SMART GRID TASK FORCE
EG2 DELIVERABLE

Proposal for a list of security measures for smart grids

enisa European Network and Information Security Agency

11 # DOCUMENT HISTORY

12

Date	Version	Modification	Author
14/5/2013	0.0	Preliminary draft	Konstantinos Moulinos
19/8/2013	1.0	First draft	Konstantinos Moulinos, Expert group
10/9/2013	2.0	Second draft - Threats and assets	Louis Marinos, Konstantinos Moulinos
13/11/2013	3.0	Third draft	Konstantinos Moulinos, Expert group
9/12/2013	4.0	Final	Konstantinos Moulinos, Expert group

13

Contributors to this report

It has to be noted that the contribution of the experts, in the list below, reflect the personal opinion of the experts and by no means do they present the official position of the affiliated organisation. Following is the list of the experts who contributed to this report in collaboration with ENISA:

de Wijs	Bart,	ABB
Braendle	Markus,	ABB
Mennella	Jean Pierre,	ALSTOM
Fourati	Alia,	EDF R&D
John	Michael,	Elster
Alagna	Valentina,	ENEL
Francois	Ennesser,	Gemalto
Libal	Vit,	Honeywell
Josi	Monika,	Microsoft
Ruprai	Raminder,	UK NATIONAL GRID
Kursawe	Klaus,	ENCS
Karnouskos	Stamatis,	SAP
Sanchidrian	Guido,	Symantec
Eckmaier	Ralph,	ESEC
Banayoti	Hani,	Atos Origin
Riccetti	Simone,	IBM
Bergknut	Gitte,	EON
Oosterbaan	Wouter,	FoxIT
Rambi	Johan,	Alliander
Menting	Jos,	Laborelec
Honecker	Hans,	Bundesamt für Sicherheit in der Informationstechnik, BSI
Rattas	Ragnar,	Estonian Information System's Authority

Rajesh	Nair,	Swissgrid
Strunge	Carsten,	Energinet
Heyn Roed Andersen	Jens	Energinet
Sjokvist	Kristoffer,	SvK
Lodi	Riho,	Elering
Hlavaty	Richard,	Technologická platforma „Energetická bezpečnost ČR
Assaily	Patrick,	RTE
Dauncey	Joe,	SSE
Stefanini	Alberto,	ESSENCE project - Novareckon
Ronning	Ragnhild,	Statnett
Handrack	Ines	Bundesnetzagentur, BNetZa

Affiliated organizations are considered to represent the following actors in the smart grid eco-system:

- Vendors
- Manufacturers
- Distribution System Operators (DSOs)
- Transmission System Operators (TSOs)
- Standardisation initiatives
- Public Authorities (with a mandate on smart grids' security)
- Research community
- Security service providers

Contact details

For questions related to this document, please use the following details:

Dr Konstantinos MOULINOS, Expert in Network & Information Security - Resilience and CIIP, European Network and Information Security Agency – ENISA,

Email: Konstantinos.Moulinos@enisa.europa.eu

Disclaimer

43 ## Contents

Preface

The EU Commission has recognised that smart grids, the blending of the energy (power) and telecommunication critical infrastructures, should operate securely and by respecting end users' privacy. In order for the European smart grid service providers[1] to improve the security and the resilience of their infrastructures and services, they have to first assess the risk and then take appropriate measures to mitigate this risk. On the other hand, Member States should ensure that smart grid providers have taken all the appropriate organisational and technical measures in order to face the risk factors posed to their assets. From that perspective, the reader can easily assume that a unified and common approach across Member States is needed when addressing these two fundamental elements, namely the risk assessment and the relevant security measures.

The contribution of this report is that it provides the European smart grid asset owners with a catalogue of 45 available security measures, grouped in 11 domains, that might help smart grid providers in improving the level of the cyber security of their installations. It is stressed that this list is guidance and not a mandatory list. Proposed security measures don't address data privacy which is out of scope of this document.[2]

This document reflects the opinion of the members of the group referred in the 'Contributors' section above.

[1] *A list with acronyms and terms can be found in Annex I, at the end of the document.*

[2] *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. Furthermore, it initiated action under the auspices of the Smart Grids Task Force with a dedicated Expert Group (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 cybersecurity 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 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 .*

1 Introduction

The adoption of a particular set of security measures needs the consensus and cooperation of various stakeholders in the smart grid community. A coordination initiative could allow a common and generally accepted approach to addressing smart grid security issues. Moreover, the development of a common approach to addressing smart grid cyber security measures will help not only regulators by harmonising the complex smart grid's environment but also by providing incentives to other involved stakeholders to continuously strive for the improvement of their cyber security.

In this light EG2 has decided to organise consultations on minimum security requirements with industry and national cyber security authorities. This document is the result of these consultations.

1.1 Background

ENISA has already consulted, on the same topic, with the industry through a dialogue promoting process[3] which ended up with a report on the appropriate security measures for smart grids[4]. This report is the starting point for the consultations. Apart from this, in its Work Programme for 2013 ENISA will develop a threat landscape for smart grids. Part of this work is the mapping between the proposed security measures and the threats identified (section 4) as well as a dictionary of threat and asset types for smart grids (see Annexes II and III). Finally, the European Commission has recently issued a Communication on a cyber-security strategy of the EU and the proposal of Directive on Network and Information Security[5] where one of the objectives (1.4.2) is '*To put in place a minimum level of NIS in the Member States and thus increase the overall level of preparedness and response*.' This activity clearly supports this objective by

- aligning the varying levels of security and resilience of the asset owners with a consistent minimum framework;
- providing an indication of a minimum level of security and resilience in the Member States with regards to the smart grids, thereby avoiding the creation of the "weakest link";
- ensuring a minimum level of harmonisation on security and resilience requirements for smart grids across Member States and thus reducing compliance and operational costs; and
- setting the basis for a minimum auditable framework of controls across Europe.

[3] http://www.enisa.europa.eu/activities/Resilience-and-CIIP/workshops-1/2012/Validation%20Workshop.

[4] *Available at https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/smart-grids-and-smart-metering/appropriate-security-measures-for-smart-grids.*

[5] *Available at* http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security.

1.2 Aim

The aim of this report is more to help smart grid asset owners to define what is good practice rather than to provide them with a set of minimum or appropriate security measures. The asset owners should first perform a risk assessment (define appropriateness) and then pick up some or all out of the security measures catalogue we describe in this document based on their risk mitigation decisions. The catalogue cannot be comprehensive; therefore further measures not listed in this catalogue may also be necessary.

1.3 Scope

This technical report addresses smart grid networks[6] and services which are critical and whose compromise would have a significant impact on society. Data privacy issues, however, are considered out of scope of this document (see footnote no. 2). The definition of 'significance' of the impact is not part of the work of this group and is left at the discretion of the Member States. Finally, the safety and environmental aspects of the smart grids are not considered to be part of this report as well.

Smart grid is an environment of rapid technology changes and dynamic threats. For this reason, it is of paramount importance that the security measures addressing these threats should be up-to-date. As a result, it is recommended that the pool of measures described in this document should be regularly reviewed and updated. The details of this process are also beyond the scope of this document.

1.4 Target audience

The present document is focused on the following actors:

- Legislator(s) and the regulator(s) at various levels (EU, Member State);
- Distribution system operators (DSO);
- Transmission system operators (TSO);
- Bulk generation and 'bulk' renewables (e.g., wind farm) operators;
- Third party service and solutions providers;
- Energy traders;
- Third party financial services;
- Smart Grid equipment manufacturers and system integrators;
- Generators, consumers and prosumers[7].

