20-22 // [9.1].24 // [9.1].26 // [9.1].28 // [9.1].35 // [9.2.1].1 // [9.2.2].45-47 // [9.2.2].49
	Sabotage		[9.1].1-2 // [9.1].4 // [9.1].8 // [9.1].10-17 // [9.1].22 // [9.1].26-29 // [9.1].31 // [9.1].33-35 // [9.1.4].13 // [9.2.1].1	[9.2.1].1 // [9.2.1].7-19 // [9.2.2] // [9.2.3].1 // [9.2.3].5-8	[9.1].1-4 // [9.1].6-11 // [9.1].13 // [9.1].15 // [9.1].16 // [9.1].17 // [2.1.].22-24 // [9.1].26-35 // [9.1.4].13 // [9.1.5].4 //	[9.1].12 // [9.1].14 // [9.1].20-22 // [9.1].23 // [9.1].24 // [9.1].26 // [9.1].28 // [9.1].35 // [9.2.1].1 // [9.2.2].45-47 //

			SOURCES			
Threat Group	Threat	Threat details	NIST[20]	Enhancing Security Throughout the Supply Chain (IBM Center)[36]	Smart grid Information Assurance and Security Technology Assessment (Sacramento State)[19]	Other[21,37,38,39,40,41,42]
						[9.2.2].49
	Vandalism		[9.1].1-2 // [9.1].4 // [9.1].8 // [9.1].10-15 // [9.1].17 // [9.1].22 // [9.1].26-29 // [9.1].31 // [9.1].33-35 // [9.1.4].13 // [9.2.1].1	[9.2.1].1 // [9.2.1].7-19 // [9.2.2] // [9.2.3].1 // [9.2.3].5-8	[9.1].1-4 // [9.1].6-11 // [9.1].13 // [9.1].15 // [9.1].17 // [2.1.].22-24 // [9.1].26-35 // [9.1.4].13 // [9.1.5].4 //	[9.1].12 // [9.1].14 // [9.1].20-22 // [9.1].23 // [9.1].24 // [9.1].26 // [9.1].28 // [9.1].35 // [9.2.1].1 // [9.2.2].45-47 // [9.2.2].49
	Theft (of devices, storage media and documents)		[9.1].1-2 // [9.1].4 // [9.1].8 // [9.1].10-15 // [9.1].22 // [9.1].26-29 // [9.1].31 // [9.1].33-35 // [9.2.1].1	[9.2.1].1 // [9.2.1].7-19 // [9.2.2] // [9.2.3].1 // [9.2.3].5-8	[9.1].1-4 // [9.1].6-11 // [9.1].13 // [9.1].15 // [2.1.].22-24 // [9.1].26-35 //	[9.1].12 // [9.1].14 // [9.1].20-22 // [9.1].23 // [9.1].24 // [9.1].26 // [9.1].28 // [9.1].35 // [9.2.1].1 // [9.2.2].45-47 // [9.2.2].49
	Information leakage/sharing		[9.1].1-2 // [9.1].4 // [9.1].8 // [9.1].10-15 // [9.1].22 // [9.1].26-29 // [9.1].31 // [9.1].33-35 // [9.1.4].13 // [9.2.1].1	[9.2.1].1 // [9.2.1].7-19 // [9.2.2] // [9.2.3].1 // [9.2.3].5-8	[9.1].1-4 // [9.1].6-11 // [9.1].13 // [9.1].15 // [2.1.].22-24 // [9.1].26-35 // [9.1.4].13 // [9.1.5].4 //	[9.1].12 // [9.1].14 // [9.1].19 // [9.1].20-22 // [9.1].23 // [9.1].24 // [9.1].26 // [9.1].28 // [9.1].35 // [9.2.1].1 // [9.2.2].45-47 // [9.2.2].49
	Unauthorized physical access / Unauthorised entry to premises		[9.1].1-2 // [9.1].4 // [9.1].8 // [9.1].10-16 // [9.1].22 // [9.1].26-29 // [9.1].31 // [9.1].33-35 // [9.1.4].13 // [9.2.1].1	[9.2.1].1 // [9.2.1].7-19 // [9.2.2] // [9.2.3].1 // [9.2.3].5-8	[9.1].1-4 // [9.1].6-11 // [9.1].13 // [9.1].15 // [9.1].16 // [2.1.].22-24 // [9.1].26-35 // [9.1.4].13 // [9.1.5].4 //	[9.1].12 // [9.1].14 // [9.1].20-22 // [9.1].23 // [9.1].24 // [9.1].26 // [9.1].28 // [9.1].35 // [9.2.1].1 // [9.2.2].45-47 // [9.2.2].49
	Coercion, extortion or corruption		[9.1].1-2 // [9.1].4 // [9.1].8 // [9.1].10-15 // [9.1].17 // [9.1].19 // [9.1].22 // [9.1].26-29 //	[9.2.1].1 // [9.2.1].7-19 // [9.2.2] // [9.2.3].1 // [9.2.3].5-8	[9.1].1-4 // [9.1].6-11 // [9.1].13 // [9.1].15 // [9.1].17 // [2.1.].22 // [9.1].24 // [9.1].26-35 //	[9.1].12 // [9.1].14 // [9.1].19 // [9.1].20-22 // [9.1].24 // [9.1].26 // [9.1].28 // [9.1].35 //

			SOURCES			
Threat Group	Threat	Threat details	NIST[20]	Enhancing Security Throughout the Supply Chain (IBM Center)[36]	Smart grid Information Assurance and Security Technology Assessment (Sacramento State)[19]	Other[21,37,38,39,40,41,42]
			[9.1].31 // [9.1].33-35 // [9.2.1].1			[9.2.1].1 // [9.2.2].45-47 // [9.2.2].49
Unintentional damage (accidental)	Information leakage/sharing due to user error		[9.1].2 // [9.1].8 // [9.1].11-13 // [9.1].15-19 // [9.1.5].3		[9.1].2-3 // [9.1].8 // [9.1].11 // [9.1].13 // [9.1].15-18 // [9.1].23 // [9.1.2].5 // [9.1.3].7 // [9.1.4].15-16 // [9.1.5].3	[9.1].12-13 // [9.1].19 // [9.1].23
	Erroneous use or administration of devices and systems		[9.1].2 // [9.1].8 // [9.1].11-13 // [9.1].15-19 // [9.1.5].3		[9.1].2-3 // [9.1].8 // [9.1].11 // [9.1].13 // [9.1].15-18 // [9.1].23 // [9.1.2].5 // [9.1.3].7 // [9.1.4].15-16 // [9.1.5].3	[9.1].12-13 // [9.1].19 // [9.1].23
	Using information from an unreliable source		[9.1.5].3		[9.1.2].5 // [9.1.3].7 // [9.1.4].15-16 // [9.1.5].3	
	Unintentional change of data in an information system		[9.1].2 // [9.1].8 // [9.1].11-13 // [9.1].15-19 // [9.1.5].3		[9.1].2-3 // [9.1].8 // [9.1].11 // [9.1].13 // [9.1].15-18 // [9.1].23 // [9.1.2].5 // [9.1.3].7 // [9.1.4].15-16 // [9.1.5].3	[9.1].12-13 // [9.1].19 // [9.1].23
	Unintentional loss of data		[9.1].2 // [9.1].8 // [9.1].11-13 // [9.1].15-19 // [9.1.5].3		[9.1].2-3 // [9.1].8 // [9.1].11 // [9.1].13 // [9.1].15-18 // [9.1].23 // [9.1.2].5 // [9.1.3].7 // [9.1.4].15-16 // [9.1.5].3	[9.1].12-13 // [9.1].19 // [9.1].23
	Inadequate system design and planning or lack of adaptation		[9.1].43		[9.1].43 // [9.1.5].1	[9.2.1].6
	Lack of awareness		[9.1].1 // [9.2.1].1	[9.2.1].1-2 // [9.2.2].1-6	[9.1].1	[9.2.1].1-2

