March 19, 2012

Work Package 1.3

Countermeasure Taxonomy

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

Version 0.99

Table of contents

1. Introduction

1.1. Mission, vision and goals

The goal of this taskforce is to define specific countermeasures against threats to the ICT of Smart Grids and how they can be classified using a taxonomy. Countermeasures against new emerging risks are required to ensure that the Smart Grid operates well and in particular the security of supply is ensured. This includes all ICT components which directly deal with energy for monitoring and control, i.e., Supervisory Control and Data Acquisition (SCADA) Systems including Advanced Metering Infrastructure (AMI) etc. The security of these systems is of paramount importance since successful attacks may directly influence the security of supply. Likewise, the security of ICT components of the Smart Grid which are not dealing directly with energy must be ensured. For example, the ICT for the energy market must also be secured by applying appropriate countermeasures against attacks. Countermeasures depend upon several prerequisites:

1. A clear policy should be in place in which way the SG system is used and which purposes it has to cover.

2. The architecture of the SG system should be defined, as well as the according security requirement specification. Within the architecture appropriate countermeasures, i.e., security mechanisms are implemented. It should be noted that it is not sufficient to simply add security mechanisms to the individual components; i.e., a holistic security architecture considering the whole system is required.

3. For a given system, a risk assessment must be performed to set priorities of the countermeasures under consideration of the security requirement specification – if available. From the countermeasure priorities a security implementations plan should be elaborated.

Having discussed the three scientific prerequisites and knowing that this is the only way to 100% justify the countermeasures, we will cover the given task anyway in a "best fit" manner: the experts know of the changing technology and the caveat of implementing countermeasures: With this knowledge we created high level countermeasure recommendation (proposal for Europe how to address the challenge with political and technical means).

Knowing today's scarcity of IT-security in Smart Grid[1] a review of State-of-the-Art (primary directed to electrical engineering workforce without digital security background) and the identification of commonly agreed and missing principles and measures are good to be presented. Therefore in Chapter 1.7 and in the Annexes selected examples are given how to address the challenge.

Documents like Recommendations for Europe and Member States [ENISA D] did work with budget and on a larger scale. Coverage and level of details is not comparable. However, through the interdisciplinary discussion (Energy and IT-Security) the WP1.3 team could elaborate some new views on the topic (cf. especially Chapter 1.5.5)

As the selected examples demonstrate, there is not one countermeasure, but hundreds of them. In a fine grained risk management process, countermeasures have to be selected under the limitations of available investment fund, such that with least investment the best possible security will be generated.

Also, in some cases pending (IT-)security issues are known for a while, most of these can be resolved with the measures proposed.

The elaborated high level recommendations (cf. Chapter 1.5) should stimulate the grid stakeholder community and policy support to initiate studies for clarifying countermeasure details and the recommendations. For

[1] Control systems are more and more connected to corporate networks – or even to the Internet. Many systems have an interim period with insufficient protection. This statement is valid for grid control systems and smart grid. However, many extremely good solutions were prepared by research for "Smart Grid". But these are not the applied in field applications and are not lived practice all over Europe.

European policy might support these high level recommendation such that a more secure and resilient Smart Grid in Europe will be available to face the new challenges of renewable energy producers and electrical vehicle recharging.

The low level countermeasures (IT-security good practice) are referenced and clarified with some examples. However, do to the limited volunteering effort these references remain incomplete and have more the character of elucidating the pain points.

Another view on Smart Grid security is the perspective of high impact and low frequency (HILF) risks: The European high voltage grid should not break apart: Direct costs are extremely high and indirect costs are even not really to calculate because of the magnitude. Therefore, adding resilience to a secure infrastructure with the target to have an availability of nearly 100% is the right way to go. The level of the resilience against HILF risks is finally a political decision depending on:

- the general views during a given time period: how society perceive risks and is willing to live with risks[2],
- the willingness to agree on service level, or degraded service levels, and
- the ability to invest into security.

Experts – as in this working group - can make proposals which are supported by the community to guide the policy process which is the goal of the WP1.3 document.

WP 1.1[3] is stating that each part of the Smart Grid system which may have impact – directly or indirectly – to 2 GW or more within the European power grid is an **ultimate critical** part of the European energy system. Those parts must not fail, under any condition not depending on a specific risk level: A fail save and self-healing approach is needed. For all other operations, a very high and reasonable protection of **non-ultimate critical** process control (incl. SCADA) infrastructure with an impact less than 2 GW is mainly covered by the corporate security measures[4] and the commercial interest by company owned **Security Control Networks** SCN. The SCN is basically the SCADA and Smart Grid Network as it exists by today – assuming that all good practise measures (see later in this chapter) have been implemented. For the design of the SCN some basic requirements and good practices from companies with advanced Smart Grid security are given later in this chapter (cf. Section 1.7). The SCN is a company owned secure network and is not necessarily harmonized, i.e., using a common standard. Interfaces and gateways are the method to interconnect companies.

WP 1.3 is organised as follows: Chapter 1.1 gives an overview on the topic, Chapter 1.2 describes the strategy, Chapter 1.3 defines in scope and out of scope, which means that selected standards can be discussed and high level recommendation can be created and in Chapter 1.4 the CV of team members are presented.

In Chapter 1.5, the high level recommendations are presented in a management summary, in Chapter 1.6 some background is given, how WP1.3 is based on WP 1.1 and WP 1.2. Chapter 1.7 discusses the background of standards, recommendation and state-of-the-art with selected available sources, but knowing that this is incomplete and many additional sources should be considered as well. Chapter 1.8 lists the most important references to the topic.

The Annexes provide more information for interested experts, and experts which needs more background in the given topic: Annex I presents the OECD Strategy to Smart Grid Security to show the large scope of the topic. In Annex II, cross-organisation and cross-border dependency are reflected; according to recommendations of the Centre for European Policy Studies CEPS. In Annex III, a background for SCADA Security is reproduced for experts who would like to be introduced to the topic. In Annex IV, potential elements of a SCADA Countermeasure Ontology / Taxonomy are given as result of discussions in the team. Finally, Annex V presents a well elaborated approach to classify security countermeasures for Smart Grids which is based on recommendations of the German IT-Security Agency BSI: A good Practice approach.

---

[2] E.g. the Fukushima incident turned in Europe the risk perception of nuclear power.
[3] Please consult WP1.1 of this project.
[4] Corporate Security Measures: These measures provide the security for a given corporation, aligned with the corporation security needs and the corporations will for prosperity and survival.

1.2. Strategy

Approach: The approach would be to study which other taxonomies in the field of countermeasures to threats are already available and to assess to which extend these taxonomies would hold specifically for Smart Grid security.

Caveat: Given its short lifetime and limited, voluntary resources, and dependency on the WP 1.1 and WP 1.2 developments and results, the team came to the conclusion that the completion of the attempted task has to focus on specific issues, which differ from the State-of-the-Art and international publications:

- Therefore a section State-of-the-Art and international background was elaborated to connect to these standards.
- Classification of the efficacy of the countermeasures: This is not appropriate, because the orchestration of the countermeasure (or combined set of countermeasures) is as important as the quality and efficacy of each single countermeasure. (There is no reference architecture available by now.)
- In real projects - with a given SCADA architecture - countermeasures should base on risk assessment, which is not available by now. However, high level countermeasures that serve as input to the policy document that the Commission is drafting and for stakeholders to have a sort of guidance can be identified by the team members in a broad discussion with industry delegates.

The effort to cover the caveat exceeds the current unsponsored efforts. But it would be of utmost importance to develop a balanced and coordinated understanding in the EU for the countermeasure efficacy.

1.3. Scope

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

Given WP1.1 identification of European critical risk, threat and vulnerabilities and the "threat and attack taxonomy" elaborated in WP 1.2 we focus our working WP 1.3 on c**ountermeasures** to improve and reach resilience and reliability of energy grids and how these countermeasures can be classified using taxonomy. We focus on three working domains: (1) General known good practise in coverage of information, (2) IT-security, good practices of DSO and TSO, and (3) recommendation for actions which should be initiated and supported by the commission. A life cycle approach – as used in other studies - will be summarised to complement the measures.

Results / Deliverables

1. Mandatory part of the document: Mission, Strategy, Scope Team.
2. Recommendation for actions: The focus emphasis specific and up to now not everywhere implemented countermeasures for Smart Grid.
3. Good practices of DSO and TSO
4. General known good practise in coverage of information and IT-security
5. References to similar work in US and OECD, good practise and standards.

To be considered, but not covered in this document:

- The human aspects in detail and the awareness level are of utmost importance for the security level, i.e., the security awareness level of the workforce, the skill mix, and long term security behaviour.
- Classification of the efficacy of the countermeasures: Even so efficacy of countermeasures is very important for this group the size for such a project exceeds by far volunteering groups capacity.

Countermeasures provide resilience in several dimensions: availability, resistance against attacks (e.g., DOS and DDoS, integrity, confidentiality, authenticity attribution (forensics capabilities) fake ID).

- Cross organisational aspects in detail are issues between producer and consumer, harmonisation of the control/ production between competing TSO and producer.

Elaborating in-depth (more than in Chapter 1.5.3) the (cross-) organisational and cross boarder aspects have to be postponed in separate projects and the human aspects and awareness issues are fully addressed in awareness and education WP.

1.4. Team

Team leader:

- Bernhard Haemmerli Acris GmbH is CEO Acris GmbH and professor for Networking and Information Security at University of applied Science Lucerne, Switzerland and University Collage Gjovik, Norway. His main interest in research is information security and CIIP (Critical Information Infrastructure Protection). He has participated in three EU FP CIIP research program the last on is Protection and Trust in Financial Infrastructures www.parsifal-project.eu. He is editor of the European CIIP Newsletter called ECN www.irriis.eu. He is president of the Swiss Informatics Society and chair of "scientific and international affairs" in the Information Security Society Switzerland ISSS. In 2007 he was assigned as seconded national expert on Critical Infrastructure Protection CIP from Switzerland to Joint Research Centre of the European Commission. He is now chairing the Critical Infrastructure Protection CIP task force at the Centre for European Policy Studies CEPS in Brussels www.ceps.be . In consulting his corporation Acris GmbH offers service in the same field.

