

14 March 2012

Work Package 1.2

Threat Analysis

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

Version 7.2

Table of contents

1.	Introduction	3
<hr/>		
1.1.	Mission, vision and goals	3
1.2.	Strategy	3
1.3.	Scope	3
1.4.	Background	4
1.5.	The complete Smart Grid threat taxonomy	6
1.6.	Threats to the total Smart Grid system	7
1.7.	Threats to the Smart Grid Components set I	8
1.8.	Threats to the Smart Grid Components set II	9
1.9.	Attack vectors / attack avenues	9
1.10.	References	11
1.11.	Team	4
Annex I – Threat taxonomy for Smart Grids (additional to current)		12
Annex II – Threats to Components Set I (bulk – transmission – distribution)		17
Annex III – Threats to Components Set II (consumers/prosumers – distribution – distributed generation)		22

1. Introduction

This work package contains extensive threat taxonomy for Smart Grids. Pruned versions of the threat taxonomy are presented for each of the Smart Grid Components sets I and II (as identified in WP1.1). Some initial thoughts are presented on attack avenues. As the intended result needs to be unclassified, details of attack avenues are not presented here. A number of policy and research challenges have been identified by this team.

1.1. Mission, vision and goals

In order to be aware of the various threats that are relevant to Smart Grids, the team designed an *all hazards* threat taxonomy taking into account threats that may harm Smart Grid stakeholders. The analysis and weighting of these threats makes it easier to determine how measures can be taken in order to mitigate the overall risk of Smart Grid operations *across service-chains* of *multiple organisations* which may even be competitors.

In consistency with the overall mission of the Expert Group, the WP 1.2 objective is to address all actors involved in providing a reliable energy service with a taxonomy of threats that need to be considered when developing and deploying Smart Grid infrastructures in the European Union.

This threat identification step encompasses both the information and the infrastructure dimensions of Smart Grids and comprises (1) threats to the confidentiality, availability and integrity of data in the system, (2) threats to the resilience, security and proper use of the infrastructure as a whole, (3) threats to the environment of Smart Grid operations, and (4) inter-organisational related threats.

1.2. Strategy

Strategic tasking. The team was tasked to research which threat taxonomies are already available and to assess to which extend these taxonomies would hold specifically for Smart Grid security.

The team was also tasked to identify key deliberate attack avenues and scenarios, encompassing the full palette for example from individual fraud attempts to large scale attacks against the Smart Grid infrastructure.

Understanding. The team task takes the WP1.1 results as input; the output of WP1.2 will be used to assess risk and to create a list of identified policy and technical challenges.

As the threat landscape for Smart Grids may evolve, the WP1.2 deliverable is developed in a way which allows the re-use of the approach, both by the EU, Member States and other stakeholders.

Caveat. Given its short lifetime and limited, voluntary resources, and dependency on the WP 1.1 developments and results, the team came to the conclusion that the completion of the first task was feasible and that the second task effort exceeds by far what decently may be expected by the Commission from unsponsored work. Such an effort anyway requires a clear EU view on how to balance the all hazard risk with the hostile intent avenues. Moreover, an elaboration on attack avenues requires a discussion on the *required information security classification* of the attack avenue analysis results.

1.3. Scope

The overall scope of the work of the Expert Group is the security and resilience of communication and information systems that determine the performance of the physical - Smart Grid enhanced - energy infrastructure in the end.

Given (1) existing threat analysis and mitigation methods in daily use at power grid operators, and (2) time constraints, the WP 1.2 team focused its work on **threats**¹ that may harm the resilience and reliability of energy grids **by the addition of Smart Grid hardware, software, services and operations.**

Note: as part of a balanced risk analysis, operators need to consider their current sets of threats and augment them with the threats to the new Smart Grid operations, services and components.

1.4. Team

Team leader:

- Eric Luijff, TNO, The Netherlands.

M.Sc. in Mathematics at the Technical University Delft in 1975. Officer in the Royal Netherlands Navy for his duties. He joined the TNO end of 1977. Since 1995, he works as Principal Consultant Information Operations and Critical (Information) Infrastructure Protection (C(I)IP). He supports the Dutch Government on policy and technology related issues regarding C(I)IP, Cyber Operations and National Risk Assessment. He has been involved in many national and EU studies on C(I)IP including VITA, IRRIS, DIESIS, EURACOM, and RECIPE. Eric maintains a unique database on CI disruptions, cascading effects and consequences based upon public sources. Eric is part-time employed by the Dutch Centre for Protection of National Infrastructure (CPNI.NL) as ICS and Smart Grid security expert. His SCADA Good Practices book has been translated into English, Japanese and Italian. Eric has been interviewed many times by national and international press, radio and TV, and has published many popular articles, reports, and scientific publications.

Team members:

- Elyoenai Egozcue, S21sec, Spain.

M.Sc. in Telecommunications Engineer from the UPNA University of Pamplona, Spain. Master Thesis on the study of integrated QoS in IP over WDM networks at the VUB University of Brussels, Belgium. Security researcher at S21sec Labs since 2006 on RFID, MPLS and biometrics. From 2008 to 2011, technical manager of various research projects at national and European level, dealing with digital security of control systems used in Critical Infrastructures. Visible head of S21sec for the 7th Framework Programme's INSPIRE project. Since 2011, project manager of several R&D and customer-oriented projects on ICS/SCADA and Smart Grid security. These projects include technical consultancy and assessments as well as compliance consultancy on nuclear power plants, gas and electricity distribution and advanced metering infrastructures. Additionally, Elyoenai Egozcue has been in charge of leading two key projects on ICS and Smart Grid Security in Europe commissioned to S21sec by the European Network and Information Security Agency (ENISA).

1.5. Background

A large number of actors – many of them being competitors - have to assure the power grid balance in a dynamically changing physical grid with a wide variety of power generators (Micro Power Producers (MPP), Independent Power Producers (IPP) and bulk generation), a higher dynamics of load due to intelligent appliances while providing more reliable services, higher efficiency, less CO₂ against lower costs (e.g., see EU's 20/20/20 objectives [EC2020]). Considering the unbundled liberalised energy market in Europe, the fully fletched energy Smart Grid comprises the following actors:

- end-users: consumers and businesses with dynamic load request through smart appliances and electric vehicle power storage,
- prosumers: consumers and businesses with micro-power production (MPP) or combined heat-power abilities which may dynamically trade produced power and supply it to the grid,
- distribution system operators (DSO),
- independent power producers (IPP), e.g., renewables, small wind power production,
- transmission system operators (TSO),
- bulk generation and 'bulk' renewables (e.g., wind farm) operators,
- market operators and shippers (various kinds),
- energy (power, gas, CO₂ rights) exchanges (spot market).