			SOURCES			
Threat Group	Threat	Threat details	NIST[20]	Enhancing Security Throughout the Supply Chain (IBM Center)[36]	Smart grid Information Assurance and Security Technology Assessment (Sacramento State)[19]	Other[21,37,38,39,40,41,42]
				// [9.2.2].28-32		
Disaster (natural, environmental)	Disaster (natural earthquakes, floods, landslides, tsunamis)		[9.1].15 // [9.1].17	[9.2.2].24 // [9.2.2].49	[9.1].15 // [9.1].17	[9.2.2].49
	Disaster (environmental - fire, explosion, dangerous radiation leak)		[9.1].15 // [9.1].17	[9.2.2].24 // [9.2.2].49	[9.1].15 // [9.1].17	[9.2.2].49
	Fire		[9.1].15 // [9.1].17	[9.2.2].24 // [9.2.2].49	[9.1].15 // [9.1].17	[9.2.2].49
	Flood		[9.1].15 // [9.1].17	[9.2.2].24 // [9.2.2].49	[9.1].15 // [9.1].17	[9.2.2].49
	Pollution, dust, corrosion		[9.1].15 // [9.1].17	[9.2.2].24 // [9.2.2].49	[9.1].15 // [9.1].17	[9.2.2].49
	Thunder stroke		[9.1].15 // [9.1].17	[9.2.2].24 // [9.2.2].49	[9.1].15 // [9.1].17	[9.2.2].49
	Water		[9.1].15 // [9.1].17	[9.2.2].24 // [9.2.2].49	[9.1].15 // [9.1].17	[9.2.2].49
	Unfavourable climatic conditions		[9.1].15 // [9.1].17	[9.2.2].24 // [9.2.2].49	[9.1].15 // [9.1].17	[9.2.2].49
	Major events in the environment		[9.1].15 // [9.1].17	[9.2.2].24 // [9.2.2].49	[9.1].15 // [9.1].17	[9.2.2].49
	Animal		[9.1].15 // [9.1].17	[9.2.2].24 // [9.2.2].49	[9.1].15 // [9.1].17	[9.2.2].49
Damage/Loss (IT Assets)	Damage caused by a third party		[9.1].1-2 // [9.1].4 // [9.1].8 // [9.1].10-15 // [9.1].22 // [9.1].26-29 // [9.1].31 // [9.1].33-35 // [9.2.1].1	[9.2.1].1 // [9.2.1].7-19 // [9.2.2] // [9.2.3].1 // [9.2.3].5-8	[9.1].1-4 // [9.1].6-11 // [9.1].13 // [9.1].15 // [2.1.].22-24 // [9.1].26-35 //	[9.1].12 // [9.1].14 // [9.1].20-22 // [9.1].23 // [9.1].24 // [9.1].26 // [9.1].28 // [9.1].35 // [9.2.1].1 // [9.2.2].45-47 // [9.2.2].49
	Damages resulting from penetration testing		[9.1].5 // [9.1].14 // [9.1].22 // [9.1].26 // [9.1].28-29 // [9.1].31 // [9.1].33-37 // [9.1].39 //		[9.1].5 // [9.1].22-24 // [9.1].26 // [9.1].28-38 // [9.1].40-44 // [9.1.1].1-3 // [9.1.2]. 2 // [9.1.3].4-6 //	[9.1].14 // [9.1].22 // [9.1].23-26 // [9.1].28 // [9.1].35 // [9.1].39

			SOURCES			
Threat Group	Threat	Threat details	NIST[20]	Enhancing Security Throughout the Supply Chain (IBM Center)[36]	Smart grid Information Assurance and Security Technology Assessment (Sacramento State)[19]	Other[21,37,38,39,40,41,42]
			[9.1].42-44 // [9.1.1].1-2 // [9.1.2]. 2 // [9.1.3].4 // [9.1.4].3-4 // [9.1.4].14 // [9.1.4].17-18 // [9.1.4].20 // [9.1.5].5-6 // [9.1.5].8		[9.1.3].8 // [9.1.4].3-5 // [9.1.4].14 // [9.1.4].17-18 // [9.1.4].20 // [9.1.5].5-8	
	Loss of (integrity of) sensitive information		[9.1].5 // [9.1].8 // [9.1].10-11 // [9.1].22 // [9.1].26 // [9.1].33-36 // [9.1].39 // [9.1].43-44 // [9.1.1].1-2 // [9.1.2].1 // [9.1.3].10 // [9.1.4].1 // [9.1.4].7-8 // [9.1.4].10-11 // [9.1.4].14 // [9.1.4].19 // [9.1.5].8		[9.1].5-8 // [9.1].10-11 // [9.1].24 // [9.1].26 // [9.1].33-36 // [9.1].38 // [9.1].40-41 // [9.1].43-44 // [9.1.1].1-3 // [9.1.2].1 // [9.1.3].2 // [9.1.3].5 // [9.1.3].10 // [9.1.4].1-2 // [9.1.4].7-8 // [9.1.4].10-11 // [9.1.4].14 // [9.1.4].19 // [9.1.5].1-2 // [9.1.5].8	[9.1].22 // [9.1].24-26 // [9.1].35 // [9.1].39
	Loss of devices, storage media and documents	Media scavenging	[9.1].1-2 // [9.1].4 // [9.1].8 // [9.1].10-15 // [2.1.].22 // [9.1].26-29 // [9.1].31 // [9.1].33-35 // [9.2.1].1	[9.2.1].1 // [9.2.1].7-19 // [9.2.2] // [9.2.3].1 // [9.2.3].5-8	[9.1].1-4 // [9.1].6-11 // [9.1].13 // [9.1].15 // [2.1.].22-24 // [9.1].26-35 //	[9.1].12 // [9.1].14 // [9.1].20-22 // [9.1].23 // [9.1].24 // [9.1].26 // [9.1].28 // [9.1].35 // [9.2.1].1 // [9.2.2].45-47 // [9.2.2].49
	Destruction of records, devices or storage media		[9.1].1-2 // [9.1].4 // [9.1].8 // [9.1].10-15 // [2.1.].22 // [9.1].26-29 // [9.1].31 // [9.1].33-35 // [9.2.1].1	[9.2.1].1 // [9.2.1].7-19 // [9.2.2] // [9.2.3].1 // [9.2.3].5-8	[9.1].1-4 // [9.1].6-11 // [9.1].13 // [9.1].15 // [2.1.].22-24 // [9.1].26-35 //	[9.1].12 // [9.1].14 // [9.1].20-22 // [9.1].23 // [9.1].24 // [9.1].26 // [9.1].28 // [9.1].35 // [9.2.1].1 // [9.2.2].45-47 // [9.2.2].49
	Information Leakage		[9.1].1-2 // [9.1].4 //	[9.2.1].1 // [9.2.1].7-19	[9.1].1-4 // [9.1].6-11 //	[9.1].12 // [9.1].14 //

			SOURCES			
Threat Group	Threat	Threat details	NIST[20]	Enhancing Security Throughout the Supply Chain (IBM Center)[36]	Smart grid Information Assurance and Security Technology Assessment (Sacramento State)[19]	Other[21,37,38,39,40,41,42]
			[9.1].8 // [9.1].10-15 // [9.1].19 // [2.1.].22 // [9.1].26-29 // [9.1].31 // [9.1].33-35 // [9.1.4].13 // [9.2.1].1	// [9.2.2] // [9.2.3].1 // [9.2.3].5-8	[9.1].13 // [9.1].15 // [2.1.].22-24 // [9.1].26-35 // [9.1.4].13 // [9.1.5].4 //	[9.1].19 // [9.1].20-22 // [9.1].23 // [9.1].24 // [9.1].26 // [9.1].28 // [9.1].35 // [9.2.1].1 // [9.2.2].45-47 // [9.2.2].49
Failures/ Malfunction	Failure of devices or systems		[9.1].2 // [9.1].8 // [9.1].11-13 // [9.1].15-19 // [9.1.2].5 // [9.1.3].7 // [9.1.4].15-16 // [9.1.5].3		[9.1].2-3 // [9.1].8 // [9.1].11 // [9.1].13 // [9.1].15-18 // [9.1].23 // [9.1.2].5 // [9.1.3].7 // [9.1.4].15-16 // [9.1.5].3	[9.1].12-13 // [9.1].19 // [9.1].23
	Failure or disruption of communication links (communication networks)				[9.1].40	[9.1].42
	Failure or disruption of main supply		[9.1.3].9	[9.2.1].16 // [9.2.2].26	[9.1.3].9	
	Failure or disruption of service providers (supply chain)		[9.2.1].1	[9.2.1].1 // [9.2.1].4-11 // [9.2.1].14-19		[9.2.1].1-2 // [9.2.1].4-6 // [9.2.1].8
	Malfunction of equipment (devices or systems)		[9.1].2 // [9.1].8 // [9.1].11-13 // [9.1].15-19 // [9.1.2].5 // [9.1.3].7 // [9.1.4].15-16 // [9.1.5].3		[9.1].2-3 // [9.1].8 // [9.1].11 // [9.1].13 // [9.1].15-18 // [9.1].23 //[9.1.2].5 // [9.1.3].7 // [9.1.4].15-16 // [9.1.5].3	[9.1].12-13 // [9.1].19 // [9.1].23
	Insecure Interfaces (APIs)					[9.1].25
Outages	Lack of resources		[9.2.1].1	[9.2.1].1 // [9.2.1].4-11 // [9.2.1].14-19		[9.2.1].1-2 // [9.2.1].4-6 // [9.2.1].8
	Loss of electricity		[9.1.3].9	[9.2.1].16 // [9.2.2].26	[9.1.3].9	