Team members:

- Eric Luiijf, 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, IRRIIS, 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.

- Eric van Aken, Alliander, The Netherlands, Bachelor of Engineering degree in engineering and telecommunication since 1997, after completing basic and medium engineering education and duty. Since 2007 he works now as a Consultant at Liandon (an Alliander company), holds 15 years of experience with various companies in communications and utilities industries. He was involved in several projects among which - Alliander telecom vision, Enterprise fiber network, interaction with DG Infso on Utility-Telco cooperation on EU goals, CCTV Fiber project for Dutch railway "Betuweroute", Report about future alternatives in relation to installed tone frequency communication solutions, report on communication aspects of the smart meter, active member of the European Utilities Telecom Council.
  Topics of expertise are: Smart grid communication, Substation Automation Communication, Process Control Security, ISO 9001 Auditing.

- Claudia Eckert: Professor Dr. Claudia Eckert is director of the Fraunhofer Research Institution for Applied and Integrated Security AISEC (www.aisec.fraunhofer.de) and professor at the Technische Universität München (TUM) where she holds the Chair of the IT Security Department. As a member of various national and international industrial and scientific advisory committees she advises companies, trade associations and public authorities in all aspects of IT security. As a member of expert committees she is involved in the

design of the technical and scientific environment in Germany and in the design of scientific programs on EU and NATO level.

- Christoph Krauß: Dr. Christoph Krauß is head of the department Innovation and Strategy at Fraunhofer Research Institution for Applied and Integrated Security AISEC. He is responsible for planning strategic directions of the institute, identifying innovative research topics, and executing initial research projects. Furthermore, he coordinates the research topic "Smart Grid Security". Before joining Fraunhofer, he studied computer science at TU-Darmstadt where he received his diploma in 2004. Between 2004 and 2009 he was a research assistant in the research group IT-Security at TU-Darmstadt where he did his PhD in the area of security in wireless sensor networks.

- Bernard Hourtané: Bernard Hourtané, EDF Research and Development, Director of the program on Distribution networks. Dipl. Engineer in Electricity and Industrial Computing, he has more than 20 years of experience in Distribution networks on many aspects : operations on MV/LV networks, HV/MV substations, metering, remote control and telecommunications, human resources, purchase, supply chain, IS projects management. He is a lecturer at the École Centrale of Lille on the challenges of a smarter power system.

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

- ENISA staff has contributed to the review. We thank Dr. Evangelos Ouzunis, Konstantinos Moulinos and Rafal Leszczyna for their support.

1.5. Recommendations

1.5.1. Self-assessment methodology for SG cyber security

Cyber security is – for a few electrical grid domains - a completely new and often not sufficiently covered topic in EU. Other electrical grid domains have paid attention and are more developed. A well-defined self-assessment guide for the ICT security experts in SCADA and Smart Grid enables each Smart Grid stakeholder to identify potential risk and to assess vulnerabilities. The results can be used as health check to define countermeasures and to reapprove security specifications. Also in long term it would be desirable that the stakeholder would agree on minimum standards.

1.5.2. Promote application and adaption to Smart Grid of well-established ICT Security good practices

Information security and ICT-security is a well elaborated field in research and in practical solutions. This is especially true for corporate information systems. For Industrial Control, Systems (ICS) there are the real time and 24/7 operation requirements, which need extra measures. Until recently ICS were not internetworked with the Internet and interconnected widely. For maintenance, efficiency, and monitoring purposes, ICS are connected to the corporate networks which often have several interconnections – either open declared or hidden – to public networks. As background is the explanation of ICS security topic in [Franc 2012] reproduced in Annex III. More can be found in the CPNI.NL SCADA Security booklet [Luiijf2010].

We distinguish two categories of critical infrastructure against the background of dependability analysis. Notice: Crises start always local and spread out. But there are components, which can cause an European wide blackout, and others which have not this potential:

1. Smart Grid controlled **general critical infrastructure** which has large impact on local society, on revenue of local companies, on local economy, but will not crash major parts of the European or national Grid.

2. Smart Grid controlled **ultimate critical infrastructure** which could harm or crash the European Grid or major parts of it.

The general critical infrastructure stated in point 1 should be controlled through the Security Control Network (SCN). SCN is designed on existing standards, e.g., BSI, NIST, NERC, or according the lines of good practices, e.g., OECD, SABSA (see Chapter 1.7) covering all requested domains. Please note that this list of standards and practices just illustrate some examples and is not complete.

The number of connections in the grid control network is still really large and the potentially dangerous connections to public telecommunication networks cannot be completely excluded, even when it is a DSO / TSO owned network with wireless connectivity[5].

Security measures recommended in the above standards reflect good practices and should be applied in any case. Below we give some issues from the standards, incomplete and not replacing in-depth studies as, e.g., [ENISA 2012 A...D] and similar qualified work. The selected issues demonstrate the most important challenges which must be addressed.

- Apply availability, integrity, and confidentiality mechanisms for the ICS. This includes but is not limited to:
  - Device Protection (Firewall, Anti-Virus, Anti Malware (Trojan Horses etc.), Anti Sabotage, Anti Covert Channels, physical protection of nodes (e.g., Smart Meters), digital manipulation protection including reading of cryptographic keys, application of hardware security modules etc.
  - Update capability for the device
  - Proper physical protection,
  - Regular Penetration Test
  - Social Engineering and Physical tests
  - Secure ID for each node
  - Security by Design and Security during operation
  - Defence-in depth (multiple level and nested security countermeasures)

  However, it is utmost important to develop a balanced and coordinated understanding in the EU for the countermeasures and their efficacy in a separate project.

- Apply zoning concepts for security on all layers: physical (buildings), digital (network zones), and human (certification for physical and digital access): Provide according policies, awareness programs, and training programs which are mandatory for each additional zone.
  Be especially security aware of contractors and outsourced services such as cleaning, painting, mowing etc. and the potential damage, which could be generated.
  For the digital zones it means a thinking of isolated zones, which can perform the task in best way in a local operation mode; even so the global optimum would be somewhat better. The isolated zones are security compartments with no uncontrolled exchange towards other parts of the system.

- According to the needs of risk analysis, apply separation of duty on node level: make different secure channel for:
  a) SCADA and AMI operation
  b) update mechanism
  c) intertripping (emergency actions)

- Restriction of numbers of protocols, nr of ports to a minimum with the option of black and white listing: this enables to control the security of the system and even to enable security verification technologies.

[5] Wireless connection must be either completely excluded, or accepted that they are around – even when indirectly only. Examples: Corporate network (with SCDA connection) and wireless hubs, maintenance laptop using GSM or wireless. The variety of inconspicuous connections is really large.

- Develop ID-Management: Control expiration date of certificates (e.g., device ID) and generate a maintenance circle to have continuously working, secure and non-expired ID's. Provide warning mechanism, and stability procedure for continuous service in case of problems.

1.5.3. Stimulate Inter-Organisation Actions

In general, standardization is the mean to cooperate between organisations and cross borders. Today many standards are elaborated, but merging of existing standa4rds and adaption for international co-operation is still a need.

- Public-Private Partnership: Stimulate Industrial-Control-System specific exchange of Information, knowledge and expertise at national and international level.

- Exercises: Regular and specific exercises for ICS incidents and combined ICS cyber incident must be planned, executed, and evaluated. Especially the following should be considered:
  - Combination of different organisational culture
  - Combination of profile culture energy- electrical and Telco / IT engineering.
  - Exercise should scope all situations including the ability to cold start all systems, knowing, that this could take years until the scope is properly covered.

- Provide a European wide (plus connected neighbourhood countries including links to Africa and Asia) and accepted vocabulary to enable and stimulate exchange. This vocabulary (probably in English) should have translation in each local language and must cover the variety of manufacturer and vendor specific terms.

- Smart meter of renewable producers or prosumers: Up to recently smart meters were just needed for accounting. Adding more functionality to smart meters could enable better asset security and interfaces to a large scale energy management system. The ultimate goal of these additional functionalities is the improvement of the energy quality in terms of availability management, but also in prediction of energy prosumers and controlling variation in voltage magnitude, harmonic content in the waveforms for AC power.

- Secure maintenance and repair: DSO have been adding to the pure one direction distribution the option to feed renewable energy into the DSO network. Switching off the DSO network requires today the down-stream switching off and switching off all renewables. Although existing network operation standards ensure the safety of the field agents working on the network, additional smart meter functionality or smart connector could allow central switching off capability. The trade-off between IT-security risks and safety risks must be elaborated in separate discussions and studies.

1.5.4. Apply security improvement management systems

Security is nearly always not perfect, because there is no source to finance all over perfect security, neither would it be economically viable. Usually risk assessment shows up to which degree protection is needed. Experts assume, that in some cases, e.g., in the core of the European grid, approaching perfect security is a real need. For SCADA this means to provide compartment security (highest level secure zone) with ideally no public network access (air gap principle of shielded networks). From the Stuxnet case, all experts learned that an ultimate air gap does not work in real environments.

The security level of given SCADA systems should be monitored, observed and continuously improved. Security improvement systems are:

- Incident and near incident monitoring and handling: Incident and near incidents are always a living proof of vulnerabilities. With an appropriate handling and monitoring systems improvement over time the security of a given system – even the system is always changing – will result, at a high level.
  The security management cycle should encompass at least three separate levels of SCADA:
  a) system elements
  b) procedures and
  c) system / architecture.