¹ Any entity, action, or occurrence, whether natural or man-made, that has or indicates the potential to pose violence or danger to life, information, operations, environment, economy, operations, property, social stability and coherence, functioning of government and society, and/or territorial security.

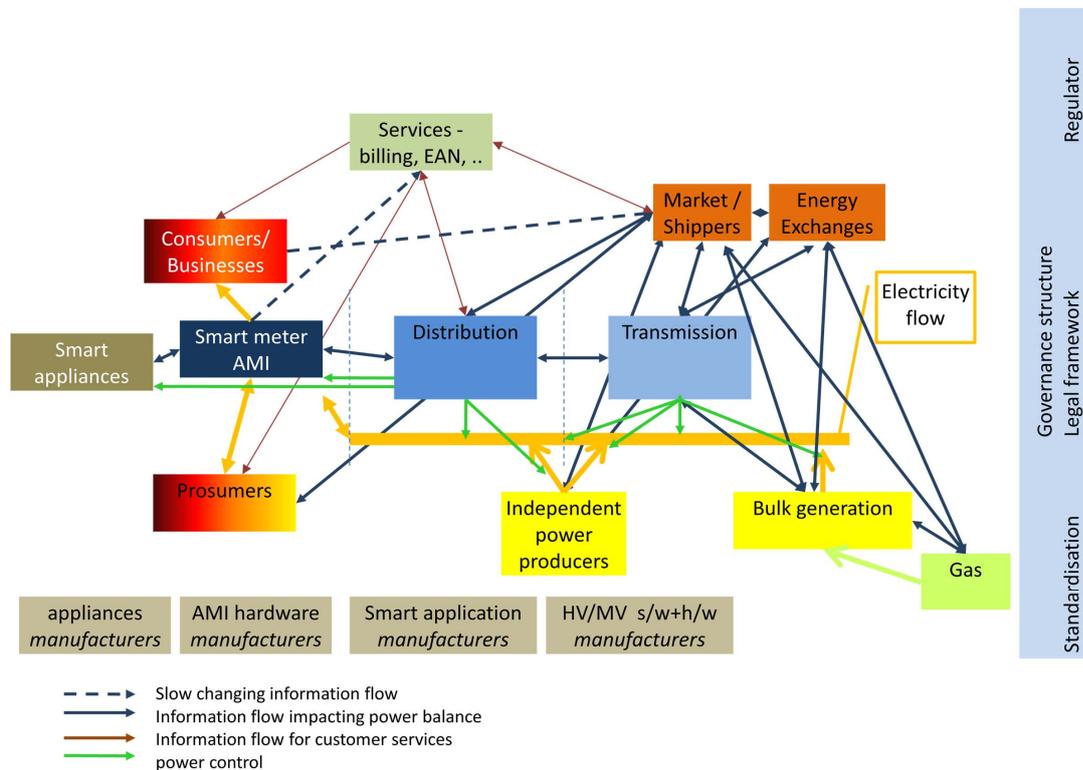


Figure 1: Overview of Smart Grid actors (source: TNO, 2012)

Apart from these actors directly involved in maintaining the balance between load and supply of the total energy grid and securing the physical energy flow, other parties are involved in the energy provisioning chain:

- third party service providers: meter operator, billing, financial services for loading/unloading electric vehicle batteries, and weather information services,
- secondary market operators (e.g., CO₂, steam),
- Smart Grid equipment manufacturers,
- Smart Grid operations, planning and optimisation application providers (Central Management Systems),
- Smart Grid (information) services application providers (for end users, MPP, IPP, ...),
- third party provided information and communication technology (ICT) services, e.g. certificate providers/trustees.

Another set of stakeholders is involved in the dynamics of the Smart Grid developments and operation: the legislator(s) and the regulator(s) at various levels (EU, Member State, ...). And last, not but least, the manufacturers and system integrators which provide smart appliances (home environment), Smart Grid components, Advanced Metering Infrastructure (AMI) components, and Smart Grid service software.

Comparing the Smart Grid understanding in the USA with EU's main Smart Grid objectives, we observe major differences. Most nations in Europe have a very reliable power supply (see Figure 2). An average outage in the range of twenty to thirty minutes/year per customer and an average duration of one and a half hours of a disruption is not uncommon. In the USA and Canada, no (recent) public figures of average power outage duration per customer are available. Outages of multiple days and multiple times per year per customer occur. In the USA Smart Grids shall help to resolve this grid unreliability problem where Europe is focussing on the 20-20-20 goals:

- coping with the massive introduction and use of electric vehicles,
- introduction of smart energy appliances at home,
- a major shift in generation to local generated power, e.g., solar panels, and wind power,
- a major shift in generation, such as wind farms and renewable energy sources.

Threats to the fully fledged smart energy grid system may harm a single actor directly, but also may stem from or passed on by an upstream service provider or a downstream customer/prosumer (or his/hers appliances).