[6] *Covering today's electrical grid , their continuous further development and even the visionary future holistic smart grid.*

[7] *Prosumers: combination of the roles of consumer and producer. In the energy context is the combination of the roles generator and energy user. (see Annex I – Glossary).*

1.5 Development approach

This document is the result of a consultation process which started by a physical meeting on 13rd of May 2013 in Brussels. This consultation has been divided in the following steps:

Step 1: Security experts coming from ICT and smart grid industries, selected by European Commission and ENISA, are the contributors to this phase. This is the **first** group of experts. ENISA drafted the preliminary document[8] and disseminated to the members of the first group. A period of a three week open consultation followed during which the experts of the first group had the opportunity to submit their written comments. After accommodating the comments, a conference call took place (9/7/2013) in order to synchronise the efforts of the group. Then the first draft prepared (19/8/2013) by taking into account the results of the conference call.

Step 2:

In its WP for 2013, ENISA has developed a threat landscape for smart grids. Part of this work involves the mapping between the appropriate security measures, assets and threats. Identified gaps communicated to the group as input to the consultations[9].The draft, produced in the previous step, together with the gaps (if any) identified by ENISA's smart grid land scape was the input to this phase.

National authorities or authorities with a mandate on smart grid cyber security (NCSAs) and Transmission System Operators (TSOs) have been the contributors to this phase. Other relevant entities have been involved such as ACER, ENTSO-E etc or other entities selected by the European Commission This is the **second** group of experts.

The meeting of the second group held on 18th of September 2013 in Brussels. Similarly to the previous step, a three week consultation followed together with a synchronisation conference call. The result of this consultation phase is the semi-final document (16/11/2013).

Step 3: A plenary (both groups involved) conference call took place on 6th of December 2013. The semi-final document was finalised and then forwarded to DG-ENER. The final document may be the subject of discussion for an open workshop.

The whole process was chaired by ENISA, in close cooperation with the European Commission.

1.6 Other relevant activities

In the first meeting, it was agreed that a permanent communication channel with M/490 SGIS should be maintained. A formal liaison has been established with this group. All relevant stakeholders should take into account that all present and future components of smart grids ensure compliance with the 'security-relevant' standards developed by European

[8] *Using as a starting point the report on minimum security measures published by ENISA in December 2012.*

[9] *This work is expected to be finalised by end of Q3 2013.*

193 standardisation organisations, including the smart grid cyber security essential requirements
194 in the Commission's standardisation mandate M/490.

195

2 Approach to identifying appropriate security measures

2.1 References

In order to develop the list of the proposed security measures, the expert group took inspiration from the following key documents:

- NISTIR (National Institute of Standards and Technology Internal Report) 7628: Guidelines for Smart Grid Cyber Security;
- ISO/IEC (International Organization for Standardization) 27002:2005: Information technology —Security techniques — Code of practice for information security management;
- ISO/IEC (International Organization for Standardization) DIS 27036-2, Information technology – Security techniques – Information security for supplier relationships - Part 2: Requirements;
- ISO/IEC 27011:2008: Information technology — Security techniques — Information security management guidelines for telecommunications organizations based on ISO/IEC 27002;
- NERC CIP (North American Electric Reliability Corporation Critical Infrastructure Protection) series of standards;
- IEC (International Electrotechnical Commission) 62443: Technical Specification - Industrial Communication Networks - Network and System Security;
- IEC (International Electrotechnical Commission) 62351: Power Systems Management and Associated Information Exchange – Data And Communications Security;
- ISO/IEC TR (Technical Report) 27019: Information technology — Security techniques — Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy industry;
- BDEW (BDEW Bundesverband der Energie- und Wasserwirtschaft) - White Paper Requirements for Secure Control and Telecommunication Systems.

It has to be noted that the CEN-CENELEC-ETSI Smart Grid Coordination Group, Smart Grid Reference Architecture[10] has been used in order to identify different components of a general Smart Grid and the links between these components.

2.2 The role of risk assessment

The scope of the security measures is defined as follows.

[10] *ftp://ftp.cencenelec.eu/EN/EuropeanStandardization/HotTopics/SmartGrids/Reference_Architecture_final.pdf*.

Scope: The proposed security measures target the protection of assets against threats they are exposed to. All assets of the asset owner which, when breached and/or failing, can have a negative impact on the security or continuity of smart grid networks or services are subject to this protection. The proposed protection covers the exposure of smart grid assets to cyber-threats.

The risk assessment allows the asset owner to define a threshold for the minimum acceptance level before the establishment of a risk value and to perform the risk assessment for the assets in scope. Therefore, a risk assessment is the important step that should be conducted in order to understand what risk level is acceptable for each organisation before deciding upon the required cyber security measures chosen by the asset owner.

A risk assessment should be performed throughout the life cycle of a smart grid infrastructure, in particular during requirements definition, procurement, control definition and configuration, system operations, and system end of lifecycle.

Asset owners should perform risk assessments, specific for their particular setting, to determine which assets are in scope. This guideline does not address any risk assessment in detail. However, on request of relevant stakeholders, a threat assessment has been performed. Based on this threat assessment, the deployment of the proposed security controls has been substantiated.

The proposed list of security measures is thought as a tool for smart grid asset owners in improving the security of the offered services. It is stressed that the responsible entity for the final decision on the appropriateness of the measures it is always the asset owner.

By providing the list of measures by no means it is not implied that the asset owners should implement all of these measures. Asset owners should perform the risk assessment and then take reasoned decisions on which of the measures described in the following sections are more appropriate for their installations. Knowing the impact on assets, their vulnerabilities and the threat exposure described in this report, asset owners will be in the position to determine the protection that seems appropriate to them. It is expected that, depending on the impact, even additional measures – not part of this report – may be necessary.

2.3 Smart grid assets

Smart grid may consist of a plethora of asset types. 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 1). A more detailed description of these assets is given in Annex II - Description of Smart Grid assets.

Besides these smart grid assets, some composite, more complex assets have been identified. These assets have been undertaken from the Smart Grid Architecture Model (SGAM). By considering these assets, our intention is to take into account this standard, while at the same time showing the decomposition of the SGAM[11] assets by means of the assets of Figure 1. This will allow interested individuals to find threats applying to such complex assets by cumulating the threats of their counterparts.

Despite the relatively young age of smart grid, it has to be taken for granted 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[12] and smart mobility[13]. 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://ec.europa.eu/energy/gas_electricity/smartgrids/doc/xpert_group1_reference_architecture.pdf, *accessed 10 Sept 2013*