Additionally it is very important to have well-educated and sufficient digital forensic capacity, such that incidents and near incidents can be investigated in-depth and according lessons can be identified. For the more technical hands on part, an Industrial-Control-System specific CERT should be discussed.

- European and national reporting entity[6]: SCADA and SCADA-Cyber incidents should be European wide reported to a suitable entity to stimulate the learning curve between member states and inter-company. This reporting should be comparable to the airlines industry incident reporting system of IATA.

- Provide sufficient reaction capacity: Security – especially SCADA cyber security is never perfect. Therefore post incident measures must be in place up front. This includes contingency planning but also to be prepared for a complete "plan B". The reaction capacity should start at intra-company level, extended by support contracts of collaborators, manufacturers, service companies, and in serious cases gradually enlarged up to international PPP level.

- Regular penetration tests for critical systems: Penetration tests and security audits – preferably in a risk based repetition interval - are the means to assess the real security and remaining vulnerabilities up to the skill level of the specialised penetration testing / audit team. In practice, most of the environments will be penetrated or will show potential for optimization in case of audit which triggers as a follow up learning process.

- Elaborate and plan financing: Security level and available funding for security measures is a strongly coupled and interdependent pair. Ideally, a security requirement specification is given and the according measures will result. However, in practice, responsible agencies and boards try to circumvent this discussion, knowing that clear decisions could result in not controllable costs. Therefore, good practices have to be fostered by the community such that the pressure on European and member state regulators and owners will result in the demand to comply with good practice and standards such that reasonable funds for preventive and after incident reactive security are available. Standards and good practice are means to leverage security concerns of organisational members to a non-personal compliance issue.

1.5.5. Approaching the Highest Security Control Network HSCN

As already stated in the introduction, the high impact control devices in Smart Grids (aggregated overall impact 2 GW[7] and higher) require ultimate security[8] because there is no tolerance against system failure. The concept is: the ultimate critical assets are interconnected by the ultimate Highest Security Control Network HSCN. Against the background of 100 known bottle necks on highest voltage transmission lines [ENTSO 2012] the need for HSCN is underlined. Reflecting this fact, a highest security control network – ideally completely separated from the internet is postulated.

The **H**ighest **S**ecurity **C**ontrol **N**etwork HSCN concept must be built having in mind – neither direct nor indirect – connection to the public network which includes Internet, ISDN, and wireless networks.

Being aware that "no connection" is a theoretical principle and has to be replaced by the fewest amount and only known and well-defined connection: Today's TSO and bulk generators need to exchange current load, demand, expected load, and demand and RESERVE status directly from their SCADA environment. A low number of exceptions which has to be handled by protocol verification secure transitions and all additional security increasing options must be considered. Even with these exceptions the protection of such a network is far more secure than any open link to the public network. The exceptions could be handled using the principle of utmost limited numbers of ports and commands related to ports: Therefore, the transition security to and

[6] Incident reporting and administration is part of the improvement process and may complement collaborative early warning system, as partly available by today, but not sufficiently covering the specific SACDA security needs.
[7] To create the right expectation for the readers, in praxis this would mean, that many device collections with an impact of more than 100 MW already would be connected to HSCN. See WP1.1 of Expert Group on the security and resilience of Communication networks and Information systems for Smart Grids
[8] No system failure means to apply fail save technology, redundancy, self-healing and similar technologies to reach n-1, n-2 or n-3 security. (n-3: three components may fail without degrading normal operation)

from the HSCN will be verifiable with according software and therefore being aligned with today's best known security practise.

HSCN needs to be discussed and specified in a separate project. However, HSCN could serve several applications:

- In a country or in a limited size area, HSCN could be used as real time network with max reaction of 4msec: With this specification HSCN could be used for intertripping or protecting relaying.
- Communication of risk level and estimation global risk situation by communication between the stakeholders: TSO / DSO / bulk generation / Distributed Energy Resources (DER)
- To combine energy market information and SCADA in a secure way to achieve better resilience.

HSCN separation from the Internet: Even this SCADA network may use Internet Protocol, considering IPv6 if feasible, the Highest Security Control Network HSCN is for nearly all protocols completely separated from the commercial Internet. In specific cases even a VPN data stream may be put in commercial network and coupled out at the destination in an ultimate secure way.

As a consequence, the usual vulnerabilities of public networks will be eliminated or at least reduced to the lowest possible number. HSCN could work in a similar way as SWIFT does for the financial world. In many core regions SWIFT has 100% availability: even the architecture is designed for providing continuous service with no interruption. However, the stakeholder of the sector will decide on the business model having in mind the SWIFT case.

Specific requirements, such as propagation delay, other key properties, and feasibility have to be elaborated in a separate study. Also the expert debate setting the policies including the very strictly handling of exceptions is in scope of such a study.

Being well aware, that HSCN is essential shift of all paradigm of today, the argumentation for this network is consistent and compelling. WP1.3 therefore recommends reflecting HSCN in a study program.

1.6. Working Group Background

WP 1.3 team work is based on the results of WP 1.1 Identification and Categorisation of all relevant Smart Grid Assets and WP 1.2 Threat Analysis.

From WP 1.1 we need to consider the proposed 2 GW threshold:

> Horizontal or collective impact threshold based categorisation where failure may impact more end points (as Intelligent devices massive attack) which collectively can have an impact over 2 GW in supply, demand and transport. This will include all Grid assets (like SCADA and communication systems) and Smart assets (independent Power Producers, smart meters, prosumers, and smart appliances) which cover over 2 GW collective connected load or supply) which cross the threshold.

From WP 1.2 we get a complete overview on vulnerabilities assuming the following architecture according Figure 1 is applied. Furthermore: The WP 1.2extensive lists of *Threat Taxonomy and Assets for Smart Grids* in Appendix I to III[9] are pretty complete and suitable for assessing the risk factors within Smart Grid Assets.

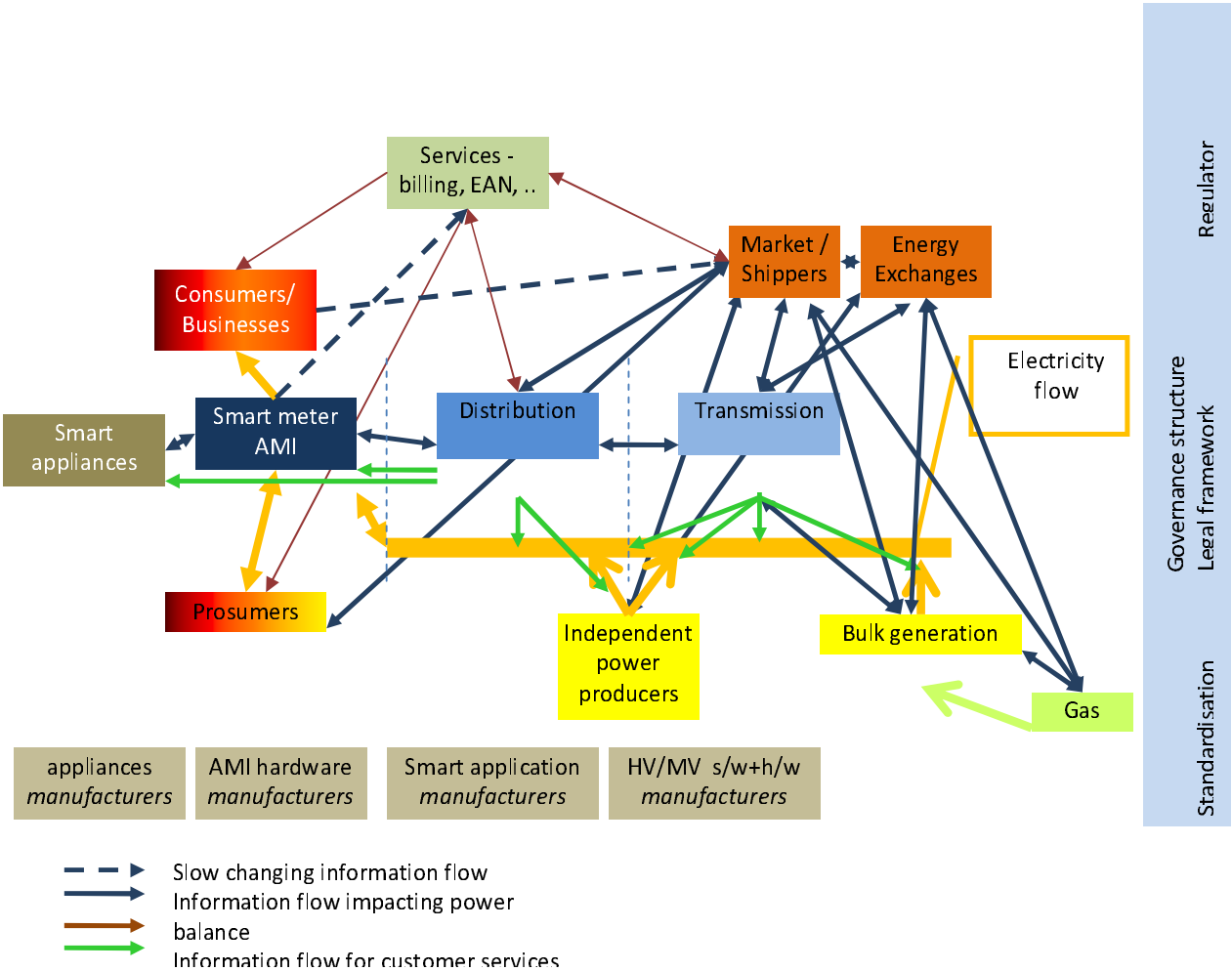


Figure 1: Overview of smart grid actors (source: TNO, 2011)

WP 1.2 an overview of smart grid actors (Figure 1) is reproduced to demonstrate the diversity of actors and their complex interaction scheme.