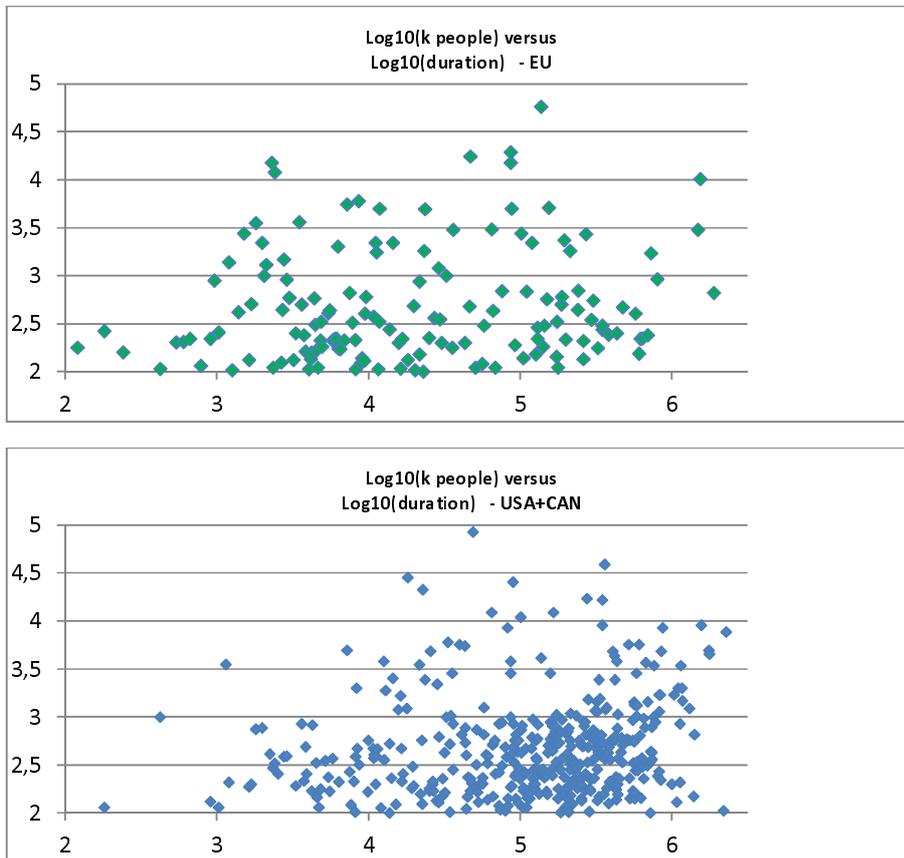


Figure 2: Power outage duration (horizontal) versus number of people affected (vertical)
[source: TNO, status 13-1-2012]

	2	3	4	5	6	7
Duration	2 min	20 min	3 hours	1.25 days	11.5 days	4 months
# of people	100.000	1 million	10 million	100 million		

1.6. The complete Smart Grid threat taxonomy

The planned approach was to research which threat taxonomies are already available and to assess to which extend these taxonomies would hold specifically for Smart Grid security. The team first turned to the results of the EU PASR²-sponsored Vital Infrastructure Threats and Assurance (VITA) project. That study came to the conclusion that there is a lack of threat taxonomies for critical infrastructures such as Smart Grids which cover the all hazards spectrum. For that reason, the VITA project developed its own Extensible Threat Taxonomy for critical infrastructures. A full description of the method can be found in [Luijff2008] and [Luijff2006].

A short scan by the team did not reveal other threat taxonomies which could be of use. All other threat list developments found had a limited scope or came from a limited outlook. Therefore, the team decided to build its work on the aforementioned work of the VITA consortium and target and augment the results for the

² PASR = Preparatory Action on Security Research

specifics of the Smart Grid domain. In its tasking, the team was asked to consider the work done by other EU groups such as the SGIS which uses a set of threats and use cases.³

A quick scan of the materials of the SGIS (received mid of January 2012) revealed some essential differences:

- The SGIS discusses sabotage and terror as threats; VITA provides the arguments that this is wrong. One should consider the base threats. The human intent should be considered as a totally different level on top of the set of threats. The human intent is about probability, not the how.
- The SGIS approach mainly covers the Smart Grid area identified by WP 1.1 as Components Set I. The Smart Grid Components set II assets and the threats to it are hardly covered.
- Finally, the VITA threat taxonomy is one of the most extensive taxonomies for critical infrastructures that exists. To make the list usable, an intelligent grouping into sets of threats has to take place. Nevertheless, it is obvious that the current SGIS approach misses *essential* threats to the Smart Grid value chain given its focus on existing and to be augmented standards.

In short, the VITA threat taxonomy makes a sharp split between threats, threat cause categories (nature, human, or both), and human intent. The VITA approach makes clear that **activism, sabotage and terror are not threats**. They just are an expression of human **intent using an existing threat** (or combination of existing threats). For example, the potential threat of snow causing an avalanche may be initiated by too much sun shine (nature), a stupid human (skiing at the wrong spot), intentionally by mountain safety troops launching a grenade, and a terrorist setting the avalanche off using a shoulder-fired rocket. The differences here are the intent and probability, but it is still the same threat!

The VITA approach therefore uses a three level approach: the first layer comprises all hazards organised in a taxonomy tree. The next layer analyses whether a hazard is just a natural phenomena which cannot be initiated by human influences (e.g., a storm), is a threat which exists only because humans created it (e.g., a technical threat), or is a threat that can be triggered both by natural and human influence causes (e.g., an earth quake, avalanche). The third and EU classified layer of the threat taxonomy shows which hazards can be used by humans with the intent to harm society, more specific: radicalising activists, terrorists, and rogue nation state actors.

Moreover, the VITA extensible threat taxonomy includes both threats with an instantaneous effect, and those which describe slow and very slow threat processes. It also covers those threats that have a very visible high incidence rate and those that have a very low probability and occurrence rate and which are often neglected due to that fact. The current 2012 (copyrighted) version of the earlier VITA threat taxonomy to critical infrastructures organises a set of over 440 threats.

The team started with that list, and given its task and scope, an initial pruning of this extensive set of all hazard threats took place. During the pruning, we removed all the threats to the energy grids covered by current operations **and which are not amplified by the addition of Smart Grids organisation, services and components**. Then some specific threats for Smart Grids which were not captured yet by the VITA threat taxonomy were added. These additions stem from the threat taxonomy of the European Research Network on CIP in Annex 2 of [ERN2010] and input by the S21sec company. Then the threat taxonomy with 132 *additional* threats to the total energy system due to the *smart-gridisation* of the energy grid was drawn (Annex I).

1.7. Threats to the total Smart Grid system

The WP 1.1 team has identified two Components sets making up Smart Grids in relation to Figure 1: set I related to the regulated high voltage grids of TSO, DSO, and bulk generation, and set II related to DSO, local power production (IPP and prosumers), end-users, AMI, smart appliances, and electric vehicles.

However, before looking at the threats to assets that are part of the Components sets I and II in relation with *specific stakeholders*, we have to consider threats to the whole grid. As European Smart Grids in the end comprise up to hundreds or thousands energy suppliers, transmitters and distributors, millions of customers/prosumers and millions of smart appliances, electric vehicles, etceteras which *together* operate in the end the energy value-chains, also the (1) deliberate and (2) common mode failure threats to the multi-stakeholder value-chains need to be recognised. An example of (1) is the Western U.S. Energy Crisis of 2000

³ Subject Expert Group 1 (2011) ICT security and resilience of Smart Grids: High Level Risk Analysis and Security Requirements

and 2001 where competing companies created a power demand supply gap with brownouts as a result. Therefore, Europe has to govern the total Smart Grid chain threats. The following threat challenges stand out:

Threat challenge 1: The subset of ICT-related threats dealing with the manipulation and disruption of the inter-organisational Smart Grid information chain that governs power supply.