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

[13] http://www.mobincity.eu/, *accessed 5 September 2013.*

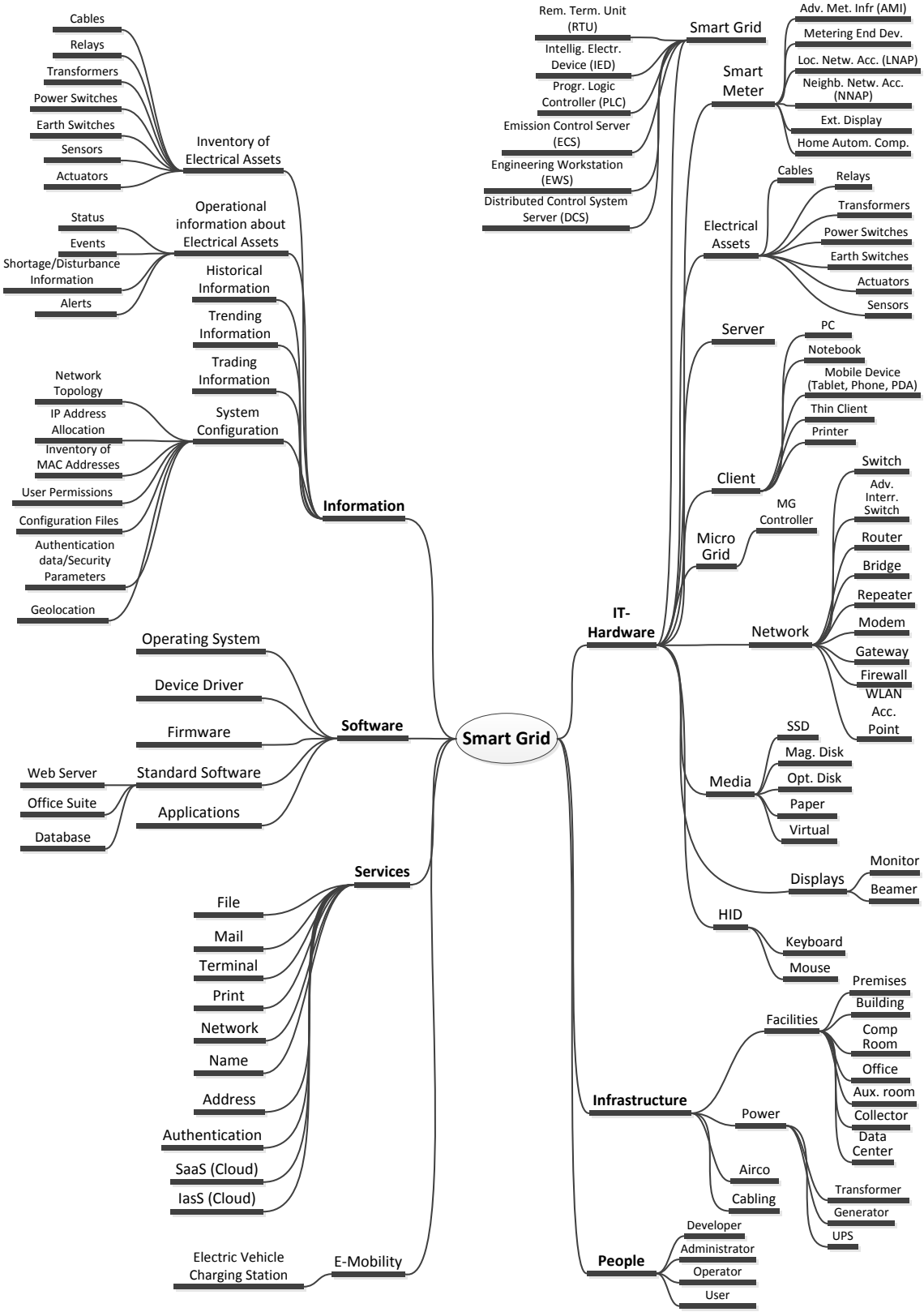

Smart Grid
Information
Inventory of Electrical Assets
Cables
Relays
Transformers
Power Switches
Earth Switches
Sensors
Actuators
Operational information about Electrical Assets
Status
Events
Shortage/Disturbance Information
Alerts
Historical Information
Trending Information
Trading Information
System Configuration
Network Topology
IP Address Allocation
Inventory of MAC Addresses
User Permissions
Configuration Files
Authentication data/Security Parameters
Geolocation
Software
Operating System
Device Driver
Firmware
Standard Software
Web Server
Office Suite
Database
Applications
Services
File
Mail
Terminal
Print
Network
Name
Address
Authentication
SaaS (Cloud)
IasS (Cloud)
E-Mobility
Electric Vehicle Charging Station
IT-Hardware
Smart Grid
Rem. Term. Unit (RTU)
Intellig. Electr. Device (IED)
Progr. Logic Controller (PLC)
Emission Control Server (ECS)
Engineering Workstation (EWS)
Distributed Control System Server (DCS)
Smart Meter
Adv. Met. Infr (AMI)
Metering End Dev.
Loc. Netw. Acc. (LNAP)
Neighb. Netw. Acc. (NNAP)
Ext. Display
Home Autom. Comp.
Electrical Assets
Cables
Relays
Transformers
Power Switches
Earth Switches
Actuators
Sensors
Server
Client
PC
Notebook
Mobile Device (Tablet, Phone, PDA)
Thin Client
Printer
Micro Grid
MG Controller
Network
Switch
Adv. Interr. Switch
Router
Bridge
Repeater
Modem
Gateway
Firewall
WLAN Acc. Point
Media
SSD
Mag. Disk
Opt. Disk
Paper
Virtual
Displays
Monitor
Beamer
HID
Keyboard
Mouse
Infrastructure
Facilities
Premises
Building
Comp Room
Office
Aux. room
Collector
Data Center
Power
Transformer
Generator
UPS
Airco
Cabling
People
Developer
Administrator
Operator
User

Figure 1: Overview of smart grid assets

The SGAM composite assets are decomposed by means of the asset groups shown in Figure 1. The decomposition of SGAM assets is presented in 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[11] 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

2.4 Threats

The threats included in this collection of threats are all applicable to the smart grid assets presented in the previous section. It is worth mentioning that the presented threat is a

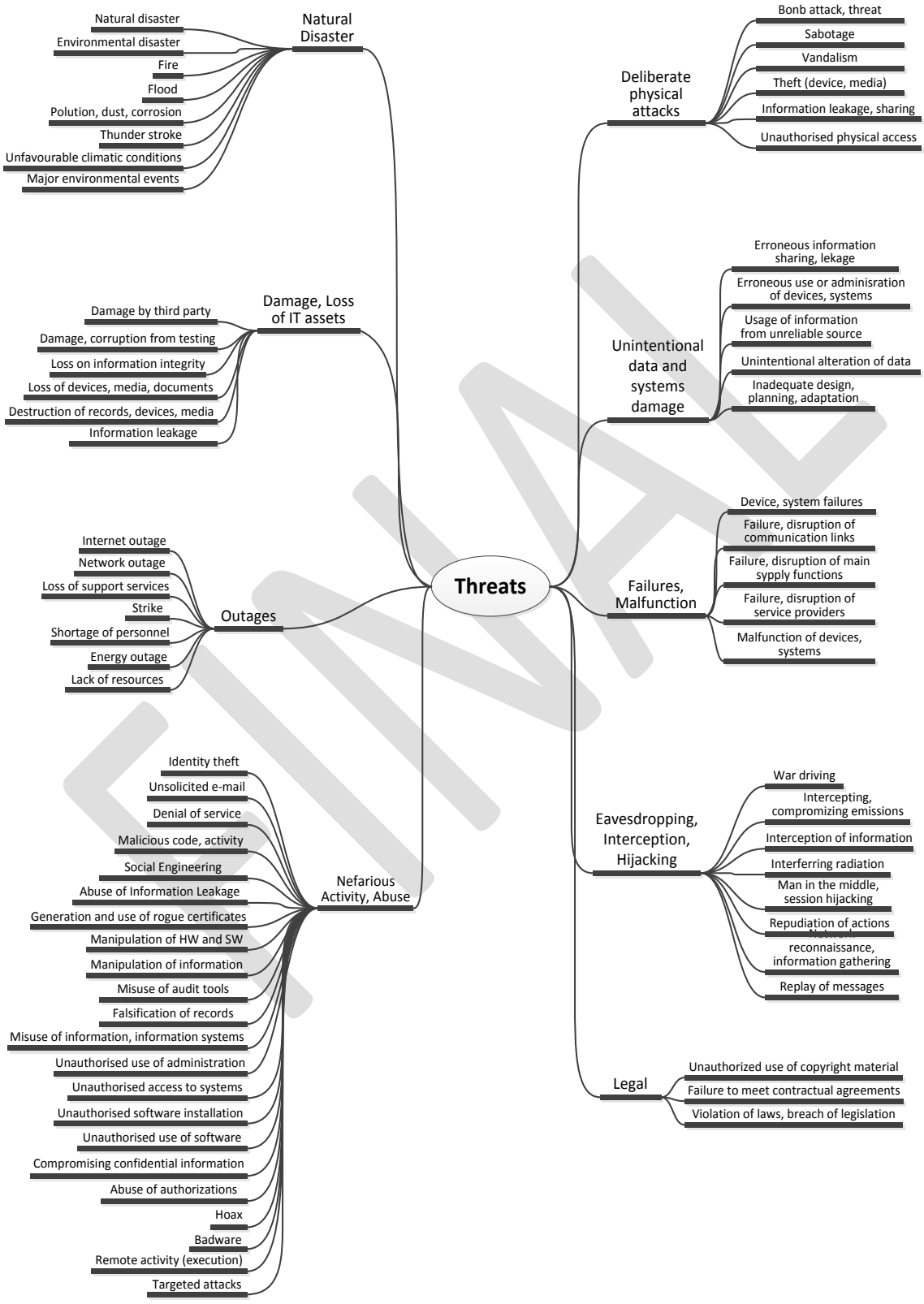
consolidation of threats from the ENISA Threat Landscape[14] and threats used within a smart grid assessment performed by the Expert Group on the security and resilience of Communication networks and Information systems for Smart Grids. [15]