			SOURCES			
Threat Group	Threat	Threat details	NIST[20]	Enhancing Security Throughout the Supply Chain (IBM Center)[36]	Smart grid Information Assurance and Security Technology Assessment (Sacramento State)[19]	Other[21,37,38,39,40,41,42]
	Absence of personnel			[9.2.2].1-2 // [9.2.2].25 // [9.2.2].50		
	Strike			[9.2.2].1-2 // [9.2.2].25 // [9.2.2].50		
	Loss of support services		[9.2.1].1	[9.2.1].1 // [9.2.1].4-11 // [9.2.1].14-19		[9.2.1].1-2 // [9.2.1].4-6 // [9.2.1].8
	Internet outage				[9.1].40	[9.1].42
	Network outage				[9.1].40	[9.1].42
	Lack in the supply line		[9.2.1].1	[9.2.1].1 // [9.2.1].4-11 // [9.2.1].14-19		[9.2.1].1-2 // [9.2.1].4-6 // [9.2.1].8
Eavesdropping/ Interception / Hijacking	War driving		[9.1].5 // [9.1].34-35 // [9.1].39 // [9.1.1].1-2 // [9.1.5].8		[9.1].5 // [9.1].34-35 // [9.1.1].1-3 // [9.1.5].8	[9.1].35 // [9.1].39 //
	Intercepting, compromising emissions		[9.1].5 // [9.1].8 // [9.1].10-11 // [9.1].14 // [9.1].22 // [9.1].26 // [9.1].28-29 // [9.1].31 // [9.1].33-37 // [9.1].39 // [9.1].42-44 // [9.1.1].1-2 // [9.1.2].1-2 // [9.1.3].4 // [9.1.3].10 // [9.1.4].1 // [9.1.4].3-4 // [9.1.4].7-8 // [9.1.4].10-11 // [9.1.4].14 // [9.1.4].17-20 // [9.1.5].1 // [9.1.5].5-6 // [9.1.5].8		[9.1].5-8 // [9.1].10-11 // [9.1].22-24 // [9.1].26 // [9.1].28-38 // [9.1].40-44 // [9.1.1].1-3 // [9.1.2].1-2 // [9.1.3].2 // [9.1.3].4-6 // [9.1.3].8 // [9.1.3].10 // [9.1.4].1-5 // [9.1.4].7-8 // [9.1.4].10-11 // [9.1.4].14 // [9.1.4].17-20 // [9.1.5].1-2 // [9.1.5].5-8	[9.1].14 // [9.1].22 // [9.1].23-26 // [9.1].28 // [9.1].35 // [9.1].39
	Interception of information	Hijacking of the meter connection	[9.1.4].1 // [9.1.4].3-4 // [9.1.4].7-9 // [9.1.4].11 // [9.1.4].13-14 //		[9.1.4].1-5 // [9.1.4].7-9 // [9.1.4].11-20 // [9.1.4].22	

			SOURCES			
Threat Group	Threat	Threat details	NIST[20]	Enhancing Security Throughout the Supply Chain (IBM Center)[36]	Smart grid Information Assurance and Security Technology Assessment (Sacramento State)[19]	Other[21,37,38,39,40,41,42]
			[9.1.4].17-20 // [9.1.4].22			
		Side-channel attack	[9.1.3].9 // [9.1.4].1 // [9.1.4].8 // [9.1.4].13		[9.1.3].9 // [9.1.4].1-2 // [9.1.4].8 // [9.1.4].13	
		Scanning / Sniffer / External traffic analyser	[9.1].1-2 // [9.1].4 // [9.1].11-14 // [9.1].19 // [9.1].34-37 // [9.1].39 // [9.1.1].1-3 // [9.1.4].7 // [9.1.4].11		[9.1].1-4 // [9.1].11 // [9.1].13 // [9.1].23-24 // [9.1].34-38 // [9.1.1].1-3 // [9.1.4].7 // [9.1.4].11	[9.1].12 // [9.1].14 // [9.1].19 // [9.1].23-24 // [9.1].35 // [9.1].39 //
	Interfering radiation	EM /RF Interception. Tempest attack	[9.1.3].9 // [9.1.4].1 // [9.1.4].8 // [9.1.4].13		[9.1.3].9 // [9.1.4].1-2 // [9.1.4].8 // [9.1.4].13	
	Replay of messages	Acknowledges forgery	[9.1.1].1 // [9.1.4].9		[9.1].38 // [9.1.1].1 // [9.1.4].9	
	Network Reconnaissance and Information gathering		[9.1].1-2 // [9.1].4 // [9.1].11-14 // [9.1].19 // [9.1].34-37 // [9.1].39 // [9.1.1].1-3 // [9.1.4].7 // [9.1.4].11		[9.1].1-4 // [9.1].11 // [9.1].13 // [9.1].23-24 // [9.1].34-38 // [9.1.1].1-3 // [9.1.4].7 // [9.1.4].11	[9.1].12 // [9.1].14 // [9.1].19 // [9.1].23-24 // [9.1].35 // [9.1].39 //
	Man in the middle/ Session hijacking		[9.1].5 // [9.1].8 // [9.1].10-11 // [9.1].14 // [9.1].22 // [9.1].26 // [9.1].28-29 // [9.1].31 // [9.1].33-37 // [9.1].39 // [9.1].42-44 // [9.1.1].1-2 // [9.1.2].1-2 // [9.1.3].4 // [9.1.3].10 // [9.1.4].1 // [9.1.4].3-4 // [9.1.4].7-8 // [9.1.4].10-11 // [9.1.4].14 // [9.1.4].17-		[9.1].5-8 // [9.1].10-11 // [9.1].22-24 // [9.1].26 // [9.1].28-38 // [9.1].40-44 // [9.1.1].1-3 // [9.1.2].1-2 // [9.1.3].2 // [9.1.3].4-6 // [9.1.3].8 // [9.1.3].10 // [9.1.4].1-5 // [9.1.4].7-8 // [9.1.4].10-11 // [9.1.4].14 // [9.1.4].17-20 // [9.1.5].1-2 // [9.1.5].5-8	[9.1].14 // [9.1].22 // [9.1].23-26 // [9.1].28 // [9.1].35 // [9.1].39

			SOURCES			
Threat Group	Threat	Threat details	NIST[20]	Enhancing Security Throughout the Supply Chain (IBM Center)[36]	Smart grid Information Assurance and Security Technology Assessment (Sacramento State)[19]	Other[21,37,38,39,40,41,42]
			20 // [9.1.5].1 // [9.1.5].5-6 // [9.1.5].8			
	Repudiation of actions		[9.1].5 // [9.1].11-12 // [9.1].26-27 // [9.1].34 // [9.1].39-40 // [9.1.1].1-2 // [9.1.2].1-4 // [9.1.3].4 // [9.1.3].10 // [9.1.4].4 // [9.1.4].6-8 // [9.1.4].11 // [9.1.4].14 // [9.1.4].17-18 // [9.1.4].22 // [9.1.5].8		[9.1].5-7 // [9.1].11 // [9.1].26-27 // [9.1].34 // [9.1].40 // [9.1.1].1-3 // [9.1.2].1-4 // [9.1.3].4 // [9.1.3].6 // [9.1.3].8 // [9.1.3].10 // [9.1.4].4 // [9.1.4].6-8 // [9.1.4].11-12 // [9.1.4].14-15 // [9.1.4].17-18 // [9.1.4].22 // [9.1.5].8	[9.1].12 // [9.1].26 //[9.1].39
Nefarious Activity/ Abuse	Identity theft		[9.1].5 // [9.1].8 // [9.1].10-11 // [9.1].14 // [9.1].22 // [9.1].26 // [9.1].28-29 // [9.1].31 // [9.1].33-37 // [9.1].39 // [9.1].42-44 // [9.1.1].1-2 // [9.1.2].1-2 // [9.1.3].4 // [9.1.3].10 // [9.1.4].1 // [9.1.4].3-4 // [9.1.4].7-8 // [9.1.4].10-11 // [9.1.4].14 // [9.1.4].17-20 // [9.1.5].1 // [9.1.5].5-6 // [9.1.5].8		[9.1].5-8 // [9.1].10-11 // [9.1].22-24 // [9.1].26 // [9.1].28-38 // [9.1].40-44 // [9.1.1].1-3 // [9.1.2].1-2 // [9.1.3].2 // [9.1.3].4-6 // [9.1.3].8 // [9.1.3].10 // [9.1.4].1-5 // [9.1.4].7-8 // [9.1.4].10-11 // [9.1.4].14 // [9.1.4].17-20 // [9.1.5].1-2 // [9.1.5].5-8	[9.1].14 // [9.1].22 // [9.1].23-26 // [9.1].28 // [9.1].35 // [9.1].39
	Unsolicited E-mail Anonymous or Unsolicited e-mail to smart grid staff		[9.1].22 // [9.1].26 // [9.1.1].1-2 // [9.1.2].4 // [9.1.3].3 // [9.1.4].4 // [9.1.5].5		[9.1].22 // [9.1].26 // [9.1.1].1-3 // [9.1.2].4 // [9.1.3].3 // [9.1.3].6 // [9.1.4].4 // [9.1.5].5	[9.1].26