Threat challenge 2: The subset of ICT-related threats dealing with the manipulation and disruption of the inter-organisational Smart Grid information chain that governs power demand.

Threat challenge 3: The subset of ICT-related threats dealing with the manipulation and disruption of the inter-organisational Smart Grid information chain balances power demand and supply at the various power grid levels.

Threat challenge 4: Earlier Smart Grid investments by a stakeholder could be of no or limited value due to the appearance of disruptive technology.

Threat challenge 5: Bulk generation, power transmission and distribution companies are used to slowly changing technology and long economic depreciation cycles, thirty to forty years are not uncommon. On the other hand, ICT has short technology aging cycles. The move to smart energy grids will require the aforementioned organisations to change their investment and depreciation cycles as well as incurring costs for continual ICT updates.

Threat challenge 6: The subset of ICT-related threats which may disrupt components that are deployed in massive rollouts, e.g. smart meters, smart appliances, electric vehicles. Crisis management of Smart Grid stakeholders need to be prepared for fast update cycles at hundred thousands to millions of customer and prosumer sites and/or pieces of equipment after the appearance of a vulnerability. When not mitigated in time, a vulnerability in such a component may cause criminals, activists or even terrorists to take control over (parts of) the ICT-side of the Smart Grid.

Threat challenge 7: Earlier Smart Grid investments could be of no or limited value due to adverse laws and ruling by EU, Member States or Regulators (e.g., export license control, privacy-related ruling not supported by hardware).

1.8. Threats to the Smart Grid Components set I

The Smart Grid Components set I comprises the assets related to the Security Guidelines from the EU as identified by WP 1.1. Annex II shows the resulting set of threats relevant to the Smart Grid Components set I. The Annex II threat set is derived from the extensive set of threats discussed above (Annex I) and comprises 100 threats. These threats obviously can be grouped in subsets that can e.g., be mitigated by product development, grid design and deployment; maintenance; organisational measures; education and training of personnel; etceteras.

Threat challenge 8 comprises the following non-exhaustive list of subsets of threats that may affect the Components set I assets:

1. Natural and environment threats to the Smart Grid equipment and cabling during its deployment in the field and technical locations (humidity, heat, cold, flooding, electromagnetic influencing including GIC, lightning, storm, earth movements, animals, fire, etc.). It is envisioned that the majority of equipment and cabling will be located in the field or in nearby 'huts', therefore a common mode failure of both the ICT-layer and the power supply chain in Smart Energy grids may occur.
2. Physical damage to key Smart Grid equipment (collateral damage, deliberate attacks).
3. Human factor aspects (e.g., insufficient information-security training and awareness of personnel, unavailability of key personnel).
4. Inappropriate algorithms, quality of software, information exchange and software services which control the energy grid supply and demand resources.

5. Maintenance related threats (patching, hardware replacement, etc.).
6. Dependency threats due to the use of (public) telecommunications in controlling the grid, Smart Grid equipment which requires electric power, and GNSS timing.
7. Improper information from weather services, e.g. due to manipulation of expected temperatures and wind strength.
8. Lack of black start ability for both the energy and the ICT-sides of a Smart Grid.

1.9. Threats to the Smart Grid Components set II

The Smart Grid Components set II comprises the assets related to the Security Guidelines which can be established by the individual control areas as identified by WP 1.1. Annex III shows the resulting set of threats relevant to the Smart Grid Components set II. The Annex III threat set is derived from the extensive set of threats discussed above (Annex I) and comprises 111 threats. As discussed above, these threats can be grouped in sets that can e.g., be mitigated by product development, grid design and deployment; maintenance; organisational measures; education and training of personnel; etceteras.

Threat challenge 9 comprises the following non-exhaustive following subsets of threats that may affect the Components set II assets:

1. Technology-Related Anger / non-acceptance of Smart Grid functionality and technology by consumers/prosumers.
2. Natural and environment threats to the Smart Grid equipment and cabling during its deployment in the field and technical locations (humidity, heat, cold, flooding, electromagnetic influencing, lightning, storm, earth movements, animals, etc.).
3. Product and value-added services related threats (large-scale counterfeiting of hardware, software vulnerabilities, maintenance / patching issues, drained battery-power, etc.), especially when dealing with mass-market equipment (Electric Vehicles, smart appliances, smart metering).
4. Threats to Smart grid components stemming from environmental factors at households, buildings, and factories (humidity, electromagnetic interference, signal jamming, etc.).
5. Maintenance related threats (patching, hardware replacement, etc.).
6. Inappropriate algorithms, quality of software, information exchange and software services which control the energy grid supply and demand resources.
7. Dependency threats due to the use of (public) telecommunications in controlling the grid and Smart Grid equipment which requires electric power.
8. The deliberate disruption of financial services causing Electric Vehicles being unable to buy power to load their batteries or to deliver (sell) power from the batteries to the local grid.

1.10. Attack vectors / attack avenues

The identified sets of threats to the Smart Grid as a total and the specific Components sets I and II show that there is a manifold of opportunities to deliberately affect the functioning of Smart Grids. Risk analysis should consider the likelihood of **specific actor** types having **the opportunity** to **exploit vulnerabilities** of Smart

Grids by **effectuating a certain threat** to a **certain (set of) deployed Smart Grid component(s) or asset(s)** using a **certain motivation** and the **availability of means**, or:

Probability (deliberate attack avenue) =

$$F(\text{actor type, opportunity, vulnerability, threat, asset, attacker motivation, availability of means})$$

Actor types (non-exhaustive list):

- Individuals (script kiddies, hacker, loosely collaborating set of hackers);
- Energy market actor (financial or market gain-oriented);
- Activist group (e.g., Anonymous, Gridprivacy);
- Organised crime;
- Terrorist individual or group;
- Rogue state-affiliated activities (cyber espionage, cyber conflict, cyber war).

Opportunity comprises elements like:

- Time (e.g., observation/information collection, attack development, time to mount the attack);
- Place (if physical or electromagnetic);
- Access (physical, connectivity, delayed);
- Bandwidth.