The threats presented in Figure 2 are an overview. All this material is a tool for smart grid asset owners who wish to perform a risk and threat analysis 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 risk and threat analysis by using asset and threat details provided in this document. A deeper analysis will be based on assessed vulnerabilities and impact statements with regard to the concrete assets participating in a smart grid infrastructure scenario.

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

[14] *http://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/ENISA_Threat_Landscape, accessed 5 September 2013.*

[15] *http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?action=display&doc_id=1763, accessed 5 September 2013.*


Threats
Natural Disaster
Natural disaster
Environmental disaster
Fire
Flood
Polution, dust, corrosion
Thunder stroke
Unfavourable climatic conditions
Major environmental events
Damage, Loss of IT assets
Damage by third party
Damage, corruption from testing
Loss on information integrity
Loss of devices, media, documents
Destruction of records, devices, media
Information leakage
Outages
Internet outage
Network outage
Loss of support services
Strike
Shortage of personnel
Energy outage
Lack of resources
Nefarious Activity, Abuse
Identity theft
Unsolicited e-mail
Denial of service
Malicious code, activity
Social Engineering
Abuse of Information Leakage
Generation and use of rogue certificates
Manipulation of HW and SW
Manipulation of information
Misuse of audit tools
Falsification of records
Misuse of information, information systems
Unauthorised use of administration
Unauthorised access to systems
Unauthorised software installation
Unauthorised use of software
Compromising confidential information
Abuse of authorizations
Hoax
Badware
Remote activity (execution)
Targeted attacks
Deliberate physical attacks
Bonb attack, threat
Sabotage
Vandalism
Theft (device, media)
Information leakage, sharing
Unauthorised physical access
Unintentional data and systems damage
Erroneous information sharing, lekage
Erroneous use or adminisration of devices, systems
Usage of information from unreliable source
Unintentional alteration of data
Inadequate design, planning, adaptation
Failures, Malfunction
Device, system failures
Failure, disruption of communication links
Failure, disruption of main sypply functions
Failure, disruption of service providers
Malfunction of devices, systems
Eavesdropping, Interception, Hijacking
War driving
Intercepting, compromizing emissions
Interception of information
Interferring radiation
Man in the middle, session hijacking
Repudiation of actions
reconnaissance, information gathering
Replay of messages
Legal
Unauthorized use of copyright material
Failure to meet contractual agreements
Violation of laws, breach of legislation

303 Figure 2: Overview of threats assumed for Smart Grid assets

304

305 2.5 Smart grid assets exposure to cyber threats

306 In this section the threat exposure of smart grid assets is being presented. The association
307 between assumed threats from Figure 2 and assets from Figure 1 is established through below.

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	Ditto		

Threat Group	Threat	Asset Group	Asset/Detail	Comment
	to user error			
	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		

Threat Group	Threat	Asset Group	Asset/Detail	Comment
	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**	
	Failure or disruption of communication links		**Network**	

Threat Group	Threat	Asset Group	Asset/Detail	Comment
	(communication networks)		**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		

Threat Group	Threat	Asset Group	Asset/Detail	Comment
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	

Threat Group	Threat	Asset Group	Asset/Detail	Comment
			Software **Persons**	
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**	

Threat Group	Threat	Asset Group	Asset/Detail	Comment
			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		
	Hoax	Ditto		
	Badware		**Network** **Information** **Service** **Software**	

Threat Group	Threat	Asset Group	Asset/Detail	Comment
	Remote activity (execution)		**Network** **Information** **Software**	
	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

2.6 Domains

The proposed measures have been grouped in domains for the sake of clarity and comprehensiveness. The identified domains cover all the relevant topics noted by the experts and by the additional information sources, namely:

1. **Security governance & risk management:** measures relevant to proper implementation and/or alignment with the security culture on collaborative chain of smart grid stakeholders;
2. **Management of third parties:** measures relevant to the interaction with third parties, so that the smart grid operator can reach a true and sustainable integration to the smart grid as a whole;
3. **Secure lifecycle process for smart grid components/systems and operating procedures:** measures relevant to the secure installation, configuration, operation, maintenance, and disposition, including secure disposal, of the smart grid components and systems. Therefore, the security measures included in this domain take into consideration among other things the proper configuration of the smart grid information systems and components or its change management procedures;

4. **Personnel security, awareness and training:** this domain ensures that employees of an organisation operating and maintaining a smart grid receive adequate cyber security training to perform reliable operations on the smart grid;
5. **Incident response & information exchange:** this domain covers the possible security threats, vulnerabilities, and incidents affecting smart grids in order to provide an effective response in case of a potential disruption or incident;
6. **Audit and accountability:** this domain covers the implementation of an audit and accountability policy and associated controls in order to verify compliance with energy and smart grid specific legal requirements and organisation policies;
7. **Continuity of operations:** this domain ensures the basic functions of the smart grid under a wide range of circumstances including hazards, threats and unexpected events;
8. **Physical security:** this domain covers the physical protection measures for the smart grid assets;
9. **Information systems security:** this domain covers the definition of measures to protect the information managed by the smart grid information systems using different technologies like firewalls, antivirus, intrusion detection and etc.;
10. **Network security:** this domain covers the design and implementation of required security measures that protect the established communication channels among the smart grid information system and the segmentation between business and industrial networks.
11. **Resilient and robust design of critical core functionalities and infrastructures**: this domain covers the design of the functionalities offered by the network and the supporting infrastructures in a resilient way.

3 Appropriate security measures

3.1 Introduction

This section describes a set of measures which are considered to be appropriate for the smart grid installations. It is stressed that this list is guidance and not a mandatory list. It is at the discretion of the asset owner or the Member States to address different security measures (for example, based on a national or international standard), only some of the security measures, or additional security measures. Note also that some security measures may not be fully applicable in all settings, depending on the type of network, service, or provider involved. The security measures described in this document are to be considered for systems considered in scope. Finally, it is recommended that asset owners should take into account European Commission Mandate M/490 CEN-CENELEC-ETSI SG-CG working groups recommendations[16], especially SG-CG/SGIS working group ones for cyber security concerns.

3.2 Domain 1: Security governance & risk management

The asset owner should:

1. establish and maintain an appropriate information security policy.
2. establish and maintain an appropriate structure of security roles and responsibilities.
3. establish and maintain an appropriate set of security procedures that supports the implementation of the security policy.
4. establish and maintain an appropriate risk management framework for risk assessment and risk treatment activities across the organisation which will take into account the complex operational environment.
5. establish and perform risk assessment activities to identify and evaluate the risk across the organisation at regular intervals.
6. establish and maintain an appropriate risk treatment plan in order to manage the risk across the organisation; and in collaboration with other interested parties[17] to assess the dependency risk for one's own processes and one's dependent interested parties at regular intervals, after a near-miss and after a major incident.