[9] See in WP 1.2, which reproduce basically the knowledge elaborated in the EU VITA project: http://vita.iabg.eu/

1.7. International Background & State-of–the-Art

1.7.1. Good Practices in Identifying Countermeasures

Countermeasure definition has some good practices today. Hereafter, some of the most common good practice approaches will be given.

1. Risk Analysis RA is a common practice to identify the actual risk situation. Based on the RA the risk factors are sorted out according the following options:
   a) Business impact analysis of the risks ➔ acceptable / non acceptable risk
   b) Identifying the deviation to the **S**ecurity **R**equirement **S**pecification SRS (SRS is often missing)

2. Expert's recommendation to implement best set of countermeasures with the given and available investment.

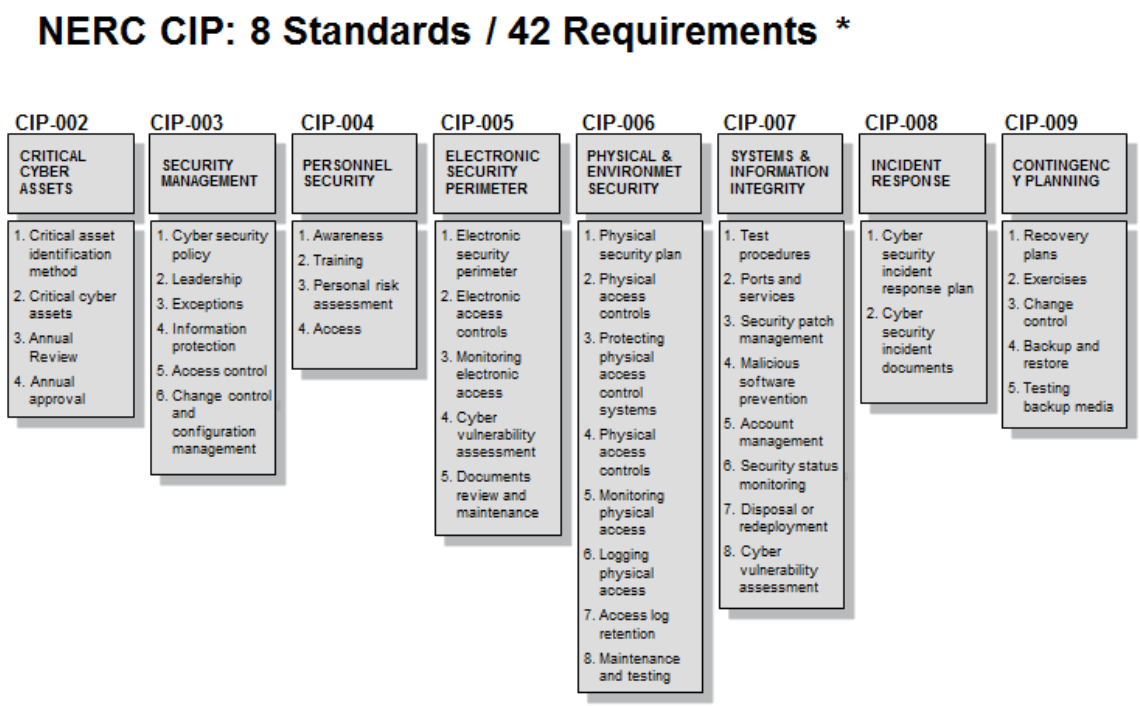
3. After incident: As reaction to guarantee a specific risk not re-occurring, a limited scope (around the last incident) is fine-grained analysed and counter fought with measures. In such cases often an overall balanced risk view is missing, being eager to absolutely avoid the re-occurrence..

4. Political demand: Especially black swan risk is normally decided on policy level in the public sector and at board level in industry.

In general, RA works fine as long as neither the likelihood is nearly zero nor the impact is nearly infinite. For both, likelihood and impact statistic figures should be available. If these are not given, the full strength of the methodology may not be realised.

1.7.2. Emphasis of NERC Standard: Definition of Requirements

The NERC Critical Infrastructure Protection (CIP) Standard identifies relevant categories for security requirements. It is important for a resilient system to cover all 42 aspects accordingly.



Note that these standards apply only to TSO and major bulk generator assets. Regarding the latter, CIP-002-4 states: generating sites with "an aggregate highest rated net Real Power capability of the preceding 12 months equal to or exceeding 1500 MW in a single Interconnection." This holds true for about 163 sites in the USA. [10]

1.7.3. Security improvement systems

[OECD 2012] proposes to first elaborate on the Vision: By 2020, resilient energy delivery systems are designed, installed, operated, and maintained to survive a cyber-incident while sustaining critical functions.

After this the major barriers have been identified and 5 working areas are defined:

1. Build a Culture of Security
2. Assess and Monitor Risk
3. Develop and Implement New Protective Measures to Reduce Risk
4. Manage Incidents
5. Sustain Security Improvements

These working areas are refined (see Annex I, [OECD 2012]). Also basic security requirements for Smart Grid are given in the same report:

Availability for energy system delivery has various time latency needs:

- ≤ 4 milliseconds (ms) for protective relaying
- Subseconds for transmission wide-area situational awareness monitoring
- Seconds for substation and feeder supervisory control and data acquisition (SCADA) data\
- Minutes for monitoring noncritical equipment and some market pricing information
- Hours for meter reading and longer term market pricing information
- Days/weeks/months for collecting long-term data, such as power quality information

Integrity for energy system operations includes the following assurance:

- Data has not been modified without authorization
- Source of data is authenticated
- Timestamp associated with the data is known and authenticated
- Quality of data is known and authenticated

Confidentiality is becoming more important with the increasing availability of customer information online. Confidentiality needs include the following:

- Privacy of customer information
- Electric market information
- General corporate information, such as payroll, internal strategic planning, etc.

Note that the electrical grid is a non-homogeneous infrastructure and that parameters identified may not be universally applicable: especially 4 milliseconds is needed for intertripping, in many other cases there is a delay of 20 milliseconds acceptable or in the energy market up to three minutes[11].

1.7.4. OECD Approach for Incidents (source: [OECD 2012])

Quality management (ISO 90XX) has the approach to:

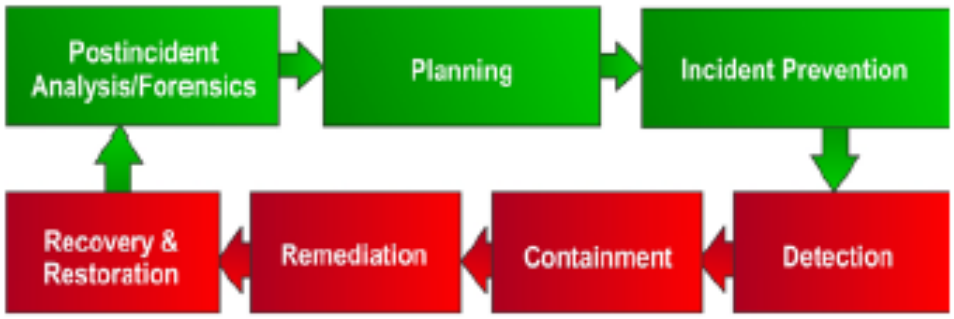
1. Describe the actual system as it works by now.

2. Improve the system with the continuous improvement plan.

[10] http://blog.industrialdefender.com/?p=813
[11] Stated by Honeywell Engineer February 28, 2012 in Brussels (US experience)

The beauty of this procedure is that it works always, even when the basic parameters for the target are identified weekly or hardly measurable. Exactly this is the situation in ICT- and Cyber-Security: Incidents, provoked incidents by penetration test, systematic audits and incidents in similar institutions demonstrate caveats of the system.

Key Elements of Effective Incident Management according to page 35 [OECD 2012]:



Source: DHS Control Systems Security Program

Consciously allowing and taking into account failures, this methodology is good as long as systems are not ultimately critical. For ultimately critical system there is zero tolerance for failures. E.g. as consequence of Fukushima we could observe, that many member states of Europe does not tolerate such faults and ask for ultimate security.

1.7.5. GAO Approach to SCADA / Smart Grid Security

United States Government Accountability Office GAO identifies in the report " CYBERSECURITY: Challenges in Securing the Modernized Electricity Grid" four domains of action needed:

- A lack of a coordinated approach to monitor industry compliance with voluntary standards
- A lack of security features built into smart grid devices
- A lack of an effective information-sharing mechanism within the electricity industry
- A lack of metrics for evaluating cyber-security.

See: http://www.gao.gov/assets/590/588914.pdf

1.7.6. SABSA Recommendation for Architectures and Risk

By Eric van Aken

The SABSA model[12] is a methodology for developing architecture for enterprise information security.

One of the tools for the setup of an architecture is the SABSA matrix that provides a relation between contextual, conceptual, logical, physical, component and service management on the one side and questions what, why, how, who, where and when that form the overview after having answered all these questions.

Amongst others SABSA also provides a risk management structure that starts with the risk context and then relates the asset at risk between a treat and an opportunity. The opportunity aspect of operational risk is embraced.

See next page the central page on balancing opportunities and risks:

[12] http://www.sabsa.org

SABSA Risk Management

In the SABSA framework there is heavy emphasis on the duality of risk – the balance between opportunity and threat. Many definitions of 'operational risk' miss this important point and focus only on the downside risks or potential loss events. This is unfortunate, because operational risk management provides many opportunities to develop operational excellence and improved service and product delivery to customers. It can also contribute significantly to meeting the performance goals of the enterprise and assisting individual line managers to achieve their personal target KPIs. SABSA embraces fully this 'opportunity' aspect of operational risk management in general and information risk management in particular. Figure 6 shows this in diagrammatic format.