Vulnerability (expression of threat possible) in for instance:

- Demand – supply chain of organisations;
- Manufacturer chain of production;
- 3rd party service (design, installation, maintenance);
- 3rd party ICT-based services (e.g., PKI, financial services; billing services);
- Dependent (critical) services;
- Individual employee;
- Group of employees;
- Processes;
- Technical component (e.g., hardware, software, firmware, network);
- Object environment.

Threats: see previous Sections (and Appendices I - III)

Potential target assets comprise for instance:

- A single technical component;
- Set of same components;
- Substations;
- Related infrastructure (buildings, hut, cabling);
- Antenna locations;
- 3rd party services;
- Interorganisational processes;
- Cross-organisations processes.

Attacker motivation comprises elements like:

- Conviction (political, religious);
- Money gain (booty, reward);
- Individual under coercion, duress, blackmail;
- Low risk (of being caught, of penal punishment);
- Personal satisfaction (intellectual challenge, technical curiosity, fun, grieve/revenge);
- Objectives of its State or organisation.

Availability of means comprises:

- Money;
- Weapons, explosives, chemicals, etc.;
- Hardware tools / equipment;
- Software tools;

- Knowledge (e.g., documentation, configuration information);
- Access to specimens of targeted equipment, systems, software, etceteras;
- Specific skills (technical, social engineering, ...);
- Man & female power.

Scenarios and so-called ‘use cases’ may help to find and rank attack avenues that relate the function elements above in relation to the (potential) impact. However, any risk mitigation need to be balanced with the risk factors stemming from the all hazard threats.

Some highly-visible examples of attacks to Smart Grids from the threats and actors identified above:

- Deliberate energy market manipulation by changing Smart Grid information about the power demand or supply in a stressed market.
- A physical and/or cyber attack on a (small set of) single-point-of-failure Smart Grid component(s).
- Technology Related Anger (TRA) of Smart Grids amplified by a very active (set of) individual(s), e.g. peoples sending tweets like ‘Smart Grid equipment radiation is deadly’, while lacking a convincing mitigation strategy.
- Organised crime manipulating larger sets of consumer premises Smart Grid components or at the data concentrators, e.g. turning a large set of smart appliances off.
- Fraudulent information about demand or supply causing automatic measures taken which try to deal with non-existing power flows. Result may be a blackout and/or high financial losses.
- The AMI being an entrance point to the Smart Grid network for hackers/criminals.
- Privacy-related information in Smart Grid components / (wireless) network links of Smart Grids that is used by criminals or hackers to create reputation loss of one or more stakeholders or even TRA and/or massive technology-related distrust by citizens.

1.11. References

- [EC2020] EC Climate and Energy Package 2020, http://ec.europa.eu/clima/policies/package/index_en.htm
- [ERN2010] ERN-CIP Analysis of Needs & Requirements from the Member States, prepared by the ERN-CIP Task Force, JRC Ispra, Italy.
- [Luijff2008] Luijff, H.A.M., Nieuwenhuijs, A.H. (2008) “*Extensible Threat Taxonomy for Critical Infrastructures*”, *Int’l Journal on Critical Infrastructures*, Int’l J. Critical Infrastructures, Vol. 4, No. 4, pp.409-417.
- [Luijff2006] Luijff H.A.M., *Threat Taxonomy for Critical Infrastructures and Critical Infrastructure Risk Aspects at EU-level*, EU VITA project Deliverables D1.1 and D1.2, July 2006.

Annex I – Threat taxonomy for Smart Grids (additional to current)

Critical infrastructure threat taxonomy - Threat cause classification - subset for Smart Grid

Base method ©TNO, VTA consortium 2005 - 2013

17-02-2012

Nature only
Human and Nature
Human only

THREATS	Nature/Natural	Earth	Air	Water	Natural radiation and natural EM-effects "ether"	Fire (Nature)	Biological	
		- Earthquake	- Kinetic energy release					- e.g. the shock waves
		- Landslide / rockfall	- Landslide / rockfall					
		- Ground settlement						- e.g. affecting cables weeks after flooding/heavy rain
		- Volcanic	- Various physical effects					
		- Wind (too much)	- Hurricane/major storm					
		- Air temperature	- Cold wave					
			- Heat wave					
		- Snow	- Various physical effects					
			- Avalanche					
		- Water (liquid form)	- Physical force					
			- Flooding / wetness					
		- Humidity	- too low humidity					- e.g. nature but also due to failing airco system
			- too high humidity					
		- Electro-magnetic	- Electro-magnetic discharge	- cloud-to-ground lightning				- e.g. EM, fire starter and air expansion impacts
				- cloud-to-cloud				- e.g. EM-impact on radiowave transmissions
			- Radiation	- Geomagnetic induced currents (GIC)				- after solar flare/flame burst / CME event
		- Smoke						
		- Physical disintegration						- e.g. soot particles from major forest fires
		- Vegetation, forest						- Nature in conflict with human infrastructure e.g. fallen tree
		- Animals						- every type of animal that gnaws, chases, bites, flies, crawls, makes love

Human induced	Environment	- Spill/loss/instability/finding of corrosive, flammable, explosive materials and contamination		- e.g. hazardous goods, fuel, WWII ammunition / bomb	
		- Aerosols / deposits		- e.g. salt or carbon deposits; corrosive aerosols	
	Incorrect produce/ products quality	- Insufficient quality control (organisational)		- e.g. including insufficient testing	
	Economic/ political	Sector(s)	- Bankruptcy of organisation with major market share or critical to chain of services - Strike / labor unrest / industrial action - Bad imago of sector - Blocking access to key assets		- e.g. by chaining people; demonstrations
		Society	- Civil disorder / riots / insurrections		
	Economic	Product	- Large-scale counterfeiting - Large-scale product piracy - Product boycott		- e.g. in certified product market (falsified equipment ICT, airplanes, ...)
		Instable market(s)	- Trading with inside knowledge - Market manipulation (organisational) - Second economy (organised crime; racketeering; fraud)		- e.g. "Mafia"
	Organisational	- Uncontrolled outsourcing critical services		- e.g. causing failed organisations and its services	
		- Unfriendly overtake outsourced services - Relocation of critical services - Lack of (re)investment - Urbanisation (mega cities) - Single-point-of-failure - Too late to adapt to disruptive technology - Too late to replace insecure technology - Broken trust relationship with other organisation/supplier		- e.g. causing slow response - e.g. causing aging infrastructure - e.g. overstressing infrastructure - e.g. utility infrastructure; single duct, single source product/service	
	Legal / national	- Inappropriate or lacking ntl. laws & regulations - Inappropriate or lacking EU laws & regulations		- e.g. block economic development, slow procedures, governance model driving towards instability	
		- Adverse decision taken by government - Politically unacceptable technical solution		- e.g. obligation to turn off all airco systems due to legionella - impact compu - e.g. blocking regulation AFTERWARDS for instance privacy reasons	
	Disruption of material flow	- Unrest exporting country/ region - Logistic organisational failure - Shortage on world market - Legal hindrance		- e.g. logistic problems spare components/materials - e.g. 'red tape' on encryption equipment - e.g. 'red tape' on encryption equipment	