[16] *http://www.cencenelec.eu/standards/sectors/SmartGrids/Pages/default.aspx.*

[17] *As defined in ISO 9000:2005, Quality management systems - Fundamentals and vocabulary. Check Annex I – Glossary for a definition.*

3.3 Domain 2: Management of third parties

The asset owner should establish and maintain:

7. appropriate third party agreements to preserve the integrity, confidentiality, availability, when required, and the quality of the information at the same level as the internal services when dealing with customers and third parties and to guarantee the non-repudiation of (electronically made) agreements/contracts with third parties.
8. mechanisms in order to monitor the compliance of contractual obligations of information and services and validate solutions against predefined acceptance criteria.

3.4 Domain 3: Secure lifecycle process for smart grid components/systems and operating procedures

Security measures applicable to smart grid **components/systems** include:

9. The asset owner should determine, define and document the necessary security requirements for smart grid components and systems during the design and procurement (before deployment), taking into consideration the existing infrastructure and components.

Security measures applicable to smart grids **operating procedures** are:

10. The asset owner should ensure that an inventory is established and maintained that represents the critical components and smart grid information systems.
11. The asset owner should ensure that the base security configuration of a smart grid's components/systems is identified, set and maintained for every instance of that component/system. [18]
12. The asset owner should ensure that adequate information regarding the installed software and configuration of a smart grid's components/systems is documented and maintained to be able to verify the integrity of these systems, especially considering configuration options addressing information security issues.

[18] *After initial installation and start-up the component/system should be configured in a fail-safe and secure manner. The defined secure baseline configuration should be documented.*

13. The asset owner should establish and maintain activities for performing routine and preventive/corrective maintenance on the components and smart grid information systems.
14. The asset owner should establish and maintain activities for software/firmware patching and upgrade on the components and smart grid information systems.
15. The asset owner should establish and maintain activities for the secure disposition, including secure disposal of smart grid components and smart grid information systems. [19]
16. The asset owner should establish change management procedures in order to minimise the likelihood of disruptions and errors resulting from changes.

Security measures applicable to smart grids **components/systems and procedures** include:

17. Security testing activities on the smart grid components/systems should be performed in order to verify its security. [20][21]

3.5 Domain 4: Personnel security, awareness and training

The asset owner should:

18. perform appropriate background checks on personnel (employees, contractors, and third-party users) if required for their duties and responsibilities.
19. establish and maintain an appropriate process for managing changes in personnel (employees, contractors, third-party users) or changes in their roles and responsibilities. For example upon termination or change of employment.
20. establish and maintain a security awareness program across the organisation.

[19] *Both paper and digital information is included.*

[20] *It is recognized that it is important and desirable to additionally provide appropriate security certification for components and/or systems. However, given the lack of appropriate certification schemes and the current maturity level of the existing ones, it is currently not possible to generally require certification on a European scale. Further work needs to be facilitated to reach a multi-stakeholder, European wide approach for identifying security risk factors in order to be able to derive appropriate requirements. This contributes to ensure a commonly accepted certification scheme on European level for products. It is recommended to increase and accelerate efforts towards a European certification strategy to enable such a requirement.*

[21] *The asset owner can apply his own testing methods.*

21. establish and maintain security training and personnel certification programmes, taking into account its needs based on their roles and responsibilities.

3.6 Domain 5: Incident response & information exchange

The asset owner should:

22. establish and maintain capabilities to respond against cyber security incidents.
23. establish and maintain vulnerability assessment activities on the smart grid information systems.
24. establish and maintain an appropriate vulnerability management plan in order to manage vulnerabilities on smart grid information systems.
25. establish and maintain contacts with authorities, security interest groups and vendors to be aware of vulnerabilities and threats[22].

3.7 Domain 6: Audit and accountability

The asset owner should:

26. establish and maintain auditing and logging capabilities on smart grid information systems and components as appropriate and feasible.
27. establish and maintain monitoring activities on the smart grid Information systems and components.
28. protect the audit information generated.

3.8 Domain 7: Continuity of operations

The asset owner should:

29. establish and maintain capabilities to ensure essential functions after disruption events on smart grid Information systems [23] or on their staff and to return to normal operation as necessary.

---

[22] *Please consider European and national legislation regarding security incident reporting requirements in the energy sector.*

[23] *It is important to highlight the fact that the design of the smart grid architecture need to be done taking into account the requirements that will allow the implementation of a resilient infrastructure against cyber-attacks.*

30. establish, maintain and test essential/emergency communication services in case of major disasters.

3.9 Domain 8: Physical security

The asset owner should:

31. establish and maintain the appropriate physical security of the smart grid facilities/components/systems according to the criticality which has to be defined by the asset owner.
32. establish and maintain capabilities for logging and monitoring the physical access to the smart grid facilities/components taking into account the criticality of the facility.
33. Implement special additional physical protection measures to protect equipment located outside of the organisations' own grounds or premises.

3.10 Domain 9: Information systems security[24]

The asset owner should:

34. establish a policy for classification/disclosure of (sensitive/secret) information regarding smart grid information system.
35. implement security measures (e.g. cryptographic techniques, intrusion detection, spam filters) in order to protect the information on smart grid information system.
36. establish and maintain system/groups[25]/user accounts on smart grid information systems.
37. enforce logical access to authorized entities on smart grid information systems and security perimeters.
38. establish and maintain secure remote access where applicable to smart grid information systems.
39. establish and maintain appropriate information security capabilities on information systems, to provide protection against malware, viruses and other common threats.

[24] *It is important to differentiate between data security (security of raw unprocessed information) and information security (security of the data that has been processed and it is valuable for the organisation).*

[25] *Where possible/feasible*

40. establish and maintain secure procedures for the access, storage, distribution, transport, sanitization, destruction and disposal of the media assets.

3.11 Domain 10: Network security

The asset owner should establish and maintain:

41. segregated and/or dedicated networks for the smart grids with the appropriate segmentation and functional segregation.
42. the confidentiality of communications across the segregated and/or dedicated network.

3.12 Domain 11: Resilient and robust design of critical[26] core functionalities and infrastructures

The asset owner should:

43. layout critical functionalities and process infrastructures with a feasible minimum exposure to all relevant threat categories, especially taking into account those related to potential targeted and untargeted ICT-attacks, and changes in the general threat situation.[27]
44. layout different smart grid functionalities, operational and economical processes and process infrastructures in a way that they, including their specific ICT-infrastructures, can be operated in crises or emergency operation modes during general or ICT-crises or in case of breakdown of other external infrastructures.[28,29]
45. layout smart grids functionalities (critical and non-critical) and process infrastructures in a way, that they cannot endanger the critical ones, that they can safely interrupt

[26] *Critical functions are considered those whose loss would cause adverse effects to the operation of the smart grid. The identification criteria of these functions are beyond the scope of this document.*

[27] *Part of this assessment should also be the analysis of the attack threat situation.*

[28] *like breakdown or other malfunction of the internet, of general public or other multiuser ICT-networks etc.*

[29] *Special attention should be paid to attacks against economic processes. For this reason the asset owner should layout electricity and gas operational grid processes and operational infrastructures in a way, that they can safely and securely operate the smart grid in case of attacks on energy economic processes and economic infrastructures, or in case of failures or malfunctions stemming from economic processes (including data from economic processes mismatching the real grid operational situation's needs).*

491 operation under crisis conditions, they cannot endanger the critical ones and can come
492 back to normal operation after crises.