			SOURCES			
Threat Group	Threat	Threat details	NIST[20]	Enhancing Security Throughout the Supply Chain (IBM Center)[36]	Smart grid Information Assurance and Security Technology Assessment (Sacramento State)[19]	Other[21,37,38,39,40,41,42]
	Denial of service		[9.1].45 // [9.1.4].9		[9.1].45 // [9.1.4].9	
	Malicious code/ software/ activity	Exploits / Worms / Trojans / Backdoor / Trapdoor / Targeted attacks (APTs etc.)	[9.1].1-2 // [9.1].4 // [9.1].11-18 // [9.1].22 // [9.1].26 // [9.1].33-37 // [9.1].39 // [9.1.1].1-2 // [9.1.2].1-4 // [9.1.4].1 // [9.1.4].3-4 // [9.1.4].6 // [9.1.4].20 // [9.1.4].22-23 // [9.1.5].1 // [9.1.5].3 // [9.1.5]5-6 // [2.2.1.].1	[9.2.1].1 // [9.2.1].6 // [9.2.3].1	[9.1].1-4 // [9.1].11 // [9.1].13 // [9.1].15-18 // [9.1].22 // [9.1].24 // [9.1].26 // [9.1].33-38 // [9.1.1].1-3 // [9.1.2].1-5 // [9.1.4].1-6 // [9.1.4].20-23 // [9.1.5].1-3 // [9.1.5]5-7	[9.1].12 // [9.1].14 // [9.1].18-20 // [9.1].22-26 // [9.1].35 // [9.1].39 // [9.2.1].1 // [9.2.1].6 //
		Service spoofing (ARP spoofing)	[9.1].1-2 // [9.1].4 // [9.1].11-18 // [9.1].22 // [9.1].26 // [9.1].33-37 // [9.1].39 // [9.1.1].1-2 // [9.1.2].1-4 // [9.1.4].1 // [9.1.4].3-4 // [9.1.4].6 // [9.1.4].20 // [9.1.4].22-23 // [9.1.5].1 // [9.1.5].3 // [9.1.5]5-6 // [2.2.1.].1	[9.2.1].1 // [9.2.1].6 // [9.2.3].1	[9.1].1-4 // [9.1].11 // [9.1].13 // [9.1].15-18 // [9.1].22 // [9.1].24 // [9.1].26 // [9.1].33-38 // [9.1.1].1-3 // [9.1.2].1-5 // [9.1.4].1-6 // [9.1.4].20-23 // [9.1.5].1-3 // [9.1.5]5-7	[9.1].12 // [9.1].14 // [9.1].18-20 // [9.1].22-26 // [9.1].35 // [9.1].39 // [9.2.1].1 // [9.2.1].6 //
		ICMP flooding	[9.1].1-2 // [9.1].4 // [9.1].11-18 // [9.1].22 // [9.1].26 // [9.1].33-37 // [9.1].39 // [9.1.1].1-2 // [9.1.2].1-4 // [9.1.4].1 // [9.1.4].3-4 // [9.1.4].6 // [9.1.4].20 // [9.1.4].22-23 // [9.1.5].1 // [9.1.5].3 // [9.1.5]5-6 // [2.2.1.].1	[9.2.1].1 // [9.2.1].6 // [9.2.3].1	[9.1].1-4 // [9.1].11 // [9.1].13 // [9.1].15-18 // [9.1].22 // [9.1].24 // [9.1].26 // [9.1].33-38 // [9.1.1].1-3 // [9.1.2].1-5 // [9.1.4].1-6 // [9.1.4].20-23 // [9.1.5].1-3 // [9.1.5]5-7	[9.1].12 // [9.1].14 // [9.1].18-20 // [9.1].22-26 // [9.1].35 // [9.1].39 // [9.2.1].1 // [9.2.1].6 //
	Social Engineering			[9.2.2].32 // [9.2.2].34		

			SOURCES			
Threat Group	Threat	Threat details	NIST[20]	Enhancing Security Throughout the Supply Chain (IBM Center)[36]	Smart grid Information Assurance and Security Technology Assessment (Sacramento State)[19]	Other[21,37,38,39,40,41,42]
	Abuse of Information Leakage		[9.1].1-2 // [9.1].4 // [9.1].8 // [9.1].10-15 // [9.1].19 // [9.1].22 // [9.1].26-29 // [9.1].31 // [9.1].33-35 // [9.1.4].13 // [9.2.1].1	[9.2.1].1 // [9.2.1].7-19 // [9.2.2] // [9.2.3].1 // [9.2.3].5-8	[9.1].1-4 // [9.1].6-11 // [9.1].13 // [9.1].15 // [2.1.].22-24 // [9.1].26-35 // [9.1.4].13 // [9.1.5].4 //	[9.1].12 // [9.1].14 // [9.1].19 // [9.1].20-22 // [9.1].23 // [9.1].24 // [9.1].26 // [9.1].28 // [9.1].35 // [9.2.1].1 // [9.2.2].45-47 // [9.2.2].49
	Generation and use of rogue certificates		[9.1].39			[9.1].39
	Manipulation of information: authenticity	False data injection in smart grid traffic	[9.1].5 // [9.1].8 // [9.1].10-11 // [9.1].14 // [9.1].22 // [9.1].26 // [9.1].28-37 // [9.1].39 // [9.1].42-44 // [9.1.1].1-2 // [9.1.2].1-2 // [9.1.3].4 // [9.1.3].10 // [9.1.4].1 // [9.1.4].3-4 // [9.1.4].7-8 // [9.1.4].10-11 // [9.1.4].14 // [9.1.4].17-20 // [9.1.5].1 // [9.1.5].5-6 // [9.1.5].8		[9.1].5-8 // [9.1].10-11 // [9.1].22-24 // [9.1].26 // [9.1].28-38 // [9.1].40-44 // [9.1.1].1-3 // [9.1.2].1-2 // [9.1.3].2 // [9.1.3].4-6 // [9.1.3].8 // [9.1.3].10 // [9.1.4].1-5 // [9.1.4].7-8 // [9.1.4].10-11 // [9.1.4].14 // [9.1.4].17-20 // [9.1.5].1-2 // [9.1.5].5-8	[9.1].14 // [9.1].22 // [9.1].23-26 // [9.1].28 // [9.1].35 // [9.1].39
	Manipulation of information: intercept / alter / repudiation	Buffer overflow	[9.1].16		[9.1].16 // [9.1.2].5 // [9.1.4].16	
		Load redistribution attack	[9.1].16		[9.1].16 // [9.1.2].5 // [9.1.4].16	
		Deliver wrong data to operator station	[9.1].16		[9.1].16 // [9.1.2].5 // [9.1.4].16	
		Manipulation data	[9.1].16		[9.1].16 // [9.1.2].5 //	