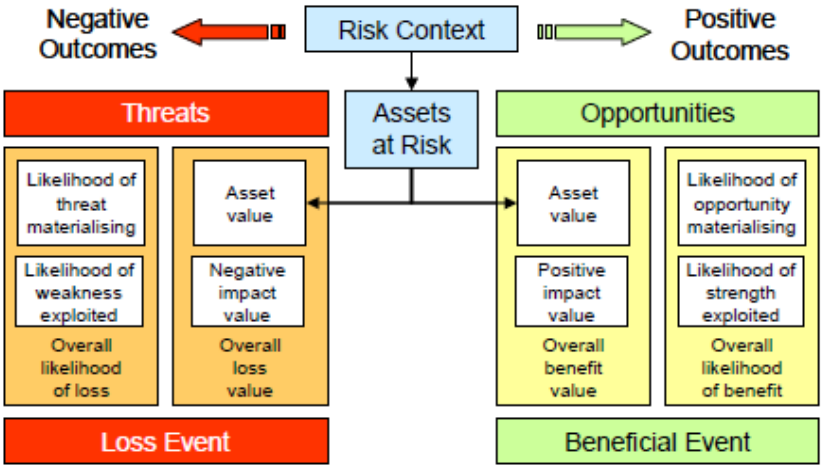


Figure 6: SABSA Model of Operational Risk

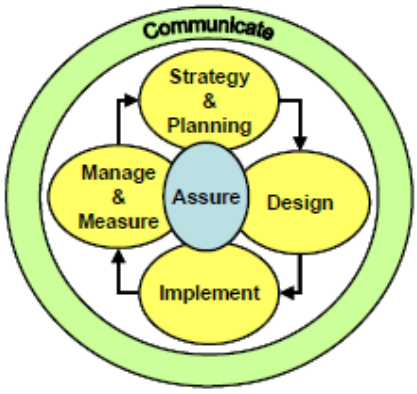


Figure 7: SABSA Risk Management Process

1.7.7. Alliander and the Dutch Good Practice

By Eric Van Aken

Alliander is an energy network company owning electricity and gas distribution grids covering roughly one third of the Netherlands and employs a workforce of approximately 6,000.

Alliander plays an important role in facilitating movements towards greater sustainability in Dutch energy supplies. The increase in sustainable, more decentralized power generation creates changing demands on the energy infrastructure and represents a challenge for network companies. Alliander sees it as its responsibility, to make that increasing sustainability possible at an acceptable cost to society, together with other market participants.

To better facilitate the energy transition Alliander has started up several strategic programs leading to new control models. These programs are aiming for more safety, health, privacy, security, availability, reliability,

integration, maintainability and flexibility. The results of these programs are (from a security point of view) amongst others:

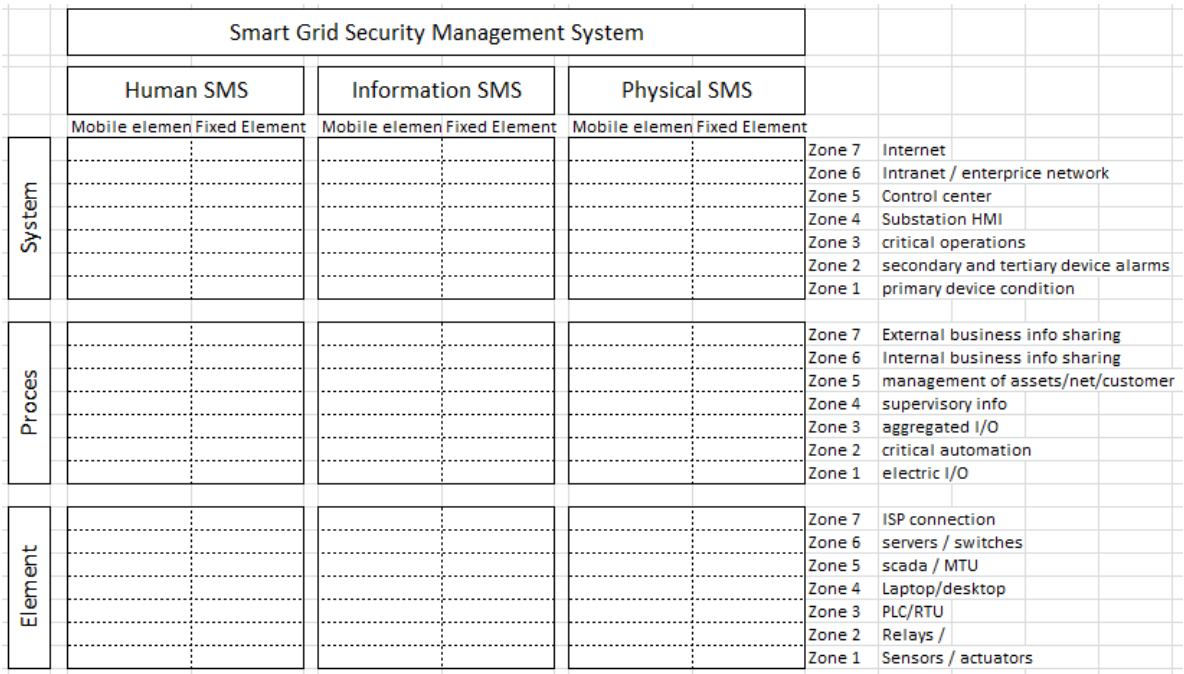
- Increase in the number of access points.
- Use of more IP-based communications networks.
- More integration between operational and corporate networks.
- Greater reliance on "standard" or commodity IT platforms.
- Security requires special attention as a response to these changes. Alliander is establishing a new security architecture based on proven technology, use of known standards and a layered architecture.

International research and developments indicates that vulnerability to cyber-attacks, despite standards, efforts and the availability of security technologies, is actually increasing.

<u>Two worlds managed by one system</u>

Many standards and publications [13] already provide zone principles as a Cyber security Architecture Element for smart girds. The only real challenge is to really use them both on the ICT office side as well as the ICS process control side. This ICT-ICS integration requires a holistic security approach in multiple dimensions.

The first dimension is related to the human involvement.
The second dimension is related to the physical place.
The third dimension is related to the digital structure.



Zone description

The number of zones differ from one standard to another, but more important is to differentiate the once that require other training, education, identity, clearance then the zone above or below. Zones offer the basics for an architectural approach to build in security by design. Crossover between zones requires conditional interconnection rules.

[13] ISA95, ISA99, NIST SP800-82, IEC62443-1, ISO27001,etc.

The first dimension is related to the human involvement.

Awareness, training and education (ATE) for the different rolls and/or functions is required on element, process and system level. Outsourcing is common today and it is expected that this will only increase due to the energy transition efforts. Therefor special attention is required that there is no difference between internal or third party personnel with regards to ATE.

The second dimension is related to the physical place.

Different zones introduce different access methodologies to support forensic investigation. Crossover between physical zones requires conditional interconnection rules.

The third dimension is related to the digital structure.

It is important to notice that personnel (internal or third party) should be trained similar in the physical or digital world. Crossover between digital zones requires conditional interconnection rules. For authorization, SCADA and patch management this requires special attention.

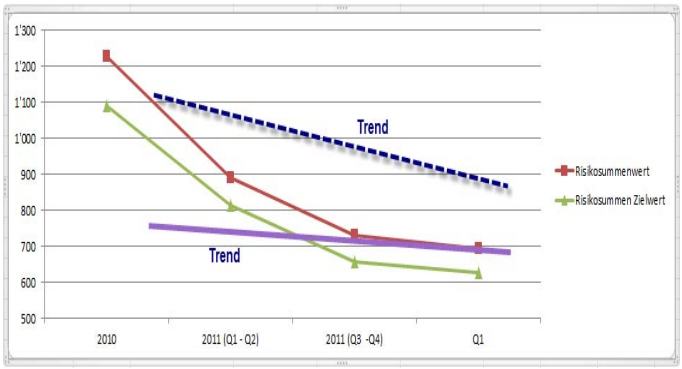
Elements can be divided in the ones that are installed in a fixed location and typically don't move. Other elements (laptops, smartphones, but also field service apparatus maintenances devices) will possible connect at various places and have intrinsic risks to distribute malware (compare STUXNET case).

1.7.8. Swissgrid Countermeasures

By Nair Rajesh

Swissgrid is the operator of the Swiss transmission system with responsibility for the operation, security and expansion of the 6700 kilometre long high-voltage grid in Switzerland. Internationally, Swissgrid plays an important role in the interconnection between the neighbouring countries Germany, France, Austria and Italy.

In line with the criticality of its operations, Swissgrid is in the process of deploying an integrated security management system. The main aspects of the system include a clear risk portfolio tracking, countermeasures deployment and active monitoring and operational intervention as required.



The Risk portfolio is developed and tracked analysing various aspects including known vulnerabilities, active threats, and impact analysis. The active portfolio of risks are evaluated, quantified, and scheduled for addressing based on the outcome of the risk methodology. The portfolio is then regularly reviewed in order to track the development of the quantified risk.

The countermeasures that are currently employed work on three dimensions: process, people, and technology. These dimensions form an integrated holistic approach, which help address the risks from multiple perspectives. Some of the countermeasures are shown below:

Process	- Process review to ensure that human errors are minimised - 4 eyes principle in the case of specific high risk security activities
People	- Background checks of people who have security relevance - Training and awareness building
Technology	- Network layer: Access control, separation of zones, encryption - Application layer: Identity management, access rights management

Active automated monitoring is also implemented to be able to track the activity and the situation at the most vulnerable aspects. Some of the tracking is enhanced with human oversight specifically on the perimeters of the organization. Pattern analysis is also implemented in certain areas.

Regular operations include the risk mitigation activities. Specific cases, where interventions are required, are supported with specific organizational processes which ensure that the management support is made available as soon as possible in and before critical situations.