4 Catalogue of security measures

This section contains a summary of the domains described above and cyber security measures.

Domain	List of Security Measures	No
Security governance & risk management	Information security policy	1
	Organisation of information security	2
	Information security procedures	3
	Risk management framework	4
	Risk assessment	5
	Risk treatment plan	6
Third parties management	Third party agreements	7
	Monitoring third parties services and validating solutions against predefined acceptance criteria	8
Secure lifecycle process for smart grid components and operating procedures	Security requirements analysis and specification	9
	Inventory of smart grid components/systems	10
	Secure configuration management of smart grid components/systems	11
	Secure configuration documentation	12
	Maintenance of smart grid components/systems	13
	Software/firmware upgrade of smart grid components/systems	14
	Disposal of smart grid components/systems	15
	Change management	16
	Security testing of smart grid components/systems	17
Personnel security, awareness and training	Personnel screening.	18
	Personnel changes	19
	Security and awareness program	20
	Security training and certification of personnel	21
Incident response & information knowledge sharing	Incident response capabilities	22
	Vulnerability assessment	23
	Vulnerability treatment	24
	Contact with authorities and security interest groups	25
Audit and accountability capability	Auditing capabilities	26
	Monitoring of smart grid information systems	27
	Protection of audit information	28
Continuity of operations capability	Continuity of operations capabilities	29
	Essential communication services	30
Physical security	Physical security	31
	Logging and monitoring physical access	32
	Physical security on third party premises	33
Information systems security	Classification/disclosure policy	34
	Data Security	35
	Account management	36
	Logical access control	37
	Secure remote access	38
	Information security on information systems	39
	Media handling	40

Network security	Functional and secure network segregation	41
	Secure network communications	42
Resilient and robust design of critical core functionalities and infrastructures	Minimum exposure	43
	Resiliency	44
	Safe interruption-Continuity of operation	45

496

497 Table 3: Domains and relevant measures summary

5 Deploying the proposed security measures

In this chapter we provide smart grid asset owners with a proposal on how the security measures can be deployed to minimize exposure to the assumed threats. The proposed security measures present an appropriate protection against the threats, nevertheless in a concrete smart grid infrastructure implementation the vulnerabilities of the assets need to be checked as well.

Table 4 below shows the correspondence between threats and appropriate security measures to protect against exposure. It must be stated, that the association of security measures has been performed per threat group. The particular threats of each threat group have been repeated in order to provide to the reader evidence/information why the particular security measures have been assigned to this threat group.

Threat Group	Threat	Security measures
Physical attack (deliberate/ intentional)		**2, 7, 18, 19, 20, 32, 32, 33, 39, 43,44,45**
	Bomb attack / threat	18, 19, 21, 31, 32, 33, 43,44,45
	Fraud	7, 18, 19, 20, 31, 32, 33, 43,44,45
	Sabotage	7, 18, 19, 21, 31, 32, 33, 43,44,45
	Vandalism	7, 18, 19, 21, 31, 32, 33, 43,44,45
	Theft (of devices, storage media and documents)	7, 10, 15, 19, 31, 32, 33, 40, 43,44,45
	Information leakage/sharing	7, 15, 18, 19, 40, 43,44,45
	Unauthorized physical access / Unauthorised entry to premises	2, 7, 19, 31, 32, 33, 43,44,45
	Coercion, extortion or corruption	7, 18, 19 20, 31, 32, 33, 43,44,45
Unintentional damage (accidental)		**7, 8, 9, 11, 12, 13, 14, 15, 16, 17, 20, 21, 25, 26, 27, 28, 29, 30, 35, 36, 37, 38, 39, 40, 41, 43,44,45**
	Information leakage/sharing due to user error	7, 15, 20, 21, 26, 27, 28, 35, 36, 37, 39, 40, 41, 43,44,45
	Erroneous use or administration of devices and systems	7, 11, 12 ,13, 14 ,16 ,20, 21, 26, 27, 28, 29, 30, 36,37,41, 43,44,45
	Using information from an unreliable source	8, 20, 21, 35, 39, 43,44,45
	Unintentional change of data in an information system	12, 13, 16, 20, 21, 26, 27, 28, 35, 36, 37, 38, 39, 40, 43,44,45
	Inadequate design and planning or lack of adaptation	9, ,11, 12, 13, 17, 20, 21, 43,44,45
Disaster (natural, environmental)		**20, 21,29, 30, 31, 33, 43,44,45**
	Disaster (natural earthquakes, floods, landslides, tsunamis)	20, 21,29, 30, 31, 33, 43,44,45
	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)		**7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17,**

Threat Group	Threat	Security measures
		20, 21, 26, 27, 28, 29, 30, 33, 35, 36, 37, 38, 39, 40, 41, 43,44,45
	Damage caused by a third party	7, 8, 10, 12, 13, 15, 16, ,20, 21, 26, 27, 28, 29, 30, 41, 43,44,45
	Damages resulting from penetration testing	9, 11, 12, 13, 16, 17, 20, 21, 26, 27, 28, 29, 30, 35, 41, 43,44,45
	Loss of (integrity of) sensitive information	11, 12, 13, 14, 15, 16, 26, 27, 29, 35, 36,37,40, 41, 43,44,45
	Loss of devices, storage media and documents	10,15,29, 30, 33, 40, 43,44,45
	Destruction of records, devices or storage media	15,33,40, 43,44,45
	Information Leakage	7, 11, 15, 17,20, 21, 26, 27, 28, 35,36,37,38, 39,40, 41, 43,44,45
Failures/ Malfunction		**7, 8, 9, 11, 12, 13, 14, 17, 21, 26, 27, 28, 29, 30, 35, 39, 41, 43,44,45**
	Failure of devices or systems	7, 8, 11, 12, 21, 29, 30, 43,44,45
	Failure or disruption of communication links (communication networks)	7, 8, 12, 29, 30, 41, 43,44,45
	Failure or disruption of main supply	7, 8, 12, 29, 30, 43,44,45
	Failure or disruption of service providers (supply chain)	7, 8, 9, 12, 17, 21, 29, 30, 43,44,45
	Malfunction of equipment (devices or systems)	7, 8, 12, 26, 27, 28, 29, 30, 39, 41, 43,44,45
	Insecure Interfaces (APIs)	7, 8, 9, 12, 13, 14, 17, 26, 27, 28, 35, 39, 43,44,45
Outages		**7, 8, 19, 21, 29, 30, 41, 43,44,45**
	Lack of resources	7, 8, 19, 21, 43,44,45
	Loss of electricity	7, 8, 29, 30, 33, 43,44,45
	Absence of personnel	7, 8, 43,44,45
	Strike	Ditto
	Loss of support services	7, 8, 29, 30, 43,44,45
	Internet outage	7, 8, 29, 30, 41, 43,44,45
	Network outage	Ditto
Eavesdropping/Interception/ Hijacking		**7, 8, 11, 14, 20, 21, 26, 27, 28, 35, 36, 37, 38, 39, 41, 42, 43,44,45**
	War driving	*7, 11, 14, 20, 21, 36, 38, 42,* 43,44,45
	Intercepting compromising emissions	*7, 11, 14, 20, 21, 26, 27, 28, 36, 38, 42,* 43,44,45
	Interception of information	*7, 11, 14, 20, 21, 26, 27, 28, 35 36, 38, 41,* 43,44,45
	Interfering radiation	*20, 21, 31, 32, 33,* 43,44,45
	Replay of messages	*7, 14, 20, 26, 27, 28, 35, 36, 37, 38, 39, 41, 42,* 43,44,45
	Network Reconnaissance and Information gathering	*7, 8, 11, 14, 20, 21, 35, ,37, 38, 39, 41, 42,* 43,44,45
	Man in the middle/ Session hijacking	*7, 14, 20, 26, 27, 28, 35, 36, 37, 38, 39, 41, 42,* 43,44,45
	Repudiation of actions	*7, 20, 26,27,28, 36, 37,* 43,44,45
Nefarious Activity/ Abuse		**7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 26, 27, 28, 35, 36, 37, 38, 39, 40, 41, 42, 43,44,45**
	Identity theft	*7, 9, 11, 12, 15, 20, 21, 26, 27, 28, 35, 36, 37, 38, 39, 40, 41, 42,* 43,44,45
	Unsolicited E-mail	*20, 21, 35, 39,* 43,44,45
	Denial of service	*7, 9, 11, 13, 14, 17, 20, 21, 26, 27, 28,*