			SOURCES			
Threat Group	Threat	Threat details	NIST[20]	Enhancing Security Throughout the Supply Chain (IBM Center)[36]	Smart grid Information Assurance and Security Technology Assessment (Sacramento State)[19]	Other[21,37,38,39,40,41,42]
		sent or received to/from TSO or central system			[9.1.4].16	
		Alter meter data, gateway configuration data, meter configuration data, CLS configuration data, etc.	[9.1].5 // [9.1].8 // [9.1].10-11 // [9.1].22 // [9.1].26 // [9.1].33-36 // [9.1].39 // [9.1].43-44 // [9.1.1].1-2 // [9.1.2].1 // [9.1.3].10 // [9.1.4].1 // [9.1.4].7-8 // [9.1.4].10-11 // [9.1.4].14 // [9.1.4].19 // [9.1.5].1 // [9.1.5].8		[9.1].5-8 // [9.1].10-11 // [9.1].24 // [9.1].26 // [9.1].33-36 // [9.1].38 // [9.1].40-41 // [9.1].43-44 // [9.1.1].1-3 // [9.1.2].1 // [9.1.3].2 // [9.1.3].5 // [9.1.3].10 // [9.1.4].1-2 // [9.1.4].7-8 // [9.1.4].10-11 // [9.1.4].14 // [9.1.4].19 // [9.1.5].1-2 // [9.1.5].8	[9.1].22 // [9.1].24-26 // [9.1].35 // [9.1].39
	Misuse of audit tools					[9.1].20
	Falsification of records		[9.1].5 // [9.1].8 // [9.1].10-11 // [9.1].14 // [9.1].22 // [9.1].26 // [9.1].28-29 // [9.1].31 // [9.1].33-39 // [9.1].20-44 // [9.1.1].1-2 // [9.1.2].1-2 // [9.1.3].4 // [9.1.3].10 // [9.1.4].1 // [9.1.4].3-4 // [9.1.4].7-8 // [9.1.4].10-11 // [9.1.4].14 // [9.1.4].17-20 // [9.1.5].1 // [9.1.5].5-6 // [9.1.5].8		[9.1].5-8 // [9.1].10-11 // [9.1].22-24 // [9.1].26 // [9.1].28-38 // [9.1].40-44 // [9.1.1].1-3 // [9.1.2].1-2 // [9.1.3].2 // [9.1.3].4-6 // [9.1.3].8 // [9.1.3].10 // [9.1.4].1-5 // [9.1.4].7-8 // [9.1.4].10-11 // [9.1.4].14 // [9.1.4].17-20 // [9.1.5].1-2 // [9.1.5].5-8	[9.1].14 // [9.1].22 // [9.1].23-26 // [9.1].28 // [9.1].35 // [9.1].39
	Misuse of information/		[9.1].2 // [9.1].8 // [9.1].11-13 // [9.1].15-19		[9.1].2-3 // [9.1].8 // [9.1].11 // [9.1].13 //	[9.1].12-13 // [9.1].19 // [9.1].23

			SOURCES			
Threat Group	Threat	Threat details	NIST[20]	Enhancing Security Throughout the Supply Chain (IBM Center)[36]	Smart grid Information Assurance and Security Technology Assessment (Sacramento State)[19]	Other[21,37,38,39,40,41,42]
	information systems		// [9.1.5].3		[9.1].15-18 // [9.1].23 // [9.1.2].5 // [9.1.3].7 // [9.1.4].15-16 // [9.1.5].3	
	Unauthorized use or administration of devices, systems and communications	Unauthorized use of facilities and infrastructure	[9.1].1 // [9.1].4-5 // [9.1].8 // [9.1].10-15 // [9.1].22 // [9.1].26-29 // [9.1].31 // [9.1].33-37 // [9.1].39 // [9.1.1].1-2 // [9.1.2].2 // [9.1.2].4 // [9.1.3].3-4 // [9.1.3].9-10 // [9.1.4].4 // [9.1.4].7-8 // [9.1.4].14 // [9.1.4].17-20 // [9.1.5].5-6 // [9.1.5].8		[9.1].1 // [9.1].4-8 // // [9.1].10-11 // [9.1].13 // [9.1].15 // [9.1].24 // [9.1].26-37 // [9.1].40-41 // [9.1.1].1-3 // [9.1.2].2 // [9.1.2].4 // [9.1.3].3-10 // [9.1.4].4-5 // [9.1.4].7-8 // [9.1.4].12 // [9.1.4].14 // [9.1.4].17-20 // [9.1.5].5-8	[9.1].12-14 // [9.1].21-22 // [9.1].24 // [9.1].26 // [9.1].28 // [9.1].39
		Unauthorized use of files and information	[9.1].1 // [9.1].4-5 // [9.1].8 // [9.1].10-15 // [9.1].22 // [9.1].26-29 // [9.1].31 // [9.1].33-37 // [9.1].39 // [9.1.1].1-2 // [9.1.2].2 // [9.1.2].4 // [9.1.3].3-4 // [9.1.3].9-10 // [9.1.4].4 // [9.1.4].7-8 // [9.1.4].14 // [9.1.4].17-20 // [9.1.5].5-6 // [9.1.5].8		[9.1].1 // [9.1].4-8 // // [9.1].10-11 // [9.1].13 // [9.1].15 // [9.1].24 // [9.1].26-37 // [9.1].40-41 // [9.1.1].1-3 // [9.1.2].2 // [9.1.2].4 // [9.1.3].3-10 // [9.1.4].4-5 // [9.1.4].7-8 // [9.1.4].12 // [9.1.4].14 // [9.1.4].17-20 // [9.1.5].5-8	[9.1].12-14 // [9.1].21-22 // [9.1].24 // [9.1].26 // [9.1].28 // [9.1].39
		Unauthorized use of software	[9.1].1 // [9.1].4-5 // [9.1].8 // [9.1].10-15 // [9.1].22 // [9.1].26-29 // [9.1].31 // [9.1].33-37 //		[9.1].1 // [9.1].4-8 // // [9.1].10-11 // [9.1].13 // [9.1].15 // [9.1].24 // [9.1].26-37 // [9.1].40-41	[9.1].12-14 // [9.1].21-22 // [9.1].24 // [9.1].26 // [9.1].28 // [9.1].39

			SOURCES			
Threat Group	Threat	Threat details	NIST[20]	Enhancing Security Throughout the Supply Chain (IBM Center)[36]	Smart grid Information Assurance and Security Technology Assessment (Sacramento State)[19]	Other[21,37,38,39,40,41,42]
			[9.1].39 // [9.1.1].1-2 // [9.1.2].2 // [9.1.2].4 // [9.1.3].3-4 // [9.1.3].9-10 // [9.1.4].4 // [9.1.4].7-8 // [9.1.4].14 // [9.1.4].17-20 // [9.1.5].5-6 // [9.1.5].8		// [9.1.1].1-3 // [9.1.2].2 // [9.1.2].4 // [9.1.3].3-10 // [9.1.4].4-5 // [9.1.4].7-8 // [9.1.4].12 // [9.1.4].14 // [9.1.4].17-20 // [9.1.5].5-8	
	Unauthorized access to the information /information system / network	Unauthorized access from customer endpoint	[9.1.2].1-4 // [9.2.3].3-4	[9.2.3].3	[9.1.1] // [9.1.2].1-4 // [9.1.5]	[9.2.3].3-4
		Masquerade (gained access and privileges escalation)	[9.1.2].1-4		[9.1.1] // [9.1.2].1-4 // [9.1.5]	
		Password attacks	[9.1].33		[9.1].33	
		Unauthorized access to the information, system or data	[9.1].1 // [9.1].4-5 // [9.1].8 // [9.1].10-15 // [9.1].22 // [9.1].26-29 // [9.1].31 // [9.1].33-37 // [9.1].39 // [9.1.1].1-2 // [9.1.2].2 // [9.1.2].4 // [9.1.3].3-4 // [9.1.3].9-10 // [9.1.4].4 // [9.1.4].7-8 // [9.1.4].14 // [9.1.4].17-20 // [9.1.5].5-6 // [9.1.5].8		[9.1].1 // [9.1].4-8 // // [9.1].10-11 // [9.1].13 // [9.1].15 // [9.1].24 // [9.1].26-37 // [9.1].40-41 // [9.1.1].1-3 // [9.1.2].2 // [9.1.2].4 // [9.1.3].3-10 // [9.1.4].4-5 // [9.1.4].7-8 // [9.1.4].12 // [9.1.4].14 // [9.1.4].17-20 // [9.1.5].5-8	[9.1].12-14 // [9.1].21-22 // [9.1].24 // [9.1].26 // [9.1].28 // [9.1].39
		Unauthorized remote access to SCADA systems	[9.1].1 // [9.1].4-5 // [9.1].8 // [9.1].10-15 // [9.1].22 // [9.1].26-29 // [9.1].31 // [9.1].33-37 //		[9.1].1 // [9.1].4-8 // // [9.1].10-11 // [9.1].13 // [9.1].15 // [9.1].24 // [9.1].26-37 // [9.1].40-41	[9.1].12-14 // [9.1].21-22 // [9.1].24 // [9.1].26 // [9.1].28 // [9.1].39