This integrated approach is always under review and enhancement as the risk portfolio develops over time. Hence it is broken down to the operational level and each operational team leader has access and can manage his or her risks.

1.8. References

[Luiijf2008] Luiijf, 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.

[Luiijf 2010] Luiijf, H.A.M., "Process Control Security in the Cybercrime Information Exchange" , NICC, december 2010, online at www.cpni.nl.

[ENISA 2011A] ENISA study: "Enabling and managing end-to-end resilience", 2011. http://www.enisa.europa.eu/act/it/library/deliverables/e2eres

[ENISA 2011B] ENISA study: "Resilience Metrics and Measurements: Technical Report", 2011. http://www.enisa.europa.eu/act/res/other-areas/metrics/reports/metrics-tech-report

[ENISA 2011C] Ontology and taxonomies of resilience Version 1.0 – December 2011

[ENSIA 2011D] Protecting Industrial Control Systems: Recommendations for Europe and Member States http://www.enisa.europa.eu/activities/res/other-areas/ics-scada/protecting-industrial-control-systems.-recommendations-for-europe-and-member-states/at_download/fullReport

[DHS 2009] Catalogue of Control Systems Security: Recommendations for Standards Developers DHS September 2009, http://www.us-cert.gov/control_systems/pdf/CatalogofRecommendationsVer7.pdf

[IEA 2011] Technology Roadmap Smart Grids, IEA ISGAN, www.iea.org/papers/2011/smartgrids_roadmap.pdf

[EOPST 2011] A POLICY FRAMEWORK FOR THE 21st CENTURY GRID: Enabling Our Secure Energy Future, EXECUTIVE OFFICE OF THE PRESIDENT NATIONAL SCIENCE AND TECHNOLOGY COUNCIL www.whitehouse.gov/sites/default/files/microsites/ostp/nstc-smart-grid-june2011.pdf

[ESCSWG 2011] Roadmap to Achieve Energy Delivery Systems Cyber-security http://energy.gov/sites/prod/files/Energy%20Delivery%20Systems%20Cybersecurity%20Roadmap_finalweb.pdf

[OECD 2012] ICT Applications for the Smart Grid OPPORTUNITIES AND POLICY IMPLICATIONS

[NERC 20XX] NERC Critical Infrastructure Protection (CIP) standards CIP-002 through CIP-009 became mandatory in 2008. The NERC CIP standards require utilities in the bulk electric system apply the following eight standrards of the CIP series:

- Identify critical cyber assets (002)
- Develop security management controls to protect these critical cyber assets (003)
- Implement personnel risk assessment, training, and security awareness (004)
- Identify and implement electronic perimeter security for critical cyber assets (005)
- Implement a physical security program to protect critical cyber assets (006)
- Protect assets and information within the electronic security perimeter (007)
- Conduct incident response reporting and response planning (008)
- Implement recovery plans for critical cyber assets (009)

[WEF 2008] World Economic Forum Davos, Global Risks 2008. A Global Risk Network Report, available online at http://www.weforum.org/pdf/globalrisk/report2008.pdf.

[CEPS 2012] Protecting Critical Information Infrastructure, Working document, 1.0, Prof. Dr. Andrea Renda CEPS, with advisors Bernard Hämmerli & Eyal Adar CEO, White Cyber Knight

[CEPS 2011] Protecting Critical Infrastructure in the EU

[BSI 2011] Federal Office for Information Security (BSI), IT-Grundschutz Catalogues, available online at https://www.bsi.bund.de/ContentBSI/grundschutz/kataloge/kataloge.html

[Eckert2011] C. Eckert, C. Krauß, and P. Schoo. Sicherheit im Smart Grid - Eckpunkte für ein Energieinformationsnetz. Stiftung-Verbundkolleg / Projekt Newise Nr. 90. 2011

[Eckert2011b] C. Eckert and C. Krauß. Sicherheit im Smart Grid - Herausforderungen und Handlungsempfehlungen. Datenschutz und Datensicherheit, 8:535-541. 2011

[Krauß2011] C. Krauß and C. Eckert. Sicherheit im Smart Grid - Sicherheitsarchitekturen für die Domäne Privatkunde. Gestaltungslinien für Sicherheit und Datenschutz im Energieinformationsnetz, Stiftung-Verbundkolleg / Projekt Newise Nr. 94. 2011

[Björk 2010] Gunnar Björkman, The VIKING Porject – Towards more Secure SCADA Systems http://www.cse.psu.edu/~smclaugh/cse598e-f11/papers/bjorkman.pdf

[Zerrbst 2010] Zone Principles as Cyber Security Architecture Element for Smart grid, jens Zerbst and Martin Schäfer and IRo Rinty Joupi, Vattenfall AB

[France 2011] Giorgio Franceschetti, homeland Security, Artech House ISBN 978-1—60807-106-7: Chapter 3 of B. Hämmerli

[ENTSO 2012] ENTSO-E 10-YEAR NETWORK DEVELOPEMENT PLAN 2012 PROJECT FOR CONSULTATION https://www.entsoe.eu/consultations/document/docdetails.do?uid=0004-e566-3a0d-af87-9e06&

[Oosterink 2012] M. Oosterink (ed) et all, White paper on Legacy in control systems, CPNI.NL, March 2012.

[Dondoss 2012] Dondossola, G, et al. « Evaluation of the Effects of Internatnional Threats to PoewerSubstation Control system, » Proceedings of the iInternatnional Workshop on Complex Network and critical Infrastructure Protection 2006, Frentari Centre, Roma,

Annex I – OECD Strategy to Smart Grid Security

[OECD 2012] Exhibit E.1 Strategies for Achieving Energy Delivery Systems Cyber security

Vision	By 2020, resilient energy delivery systems are designed, installed, operated, and maintained to survive a cyber incident while sustaining critical functions.				
Barriers	• Cyber threats are unpredictable and evolve faster than the sector's ability to develop and deploy countermeasures • Security upgrades to legacy systems are limited by inherent limitations of the equipment and architectures • Performance/acceptance testing of new control and communication solutions is difficult without disrupting operations • Threat, vulnerability, incident, and mitigation information sharing is insufficient among government and industry • Weak business case for cybersecurity investment by industry • Regulatory uncertainty in energy sector cybersecurity				
Strategies	1. Build a Culture of Security	2. Assess and Monitor Risk	3. Develop and Implement New Protective Measures to Reduce Risk	4. Manage Incidents	5. Sustain Security Improvements
Near-term Milestones (0–3 years) By 2013	1.1 Executive engagement and support of cyber resilience efforts 1.2 Industry-driven safe code development and software assurance awareness workforce training campaign launched	2.1 Common terms and measures specific to each energy subsector available for baselining security posture in operational settings	3.1 Capabilities to evaluate the robustness and survivability of new platforms, systems, networks, architectures, policies, and other system changes commercially available	4.1 Tools to identify cyber events across all levels of energy delivery system networks commercially available 4.2 Tools to support and implement cyber attack response decision making for the human operator commercially available	5.1 Cyber threats, vulnerability, mitigation strategies, and incidents timely shared among appropriate sector stakeholders 5.2 Federal and state incentives available to accelerate investment in and adoption of resilient energy delivery systems
Mid-term Milestones (4–7 years) By 2017	1.3 Vendor systems and components using sophisticated secure coding and software assurance practices widely available 1.4 Field-proven best practices for energy delivery systems security widely employed 1.5 Compelling business case developed for investment in energy delivery systems security	2.2 Majority of asset owners baselining their security posture using energy subsector specific metrics	3.2 Scalable access control for all energy delivery system devices available 3.3 Next-generation, interoperable, and upgradeable solutions for secure serial and routable communications between devices at all levels of energy delivery system networks implemented	4.3 Incident reporting guidelines accepted and implemented by each energy subsector 4.4 Real-time forensics capabilities commercially available 4.5 Cyber event detection tools that evolve with the dynamic threat landscape commercially available	5.3 Collaborative environments, mechanisms, and resources available for connecting security and operations researchers, vendors, and asset owners 5.4 Federally funded partnerships and organizations focused on energy sector cybersecurity become self-sustaining
Long-term Milestones (8–10 years) By 2020	1.6 Significant increase in the number of workers skilled in energy delivery, information systems, and cybersecurity employed by industry	2.3 Tools for real-time security state monitoring and risk assessment of all energy delivery system architecture levels and across cyber-physical domains commercially available	3.4 Self-configuring energy delivery system network architectures widely available 3.5 Capabilities that enable security solutions to continue operation during a cyber attack available as upgrades and built-in to new security solutions 3.6 Next-generation, interoperable, and upgradeable solutions for secure wireless communications between devices at all levels of energy delivery system networks implemented	4.6 Lessons learned from cyber incidents shared and implemented throughout the energy sector 4.7 Capabilities for automated response to cyber incidents, including best practices for implementing these capabilities available	5.5 Private sector investment surpasses Federal investment in developing cybersecurity solutions for energy delivery systems 5.6 Mature, proactive processes to rapidly share threat, vulnerabilities, and mitigation strategies are implemented throughout the energy sector
Goals	Cybersecurity practices are reflexive and expected among all energy sector stakeholders	Continuous security state monitoring of all energy delivery system architecture levels and across cyber-physical domains is widely adopted by energy sector asset owners and operators	Next-generation energy delivery system architectures provide "defense in depth" and employ components that are interoperable, extensible, and able to continue operating in a degraded condition during a cyber incident	Energy sector stakeholders are able to mitigate a cyber incident as it unfolds, quickly return to normal operations, and derive lessons learned from incidents and changes in the energy delivery systems environment	Collaboration between industry, academia, and government maintains cybersecurity advances