Person(s)	<ul style="list-style-type: none"> - Low attention level - Lapses in attention - Epidemic illness/pandemic - Staff turnover (too fast) - Lack of professional behaviour - Mismanagement / lack of security & safety awareness - Theft 			<ul style="list-style-type: none"> - e.g. overworked, staff shortage, work underload - e.g. overload, task scattering - biological & virus threats to humans - if too much human intervention requi
	Information leakage	<ul style="list-style-type: none"> - Human error - Social engineered attack on victim - Deliberate leakage (inside outwards) - Unintentional leakage - Deliberate leakage (outside to outwards; information theft) 		<ul style="list-style-type: none"> - e.g. staff shortage to run operations - e.g. greed, ethical reasons, extortion, activist reasons - e.g. due to insufficient training; during maintenance - e.g. due to phishing - e.g. disgrintled staff; ethics, activism
	Bad decision-taking	<ul style="list-style-type: none"> - Human error - Insufficient decision information - Manipulated decision information 		<ul style="list-style-type: none"> - e.g. disgrintled staff; ethics, activism
	Psycho - physical	<ul style="list-style-type: none"> - Technology Related Anger (TRA) 		<ul style="list-style-type: none"> - e.g. "smart meters spy on us"
Technical	Force	Dynamic force/ kinetic impact	By man-made means	<ul style="list-style-type: none"> - e.g. shovel, crashing building, excavation
		Temperature	<ul style="list-style-type: none"> - Repeated cycle tireness - Temperature shock 	
		Chemical explosion	explosives	
	Temperature (non-natural cause)	Physical disintegration	<ul style="list-style-type: none"> - Melting - Overheated - Material destruction - Non-natural fire 	<ul style="list-style-type: none"> - e.g. cables, equipment - incl. arson
	Electro-magnetic	<ul style="list-style-type: none"> - Electrostatic discharge - Overvoltage - Undervoltage - Overfrequency - Underfrequency - Jammed frequency(ies)/jamming - Spoofing signals 		<ul style="list-style-type: none"> - e.g. islanding; voltage collapse - e.g. jamming GPS timing signals - e.g. man-in-the-middle over the air
		<ul style="list-style-type: none"> - Electro-Magnetic Pulse (or EMP) 	<ul style="list-style-type: none"> - Non-nuclear - Nuclear 	<ul style="list-style-type: none"> - High Power Microwave (HPM) - High Energy Magnetic Pulse (HEMP) - e.g. high-altitude EMP
	<ul style="list-style-type: none"> - Electro-magnetic Interference (EMI) - Electro-magnetic Compatibility (EMC) failure - Electronic emanations (Van Eck) 		<ul style="list-style-type: none"> - allowing eavesdropping 	

Hardware (out-of-spec behaviour, mechanical failure)	- Material failure	- Property change - Corrosion - Material ageing - Technological ageing	- e.g. due to heat - e.g. of connectors	
	- Loss of hardware		- see other factors like theft, vandalism, ..	
	- Human organisation/ operation	- Lack of maintenance Diminishing manufacturer sources/ material shortages (DMSMS)		
	- Conflict with nature		- see above	
	- Installation /configuration fault			
	- Amplified battery power draining		- MANET nodes, battery powered nodes	
Information and communication technologies	- Software	- Software quality failure - Human organisation/ operation failure - Malware	- Design failure - Development failure - Lack of maintenance - Widespread Trojan horse - Major virus/worm outbreak - Hoax - Backdoor - Time/logic bomb	
	- Hardware	- Falsified/counterfeited/bootlegged hardware - Counterfeited firmware		
	- Communications	- Protocol weakness - Cryptology weakness - Service disruption	- technical/ other reason - (distributed) denial-of-service incl. bandwidth depletion	e.g. weak to man-in-the-middle e.g. weak credentials/certificates e.g. vulnerable for brute-force
	- Information services	- Data security	- Integrity breach - Confidentiality breach - Phishing attack	e.g. hacking e.g. hacking
		- Service unavailability	- dependency failure - many causes - under (distributed) denial-of-service attack	see below
		- Access control error - Loss of trust/confidence in ICT - Loss of trusted third party services (e.g., PKI)	- availability - trustworthiness	major failure/ long exposure other threats

- Lack of critical service (dependency)	- Energy sector	- Power to ICT	- Failed direct power - Failed backup power - Power fluctuations outside specs	- e.g. customer/prosumer - meter/connection service
			- Failed specific third party ICT-services being part of energy sector	
	- Telecommunication Sector	- Failed fixed infrastructure	- technical/human/societal failures (see elsewhere) - loss of building - overload of infrastructure	- e.g., - failed distributed - multitude of causes including major disasters
		- Failed mobile data transfer		
		- Failed satellite services	- GNSS timing signals	- e.g., precise timing failure Smart Grid & mobile infrastructure
	- Information Technology Sector	- Third party services failure		- e.g., DNS, Internet access, backbone services
	- Government services	- Regulator adverse control		
	- Information services	- Weather prediction services		
- Financial Sector (banks, insurances,..)		- Massive financial services failure disrupting Electric Vehicle power loading / unloading		
- Technical environment	- Airco/ HVAC/ access control security			
- Common mode failure		- Multiple service (dependency) failures at same time	- e.g., major ice rain storm, earth quake ...	