			SOURCES			
Threat Group	Threat	Threat details	NIST[20]	Enhancing Security Throughout the Supply Chain (IBM Center)[36]	Smart grid Information Assurance and Security Technology Assessment (Sacramento State)[19]	Other[21,37,38,39,40,41,42]
			[9.1].39 // [9.1.1].1-2 // [9.1.2].2 // [9.1.2].4 // [9.1.3].3-4 // [9.1.3].9-10 // [9.1.4].4 // [9.1.4].7-8 // [9.1.4].14 // [9.1.4].17-20 // [9.1.5].5-6 // [9.1.5].8		// [9.1.1].1-3 // [9.1.2].2 // [9.1.2].4 // [9.1.3].3-10 // [9.1.4].4-5 // [9.1.4].7-8 // [9.1.4].12 // [9.1.4].14 // [9.1.4].17-20 // [9.1.5].5-8	
		Unauthorized information manipulation or deletion	[9.1].1 // [9.1].4-5 // [9.1].8 // [9.1].10-15 // [9.1].22 // [9.1].26-29 // [9.1].31 // [9.1].33-37 // [9.1].39 // [9.1.1].1-2 // [9.1.2].2 // [9.1.2].4 // [9.1.3].3-4 // [9.1.3].9-10 // [9.1.4].4 // [9.1.4].7-8 // [9.1.4].14 // [9.1.4].17-20 // [9.1.5].5-6 // [9.1.5].8		[9.1].1 // [9.1].4-8 // // [9.1].10-11 // [9.1].13 // [9.1].15 // [9.1].24 // [9.1].26-37 // [9.1].40-41 // [9.1.1].1-3 // [9.1.2].2 // [9.1.2].4 // [9.1.3].3-10 // [9.1.4].4-5 // [9.1.4].7-8 // [9.1.4].12 // [9.1.4].14 // [9.1.4].17-20 // [9.1.5].5-8	[9.1].12-14 // [9.1].21-22 // [9.1].24 // [9.1].26 // [9.1].28 // [9.1].39
		Compromise DCS server and disable communication with controllers, manipulate configuration parameters of controllers, or stop communication with operator station	[9.1].1 // [9.1].4-5 // [9.1].8 // [9.1].10-15 // [9.1].22 // [9.1].26-29 // [9.1].31 // [9.1].33-37 // [9.1].39 // [9.1].42 // [9.1].45 //[9.1.1].1-2 // [9.1.2].2 // [9.1.2].4 // [9.1.3].3-4 // [9.1.3].9-10 // [9.1.4].4 // [9.1.4].7-9 // [9.1.4].14 // [9.1.4].17-20 // [9.1.5].5-		[9.1].1 // [9.1].4-8 // // [9.1].10-11 // [9.1].13 // [9.1].15 // [9.1].24 // [9.1].26-37 // [9.1].40-41 // [9.1].45 // [9.1.1].1-3 // [9.1.2].2 // [9.1.2].4 // [9.1.3].3-10 // [9.1.4].4-5 // [9.1.4].7-9 // [9.1.4].12 // [9.1.4].14 // [9.1.4].17-20 // [9.1.5].5-8	[9.1].12-14 // [9.1].21-22 // [9.1].24 // [9.1].26 // [9.1].28 // [9.1].39 //[9.1].42

			SOURCES			
Threat Group	Threat	Threat details	NIST[20]	Enhancing Security Throughout the Supply Chain (IBM Center)[36]	Smart grid Information Assurance and Security Technology Assessment (Sacramento State)[19]	Other[21,37,38,39,40,41,42]
			6 // [9.1.5].8			
		Compromise RTU	[9.1].1 // [9.1].4-5 // [9.1].8 // [9.1].10-15 // [9.1].22 // [9.1].26-29 // [9.1].31 // [9.1].33-37 // [9.1].39 // [9.1.1].1-2 // [9.1.2].2 // [9.1.2].4 // [9.1.3].3-4 // [9.1.3].9-10 // [9.1.4].4 // [9.1.4].7-8 // [9.1.4].14 // [9.1.4].17-20 // [9.1.5].5-6 // [9.1.5].8		[9.1].1 // [9.1].4-8 // // [9.1].10-11 // [9.1].13 // [9.1].15 // [9.1].24 // [9.1].26-37 // [9.1].40-41 // [9.1.1].1-3 // [9.1.2].2 // [9.1.2].4 // [9.1.3].3-10 // [9.1.4].4-5 // [9.1.4].7-8 // [9.1.4].12 // [9.1.4].14 // [9.1.4].17-20 // [9.1.5].5-8	[9.1].12-14 // [9.1].21-22 // [9.1].24 // [9.1].26 // [9.1].28 // [9.1].39
	Violation of the privacy of the consumer		[9.1].5 // [9.1].8 // [9.1].10-11 // [9.1].22 // [9.1].26 // [9.1].33-36 // [9.1].39 // [9.1].43-44 // [9.1.1].1-2 // [9.1.2].1 // [9.1.3].10 // [9.1.4].1 // [9.1.4].7-8 // [9.1.4].10-11 // [9.1.4].14 // [9.1.4].19 // [9.1.5].1 // [9.1.5].8		[9.1].5-8 // [9.1].10-11 // [9.1].24 // [9.1].26 // [9.1].33-36 // [9.1].38 // [9.1].40-41 // [9.1].43-44 // [9.1.1].1-3 // [9.1.2].1 // [9.1.3].2 // [9.1.3].5 // [9.1.3].10 // [9.1.4].1-2 // [9.1.4].7-8 // [9.1.4].10-11 // [9.1.4].14 // [9.1.4].19 // [9.1.5].1-2 // [9.1.5].8	[9.1].22 // [9.1].24-26 // [9.1].35 // [9.1].39
	Unauthorized changes of records		[9.1].1 // [9.1].4-5 // [9.1].8 // [9.1].10-15 // [9.1].22 // [9.1].26-29 // [9.1].31 // [9.1].33-37 // [9.1].39 // [9.1.1].1-2 // [9.1.2].2 // [9.1.2].4 // [9.1.3].3-4 // [9.1.3].9-10		[9.1].1 // [9.1].4-8 // // [9.1].10-11 // [9.1].13 // [9.1].15 // [9.1].24 // [9.1].26-37 // [9.1].40-41 // [9.1.1].1-3 // [9.1.2].2 // [9.1.2].4 // [9.1.3].3-10 // [9.1.4].4-5 // [9.1.4].7-8 //	[9.1].12-14 // [9.1].21-22 // [9.1].24 // [9.1].26 // [9.1].28 // [9.1].39

			SOURCES			
Threat Group	Threat	Threat details	NIST[20]	Enhancing Security Throughout the Supply Chain (IBM Center)[36]	Smart grid Information Assurance and Security Technology Assessment (Sacramento State)[19]	Other[21,37,38,39,40,41,42]
			// [9.1.4].4 // [9.1.4].7-8 // [9.1.4].14 // [9.1.4].17-20 // [9.1.5].5-6 // [9.1.5].8		[9.1.4].12 // [9.1.4].14 // [9.1.4].17-20 // [9.1.5].5-8	
	Unauthorized installation of software		[9.1].1 // [9.1].4-5 // [9.1].8 // [9.1].10-15 // [9.1].22 // [9.1].26-29 // [9.1].31 // [9.1].33-37 // [9.1].39 // [9.1.1].1-2 // [9.1.2].2 // [9.1.2].4 // [9.1.3].3-4 // [9.1.3].9-10 // [9.1.4].4 // [9.1.4].7-8 // [9.1.4].14 // [9.1.4].17-20 // [9.1.5].5-6 // [9.1.5].8		[9.1].1 // [9.1].4-8 // // [9.1].10-11 // [9.1].13 // [9.1].15 // [9.1].24 // [9.1].26-37 // [9.1].40-41 // [9.1.1].1-3 // [9.1.2].2 // [9.1.2].4 // [9.1.3].3-10 // [9.1.4].4-5 // [9.1.4].7-8 // [9.1.4].12 // [9.1.4].14 // [9.1.4].17-20 // [9.1.5].5-8	[9.1].12-14 // [9.1].21-22 // [9.1].24 // [9.1].26 // [9.1].28 // [9.1].39
	Compromising confidential information (data breaches)		[9.1].5 // [9.1].8 // [9.1].10-11 // [9.1].22 // [9.1].26 // [9.1].33-36 // [9.1].39 // [9.1].43-44 // [9.1.1].1-2 // [9.1.2].1 // [9.1.3].10 // [9.1.4].1 // [9.1.4].7-8 // [9.1.4].10-11 // [9.1.4].14 // [9.1.4].19 // [9.1.5].1 // [9.1.5].8		[9.1].5-8 // [9.1].10-11 // [9.1].24 // [9.1].26 // [9.1].33-36 // [9.1].38 // [9.1].40-41 // [9.1].43-44 // [9.1.1].1-3 // [9.1.2].1 // [9.1.3].2 // [9.1.3].5 // [9.1.3].10 // [9.1.4].1-2 // [9.1.4].7-8 // [9.1.4].10-11 // [9.1.4].14 // [9.1.4].19 // [9.1.5].1-2 // [9.1.5].8	[9.1].22 // [9.1].24-26 // [9.1].35 // [9.1].39
	Abuse of authorizations		[9.1].1 // [9.1].4-5 // [9.1].8 // [9.1].10-15 // [9.1].22 // [9.1].26-29 // [9.1].31 // [9.1].33-37 //		[9.1].1 // [9.1].4-8 // // [9.1].10-11 // [9.1].13 // [9.1].15 // [9.1].24 // [9.1].26-37 // [9.1].40-41	[9.1].12-14 // [9.1].21-22 // [9.1].24 // [9.1].26 // [9.1].28 // [9.1].39