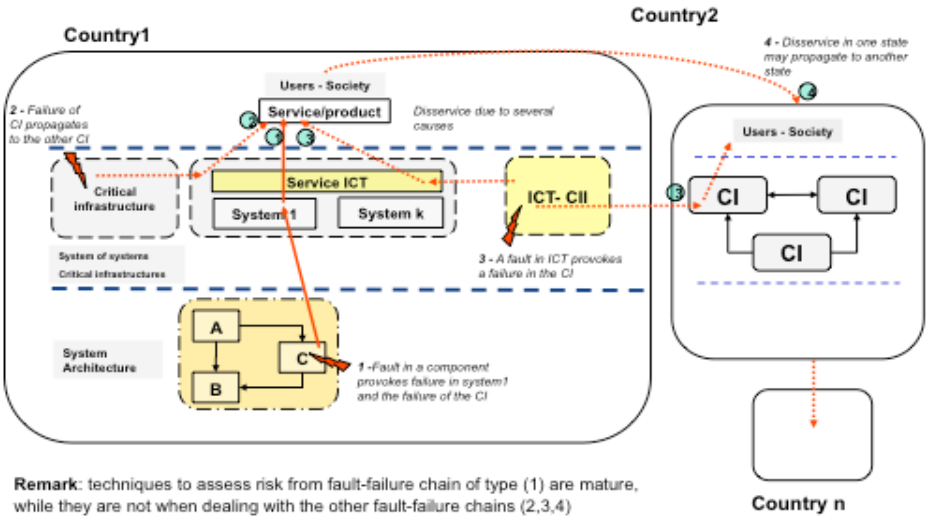
Annex II – About cross-organisation and cross-border dependency

From: [CEPS 2011], [CEPS 2012] to understand cross organisation / cross-border failures

The current development of CIP policies has led to advancements in the understanding of "type 1" problems, i.e. the causes of failure of a given infrastructure due to a fault in a single component. However, the dynamics with which the failure propagates to other critical infrastructures ("type 2"), the impact of faults in ICT on critical infrastructures ("type 3") and the inter-state propagation of failures ("Type 4") are much less known as of today.

The dynamics with which the failure propagates to other critical infrastructures ("type 2"), the impact of faults in ICT on critical infrastructures ("type 3") and the inter-state propagation of failures ("Type 4") are much less known as of today.

Figure 2 – cross-border dependencies



Source: Filippini (2010)

A recent report by Cornish et al. (2011) for Chatham House looks more in-depth into the question of cyber-dependencies, arguing *i.a.* that:

(i) organisations should look in more depth at dependencies and vulnerabilities that may be hidden in other organisations on which they are dependent and which are part of a common supply chain;

(ii) Research and investment in cyber security are essential to meeting and responding to the threat in a timely fashion and to nurturing human resource capabilities, yet this area is currently under-resourced and lacks the appropriate long-term funding in both the public and private sector;

(iii) Cyber security should be a fundamental component of an organisation's risk strategy – there is currently a need to address organisational inconsistencies in risk management and to develop a more comprehensive understanding of risk as it relates to cyber security;

(iv) Senior management will need to be more aware of the range of cyber dependencies within their organisation and the budgetary and reputational implications of vulnerabilities;

(v) in the pursuit of efficiency savings and improved quarterly returns, companies should take care not to undermine risk mitigation strategies and contingency planning. Clear plans are needed and adequate resources must be allocated for disaster recovery[14].

[14] Cornish et al. (2011)

Annex III - Background for SCADA Security

Explanation in chapter 3 by B. Hämmerli [Franc 2011]: Therefore this chapter is numbered with 3 and 3.x.x.

3.1 ICT and Society, ICT and Control Systems, the blurring from both

The development of critical infrastructures in the past 20 years has brought Information and Communication Technologies (ICT) into nearly every component of critical infrastructure as well as into offices, homes and user devices as, e.g., cars. ICT has given the society efficiency and comfort on one hand, but added complexity and vulnerability on the other hand. As a fact, in personal life, we are used to accessing ICT components every few minutes, such as cell phones, elevators, cars, internet services (e.g., e-banking or just a simple topic related search), washing machines, light regulator, and others. In public life we talk about critical infrastructure sectors such as electricity, transportation, finance, water etc. which provide crucial services to the society as whole. A blackout of one or even several critical systems at once, each one enabled through ICT, is considered today as very unlikely and the imagination of a long lasting and multiple infrastructure blackout including all consequences is not really dealt with in general public. But without any doubt: such a scenario may happen, and national governments try to prepare for such situations. If preparation is studied, often simulation games are used to train the country's main infrastructure responsible for crisis preparedness.

3.1.1 Chapter Overview

Homeland Security and Challenges in Information Systems is discussed, initially depicting the landscape of information security and its interrelation to the Critical Infrastructure (CI) and Critical Information Infrastructure (CII) or the combination of both C(I)I. When it comes to infrastructure protection the according acronyms are CIP, CIIP and C(I)IP: Definitions see [Dondoss 2012].
E-banking security and processes are used as an example to illustrate the information security challenges and its associated impact on society: we learn from E-banking about confidentiality, the meaning of identity theft and its countermeasure which are all relevant for C(I)IP (Section 3.2).
With the analysis of the financial critical IT systems within Europe, as performed in the PARSIFAL project[15], a broad European wide discussed consensus on critical financial infrastructure challenges is presented: The eight identified fields which need research in the next five years are disclosed in form of the recommendation (final report to the European Commission - information security research funding unit) (Section 3.3).
As a well-recognised fact, information sharing is a key activity for increasing the level of resilience, robustness, preparedness and consequence management such as business continuity, and disaster and recovery planning. Key factors in building up information sharing centres and the trust within the sharing group will is discussed (Section 3.4).
Mainly one specific consideration on the balance of security measures and privacy concerns is given, just to prevent potential unlimited demand to control and monitor individuals (Section 3.5), before taking overall conclusions (Section 3.6).

3.1.2 Critical Infrastructure and ICT

Intuitively everybody has an understanding of the terms *critical* and *infrastructure* as well as the combination of both. To sharpen and align the understanding the definition of European Commission[16] is reproduced:

[15] http://www.parsifal-project.eu/

[16] Commission of the European Communities. Critical Infrastructure Protection in the Fight against Terrorism (Brussels, 20 October 2004), COM(2004)702 final, p. 3. http://europa.eu.int/comm/justice_home/doc_centre/criminal/terrorism/doc/com_2004_702_en.pdf .

"Critical infrastructures consist of those physical and information technology facilities, networks, services and assets which, if disrupted or destroyed, would have a serious impact on the health, safety, security or economic well-being of citizens or the effective functioning of governments in the Member States. Critical infrastructures extend across many sectors of the economy and key government services."

Typically, the Critical Infrastructure (CI) is divided into 5-20 sectors, depending of organising entity as member states, US, EU. Typical sectors are according the EU definition[17]:

- energy installations and networks;
- communications and information technology;
- finance (banking, securities and investment);
- health care;
- food;
- water (dams, storage, treatment and networks);
- transport (airports, ports, intermodal facilities, railway and mass transit networks, traffic control systems);
- production, storage and transport of dangerous goods (e.g. chemical, biological, radiological and nuclear materials);
- government (e.g. critical services, facilities, information networks, assets and key national sites and monuments).

The sector concept helps to build groups which share a common crises language and understanding, having similar educations and are responsible as a part of their jobs to run, often a privately owned CI. Common language and common values are important to establish well-functioning collaboration. In spite of being competitors in the core business within a given sector, experts start after some time to understand that the security dimension of the critical sector is not core business and may be understood as a domain of mutual collaboration and support. Having reached this level, the work within the CI sector can start.

Usually first tasks to start with are the following:

- making an inventory of critical infrastructure,
- making an inventory of the critical services which must run, such that the CI can work (dependency analysis),
- making a vulnerability and threat analysis: the results are then the set of risk factors, when related to the probability of specific incidents. Definition of a minimum level of service which should in any case be maintained,
- defining countermeasures to improve resilience of the infrastructure on one hand and to add as a plan B disaster and recovery planning, and
- test of the countermeasures with simulated scenario and exercises, typically with one given sector at start, in a more advanced stadium also between sectors.

Understanding now the basic concept of Critical Infrastructure Protection (CIP), the information security component of CIP, the Critical Information Infrastructure Protection (CIIP) can be introduced. Scanning again through the list of sectors above specifically with ICT dimension in mind, one can start to understand the dimension of the task. The EU Commission defines CIIP[18] as follows:

"The programs and activities of infrastructure owners, operators, manufacturers, users, and regulatory authorities which aim at keeping the performance of CII in case of failures, attacks or accidents above a defined minimum level of services and aim at minimising the recovery and damage. CIIP should therefore be viewed as a cross-sector phenomenon rather than being limited to specific sectors. CIIP should be closely coordinated with CIP from a holistic perspective."

CIIP are "critical infrastructures [in] themselves or that are essential for the operation of critical infrastructures (telecommunications, computers/software, Internet, satellites, etc.)".19

[17] http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_terrorism/l33259_en.htm

[18] Commission of the European Communities. Green Paper on a European Programme for Critical Infrastructure Protection (Brussels, 17 November 2005), COM(2005) 576 final, p. 19. http://www.libertysecurity.org/IMG/pdf/EC_-_Green_Paper_on_CI_-_17.11.2005.pdf .

[19] Commission Communication 2005. p19

To distinguish between CIIP and corporate information security, we need to understand information security in more detail. The goal of corporate information security is to maintain the following properties within information systems:

Basic Properties:

- Availability;
- Confidentiality;
- Integrity.

Composite properties:

- Non repudiation (traceability, monitoring, logs);
- Authentication (who is acting);
- Compliance (local regional and global laws & standards).