Threat Group	Threat	Security measures
		29, 30, 36, 37 38, 41, 43,44,45
	Malicious code/ software/ activity	*7, 8, 11, 12, 13, 14, 16, 17, 20, 21, 26, 27, 28, 29, 30, 35, 39, 41,* 43,44,45
	Social Engineering	*15, 35, 36, 37, 38, 39, 40,* 43,44,45
	Abuse of Information Leakage	*7, 9, 11, 15, 17, 20, 21, 26, 27, 28, 35, 36, 37, 39, 38, 40, 41,* 43,44,45
	Generation and use of rogue certificates	*7, 8, 11, 14, 15, 16, 17, 20, 21, 26, 27, 28, 35, 36, 37, 39, 40,* 43,44,45
	Manipulation of hardware and software	*7,8, 9, 11, 12, 13, 14, 16, 17, 26, 27, 28, 35, 36, 37, 38, 39, 40,* 43,44,45
	Manipulation of information	*7, 8, 9, 10, 15, 26,27, 28, 35, 39, 40, 41, 42,* 43,44,45
	Misuse of audit tools	*7, 8, 11, 28,* 43,44,45
	Falsification of records	*7,89, 9, 10, 15, 26,27, 28, 35, 39, 40, 41, 42,* 43,44,45
	Misuse of information/ information systems	*7, 8, 9, 10, 11, 13, 14, 15, 16, 17, 26, 27, 28, 35, 36, 39, 40, 41, 42,* 43,44,45
	Unauthorised use or administration of devices and systems	*7, 8, 11, 12, 13, 14, 16, 17, 20, 21, 26, 27, 28, 29, 30, 35, 36, 37, 40, 41, 42,* 43,44,45
	Unauthorized access to the information system / network	*7, 8, 11, 12, 13, 14, 16, 17, 20, 21, 26, 27, 28, 29, 30, 35, 36, 37, 38, 40, 41, 42,* 43,44,45
	Unauthorized changes of records	*7, 8, 9, 10, 15, 26,27, 28, 35, 39, 40, 41, 42,* 43,44,45
	Unauthorized installation of software	*7, 8, 9, 10, 12, 16, 26, 27, 28, 35, 36, 37, 39,* 43,44,45
	Unauthorized use of software	*26, 27, 28, 35, 36, 37, 38*
	Compromising confidential information (data breaches)	*7, 8, 9, 10, 15, 26,27, 28, 35, 39, 40, 41, 42,* 43,44,45
	Abuse of authorizations	*7, 8, 11, 12, 13, 14, 16, 17, 20, 21, 26, 27, 28, 29, 30, 35, 36, 37, 38, 40, 41, 42,* 43,44,45
	Hoax	*20, 21,* 43,44,45
	Badware	*7, 8, 9, 11, 12, 13, 14, 16, 17, 26, 27, 28, 35, 36, 37, 38, 39, 40,* 43,44,45
	Remote activity (execution)	*35, 36, 37, 38, 39, 41, 42,* 43,44,45
	Targeted attacks (APTs etc.)	*7,89, 11, 12, 13, 14, 16, 17, 20, 21, 26, 27, 28, 29, 30, 35, 36, 37, 40, 41, 42,* 43,44,45
Legal		**7, 8, 26, 27, 28, 32, 37, 43,44,45**
	Violation of laws or regulations / Breach of legislation	*7,89, 26, 27, 32, 37,* 43,44,45
	Failure to meet contractual requirements	*7, 8, 9, 21,* 43,44,45
	Unauthorized use of copyrighted material	*7, 8, 20, 26, 27, 28,* 43,44,45

Table 4: Mapping between threats and security measures

Annex I - Glossary

The appropriate security measures for smart grids have been selected using a generic terminology that is detailed below, as follows:

- **Asset owner**: all parties in section 1.4 except regulators[30].
- **Communication network:** platform which interconnects exchange data among all devices within the smart grid infrastructure.
- **Cyberspace:** is a complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form.
- **Cyber security:** is the preservation of confidentiality, integrity and availability of information in cyberspace.
- **Distributed control system (DCS):** system used to monitor and control systems from the measuring instrument to the control console.
- **Domain:** in the context of this study a domain is a set of measures which have a common purpose. A domain contains two key elements:
  - Control objective**:** the desired effect of the control;
  - Appropriate security measures to fulfil the control objective.
- **Interested party**: A person or group having an interest in the performance or success of an organization [ISO 9000:2005]; interested parties might come from inside or outside of the organization. Examples of interested parties include customers, suppliers, owners, partners, employees, etc. Interested parties are also referred to as stakeholders.
- **Media assets:** this term includes compact discs, digital video discs, erasable-programmable read-only memory and embedded assets, tapes, printed reports, and documents.
- **Provider**: stakeholder which provides services to the smart grid value chain, such as:
  - Transmission System Operator (TSO): entity responsible for managing the security of the Transmission system in real time and co-ordinate the supply of and demand for electricity;
  - Distribution System Operator (DSO)[31]: entity responsible for (a) operating, (b) ensuring the maintenance of, (c) if necessary, developing the distribution

[30] *According to ISO/IEC 27001:2005, the term 'owner' identifies an individual or entity that has approved management responsibility for controlling the production, development, maintenance, use and security of the assets. The term 'owner' does not mean that the person actually has any property rights to the asset.*

[31] *It can be foreseen that the role of the DSO will change in the Smart Grid era as more and more local production will need to be managed taking advantage of the flexibility of local loads (e.g. related to e-mobility and heat pumps). One could say that*

system in a given area and, where applicable, its interconnections with other systems; and (d) for ensuring the long term ability of the system to meet reasonable demands for the distribution of electricity;

- Electricity generator: legal entity that produces electric energy and puts it into the system;
- Customer**:** entity that purchases electricity for the purpose of use;
- Electricity market: all operations related to the purchase and sale of power energy. In the electricity market, the commodity is the electrical energy which is purchased, sold or trade on short-term.
- Prosumers: combination of the roles of consumer and producer. In the energy context is the combination of the roles generator and energy user.

- **Smart grid**: an upgraded electricity network to which two-way digital communication between supplier and consumer as well as between smart grid components, intelligent metering and monitoring systems have been added. In this domain, it is important to highlight the importance of the human factor as a key component of the smart grid.
- **Smart grid components:** elements or devices that represent part of the smart grid.
- **Smart grid information system**: reflects the following key elements:
  - Information and communications technology (ICT) components: like computer or telecommunication networks;
  - Industrial control systems: like supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other control system configurations such as skid-mounted Programmable Logic Controllers (PLC);
  - Operational Technologies: like firmware or operating systems.
- **Supervisory Control and Data Acquisition (SCADA)[32]:** systems for the control of each substation, as well as for the management of the entire smart grid network.

The above definitions were selected based on the taxonomy that was most used by the participants in the study, and based on observations collected during the extensive desk research performed.

---

the DSO will need to co-ordinate the local supply of and demand for electricity in more and more active distribution grids. In order to do so more ICT is needed and therefore more security requirements will apply to the DSOs.

[32] *A more detailed description of these elements can be found on the following document http://www.tno.nl/downloads/TNO-DV%202008%20C096_web.pdf.*

Annex II - Description of Smart Grid assets

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 objectives: 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 grid 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.

638 ○ Intelligent Electronic Device (IED): term used in the electric power industry to
639 describe microprocessor-based controllers of power system equipment, such
640 as circuit breakers, transformers, and capacitor banks.

641 ○ Programmable Logic Controller (PLC): digital computer used for automation of
642 electromechanical processes, such as control of machinery on factory assembly
643 lines, amusement rides, or light fixtures.

644 • Micro grid: electrical systems that include multiple loads and distributed energy
645 resources that can be operated in parallel with the grid or as an electrical island; Micro
646 grid Controller: devices that control and enable the establishment of micro grids.

647 • Smart Meter: electrical meter that records consumption of electric energy in intervals
648 of an hour or less and communicates that information at least daily back to the utility
649 for monitoring and billing purposes. The components of smart meters to take into
650 account are:

651 ○ Metering End Device, which let us read date at the end points: Electricity; Gas;
652 Water; Heat.

653 ○ Local Network Access Point (LNAP).

654 ○ Neighbourhood Network Access Point (NNAP).

655 ○ External Display.

656 ○ Home Automation Components.

657 ○ AMI Head End (Advanced Metering Infrastructure).

658 • Servers: related with hardware, computer hardware that holds the necessary software
659 to run an infrastructure.

660 • Clients: devices from which personnel staff, end users and potential clients will
661 connect with available applications:

662 ○ PC.

663 ○ Notebook.

664 ○ Tablet.

665 ○ ThinClient.

666 ○ PDA.

667 ○ (Mobil-)Phone.

668 ○ Printer.

669 ○ Smart Appliances and Equipment (Customer): home appliances and devices
670 (i.e., thermostats, pool pumps, clothes washers/dryers, water heaters, etc.)
671 that use wireless technology to receive real-time data from the AMI system to
672 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
- Human Interaction Devices (HID): devices to let the user introduce information to the system.
    - Displays: devices to present the information to the user:
        - Monitor
        - Beamer
        - Video Wall
        - KVM
    - 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 III: Threats assumed for Smart Grid assets

Table 5: Threats assumed for Smart Grid assets

Threat Group	Threat	Threat details
Physical attack (deliberate/ intentional)		
	Bomb attack / threat	
	Fraud	
		Fraud by employees
	Sabotage	
	Vandalism	
	Theft (of devices, storage media and documents)	Theft of mobile devices (smartphones/ tablets) Theft of other hardware
	Information leakage/sharing	
	Unauthorized physical access / Unauthorised entry to premises	
	Coercion, extortion or corruption	
Unintentional damage (accidental)		
	Information leakage/sharing due to user error	Accidental leaks/sharing of data by staff Mobile privacy and mobile applications Web applications Network
	Erroneous use or administration of devices and systems	Errors in maintenance Configuration/ installation error Technological obsolescence Increasing recover time Unpatched software (delayed patching processes)
	Using information from an unreliable source	
	Unintentional change of data in an information system	

Threat Group	Threat	Threat details
	Inadequate design and planning or lack of adaptation	
Disaster (natural, environmental)		
	Disaster (natural earthquakes, floods, landslides, tsunamis)	
	Disaster (environmental - fire, explosion, dangerous radiation leak)	
	Fire	
	Flood	
	Pollution, dust, corrosion	
	Thunder stroke	
	Water	
	Unfavourable climatic conditions	
	Major events in the environment	Manmade disasters (e.g. radioactive radiation, pollution, etc.) Environmental influences (e.g. volcanic activity, solar winds, etc.)
Damage/Loss (IT Assets)		
	Damage caused by a third party	Security failure by third party
	Damages resulting from penetration testing	
	Loss of (integrity of) sensitive information	Loss of integrity of certificates
	Loss of devices, storage media and documents	Mobile devices Storage media Documentation of IT Infrastructure
	Destruction of records, devices or storage media	Infection of removable media Abuse of storage
	Information Leakage	Mobile data and data of mobile applications Web privacy and web applications Network traffic

Threat Group	Threat	Threat details
Failures/ Malfunction		
	Failure of devices or systems	Defective data media Hardware failure Failure of applications and services
	Failure or disruption of communication links (communication networks)	Failure of cable networks Failure of wireless networks Failure of mobile networks
	Failure or disruption of main supply	
	Failure or disruption of service providers (supply chain)	
	Malfunction of equipment (devices or systems)	
	Insecure Interfaces (APIs)	
Outages		
	Lack of resources	
	Loss of electricity	
	Absence of personnel	
	Strike	
	Loss of support services	
	Internet outage	
	Network outage	Outage of cable networks Outage of wireless networks Outages of mobile networks
Eavesdropping/Interception/ Hijacking	**Wardriving**	Search and cartography of 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.
	Interception of information	Corporate Espionage Unsecured Wi-Fi, rogue access points
	Interfering radiation	High frequency devices (e.g. displays) radiate. This

Threat Group	Threat	Threat details
		information can be misused.
	Replay of messages	
	Network Reconnaissance and Information gathering	The activity to collect sufficient information from legitimate channels about the structure of a network.
	Man in the middle/ Session hijacking	
	Repudiation of actions	
Nefarious Activity/ Abuse	**Identity theft**	Credentials stealing trojans
	Unsolicited E-mail	SPAM Unsolicited infected e-mails
	Denial of service	Plain denial of service (DoS) (e.g. against application services of critical infrastructure) Distributed DoS (DDoS)
	Malicious code/ software/ activity	
		Search Engine Poisoning
		Exploitation of fake trust of social media
		Worms/Trojans
		Mobile malware
		Alternation of software
		Infected trusted mobile apps
		Elevation of privileges
		Phishing attacks
		Web injection attacks (Code injection: SQL, XSS)
		Exploit Kits
	Social Engineering	Rogue security software/ Rogueware/ Scareware Ransomware
	Abuse of Information Leakage	Leakage affecting mobile privacy and mobile applications Leakage affecting web privacy and web applications Leakage affecting network traffic

Threat Group	Threat	Threat details
	Generation and use of rogue certificates	Loss of (integrity of) sensitive information Man in the middle/ Session hijacking Social Engineering (e.g. install fake trust OS updates)
	Manipulation of hardware and software	Anonymous proxies Abuse of computing power of cloud to launch attacks (cybercrime as a service) Abuse of 0-day vulnerabilities Access of web sites through chains of HTTP Proxies (**Obfuscation**) Rogue systems connected to the network Damage caused by 3rd party access
	Manipulation of information	
	Misuse of audit tools	
	Falsification of records	
	Misuse of information/ information systems	
	Unauthorised use or administration of devices and systems	
	Unauthorized access to the information system / network	Network Intrusion
	Unauthorized changes of records	
	Unauthorized installation of software	Drive-by download / malicious URLs
	Unauthorized use of software	
	Compromising confidential information (data breaches)	
	Abuse of authorizations	
	Hoax	False rumour and/or a fake warning
	Badware	Spyware or deceptive adware
	Remote activity (execution)	Remote Command Execution Botnets / Remote activity
	Targeted attacks (APTs etc.)	Spear phishing attacks

Threat Group	Threat	Threat details
		Installation of sophisticated and targeted malware
Legal	**Violation of laws or regulations / Breach of legislation**	
	Failure to meet contractual requirements	
	Unauthorized use of copyrighted material	File Sharing services

737

P.O. Box 1309, 71001 Heraklion, Greece
www.enisa.europa.eu