Human induced	Environment	- Spill/loss/instability/finding of corrosive, flammable, explosive materials and contamination		- e.g. hazardous goods, fuel, WWII ammunition / bomb	
		- Aerosols / deposits		- e.g. salt or carbon deposits; corrosive aerosols	
	Economic/ political	Sector(s)	- Bankruptcy of organisation with major market share or critical to chain of services - Blocking access to key assets		e.g. MARKET OPERATOR - e.g. by chaining people; demonstrations
		Economic	Instable market(s)	- Trading with inside knowledge	
				- Market manipulation (organisational)	
				- Second economy (organised crime; racketeering; fraud)	- e.g. "Mafia"
		Organisational	- Uncontrolled outsourcing critical services	- e.g. causing failed organisations and its services	
			- Unfriendly overtake outsourced services		
			- Relocation of critical services	- e.g. causing slow response	
			- Lack of (re)investment	- e.g. causing aging infrastructure	
- Urbanisation (mega cities)	- e.g. overstressing infrastructure				
Legal / national	- Single-point-of-failure	- e.g. utility infrastructure; single duct, single source product/service			
	- Too late to adapt to disruptive technology				
	- Too late to replace insecure technology				
	- Broken trust relationship with other organisation/supplier				
Disruption of material flow	- Inappropriate or lacking ntl. laws & regulations	- e.g. block economic development, slow procedures, governance model driving towards instability			
	- Inappropriate or lacking EU laws & regulations				
	- Adverse decision taken by government	- e.g. obligation to turn off all airco systems due to legionella - impact compu			
Person(s)	- Staff turnover (too fast) - Lack of professional behaviour - Mismanagement / lack of security & safety awareness - Theft	- Politically unacceptable technical solution	- e.g. blocking regulation AFTERWARDS for instance privacy reasons		
		- Logistic organisational failure			
		- Shortage on world market	- e.g. 'red tape' on encryption equipment		
Information leakage	- Human error - Social engineered attack on victim - Deliberate leakage (inside outwards) - Unintentional leakage - Deliberate leakage (outside to outwards; information theft)	- Legal hindrance	- e.g. 'red tape' on encryption equipment		
		- Staff turnover (too fast)	- e.g. staff shortage to run operations		
		- Lack of professional behaviour	- e.g. copper cables		
Bad decision-taking	- Human error - Insufficient decision information - Manipulated decision information	- Theft	- e.g. due to insufficient training; during maintenance - e.g. due to phishing - e.g. disgruntled staff; ethics, activism		
		- Information leakage			

Technical	Force	Dynamic force/ kinetic impact	-By man-made means	- e.g. shovel, crashing building, excavation	
			-Chemical explosion	-explosives	
	Temperature (non-natural cause)	-Physical disintegration	Melting	- e.g. cables, equipment	
			-Overheated -Material destruction -Non-natural fire	- incl. arson	
	Electro-magnetic	-Electrostatic discharge -Overvoltage -Undervoltage -Overfrequency -Underfrequency -Jammed frequency(ies)/jamming -Spoofing signals	GPS / LORAN clocks	- e.g. jamming GPS timing signals	
			GPS / LORAN clocks	- e.g. man-in-the-middle over the air	
			-Electro-Magnetic Pulse (or EMP)	- Non-nuclear	- High Power Microwave (HPM) - High Energy Magnetic Pulse (HEMP)
			-Electro-magnetic Interference (EMI) -Electro-magnetic Compatibility (EMC) failure		
	Hardware (out-of-spec behaviour, mechanical failure)	-Material failure	-Corrosion	- e.g. of connectors	
			-Material ageing		
-Technological ageing					
-Loss of hardware			- see other factors like theft, vandalism, ..		
-Human organisation/ operation		-Lack of maintenance			
		Diminishing manufacturer sources/ material shortages (DMSMS)			
	-Installation /configuration fault				

Information and communication technologies	Software	Software quality failure			
		Human organisation/ operation failure	Design failure Development failure Lack of maintenance		
		Malware	Widespread Trojan horse Major virus/worm outbreak Backdoor Time/logic bomb		
	Hardware	Falsified/counterfeited/bootlegged hardware Counterfeited firmware			
		Communications	Protocol weakness Cryptography weakness Service disruption	<i>technical/ other reason</i> (distributed) denial-of-service incl. bandwidth depletion	e.g. weak to man-in-the-middle e.g. weak credentials/certificates e.g. vulnerable for brute-force
	Information services	Data security	Integrity breach		e.g. hacking
			Confidentiality breach		e.g. hacking
		Service unavailability	<i>dependency failure - many causes</i>		<i>see below</i>
			under (distributed) denial-of-service attack		
		Access control error			
Loss of trusted third party services (e.g., PKI)	availability trustworthiness				

- Lack of critical service (dependency)	- Energy sector	- Power to ICT	- Failed direct power - Failed backup power - Power fluctuations outside specs	TO THE SMART GRID
		- Failed specific third party ICT-services being part of energy sector		- e.g. market operations
	- Telecommunication Sector	- Failed fixed infrastructure	- technical/human/societal failures (see elsewhere) - loss of building - overload of infrastructure	- e.g., failed distribution, switching, gateways, backbones
		- Failed satellite services	- GNSS timing signals	- e.g., precise timing failure Smart Grid & mobile infrastructure
	- Information Technology Sector	- Third party services failure		- e.g., DNS, Internet access, backbone services
	- Government services	- Regulator adverse control		
	- Information services	- Weather prediction services		
- Technical environment	- Airco/ HVAC/ access control security			
- Common mode failure	- Multiple service (dependency) failures at same time		e.g., major ice rain storm, earth quake ...	

Annex III – Threats to Components Set II (consumers/prosumers – distribution – distributed generation)

Critical infrastructure threat taxonomy - Threat cause classification - subset for Smart Grid

Base method ©TNO, VITA consortium 2005 - 2013

17-02-2012

Nature only
Human and Nature
Human only

THREATS	Nature/Natural	Earth	Air	Water	Natural radiation and natural EM-effects "ether"	Fire (Nature)	Biological
		<ul style="list-style-type: none"> - Earthquake - Kinetic energy release - e.g. the shock waves - Landslide / rockfall - Landslide / rockfall - Ground settlement - e.g. affecting cables weeks after flooding/heavy rain - Volcanic - Various physical effects 	<ul style="list-style-type: none"> - Air temperature - Cold wave - Heat wave 	<ul style="list-style-type: none"> - Snow - Various physical effects - Water (liquid form) - Physical force - Flooding / wetness - Humidity - too low humidity - <i>ICT equipment is sensitive</i> - e.g. nature but also due to failing airco system - too high humidity - <i>ICT equipment is sensitive</i> 	<ul style="list-style-type: none"> - Electro-magnetic - Electro-magnetic discharge - cloud-to-ground lightning - e.g. EM, fire starter and air expansion impacts - cloud-to-cloud - e.g. EM-impact on radio wave transmissions - Radiation - Geomagnetic induced currents (GIC) - after solar flare/flame burst / CME event 	<ul style="list-style-type: none"> - Smoke - Physical disintegration - e.g. soot particles from major forest fires 	<ul style="list-style-type: none"> - Animals - every type of animal that gnaws, chases, bites, flies, crawls, makes love