			SOURCES			
Threat Group	Threat	Threat details	NIST[20]	Enhancing Security Throughout the Supply Chain (IBM Center)[36]	Smart grid Information Assurance and Security Technology Assessment (Sacramento State)[19]	Other[21,37,38,39,40,41,42]
			[9.1].39 // [9.1.1].1-2 // [9.1.2].2 // [9.1.2].4 // [9.1.3].3-4 // [9.1.3].9-10 // [9.1.4].4 // [9.1.4].7-8 // [9.1.4].14 // [9.1.4].17-20 // [9.1.5].5-6 // [9.1.5].8		// [9.1.1].1-3 // [9.1.2].2 // [9.1.2].4 // [9.1.3].3-10 // [9.1.4].4-5 // [9.1.4].7-8 // [9.1.4].12 // [9.1.4].14 // [9.1.4].17-20 // [9.1.5].5-8	
	Remote activity (execution)		[9.1].11 // [9.1].13-14 // [9.1] 26-29 // [9.1].31 // [9.1].33 // [9.1].39 // [9.1.2].3 // [9.1.3].3-4 // [9.1.3].9-10 // [9.1.4]1 // [9.1.4].3-4 // [9.1.4].8 // [9.1.5].1 // [9.1.5].3 // [9.1.5]5-6 // [9.1.5].8		[9.1].11 // [9.1].13 // [9.1] 26-33 // [9.1.2].3 // [9.1.3].3-10 // [9.1.4]1-5 // [9.1.4].8 // [9.1.5].1-8	[9.1].13-14 // [9.1].26 // [9.1].28 // [9.1].39 //
	Communication jamming		[9.1.3].9 // [9.1.4].1 // [9.1.4].8 // [9.1.4].13		[9.1.3].9 // [9.1.4].1-2 // [9.1.4].8 // [9.1.4].13	
	Bypass of devices (bypass security controls)		[9.1].1 // [9.1].4-5 // [9.1].8 // [9.1].10-15 // [9.1].22 // [9.1].26-29 // [9.1].31 // [9.1].33-37 // [9.1].39 // [9.1.1].1-2 // [9.1.2].2 // [9.1.2].4 // [9.1.3].3-4 // [9.1.3].9-10 // [9.1.4].4 // [9.1.4].7-8 // [9.1.4].14 // [9.1.4].17-20 // [9.1.5].5-6 // [9.1.5].8 // [9.2.3].3-4	[9.2.3].3	[9.1].1 // [9.1].4-8 // // [9.1].10-11 // [9.1].13 // [9.1].15 // [9.1].24 // [9.1].26-37 // [9.1].40-41 // [9.1.1].1-3 // [9.1.2].2 // [9.1.2].4 // [9.1.3].3-10 // [9.1.4].4-5 // [9.1.4].7-8 // [9.1.4].12 // [9.1.4].14 // [9.1.4].17-20 // [9.1.5].5-8	[9.1].12-14 // [9.1].21-22 // [9.1].24 // [9.1].26 // [9.1].28 // [9.1].39 // [9.2.3].3-4

			SOURCES			
Threat Group	Threat	Threat details	NIST[20]	Enhancing Security Throughout the Supply Chain (IBM Center)[36]	Smart grid Information Assurance and Security Technology Assessment (Sacramento State)[19]	Other[21,37,38,39,40,41,42]
	Insider attack					
	Hardware, Software and Device manipulation	PCT manipulation	[9.1].1 // [9.1].4-5 // [9.1].8 // [9.1].10-15 // [9.1].22 // [9.1].26-29 // [9.1].31 // [9.1].33-37 // [9.1].39 // [9.1.1].1-2 // [9.1.2].2 // [9.1.2].4 // [9.1.3].3-4 // [9.1.3].9-10 // [9.1.4].4 // [9.1.4].7-8 // [9.1.4].14 // [9.1.4].17-20 // [9.1.5].5-6 // [9.1.5].8		[9.1].1 // [9.1].4-8 // // [9.1].10-11 // [9.1].13 // [9.1].15 // [9.1].24 // [9.1].26-37 // [9.1].40-41 // [9.1.1].1-3 // [9.1.2].2 // [9.1.2].4 // [9.1.3].3-10 // [9.1.4].4-5 // [9.1.4].7-8 // [9.1.4].12 // [9.1.4].14 // [9.1.4].17-20 // [9.1.5].5-8	[9.1].12-14 // [9.1].21-22 // [9.1].24 // [9.1].26 // [9.1].28 // [9.1].39
		Firmware manipulation	[9.1.4].14		[9.1.4].14	
		Compromise Central Systems to switch off homes with E-meters, deletes all keys for the E-meters and distribute malicious firmware.	[9.1.4].1 // [9.1.4].3-4 // [9.1.4].6 // [9.1.4].8-11 // [9.1.4].13-14 // [9.1.4].17-20 // [9.1.4].22-23		[9.1.3] // [9.1.4].1-6 // [9.1.4].8-23 // [9.1.5]	
	Time manipulation		[9.1.4].8 //[9.1.4].11 //[9.1.4].13-14		[9.1.4].8 //[9.1.4].11 //[9.1.4].13-14	
Legal	Violation of laws or regulations / Breach of legislation		[9.1.4].1 // [9.2.1].1	[9.2.1].1-3 // [9.2.2].1-2	[9.1.4].1-2	[9.2.1].1-3
	Failure to meet contractual requirements		[9.1.4].1 // [9.2.1].1	[9.2.1].1-3 // [9.2.1].4 // [9.2.1].17-18 // [9.2.2].1-3 // [9.2.2].21 //	[9.1.4].1-2	[9.2.1].1-3 // [9.2.1].4

			SOURCES			
Threat Group	Threat	Threat details	NIST[20]	Enhancing Security Throughout the Supply Chain (IBM Center)[36]	Smart grid Information Assurance and Security Technology Assessment (Sacramento State)[19]	Other[21,37,38,39,40,41,42]
				[9.2.2].33 // [9.2.2].35-37 // [9.2.2].39 // [9.2.2].52 // [9.2.3].2		
	Unauthorized use of copyrighted material		[9.1.4].1 // [9.2.1].1	[9.2.1].1-3 // [9.2.2].1-2	[9.1.4].1-2	[9.2.1].1-3

Annex D: Collected Information: Inventory of Smart Grid Documents

	Name of the Information Item/Document	Information Item (URL or file)	Relevance (High/Medium/Low)	DATE of Item	Comments
1	M/490 Document base	http://www.cencenelec.eu/STANDARDS/HOTTOPICS/SMARTGRIDS/Pages/default.aspx	High		
2	Documentation on Smart Grids of DG-CONNECT	http://ec.europa.eu/information_society/newsroom/cf/dae/itemdetail.cfm?item_id=9817	High relevance. It includes a threat assessment.		
3	Documents on Smart Grid of DG ENERGY	http://ec.europa.eu/energy/gas_electricity/smartgrids/taskforce_en.htm	High		
4	Draft of M/441 on Smart Meters regarding Privacy and Security approach	SM-CG AHWG PS report v0 9.pdf	High		
5	ENISA Documents from last year's survey	Items are available at ENISA. Can be delivered on demand	Medium	Mid 2012	
6	BSI Protection Profile for Smart Meters	https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/SmartMeter/PP-SmartMeter.pdf?__blob=publicationFile	High	March 2013	
7	Crisalis risk assessment	crisalis_deliverable-D 2.2.pdf	High	May 2013	Risk Assessment
8	Functional reference architecture for communications in smart metering systems. (Technical Report CEN/CLC/ETSI/TR 50572)	ftp://ftp.cen.eu/cen/Sectors/List/Measurement/Smartmeters/CENCLCETSI_TR50572.pdf http://www.cenelec.eu/aboutcenelec/whatwedo/technologysectors/smartmetering.html	Medium	December 2011	
9	Steps towards implementing a European cyber-security strategy	http://www.eos-eu.com/files/Documents/WhitePapers/Steps_cyber_security.pdf	Low	November 2011	
10	EURACOM (EUropean Risk Assessment and Contingency planning Methodologies for	http://www.eos-eu.com/?Page=euracom	Medium	2012	Main objectives: - Promote a