Corporations want to minimise their economic losses caused by information security incidents. It is not about avoidance in any case of incidents, but it is about awareness of ICT risks and to guard risks and – if necessary – to increase countermeasures. The background of corporate information security relates always to maximisation of revenue considering all aspects including investments into corporate information security, loss caused by information security incidents and reputation. But societal impacts caused by blackout of CI sectors are not sub summarised within the umbrella of corporate information security. The investment of the delta when increasing from corporate information security to CIIP level has, of course, associated cost. Those costs are part of the debate, who should carry those costs? Some options are given:

- Regulation: Laws make CIIP provider and operator to carry the costs;
- PPP: Public Private Partnership model (discussed later into more detail) operates on partnerships, where each contributor carries its own costs;
- Governments pay for the additional costs.

Historically, up to 1990, most critical infrastructure was State owned and was provided by one single corporation. Governments were labelled as too expensive and being not sufficiently efficient. At this time, competition was considered to be the solution to increase efficiency and to reach lower prices. As we know both situations eventually happened, but with a subsequent loss of control on the critical infrastructure. After many years of deregulation of critical infrastructures, national governments started to understand the challenge to provide an additional CIIP level of security to the corporate security of multiple companies in a deregulated market.

The attempted goal is to act on both, increasing information security in general as well to increase resilience and preparedness of CI and CII.

3.1.3 Critical Infrastructure and Control Systems

In recent years, operators of any infrastructure have started to connect their control system at least to the internal Ethernet, which is in most cases somehow connected to the Internet, or even directly to the Internet. The basic background for this connection is to save costs by:

- Using the internal net instead of adding a second and separate cabling;
- Taking advantage of networked infrastructure by inspecting the control system data through applications and user interfaces anywhere in the world. However, the risks associated with this connection types are in most cases not already assigned properly, and mitigation of risk is often not - or only poorly - addressed.
  Example 1: Direct dependency electricity production and distribution: for metering and control system maintenance an internet connection is installed. The risks factors associated with this

connection are not sufficiently assessed. In a test laboratory was proofed, what could happen by this connection: pretty much all vulnerabilities which were expected (DoS, Trojan Horse, Viruses) could be verified [1].

Example 2: indirect dependency: EU energy sectors' trading platform for electricity: This trading platform was based on the public internet. Risk assessment disclosed, that trading is essential to operate the electrical grid properly, and without trading, it is very difficult to control the flow in the transmission lines. This example demonstrates an internet dependency of the energy sector.

Even so, that these two examples might be justified by a few cases only, the principle challenge remains in the electrical community.

Control systems are using Real-Time Computing (RTC), or reactive computing, which have hardware and software *real-time constraint*—i.e., operational deadlines (typically milliseconds or even less) from event to system response. By contrast, a *non-real-time system* is one for which there is no deadline, even if fast response or high performance is desired or preferred. A real time system may be one where its application can be considered (within context) to be mission critical. A real-time deadline must be met, regardless of any circumstances as, e.g., system load.

Supervisory Control and Data Acquisition (SCADA) is the term often used in the context of homeland security. SCADA generally refers to an industrial control system: a computer system monitoring and controlling a process. The process can be industrial, infrastructure or facility-based and Wikipedia[20] defines the application field as follows:

- Industrial processes include those of manufacturing, production, power generation, fabrication, and refining, and may run in continuous, batch, repetitive, or discrete modes.
- Infrastructure processes may be public or private, and include water treatment and distribution, wastewater collection and treatment, oil and gas pipelines, electrical power transmission and distribution, Wind Farms, civil defence siren systems, and large communication systems.
- Facility processes occur both in public facilities and private ones, including buildings, airports, ships, and space stations. They monitor and control Heating, Ventilating and Air Conditioning (HVAC), access, and energy consumption.

SCADA systems have several properties (see [Luiijf 2010]) which make them much more difficult to defend against internet attacks than normal information systems:

- A continuous computational effort with well-defined deadlines ran on a hardware, which is minimal and cost optimised, i.e. there is not much computing power left for security.
- Because of the time criticality and always performing job often for several years, usual update mechanism as used, e.g., in windows systems are not admitted: The system may not be interrupted or restarted at any time it performs. Vulnerabilities cannot be fixed, even when well-known and patches available.
- Long hardware and software depreciation times and staff-turnover which cause SCADA systems to become legacy (old hardware; no replacement components available; outdated software (e.g., Windows 95 and 2000; and lost knowledge as people left and nothing was documented – see (Oosterink 2012)).

Of course, there are some solutions and work around available by protecting the control entities with particular system architectures and front end computers, which terminates links in an appropriate way. However, the community is still far away from optimal and off the shelf solutions.

[20] http://en.wikipedia.org/wiki/SCADA

Annex IV – Potential Elements of a SCADA Countermeasure Ontology / Taxonomy

Annex IV and V are supplementing and coincidental to each other: Where Annex IV covers early idea of the volunteering team Annex V covers a widely recognised taxonomy, but for general Information system, not fine-tuned to SCADA.

Covering all Aspects:
All aspect of IT- and Information security are in scope: Confidentiality, Integrity (for contracts between producer, operator and distributer, as specialised aspect of Integrity), Availability, Non-repudiation, Resilience and Robustness in all mode of operation and others non mentioned.

General IT security measures

1. Documented configurations and infrastructure
2. Firewall
3. Malware control
4. IDS / IPV
5. Update and patching of SCADA software during in SCADA operation???
6. Secure Identification (ID)
7. (Distributed) Denial of Service prevention
8. Code verification / certification
9. Protocol and command verification mode
10. Physical security to provide availability and timeliness of communication (e.g., against jamming, EM-disturbance, nature threats)

Offline / not real-time measures

1. Backup / restore / well-documented configuration
2. Hot spare configurations / hardware replication
3. Secure fall back and offline modus
4. Penetration test ← organisational
5. Security audit and review ← organisational
6. EMC robustness
7. Uninterruptable Power Supply / backup power
8. ICT services dependency resilience (e.g., DNS, digital certificates, ...)
9. Precise timing infrastructure resilience (e.g., against GPS signal corruption)

Environment

1. Anti-earth-quake robustness
2. Flooding / heavy rainfall / snow robustness
3. bomb resistance
4. lightning protection
5. ...

Organisational

1. Awareness
2. Physical security: Also against hard-core military weapons? EMP protection key systems
3. Physical access
4. Strong authentication with verification and background testing process
5. Security culture
6. Security organisation
7. Social engineering and penetration test.
8. Business Continuity Plan / Disaster Recovery Plan
9. C(I)IP: Dependability and mutual dependency analysis and counter reaction plans
10. Exercises preparing for incident response
11. Being networked in one or several information sharing secret circles
12. Financial planning, budgeting and reserve building for incidents and countermeasures

Cross-Organisational

In General, many of the topics in chapter 1.5 cover the cross-organisational aspect. Additionally have to be considered:

1. Penalties for non-conformance and non-compliance
2. Oversight by regulator
3. .....

Architectural

It is important to realise that aspect security in one or several specific areas does not reflect the overall security: the concentration of all aspects resulting in the overall architecture and design can be implemented in more and inferior secure way. Beside of some audit guidelines it will be very challenging to give taxonomy on this aspect.

Annex V- BSI Countermeasures - A good Practice approach

The German Federal Office for Information Security defines in the IT-base line protection manual (Grundschutz Katalog) [BSI 2011] general security countermeasures which can also be applied to the ICT components of Smart Grids. They distinguish between the following 6 categories:

1. Infrastructure
2. Organisation
3. Personnel / Staff, contractors and service providers
4. Hardware & software
5. Communication
6. Contingency planning

For each of these categories, a multitude of measures are listed. In the following, we summarise the most relevant ones for Smart Grids.

Infrastructure

- Compliance with relevant DIN standards/VDE specifications etc.
- Access control to infrastructure systems
- Physical protection of infrastructure systems
- Safety mechanisms (lightning protection, fire-protection, emergency plans etc.)
- Ensure availability of systems (redundancy, UPS etc.)

Organisation

- Specification of responsibilities and of provisions for the use of IT
- Resource management
- Maintenance / repair regulations
- Authorisation management
- Guidelines for approved soft- and hardware and usage regulations
- Security trainings, guidelines, auditing, reviews, awareness
- Physical security and access regulations and enforcement
- Regular documentation and inspection
- Emergency response regulations, e.g., for violations of security policies
- Security organisation, e.g., key management, access control

- Development, implementation, and update of security concepts, policies etc., e.g., virus protection of systems etc.

Personnel

- Security trainings, guidelines, auditing, reviews, awareness for personnel
- Commitment of staff members to compliance with relevant laws, regulations and provisions

Hardware & software

- Access control for IT systems
- Logging, Monitoring
- Virus protection
- Protection of confidential data
- Using encryption, checksums or digital signatures
- Use of a appropriate security products for IT systems
- Testing of new hardware and software
- Updating / upgrading / patching of software and hardware
- Cryptography modules
- Physical security of crypto modules
- Operating system security (installation, configuration, operation ...)
- Use of cryptographic procedures on the various layers of the ISO/OSI reference model
- Regular system integrity checking, code verification
- Security Gateways and active content
- Firewalls
- Appropriate choice of authentication mechanisms

Communication

- Selection of an appropriate network topology
- Network management
- Regular security checks of the network
- Logging at servers
- Use of network security services
- Use of appropriate mechanisms for encryption, authentication, integrity protection

- Secure use of communication software
- Protection against DoS attacks
- Intrusion detection and intrusion response systems
- Security aspects of routing protocols

Contingency planning

- Survey of availability requirements
- Definition of "emergency"
- Development of an Emergency Procedure Manual
- Responsibilities in an emergency
- Contingency plans for breakdown of data transmission, systems, and other selected incidents
- Development of a post-incident recovery plan
- Specifying priorities for handling security incidents
- Emergency preparedness exercises
- Development and execution of a data backup plan
- Use of redundant systems, e.g., redundant arrangement of network components