Human induced	Environment	Aerosols / deposits		- e.g. salt or carbon deposits; corrosive aerosols	
	Incorrect produce/ products quality	Insufficient quality control (organisational)		- e.g. including insufficient testing	
	Economical/ political	Sector(s)	Bankruptcy of organisation with major market share or critical to chain of services		
		Economic	Product	Large-scale counterfeiting Large-scale product piracy	- e.g. in certified product market (falsified equipment ICT, airplanes, ...)
			Instable market(s)	Trading with inside knowledge Market manipulation (organisational) Second economy (organised crime; racketeering; fraud)	
		Organisational		Uncontrolled outsourcing critical services Unfriendly overtake outsourced services Relocation of critical services Lack of (re)investment Urbanisation (mega cities) Single-point-of-failure Too late to adapt to disruptive technology Too late to replace insecure technology Broken trust relationship with other organisation/supplier	- e.g. causing failed organisations and its services - e.g. causing slow response - e.g. causing aging infrastructure - e.g. overstressing infrastructure - e.g. utility infrastructure; single duct, single source product/service
			Legal / national	Inappropriate or lacking ntl. laws & regulations Inappropriate or lacking EU laws & regulations	- e.g. block economic development, slow procedures, governance model driving towards instability
				Adverse decision taken by government	- e.g. obligation to turn off all airco systems due to legionella - impact compu
				Politically unacceptable technical solution	- e.g. blocking regulation AFTERWARDS for instance privacy reasons
	Disruption of material flow	Logistic organisational failure Shortage on world market Legal hindrance	- e.g. 'red tape' on encryption equipment - e.g. 'red tape' on encryption equipment		
Person(s)	Staff turnover (too fast) Lack of professional behaviour Mismanagement / lack of security & safety awareness Theft		- e.g. staff shortage to run operations - e.g. greed, ethical reasons, extortion, activist reasons		

	- Information leakage	- Human error - Social engineered attack on victim - Deliberate leakage (inside outwards) - Unintentional leakage - Deliberate leakage (outside to outwards; information theft)		- e.g. due to insufficient training; during maintenance - e.g. due to phishing - e.g. disgrintled staff; ethics, activism	
	- Bad decision-taking	- Human error - Insufficient decision information - Manipulated decision information		- e.g. disgrintled staff; ethics, activism	
	- Psycho - physical	- Technology Related Anger (TRA)		- e.g. "smart meters spy on us"	
Technical	Force	Dynamic force/ kinetic impact	- By man-made means	- e.g. shovel, crashing building, excavation	
			- Chemical explosion	- explosives	
	Temperature (non-natural cause)	- Physical disintegration	- Melting - Overheated - Material destruction - Non-natural fire	- e.g. cables, equipment - incl. arson	
	Electro-magnetic	- Electrostatic discharge - Overvoltage - Undervoltage - Overfrequency - Underfrequency - Jammed frequency(ies)/jamming - Spoofing signals			- e.g. jamming GPS timing signals - e.g. man-in-the-middle over the air
		- Electro-Magnetic Pulse	- Non-nuclear	- High Power Microwave (HPM)	
		- Electro-magnetic Interference (EMI) - Electro-magnetic Compatibility (EMC) failure - Electronic emanations (Van Eck)			- allowing eavesdropping
Hardware (out-of-spec behaviour, mechanical failure)	- Material failure	- Corrosion - Material ageing - Technological ageing		- e.g. of connectors	
	- Loss of hardware			- e.g., theft, vandalism, ..	

	- Human organisation/ operation	- Lack of maintenance			
		- Diminishing manufacturer sources/ material shortages (DMSMS)			
	- Conflict with nature			- see above	
	- Installation /configuration fault				
	- Amplified battery power draining			- MANET nodes, battery powered nodes	
Information and communication technologies	- Software	- Software quality failure			
		- Human organisation/ operation failure	- Design failure - Development failure - Lack of maintenance		
		- Malware	- Widespread Trojan horse - Major virus/worm outbreak - Hoax - Backdoor - Time/logic bomb	e.g. at consumer / prosumer level ==> TRA	
	- Hardware	- Falsified/counterfeited/bootlegged hardware - Counterfeited firmware			
	- Communications	- Protocol weakness - Cryptology weakness - Service disruption	- technical/ other reason - (distributed) denial-of-service incl. bandwidth depletion	e.g. weak to man-in-the-middle e.g. weak credentials/certificates e.g. vulnerable for brute-force	
	- Information services	- Data security	- Integrity breach		e.g. hacking
			- Confidentiality breach	- Phishing attack	e.g. hacking e.g. at consumer / prosumer level
		- Service unavailability	- dependency failure - many causes - under (distributed) denial-of-service attack		see below
		- Access control error - Loss of trust/confidence in ICT - Loss of trusted third party services (e.g., PKI)	- availability - trustworthiness		major failure/ long exposure other threats

Lack of critical service (dependency)	Energy sector	- Power to ICT	- Failed direct power - Failed backup power	
			- Failed specific third party ICT-services being part of energy sector	- e.g. customer/prosumer - meter/connection service
	Telecommunication Sector	- Failed fixed infrastructure	- technical/human/societal failures (see elsewhere) - loss of building - overload of infrastructure	- e.g., failed distribution, switching, gateways, backbones
		- Failed mobile data transfer		- multitude of causes including major disasters
		- Failed satellite services	- GNSS timing signals	- e.g., precise timing failure Smart Grid & mobile infrastructure
	Information Technology Sector	- Third party services failure		- e.g., DNS, Internet access, backbone services
	Government services	- Regulator adverse control		
	Financial Sector (banks, insurances,..)		- Massive financial services failure disrupting Electric Vehicle power loading / unloading	
Technical environment		- Airco/ HVAC/ access control security failure		
Common mode failure		- Multiple service (dependency) failures at same time	- e.g., major ice rain storm, earth quake ...	