	Name of the Information Item/Document	Information Item (URL or file)	Relevance (High/Medium/Low)	DATE of Item	Comments
	interconnected networks) reports and deliverables				dialogue between energy and security stakeholders to attend the security of energy infrastructures. - Support European policies for the protection of critical energy infrastructures.
11	Sicherheit im Smart Grid. Eckpunkte für ein Energieinformationsnetz	http://www.stiftungaktuell.de/files/sr90_sicherheit_im_energieinformationsnetz_gesamt.pdf	Medium	2011	Key elements of a smart grid security.
12	NISTIR 7628. Guidelines for Smart Grid Cyber Security	http://csrc.nist.gov/publications/nistir/ir7628/introduction-to-nistir-7628.pdf	High	September 2010	
13	Supply Chain Solutions for Smart Grid Security: Building on Business Best Practices	http://www.us-nesco.org/files/2013/01/SupplyChain-Solutions-for-Smart-Grid-Security.pdf	High	2012	Emerging risks and supply chain solutions. Business best practices to secure the smart grid supply chain.
14	Smart Grid Cyber Security. Potential Threats, Vulnerabilities and Risks	http://www.energy.ca.gov/2012publications/CEC-500-2012-047/CEC-500-2012-047.pdf	High	May 2012	
15	Cisco Smart Grid Security Solutions	http://www.cisco.com/web/strategy/docs/energy/CiscoSmartGridSecurity_solutions_brief_c22-556936.pdf	Medium	2009	www.cisco.com/go/smartgrid
16	Cisco GridBlocks Reference Model	http://www.cisco.com/web/strategy/docs/energy/gridblocks_ref_model.pdf	Medium	2011	www.cisco.com/go/smartgrid
17	Cisco GridBlocks Overview	http://www.cisco.com/web/strategy/docs/energy/overview_gba.pdf	Medium	2012	www.cisco.com/go/smartgrid
18	Smart Grid Security: Threats, Vulnerabilities and Solutions	http://www.aloul.net/Papers/faloul_ijsgce12.pdf	High	September 2012	Research paper

	Name of the Information Item/Document	Information Item (URL or file)	Relevance (High/Medium/Low)	DATE of Item	Comments
19	Cyber Attack Exposure Evaluation Framework for the Smart Grid	http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6025254	Medium	December 2011	Research paper
20	Cyber Security and Power System Communication—Essential Parts of a Smart Grid Infrastructure	http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5452993	Medium	July 2010	Research paper
21	Security Technology for Smart Grid Networks	http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5460903	Medium	June 2010	Research paper
22	Smart-grid security issues	http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5403159	Medium	Feb 2010	Research paper
23	Towards a Framework for Cyber Attack Impact Analysis of the Electric Smart Grid	http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5622049	Medium	2010	Research paper
24	Decreased time delay and security enhancement recommendations for AMI smart meter networks	http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5434780	Medium	2010	Specific Research paper
25	Smart Grid Privacy via Anonymization of Smart Metering Data	http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5622050	Medium	2010	Specific Research paper
26	Security and Privacy Challenges in the Smart Grid	http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5054916	Medium	June 2009	Specific Research paper
27	Securing where smart grids meets SCADA	http://www.embedded.com/design/safety-and-security/4413576/4/Securing-the-smart-grid-and-SCADA	Medium	May 2013	
28	Energy measurement and security for the smart grid – too long overlooked	http://www.maximintegrated.com/app-notes/index.mvp/id/5536	Medium	Jan 2013	
29	Information of EEUU initiatives in smart grids.	http://www.smartgrid.gov/ and http://www.smartgrid.gov/library	High	Currently updated	

	Name of the Information Item/Document	Information Item (URL or file)	Relevance (High/Medium/Low)	DATE of Item	Comments
30	21 steps to improve cyber security of SCADA networks	21 Steps to improve CS of SCADA networks	High	Not specified	
31	AMI System Security Requirements	http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/14-AMI_System_Security_Requirements_updated.pdf	Medium	17/12/2008	
32	Industrial control systems security	Industrial Control Systems Security	Medium	4Q 2012	
33	Infrastructure protection: U.S. power plants, utilities face growing cyber vulnerability	http://www.homelandsecuritynewswire.com/dr20130819-u-s-power-plants-utilities-face-growing-cyber-vulnerability	Medium	19 august 2013	
34	Guidelines for Assessing Wireless Standards for Smart Grid Applications	http://collaborate.nist.gov/twiki-sggrid/pub/SmartGrid/PAP02Wireless/NISTIR7761.pdf	Medium	February 2011	
35	Protecting SCADA devices from threats and hackers	http://www.embedded.com/design/safety-and-security/4397214/Protecting-SCADA-devices-from-threats-and-hackers-	Medium	September 2012	
36	Recommendations for smart grid standardization	http://www.etsi.org/WebSite/document/0905_RA%20smart%20grids-Bdef.pdf	Medium	May 2011	
37	Utility Cyber Security Seven Key Smart Grid Security Trends to Watch in 2012 and Beyond	http://www.navigantresearch.com/wp-assets/uploads/2011/11/UCS-11-Pike-Research.pdf	Medium	4Q 2011	Research report
38	Smart Grid: 10 Trends to Watch in 2013 and Beyond	http://www.navigantresearch.com/wp-assets/uploads/2013/03/WP-SG10T-13-Navigant-Research.pdf	Medium	1Q 2013	White paper
39	Smart Grid Information Security	http://ec.europa.eu/energy/gas_electricity/smartgrids/doc/xpert_group1_security.pdf	Medium	November 2012	
40	Smart Grid Security:	http://s3.amazonaws.c	High	October 2012	PPT

	Name of the Information Item/Document	Information Item (URL or file)	Relevance (High/Medium/Low)	DATE of Item	Comments
	threats, vulnerabilities & potential countermeasures	om/sdieee/207-SG-Threats_Vulns_Countermeasure.pdf			presentation
41	Cyber security in smart grids - survey and challenges	http://www.ece.ncsu.edu/netwis/papers/13wl-comnet.pdf	High	January 2013	
42	2012 DOE Smart Grid Cybersecurity Information Exchange	http://www.smartgrid.gov/sites/default/files/doc/files/2012_Cybersecurity_Information_Exchange.pdf	High	December 2012	It shows a summary of best practices exposed in the event.
43	Smart management is the key to smart grid meter security	http://www.embedded.com/design/connectivity/4211457/Smart-management-is-the-key-to-smart-grid-meter-security	High	December 2010	The article defends the smart management for smart grids.
44	Supply Chain Solutions for Smart Grid Security: Building on Business Best Practices	US_ResilienceProject	High	2012	
45	Load Redistribution Attacks and Protection Strategy in Electric Power Systems	Load Redistribution Attacks and Protection Strategy in Electric Power Systems	Medium	2012	
46	Developing a Solid SCADA Security Strategy	DevelopingASolidSCADASecurityStrategy	Medium	11/2002	
47	Next Generation SCADA Security: Best Practices and Client Puzzles	NextGenerationSCADAsecurityBestPracticesAndClientPuzzles	High	2005	
48	Security as a New Dimension in Embedded System Design	SecurityASANewDimensionInEmbeddedSystemDesign	High	2004	
49	Enhancing security Throughout the Supply Chain	http://www-304.ibm.com/jct03001c/procurement/proweb.nsf/objectdocswebview/filesupply+chain+security+white+paper+and+assessment+guide+april+2004/$file/supply+chain+security+white+paper+and+assessment+guide+april+2004.pdf	High	2004	
50	Smart grid information assurance and security technology assessment	http://www.energy.ca.gov/2013publications/CEC-500-2013-056/CEC-500-2013-056.pdf	High	2010-2013	

	Name of the Information Item/Document	Information Item (URL or file)	Relevance (High/Medium/Low)	DATE of Item	Comments
51	Best practices in the deployment of smart grids technologies	BestPracticesInTheDeploymentOfSmartGridTechnologies	High	2010	
52	Privacy by Design Achieving the gold standard in data protection for the smart grid.	Privacy by Design: Achieving the Gold Standard in Data Protection for the Smart Grid	High	2010	
53	Embedding Privacy into Smart Grid Initiatives	Embedding privacy in smart grids	High	2010	
54	Towards Addressing Common Security Issues in Smart Grid Specifications	http://ieeexplore.ieee.org/xpl/articleDetails.jsp?reload=true&arnumber=6309314	High	2012	

ENISA
European Union Agency for Network and Information Security
Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

Athens Office
1 Vass. Sofias & Meg. Alexandrou
Marousi 151 24, Athens, Greece

PO Box 1309, 710 01 Heraklion, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu