artec
Forschungszentrum
Nachhaltigkeit

# Vulnerability and resilience of cyber-physical power systems

## Results from an empirical-based study

Mariela Tapia, Pablo Thier, Stefan Gößling-Reisemann

Universität Bremen

artec Forschungszentrum Nachhaltigkeit
Enrique-Schmidt-Str. 7, 28359 Bremen

www.uni-bremen.de/artec

artec-paper Nr. 222

April 2020

ISSN 1613-4907

Das artec Forschungszentrum Nachhaltigkeit ist ein interdisziplinäres Zentrum der Universität Bremen zur wissenschaftlichen Erforschung von Fragen der Nachhaltigkeit. Das Forschungszentrum Nachhaltigkeit gibt in seiner Schriftenreihe „artec-paper“ in loser Folge Aufsätze und Vorträge von Mitarbeiter*innen sowie ausgewählte Arbeitspapiere und Berichte von Forschungsprojekten heraus.

# Impressum

**Herausgeber:**

Universität Bremen
artec Forschungszentrum Nachhaltigkeit
Postfach 33 04 40
28334 Bremen
Tel.: 0421 218 61801

Fax: 0421 218 98 61801
URL: www.uni-bremen.de/ artec

**Kontakt:**

Katja Hessenkämper
E-Mail: hessenkaemper@uni-bremen.de

# Vulnerability and resilience of cyber-physical power systems

## Results from an empirical-based study

Mariela Tapia*, Pablo Thier, Prof. Dr. Stefan Gößling-Reisemann (†)

*University of Bremen, Resilient Energy Systems Research Group,*
*Enrique-Schmidt-Str. 7, 28359 Bremen, Germany*

## Abstract

Power systems are undergoing a profound transformation towards cyber-physical systems. Disruptive changes due to energy system transition and the complexity of the interconnected systems expose the power system to new, unknown and unpredictable risks. To identify the critical points, a vulnerability assessment was conducted, involving experts from power as well as information and communication technologies (ICT) sectors. Weaknesses were identified e.g., the lack of policy enforcement worsened by the unreadiness of involved actors. The complex dynamics of ICT makes it infeasible to keep a complete inventory of potential stressors to define appropriate preparation and prevention mechanisms. Therefore, we suggest applying a resilience management approach to increase the resilience of the system. It aims at a better ride through failures rather than building higher walls. We conclude that building resilience in cyber-physical power systems is feasible and helps in preparing for the unexpected.

**Keywords:** cyber-physical power systems, resilience management, vulnerability assessment, guiding principle, resilience enhancing measures

*Corresponding author. Email address: mariela.tapia @ uni-bremen.de

# Acknowledgements

We would like to express our deep gratitude to our beloved supervisor and friend Prof. Dr. Stefan Gößling-Reisemann for his highly valuable insights and contributions during the development of the research project *Strom-Resilienz*. His guidance, enthusiastic encouragement and constructive critiques were always greatly appreciated.

Our special thanks are extended to Prof. em. Dr. Arnim von Gleich for his fruitful discussions on vulnerability and resilience topics.

We would also like to thank the experts who participated in the interviews and workshops in the frame of the research project *Strom-Resilienz* for their valuable comments and insightful discussions.

Thanks to the *Institute for Ecological Economy Research* (Institut für ökologische Wirtschaftsforschung, *IÖW*) and the project partners Astrid Aretz, Mark Boost and Prof. Dr. Bernd Hirschl for the active collaboration and management of the research project *Strom-Resilienz*.

We acknowledge the support on the interview content analysis provided by Max Spengler and the assistance on the interview transcriptions and workshops organization provided by Luis Rivera. We also appreciate the support provided by Timseabasi Thomas and Cécile Pot d'or on the proofreading of this document.

This manuscript is based upon the results from the research project *Strom-Resilienz*, financially supported by the German Federal Ministry of Education and Research within the program Innovation and Technology Analysis (ITA), FKZ 16I1678. An earlier version of this work was published in German in the final project report (see (Hirschl et al., 2018)).

# Table of Contents

# List of abbreviations

| | |
|---|---|
| BDEW | Bundesverband der Energie- und Wasserwirtschaft E.V. |
| BSI | German Federal Office for Information Security |
| CERT | Computer Emergency Response Team for Federal Agencies |
| CPPS | Cyber-physical Power Systems |
| DA | Data Access |
| DDoS | Distributed Denial of Service |
| DER | Distributed Energy Resources |
| DMS | Distribution Management Systems |
| DNP3 | Distributed Network Protocol |
| DOS | Denial-of-Service |
| DSO | Distribution System Operator |
| EMS | Energy Management Systems |
| ENISA | European Network and Information Security Agency |
| EV | Electric Vehicle |
| GOOSE | Generic Object-Oriented Substation Event |
| HAN | Home Area Network |
| HMI | Human Machine Interface |
| ICS | Industrial Control Systems |
| ICT | Information and Communication Technologies |
| IDS | Intrusion Detection Systems |
| IEC | International Electrotechnical Commission |
| IED | Intelligent Electronic Devices |
| IoT | Internet of Things |
| ISMS | Information Security Management System |
| IT | Information Technology |
| ICT | Information and Communication Technologies |
| LMN | Local Metrological Network |
| MITM | Man-In-The-Middle |
| MSPC | Multivariate Statistical Process Control |
| NESCOR | National Electric Sector Cybersecurity Organization Resource |
| NIDS | Network-Based Intrusion Detection System |
| NIST | National Institute of Standards and Technology |
| oK | Open Konzequenze |

| | |
|---|---|
| OPC | OLE for Process Control |
| OT | Operation Technology |
| PKI | Public Key Infrastructure |
| PP | Protection Profile |
| PV | Photovoltaic |
| RBAC | Role-Based Access Control |
| RM | Resilience Management |
| RTU | Remote Terminal Unit |
| SAIDI | System Average Interruption Duration Index |
| SCADA | Supervisory Control and Data Acquisition |
| SEP | Smart Energy Profile |
| SGAM | Smart Grid Architecture Model |
| SMGA | Smart Meter Gateway Administrator |
| SMGW | Smart Meter Gateway |
| TNC | Trusted Network Connect |
| UPS | Energy Supply Backups |
| VA | Vulnerability Assessment |
| VDE | Verband Der Elektrotechnik Elektronik Informationstechnik |
| WAN | Wide Area Network |
| ZLL | Zigbee Light Link |

# List of Tables

# List of Figures

# 1 Introduction

Power systems are evolving through an increasing convergence with information and communication technologies (ICT), leading to complex cyber-physical power system (CPPS). This has brought opportunities to enhance the systems' performance and provide solutions to cope with the associated challenges of energy supply based on distributed and fluctuating renewable energies. However, at the same time this extended interconnection and interdependency between the electric power and ICT infrastructures expose the power system to new, unknown and unpredictable risks.

Cyber-attacks targeting power systems have been growing in number and sophistication in recent years. The cyber-attack on the Ukraine power grid in December 2015, where energy-grid operations were disrupted by unknown cyber actors causing blackouts for over 225,000 customers (Styzcynski and Beach-Westmoreland, 2017). One year later, in December 2016, a transmission level substation in Ukraine was impacted by a malware framework identified as '*Crashoverride'*, resulting in outages for an unspecified number of customers (Dragos Inc., 2017). These were the first reported attacks of its kind, but cyber-attacks on power systems have been presumed in other cases in recent years. For instance, between 2016 and 2018, access was gained to the control rooms of United States power suppliers by Russian hackers, which could have enabled them to shut down networks and cause blackouts (Cellan-Jones, 2018). In this case, the attackers won access by staging malware and by spear phishing (Department of Homeland Security, 2018). Although the connection between the attack and actual blackouts in the US power grid was not clear, this caused the Department of Homeland Security and Federal Bureau of Investigation to create detection and prevention guidelines against such activities. Another incident was reported on March 5, 2019. An electric utility in the western United States was disrupted due to a denial-of-service incident. This attack did not cause a blackout or harm to power generation and it is not clear if the Western transmission grid was an intentional target. But it did lead to a loss of visibility to certain parts of the utility's supervisory control and data acquisition (SCADA) system and therefore was placed in a concerning category (Sobczak, 2019).

Vulnerability and risk assessments are seen as a crucial measure when it comes to power system cybersecurity, see (Arghandeh et al., 2016; NIST, 2014; Rossebo et al., 2017; Teixeira et al., 2015), since the identification of known vulnerabilities and their influence on the security of the system enables the development of methods to deal with the vulnerabilities. In these studies, potential impacts and mitigation options were evaluated based on lists of potential threats and their likelihood of occurrence.

We argue that due to the dynamic nature of ICT and its complex interdependency with the power infrastructure, we have to expect surprises. It will no longer be possible to identify a comprehensive inventory of potential threats, as is the case in classic risk management. A reliable power supply is of great importance for almost all areas of life, therefore it is necessary to develop strategies that enable the power system to be prepared for expected and unexpected stressors. In other words, it is essential to apply a resilience management strategy. Many definitions of resilience exist in the scientific community (e.g., (Jesse et al., 2019)). For this study, we describe resilience as a (socio-technical) system's ability to maintain its services under stress and in turbulent conditions (Brand et al., 2017; von Gleich et al., 2010). The advantage of using this definition is that it focusses on the system services, which must be outlined together with the stakeholders/users. In this way, changes and evolutions of the system are possible, which are core aspects of transitions. The focus lies on the complex nature of interconnectedness and interdependency, and the capability of the system to maintain its services.

This manuscript presents the results of two work packages[1] of the research project *Strom-Resilienz* that focused on the vulnerability and resilience of the digitalization of power systems. It was developed by the *Resilient Energy Systems* research group at the University of Bremen in cooperation with the *Institute for Ecological Economy Research* (Institut für ökologische Wirtschaftsforschung, *IÖW*), from September 2015 to November 2017.

The main objectives of the mentioned work packages were to identify which additional vulnerabilities could arise from the digitalization of power systems and what are the required strategies to increase the resilience of power systems to ensure that the system's primary functionality is maintained, even under stress. The study was structured in two parts. First, a vulnerability assessment (VA) was performed to identify the critical properties, structures and elements that make the system vulnerable to cyber-attacks. For this purpose, an interdisciplinary approach involving energy sector stakeholders and ICT solution providers through interviews and workshops was selected. Second, a resilience strategy was developed by using a resilient management approach to identify how cyber-physical systems can be better prepared for any stressor.

The remainder of this manuscript is organized as follows: the executive summary in section 2 highlights the important aspects about the applied methods and main results. Section 3 provides a brief theoretical background regarding concepts of vulnerability and resilience, and describes in detail the applied methodologies for the vulnerability assessment and the

[1] Working package 2: *Determination and analysis of possible disturbance events and concretization of resilience criteria*, and working package 3: *Identification of options to minimize vulnerability and maximize resilience*

resilience management strategy. Section 4 discusses the results of the vulnerability assessment. In section 5, the results of the resilience management strategy are discussed. Section 6 ends the manuscript with conclusions and outlook.

# 2 Executive Summary

*Note: This section is the preprint version of the work* (Tapia et al., 2020) *already published in TATuP Vol 29 No 1 (2020): Cybersecurity. Threat, vulnerability, values, and damage. See final version in https://doi.org/10.14512/tatup.29.1.23.*

## Introduction

Power systems are evolving through an extended convergence with information and communication technologies (ICT), leading to complex cyber-physical power systems (CPPS). This has brought opportunities to enhance the systems' performance and provide solutions to cope with the associated challenges of energy supply based on distributed and fluctuating renewable energies. However, cyber-attacks targeting power systems have been growing in number and sophistication in recent years. For instance, the attacks against the Ukrainian power grid in 2015 and 2016 that resulted in power outages (Dragos Inc., 2017). Another incident against a utility in the United States was reported on March 2019 (Sobczak, 2019). Several risk and vulnerability assessments for power systems have been published in recent years e.g., (NIST, 2014; Rossebo et al., 2017). In these studies, potential impacts and mitigation options were evaluated based on lists of potential threats and their likelihood of occurrence. We argue that due to the dynamic nature of ICT and its complex interdependency with the power infrastructure, we have to expect surprises. It will no longer be possible to identify a comprehensive inventory of potential threats, as is the case in classic risk management.

A reliable power supply is of great importance for almost all areas of life, therefore it is necessary to develop strategies that enable the power system to be prepared for expected and unexpected stressors. In other words, it is essential to apply a resilience management strategy. Many definitions of resilience exist in the scientific community e.g., (Jesse et al., 2019). For this study, we describe resilience as *a (socio-technical) system's ability to maintain its services under stress and in turbulent conditions* (Brand et al., 2017; von Gleich et al., 2010). The advantage of using this definition is that it focusses on *the system services*, which must be outlined together with the stakeholders/users. In this way, changes and evolutions of the system are possible, which are core aspects of transitions. The focus lies on the complex nature of interconnectedness and interdependency, and the capability of the system to maintain its *services*.

This article presents the results of an empirical and interdisciplinary base study that involved actors from energy and ICT sectors through interviews and workshops, to get better insights

into the vulnerabilities of CPPS. The study consists of two parts. First, a vulnerability assessment (VA) was performed to identify critical points coming from the ICT infrastructure. Second, a resilience strategy was developed by using a resilience management approach to identify how CPPS can be better prepared for any stressor.

# Methodology

## Vulnerability Assessment Approach

The event-based and structural VA methods (Fig. 1) carried out in (Gößling-Reisemann et al., 2013; von Gleich et al., 2010) were used as reference for this study.

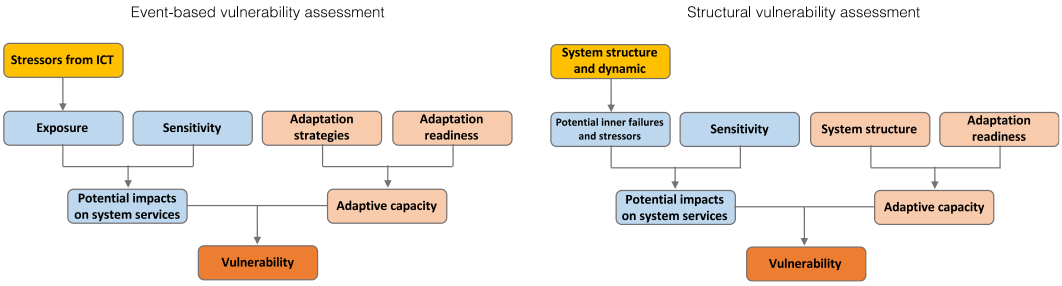


**Fig. 1** Schematic representation of the VA methodology. Left: Event-based VA. Right: Structural VA. *Source: Authors' own compilation based on* (Gößling-Reisemann et al., 2013; von Gleich et al., 2010)

The potential impacts were evaluated based on their effect on the *system services*, which were defined in this case according to parameters for both the electric and ICT infrastructures. Regarding the electric infrastructure, the quantity criteria are determined by the system's ability to supply the connected load. The quality criteria are defined by direct technical parameters, such as power quality or reliability indices, and by indirect parameters, such as socio-economic and socio-ecological impacts. Regarding the ICT infrastructure, the approach considers the effect on the security requirements, i.e. confidentiality, integrity, availability and non-repudiation of data in transit or at rest (e.g., control commands, firmware, software, etc.).

The study focused on the German and European power system covering the complete electrical energy conversion chain and was limited to evaluate stressors from the ICT infrastructure. The component layer of the Smart Grid Architecture Model[2] was used as a reference architecture model. Two workshops and 19 semi-structured interviews were conducted with experts from the sectors: energy, industrial automation, ICT, and public bodies in the time period between June 2016 to March 2017. The expert statements were evaluated

[2] http://smartgridstandardsmap.com/

by means of a comprehensive qualitative content analysis methodology based on (Mayring, 2014).

Combining the experts' opinions, relevant literature, and our own judgement, the potential impacts were qualitatively rated as high, medium or low according to the effects of stressors and structural weaknesses on the quality and quantity criteria of the system services. In order to determine the adaptive capacity, inputs from experts and literature were considered regarding existing or foreseen adaptation mechanisms and the readiness of the concerned actors to implement them. They were also qualitatively rated as high, medium or low. Consequently, the vulnerability level was the result of combining potential impacts and adaptive capacity according to the matrix showed in Fig. 2.

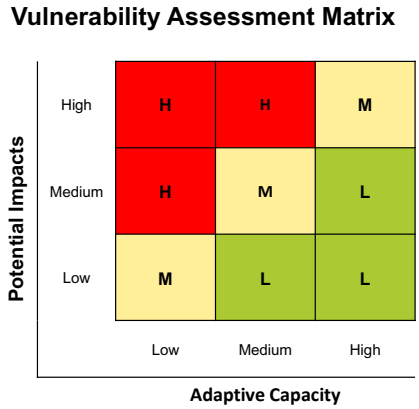


**Fig. 2:** Vulnerability assessment matrix that considers the level of potential impacts on systems services and adaptive capacity. (H: High, M: Medium, L: Low). *Source: Authors' own compilation based on* (Gößling-Reisemann et al., 2013; von Gleich et al., 2010)

## Resilience Management Approach

Resilient CPPS should have a diverse set of capabilities such as resistance/robustness, adaptation, innovation and improvisation to overcome known and unknown stressors. They help the systems to maintain their *system services* (see definition above). In this study the resilience management approach described in (Acatech et al., 2017; Goessling-Reisemann and Thier, 2019) was used as a reference. It comprises a four-phase approach: (1) Prepare and prevent, (2) Implement robust and precautionary design, (3) Manage and recover from crises, and (4) Learn for the future. The suggested measures for each step were developed based on: the VA results, the resilience design principles/elements described in (Brand et al., 2017; Goessling-Reisemann and Thier, 2019), the statements of the interviewed experts, and our own judgments (Fig. 3).

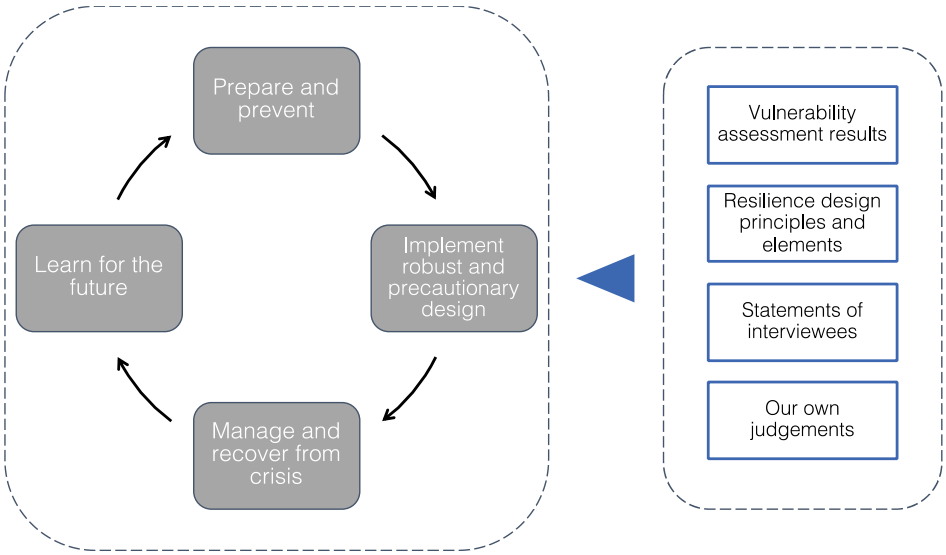


**Fig. 3:** Four phases of the resilient management approach scheme and the sources for determining the suggested measures for each phase. *Source: Authors' own compilation based on* (Acatech et al., 2017; Goessling-Reisemann and Thier, 2019)

# Vulnerability Assessment Results

The VA identified critical properties, structures and elements contributing to the vulnerability of the CPPS. Based on the qualitative content analysis results, the findings were sorted into the following four categories: (a) technology, (b) organizational security policies and procedures, (c) the human factor, and (d) regulations. Each category included subcategories and they were assessed individually using the VA methodology described above. All subcategories resulted in *high* vulnerability ratings following the combination of *medium to high* potential impacts with *medium or low* adaptive capacities (Tab. 1). The list of categories and subcategories is not intended to be comprehensive. However, it reflects the fact that the interviewees were queried about what the critical points are according to their opinion, which led to a list of high vulnerabilities. In the following section the findings for each category will briefly be described.

| Category | Subcategory | Potential Impacts | Adaptive Capacity | Vulnerability |
|---|---|---|---|---|
| Technology | Insecure endpoints | M-H | M | H |
| | Insecure communications | M-H | M | H |
| Organizational security policies and procedures | Improper patch management | M-H | M | H |
| | Lack of interdisciplinary IT-OT knowledge | M-H | M | H |
| The human Factor | Lack of security awareness in organizations | M-H | M | H |
| | Lack of security awareness among consumers | M-H | L | H |
| Regulations | Lack of effective implementation of standards and regulations | M-H | M | H |
| | Lack of coordinated effort to improve security | M-H | M | H |

**Tab. 1:** Categories and subcategories that reflect critical properties, structures and elements of CPPS and the corresponding ratings of Potential Impacts, Adaptive Capacity and Vulnerability on the scale L: Low, M: Medium, H: High. *Source: Authors' own compilation*

## Technology

The increased number of systems, endpoints and actors involved in the CPPS leads to a higher number of interconnections and communications. If these communications use unencrypted or weakly encrypted network protocols, authentication keys and data payload are exposed (NIST 2014). Using Man-in-the-Middle attacks, threat agents will be able to listen, inject or manipulate messages between nodes. From one side, legacy communication protocols used in Industrial Control Systems (ICS) in the generation, transmission and distribution domains have evolved from proprietary point-to-point links and isolated from external networks to open and standard protocols. According to the experts this represents a high security problem. The *'Crashoverride'* malware, which seems to have been used in the Ukraine blackout in 2016, is a good illustration of an advanced malware that leverages the weaknesses of certain ICS protocols (Dragos Inc., 2017). From the other side, experts also stated that the more distributed and closer to the end-consumer, the communication occurs, the more vulnerable it gets. The reason is that devices located at the customer premises (e.g., Internet-of-Things devices) are deployed with poor security features and furthermore, they are not regulated. In most of the cases they do not have capabilities for secure key management, control access, or patch management. Security challenges and threats of smart home devices are discussed in (Lee et al., 2014).

## Organizational Security Policies and Procedures

Experts agreed that due to the increasing complexity and interdependencies between IT and Operation Technology (OT) infrastructures, the knowledge needed to address the new

challenges has changed. In most of the cases interdisciplinary knowledge is missing or limited, and therefore it is difficult to properly understand, design, implement and operate the complete complex system. Normally, OT assets are maintained by ICS operators and engineers rather than experienced IT professionals, which can result in common mistakes in maintenance, configuration, and lack of hardening (Bodungen et al., 2017). Moreover, typical IT systems security measures cannot be directly applied in ICS environments, because the process stability or availability could be affected. Therefore, specific and tailored security measures are needed.

As experts stated, ICS usually tend to be outdated, either because vendors do not provide security patches or because the particular system is time-critical. As a consequence, attackers are able to gain access to different system components by exploiting known security-gaps that have not yet been patched. Nevertheless, even if all patches and mitigations are kept up-to-date, attacks are becoming more sophisticated and adversaries use unknown zero-day exploits (McLaughlin et al., 2015b).

**The Human Factor**

The lack of effective security trainings and awareness programs in power sector organizations can lead to insufficiently trained or engaged personnel in cyber-security aspects (NIST, 2014). Applying social engineering, threat agents are exploring new attack mechanisms targeting different levels in the organization. This is one of the fastest growing security problems according to the experts. In the Ukrainian blackout in 2015, attackers developed the *Blackenergy 3* tool malware and performed a phishing campaign targeting employees from the electricity distributor (Styzcynski and Beach-Westmoreland, 2017).

Disgruntled employees, or ex-employees, who are not properly managed when leaving the company may represent further potential threat actors. They could have detailed knowledge of the systems and access to critical data, allowing them to identify weak internal structures and methods to compromise the systems. Furthermore, critical information about the system configuration could even be publicly available through vendors' or asset owners' websites, employees' social media sites, etc. Attackers can leverage this information for planning the attack.

Additionally, experts mentioned also that end users represent another vulnerable point because of their lack of awareness or understanding of the consequences of eventually low security of their smart devices. A more complex problem derives from end-users being prosumers, who may not have the expert-knowledge to implement and maintain appropriate security measures for Distributed Energy Resource (DER) systems (e.g., smart inverters).

### Regulations

The lack of an effective implementation of security standards and regulations represents another critical point for CPPS. Experts considered that the absence of mandatory regulations to enforce power system operators to implement minimum required security standards, or vendors to provide the necessary security requirements in their products expose the system to possible cyber-attacks, for instance man-in-the-middle attacks on non-upgraded ICS systems running the IEC 60870-5 protocol (Maynard et al., 2014).

Different technical and organizational standards have been developed to address cyber-security requirements in smart grids (ENISA, 2012; NIST, 2014). Nevertheless, as experts stated, in most of the cases, these are only recommendations and the compliance to a minimum security level is not enforced by regulations. Furthermore, the experts mentioned that there are no economic incentives for grid operators to invest in cyber-security enhancements. The decision to upgrade legacy ICS in order to implement the security measures could be delayed until the next planned lifecycle equipment replacement, not only because of the processes' criticality, but due to the additional associated costs. Another critical point, as experts remarked, is the missing effective coordination to improve security for the overall system.

The critical points discussed in this section are related to all categories mentioned above. The relationship is seen as lack of readiness of the involved actors to implement existing adaptation strategies. Thus, increasing the vulnerability level of each category itself.

## Resilience management strategy

The VA unveiled the critical vulnerable points. Security measures, if applied, have great potential to reduce some vulnerabilities. However, they focus mainly on trying to keep the malicious attackers outside of the system. Therefore, one of the biggest challenges is to find a way to broaden the horizon in handling known and unknown stressors by including recovering, adapting and learning mechanism after successful attacks, instead of only focusing on prevention and detection. This is the objective of the second part of the study. Our main concern is how to increase the resilience in CPPS. This requires understanding that resilience is more than just eliminating identified vulnerabilities. The applied resilience management approach consists of four phases (Fig. 3).

During the **preparation and prevention** phase, weak points in the CPPS are identified and effective prevention measures must be derived. The focus here is on known stressors, thus a holistic security approach between IT-OT (IEC, 2016), and energy-focused risk analysis and

management strategies (Fischer et al., 2018) are needed. Experts also stress the importance of scalable and regularly tested security measures at endpoints (e.g., encryption, authentication, authorization, intrusion detection systems), patch management, network segmentation, as well as more effective and engaging security trainings and awareness programs. Technology-wise the implementation of additional measures for data storage and preserving unused resources - operational slack - to better deal with surprises are helpful (Fischer and Lehnhoff, 2019).

In order to enhance resilience, a **robust and precautionary system design should be implemented** from the beginning. This will empower the system to maintain its services even under stress or disturbances. The system should have a high diversity of IT components and redundancy in communication channels and devices (BNetzA, 2019). Maintaining the ability to rely only on physical parameters for operation as well as hardware-based security are helpful. Furthermore, implementing a cellular structure in order to secure a minimum and stable power supply in case of a failing central ICT infrastructure appears beneficial (VDE, 2015). Other suggestions supported by the experts are the implementation of real-time monitoring, intrusion and bad data detection (Iturbe et al., 2016; McCarthy et al., 2018), as well as periodic backups, and reducing services and functionalities in terms of data, ports, libraries, etc. (Fischer and Lehnhoff, 2019).

A resilient power system is able to ride through failures in order to **manage and recover from crises**. While the stability and security in this phase could be enhanced by multi-agent based control with decentral consensus finding (Lehnhoff and Krause, 2013), attention should also be paid to the ability to operate the system without ICT, i.e. manually, or to at least secure a *soft landing*, as experts stated. In addition, the provision of business continuity and emergency plans on a regional and local level, e.g., through *supplying islands* at least in and around public properties/buildings, and the preparation for active emergency planning and exercises based on realistic cyber-attacks have a high priority (Arghandeh et al., 2016).

Past and avoided disasters should be used in phase four **to learn for the future** in order to improve the adaptive capacity of the system. In this sense, digital forensic would allow to investigate incidents and near incidents in-depth and identify lessons. This should include the documentation of weaknesses that led to failures (*Vulnerability store*) (Gößling-Reisemann, 2016). Furthermore, strengths that avoided crises in the past or enhanced recovery are equally worth identifying, as they form the basis for planning strategies and emergency scenarios (*Solution store*) (Gößling-Reisemann, 2016). This documentation must be mandatory and publicly available.

Fig. 4 shows the summary of selected resilience-enhancing measures and elements for each phase of the resilience management approach.

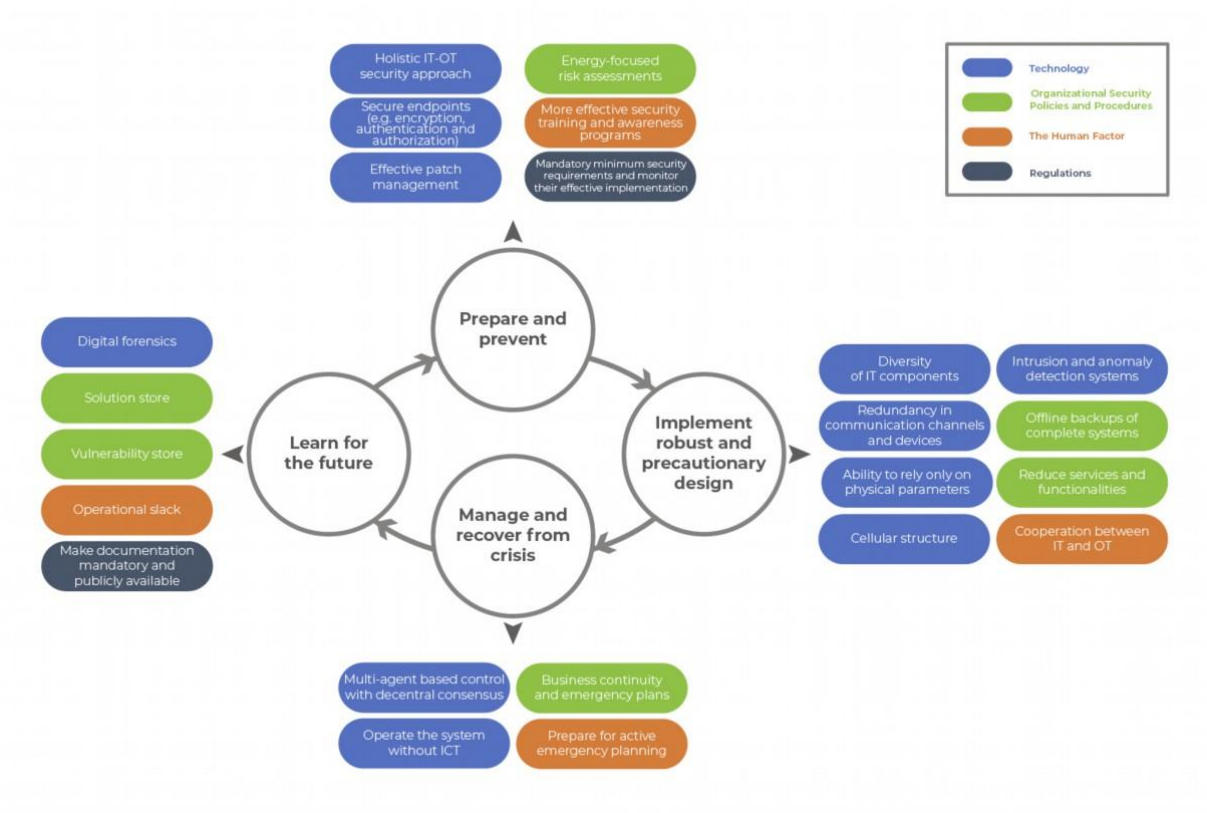


**Fig. 4:** Selection of resilience-enhancing measures and elements, sorted by the categories: Technology (blue), Organizational Security Policies and Procedures (green), the Human Factor (orange) and Regulations (grey), according to the Resilient Management approach phases. *Source: Authors' own compilation*

# Conclusions

In this study, critical properties, structures and elements contributing to the vulnerability of CPPS were identified. On one side, insecure communications or insecure end points, especially at the customer premises, resulted in a high vulnerability due to poor security features on the devices. On the other side, social engineering is a quickly growing security problem that enables threat agents to exploit one of the weaknesses present in every organization: the human factor. In spite of the existence of adaptation mechanisms that could minimize the impact, it was found that their implementation could be hindered by the lack of policy enforcement or the unreadiness of the involved actors to implement these measures. To address cybersecurity challenges, an integrated assessment considering physical, cyber and social perspectives is necessary. The aim is not only to try to keep attackers outside the system, but to design the system in a way that enables it to transform and adapt in order to cope with any kind of stressor. In other words, a resilience management strategy is needed, that considers that resilience is more than just eliminating identified vulnerabilities. This article

illustrated resilience enhancing measures assigned to the four phases of the resilience management cycle. One important measure is to establish an adequate cyber security regulation framework and monitor its effective implementation. Regarding the system architecture, a cellular structure and physical backup would build resilience in case of successful attacks. We conclude that introducing resilience principles/elements to the system and using a resilience management approach is a suitable way to prepare systems for the unexpected.

# 3 Methodology

The main objectives of the above-mentioned work packages of the *Strom-Resilienz* research project were to identify which additional vulnerabilities could arise from the digitalization of power systems and what would be the required strategies to increase the resilience of power systems to ensure that the system's primary functionality is maintained, even under stress.

In order to answer those questions, the study was performed in two parts. First, a vulnerability assessment (VA) was performed to identify the critical properties, structures and elements that make the system vulnerable to cyber-attacks. For this purpose, an interdisciplinary approach involving energy sector stakeholders and ICT solution providers through interviews and workshops was selected. Second, a resilience strategy was developed by using a resilience management approach to identify how cyber-physical systems can be better prepared for any stressor. Sections 3.1 and 3.2 describe the methodologies used in each part respectively.

## 3.1 Vulnerability Assessment Methodology

Two vulnerability assessment methodologies namely event-based vulnerability assessment (EVA) and structural vulnerability assessment (SVA), carried out during the study of climate change vulnerabilities of the energy systems in Northwest Germany (Gößling-Reisemann et al., 2013; von Gleich et al., 2010), were used as the reference for the assessment in this study. The selected methodological framework considers the vulnerability not only as a function of the system's exposure, the sensitivity of the system to external/internal stressors and the potential impacts on the power system services, but also considers the system's ability to cope with them. This ability identified as adaptive capacity, is based on existing or planned adaptation strategies and the willingness of the concerned actors to implement these measures (Gößling-Reisemann et al., 2013). Figure 1 and Figure 2 show the scheme of EVA and SVA methodologies.

It is worth mentioning that in the IT security field, the term 'vulnerability' commonly refers to a weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source (NIST, 2014). This definition differs from the one used in our VA methodologies as it only represents the system's exposure to a stressor, without considering the adaptation measures.

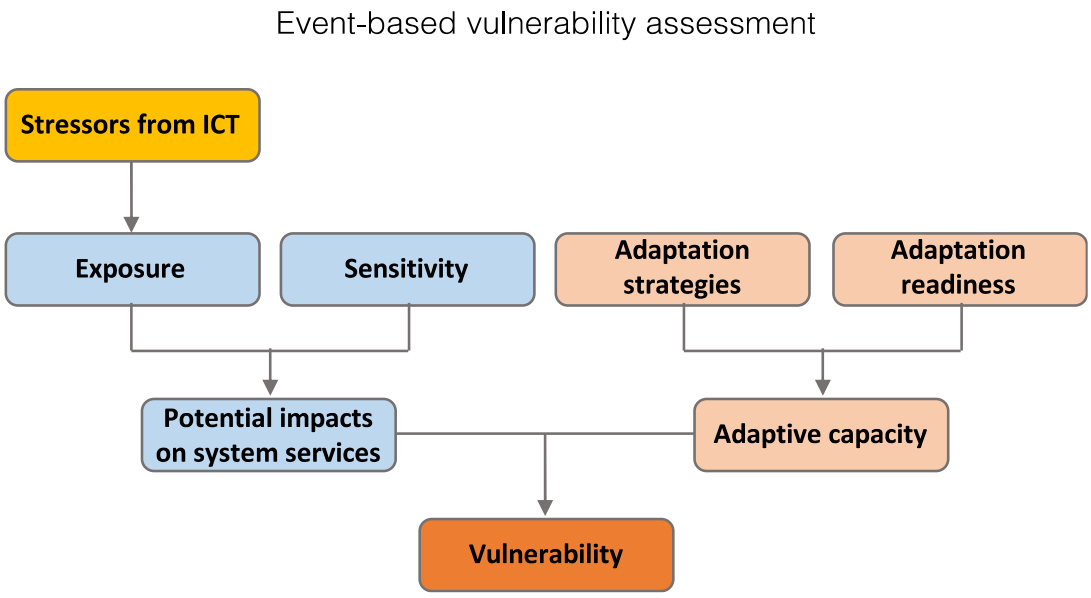


*Figure 1. Schematic representation of Event-based vulnerability assessment (EVA) methodology. Own representation based on (Gößling-Reisemann et al., 2013; von Gleich et al., 2010)*

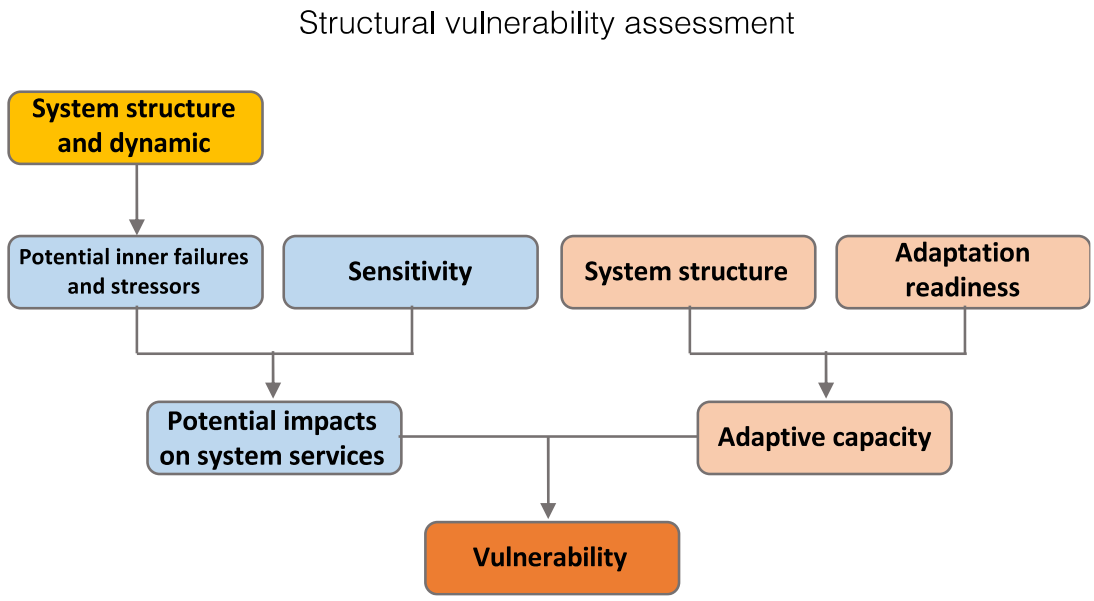


*Figure 2. Schematic representation of structural vulnerability assessment (SVA) methodology. Own representation based on (Gößling-Reisemann et al., 2013; von Gleich et al., 2010)*

The potential impacts were evaluated based on their effect on the system's services, which were defined according to specific parameters for both the power and ICT infrastructures (see Table 1).

*Table 1. Definition of system services for cyber-physical power system that considers criteria for the power infrastructure and the ICT infrastructure. Source: Authors' own compilation based on (Gößling-Reisemann et al., 2013; von Gleich et al., 2010)*

<table>
<tr><th colspan="2">Power Infrastructure</th></tr>
<tr><td colspan="2">Quantitative Criteria:</td></tr>
<tr><td colspan="2">Delivery of power</td></tr>
<tr><td colspan="2">Qualitative Criteria</td></tr>
<tr><td><u>Direct Technical Parameters</u><br>• Power quality:<br>▪ Voltage level (e.g., 400 V +/-10%)<br>▪ Frequency (e.g., 50 +/- 0.2 Hz)<br>• Reliability indices: e.g.,<br>▪ SAIDI (System Average Interruption Duration Index)</td><td><u>Indirect Parameters</u><br>• Environmental impacts: e.g.,<br>▪ $CO_2$ Emissions<br>▪ Land / Resources use<br>▪ Waste production<br>• Economic impacts: e.g.,<br>▪ Costs/Market price effects<br>▪ Competitiveness<br>• Social impacts: e.g.,<br>▪ Compromising customer privacy<br>▪ Jeopardizing technology acceptance</td></tr>
<tr><th colspan="2">Information and Communication Infrastructure</th></tr>
<tr><td>Data in transit or at rest, such as:<br>• Customer ID and location data<br>• Meter data<br>• Control commands<br>• Configuration data</td><td>• Time, clock settings<br>• Access control policies<br>• Firmware, Software and Drivers<br>• Tariff data<br>• …</td></tr>
<tr><td colspan="2">Security Requirements</td></tr>
<tr><td>• Confidentiality<br>• Integrity</td><td>• Availability<br>• Non-Repudiation</td></tr>
</table>

Regarding the power infrastructure, the quantitative criteria were determined by the system's ability to supply the connected load (Gößling-Reisemann et al., 2013). The qualitative criteria were defined by direct technical parameters, such as: power quality or reliability indices, and by indirect parameters, such as: environmental impacts, economic impacts (e.g., effects on

the energy market, billing inaccuracy) and social impacts (e.g., jeopardizing technology acceptance or invasion of customer privacy).

Regarding the ICT infrastructure, the approach considers the effect on the security requirements, i.e. confidentiality, integrity, availability and non-repudiation of data in transit or at rest (e.g., control commands, configuration data, firmware, software, meter data, etc.). The following is a short description of the security requirements (Cleveland, 2016):

- Confidentiality: preventing the unauthorized access to information
- Integrity: preventing the unauthorized modification or theft of information
- Availability: preventing the denial of service and ensuring authorized access to information
- Non-Repudiation: preventing the denial of an action that took place or the claim of an action that did not take place

### 3.1.1 Vulnerability assessment rating

Combining the experts' opinions (see sections 3.1.3 and 3.1.4 below), relevant literature and our own judgement the potential impacts on systems services were qualitatively rated as enumerated below, according to the effects of stressors and structural weaknesses on the quality and quantity criteria of the system services:

- **High,** if the quantitative criteria of power supply would be affected substantially,
- **Medium,** if the quantitative criteria were not affected substantially, but if the compromised security requirement could have a direct effect on the quantitative criteria, or at least one of the qualitative criteria parameters would be affected substantially,
- **Low,** if neither the quantitative nor qualitative criteria of power supply would be affected substantially, or if the compromised security requirement could only have an indirect effect on the qualitative or quantitative criteria.

In order to determine the adaptive capacity, inputs from experts and literature were considered regarding existing or foreseen adaptation mechanisms and the readiness of the concerned actors to implement them. They were also qualitatively rated as:

- **High,** if both an adaptation mechanism to avoid the potential impacts and the willingness to adapt were given.
- **Medium,** if either an adaptation mechanism to avoid the potential impacts or the willingness to adapt was given.

- **Low,** if neither an adaptation mechanism to avoid the potential impacts nor the willingness to adapt was given

Consequently, the vulnerability level was evaluated as the result of combining potential impacts and adaptive capacity according to the matrix showed in Figure 3. A high adaptive capacity prevents or mitigates the potential impact resulting in a vulnerability level that is one level below the potential impact level, except for the case when the potential impact is already low. A medium adaptive capacity does not change the potential impact. However, a low adaptive capacity increases the vulnerability one level above the potential impact level, based on the hypotheses that under these circumstances weak stressors can go unnoticed (and unanswered) for a long time, leading to accumulating impacts on system service (Gößling-Reisemann et al., 2013).

The measures to improve adaptation capacity have great potential to not only reduce vulnerability but to also increase the resilience of the systems. Therefore, the results from the vulnerability assessment were used as a starting point to identify the resilience strategy.

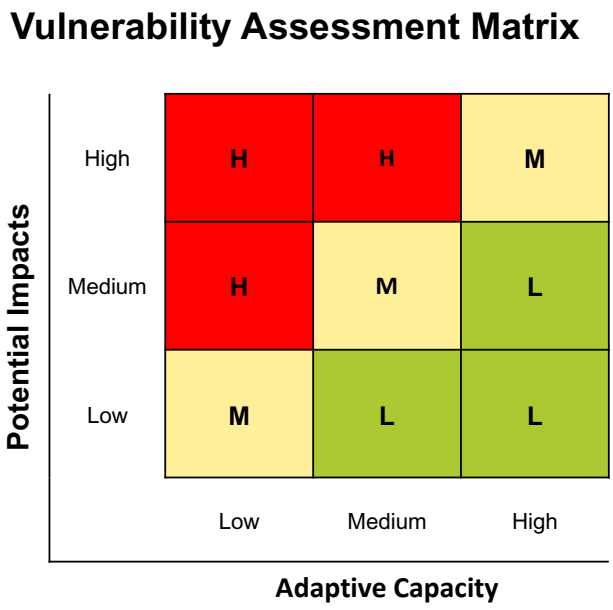


*Figure 3 Vulnerability assessment matrix that considers the level of potential impacts on systems services and adaptive capacity. (H: High, M: Medium, L: Low). Source: Authors' own compilation based on (Gößling-Reisemann et al., 2013; von Gleich et al., 2010)*

### 3.1.2 Reference architecture model

This study was focused on the German and European power system covering the complete electrical energy conversion chain. As a reference architecture model, the component layer of the Smart Grid Architecture Model (SGAM) (CEN-CENELEC-ETSI Smart Grid Coordination Group, 2012) used by the International Electrotechnical Commission (IEC) in the Smart Grid Standards Mapping Tool (IEC, 2020) was used. Figure 4 shows the reference architecture model used for the VA and Figure 5 shows a simplified view of the SGAM plane.

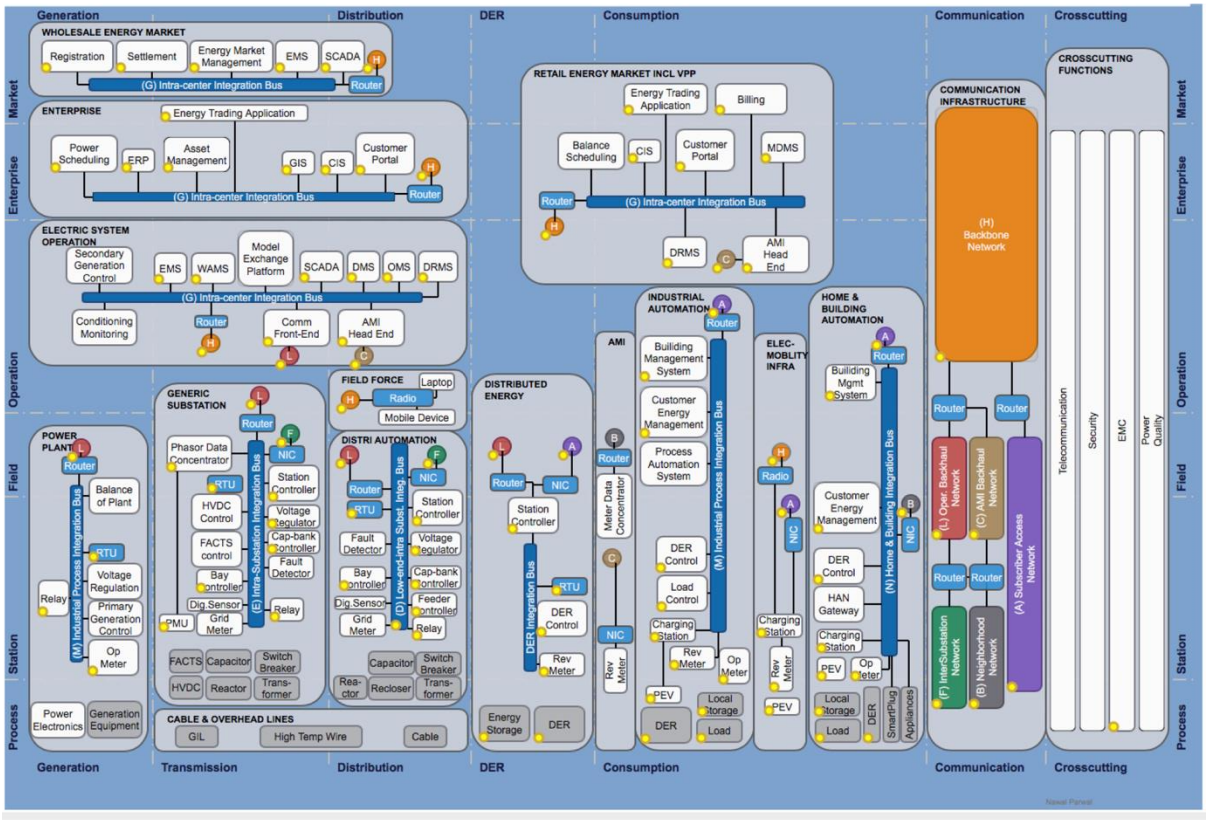


*Figure 4 Reference architecture model used for the vulnerability assessment. Source: (IEC, 2020)*

The SGAM model consists of five consistent layers representing business objectives and processes, functions, information models, communications protocols and components. Each layer covers the smart grid plane which is spanned by smart grid domains and zones. The SGAM model represents not only the current state of implementations in the electrical grid but furthermore, it represents the evolution to future smart grid scenarios by supporting the principles universality, localization, consistency, flexibility and interoperability (CEN-CENELEC-ETSI Smart Grid Coordination Group, 2012). These characteristics allowed us to use this reference architecture model as material for the expert interviews and workshops to discuss about cyber security of power systems assuming a complete implementation of the smart grid functionalities.

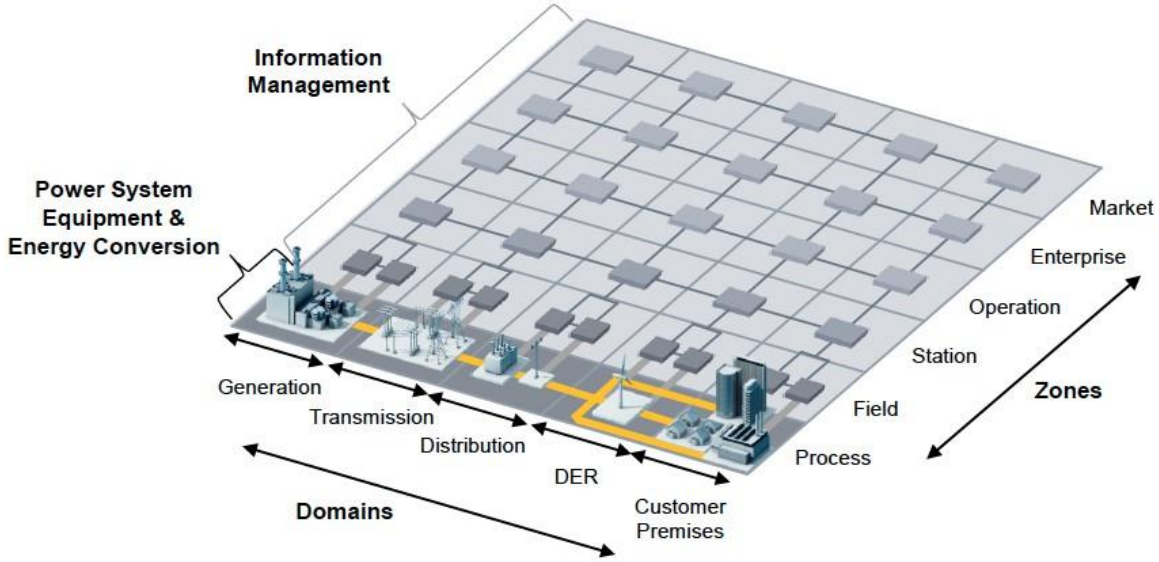


*Figure 5 Smart Grid Plane. Source: (CEN-CENELEC-ETSI Smart Grid Coordination Group, 2012)*

This study covered the different smart grid domains: generation, transmission, distribution, distributed energy resources (DER), customer premises, and smart grid zones: process, field, station, operation, enterprise and market according to the SGAM architecture (see Figure 5. The following is an overview of each SGAM domain, zone and layer (CEN-CENELEC-ETSI Smart Grid Coordination Group, 2012):

***SGAM Domains:***

| | |
|---|---|
| **Bulk Generation** | Representing generation of electrical energy in bulk quantities, such as by fossil, nuclear and hydro power plants, off-shore wind farms, large scale photovoltaic (PV) power– typically connected to the transmission system |
| **Transmission** | Representing the infrastructure and organization which transports electricity over long distances |
| **Distribution** | Representing the infrastructure and organization which distributes electricity to customers |
| **DER** | Representing distributed electrical resources, directly connected to the public distribution grid, applying small-scale power generation technologies (typically in the range of 3 kW |

| | |
|---|---|
| | to 10.000 kW). These distributed electrical resources can be directly controlled by DSO |
| **Customer Premises** | Hosting both - end users of electricity, also producers of electricity. The premises include industrial, commercial and home facilities (e.g., chemical plants, airports, harbors, shopping centers, homes). Also generation in form of e.g., photovoltaic generation, electric vehicles storage, batteries, micro turbines are hosted |

***SGAM Zones:***

| | |
|---|---|
| **Process** | Including both - primary equipment of the power system (e.g., generators, transformers, circuit breakers, overhead lines, cables, electrical loads …) - as well as physical energy conversion (electricity, solar, heat, water, wind …). |
| **Field** | Including equipment to protect, control and monitor the process of the power system, e.g., protection relays, bay controller, any kind of intelligent electronic devices (IED) which acquire and use processed data from the power system. |
| **Station** | Representing the aggregation level for fields, e.g., for data concentration, substation automation… |
| **Operation** | Hosting power system control operation in the respective domain, e.g., distribution management systems (DMS), energy management systems (EMS) in generation and transmission systems, micro-grid management systems, virtual power plant management systems (aggregating several DER), electric vehicle (EV) fleet charging management systems. |
| **Enterprise** | Includes commercial and organizational processes, services and infrastructures for enterprises (utilities, service providers, |

| | |
|---|---|
| | energy traders …), e.g., asset management, staff training, customer relation management, billing and procurement. |
| **Market** | Reflecting the market operations possible along the energy conversion chain, e.g., energy trading, mass market, retail market... |

***SGAM Layers***

| | |
|---|---|
| **Business** | Represents business cases which describe and justify a perceived business need |
| **Function** | Represents use cases including logical functions or services independent from physical implementations |
| **Information** | Represents information objects or data models required to fulfill functions and to be exchanged by communication |
| **Communication** | Represents protocols and mechanisms for the exchange of information between components |
| **Component** | Represents physical components which host functions, information and communication means |

### 3.1.3 Expert workshops

Two workshops were conducted in June 2016 and March 2017 with experts from ICT and energy sector both from industry and academia to discuss about vulnerability and resilience of cyber-physical power systems.

#### 3.1.3.1 First Expert Workshop

During the first workshop, the VA methodology approach described above was used in a limited version. For this exercise, a set of cyber security failure scenarios developed by the U.S. National Electric Sector Cyber-security Organization Resource (NESCOR) Technical Working Group 1 (NESCOR, 2015) was used as the starting point for the discussion. The

mentioned document describes for each of the failure scenarios, the relevant vulnerabilities[3], impacts and mitigation strategies. Potential impacts included power loss, equipment damage, human casualties, revenue loss, violations of customer privacy and loss of public confidence.

Small working groups in the workshop were organized according to the different domains of the power sector. Each group discussed at least one NESCOR failure scenario, in order to identify the stressors, the exposure and the sensitivity of the system under pre-described conditions. The feasibility of putting these conditions into practice was also discussed. Furthermore, the groups discussed about current adaptation mechanisms to prevent the occurrence of the scenarios and/or restore service after the failure. The NESCOR scenarios analyzed were:

- *"Threat agent causes of grid instability through control of dedicated data and voice lines between system operating center and plant (GEN.10)"*
- *"Switched capacitor banks are manipulated to degrade power quality (DGM.10)"*
- *"DER systems shut down by spoofed SCADA control commands (DER.14)"*
- *"Mass meter remote disconnect by authorized individual (AMI.1)"*
- *"Unauthorized pricing information impacts utility revenue (AMI.10)"*

The results from the workshop provided us with valuable insights about some of the main cyber-security challenges that needs to be addressed as a result of the increased complexity of ICT system in the different domains of the power system.

#### 3.1.3.2 Second Expert Workshops

In the second expert workshop, the preliminary results of the VA were presented and discussed with the participants. Based on the results from the discussions, the VA and the resilience strategy were concretized. The major focus was on the granularity of the energy system, but technical, organizational and regulatory measures to increase resilience were also discussed.

### 3.1.4 Expert interviews

In order to gain more profound knowledge for the vulnerability assessment, almost 100 experts from ICT and energy field were contacted for this study, out of which 19 participated in a personal or telephone semi-structured interview from October 2016 to March 2017. The interviewees were divided according to their field of expertise into five categories as listed in Figure 6.

[3] The term *vulnerability* from the NESCOR document is understood as *weakness*/*exposure* in our methodology.

During the interviews, the experts were inquired about cyber-vulnerability of current and envisioned power systems, potential impacts on the power systems services and possible adaptive strategies to cope, adapt or recover from them. The list of questions used in the interviews can be found in Appendix A: Interview Analysis Methodology.

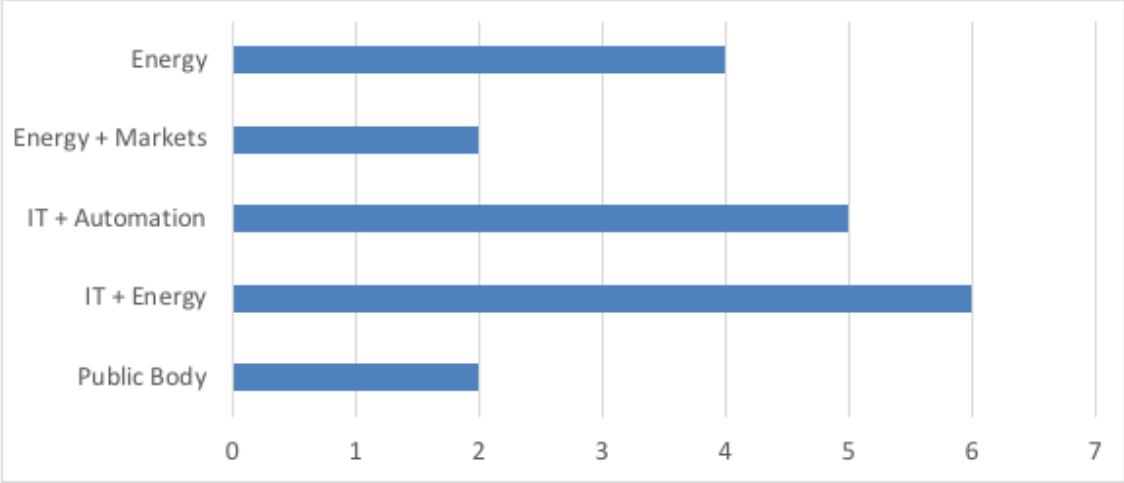


*Figure 6 Categories according the field of expertise of the interviewees and number of participants*

### 3.1.5 Qualitative content analysis

The statements from the expert workshops and interviews were evaluated by means of a comprehensive qualitative content analysis methodology based on (Mayring, 2014) and used as input information for the VA.

Due to the fact that some of the interviewed experts asked to remain anonymous, for the interview analysis it was decided to use *'Interviewee X'* as the participant identification for all of the interviewees, where *X* represent the sequential number according to the time when the interview took place. This identification will be used in the following sections to reference the statements from the interviewees.

More detailed information of the qualitative content analysis can be found in Appendix A: Interview Analysis Methodology.

## 3.2 Resilience Management Approach

In the last decade the concept of resilience has grown in popularity and multiple definitions are used by the research community (see (Jesse et al., 2019)). We describe resilience as *a (socio-technical) system's ability to maintain its services under stress and in turbulent conditions* (Brand et al., 2017; von Gleich et al., 2010). The advantage of using this definition is that it focuses on the system services, which must be outlined together with the stakeholders and/or users. In this way, changes and evolutions of the system are possible, which are core

aspects of transitions. The focus lies on the complex nature of interconnectedness and interdependency, and the capability of the system to maintain its services.

Resilience can also be interpreted as the capacity of the system to prepare for, cope with and recover from any stressor, while maintaining the system's services without necessarily knowing beforehand about the specifics of the event or the stressor (Gößling-Reisemann, 2016). Therefore, it is necessary to distinguish certain characteristics of stressors and the capabilities that a resilient system should possess in order to deal with them. Stressors can be characterized by their dynamics and the state of knowledge about their nature, as follows (Gößling-Reisemann, 2016):

- **Known/expected**: stressors that the system has already experienced in the past and where predictions of future occurrences exist
- **Unknown/unexpected**: stressors that the system has never or only very rarely been exposed to and where predictions for future occurrences do not exist
- **Gradual/creeping**: stressors that develop slowly and possibly undetected for some time
- **Abrupt/sudden**: stressors that develop suddenly or abruptly without warning

A system that is capable of preparing for, coping with and recovering from stressors with an arbitrary combination of the above-described attributes needs a diverse set of capabilities that can be summarized as robustness, adaptive capacity, innovation capacity and improvisation capacity (See Figure 7).

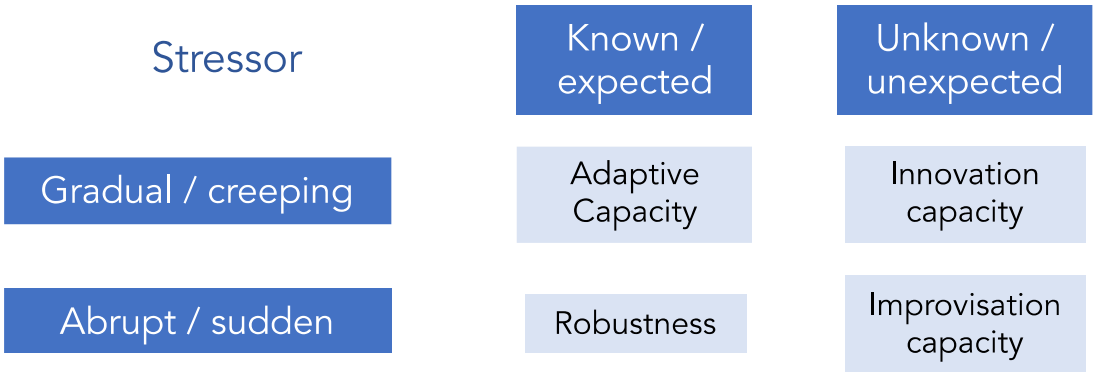


*Figure 7 Assignment of the required abilities of a system to be prepared for different stressors. The stressors are differentiated according to time of occurrence and degree of awareness. Source:(Gößling-Reisemann, 2016)*

When stressors develop gradually and are already known to the system or can be expected to occur in the near future, an adaptation of existing structures, components and organizations can be initiated to better cope with and recover from occurrences of this stressor. On the other extreme, when the stressor is unknown and develops abruptly, actors in the system will not

have time to find innovative solutions or build up resistance, thus they will have to improvise (Gößling-Reisemann, 2016).

The focus of the second part of the study was to investigate how to develop resilience within the CPPS and related organizations. For this purpose, the above definition of resilience was used as a guiding principle and the resilience management approach described in (Acatech et al., 2017; Goessling-Reisemann and Thier, 2019) was used as a reference.

This approach comprises four phases: (1) Prepare and prevent, (2) Implement robust and precautionary design, (3) Manage and recover from crises, and (4) Learn for the future, which will be briefly described in the following section. The suggested measures for each step were developed based on the VA results, the resilience design principles/elements described in (Brand et al., 2017; Goessling-Reisemann and Thier, 2019), the statements of the interviewed experts, and our own judgments (Figure 8).

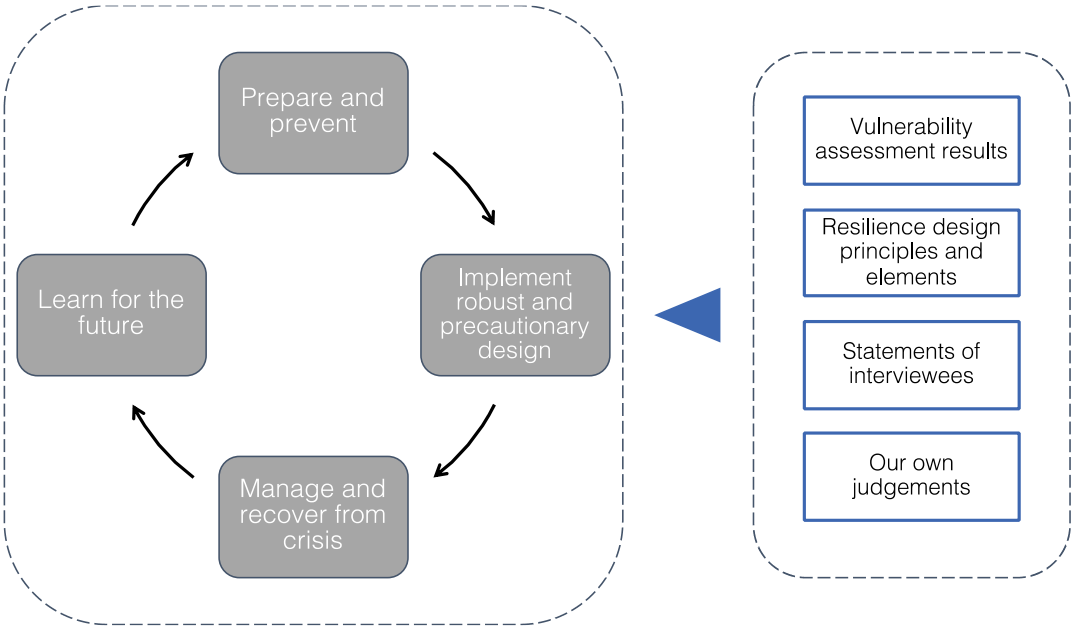


*Figure 8 Resilient management approach scheme showing the four phases and the sources for determining the suggested measures for each phase. Source: Own representation based on (Acatech et al., 2017; Goessling-Reisemann and Thier, 2019)*

### 3.2.1 Preparation and Prevention

During **preparation and prevention** phase, weak points in the system need to be identified and effective preventive measures and guidelines must be derived from the results (Acatech et al., 2017). Past crises and near accidents should be transparently documented and examined to learn about the stressors that caused them and the context in which they occurred, or in which they were avoided, respectively (Gößling-Reisemann, 2016). Further analysis should be directed at stressors that have not yet occurred, but are likely to occur in

the near future, e.g., known from trend extrapolation. Furthermore, new threats can stem from social processes, for example: increasing non-acceptance of certain technologies or unfair cost-benefit distributions in the context of energy transitions leading to protests and delays or halts in necessary system changes. Newly developing stressors can be analyzed by vulnerability assessment methodologies. Results from these assessments should then be used to adjust the design parameters of energy system components (technology level), develop testing scenarios and design guidelines for coupled infrastructures (system level) and monitor social impacts and responses to technological change with feedback to governance processes (governance level) (Gößling-Reisemann, 2016).

### 3.2.2 Implementation of a robust and precautionary system design

The second phase of building resilience focuses on the implementation of a **robust and precautionary system design** to withstand any kind of stressor. In line with the above detailed characteristic capabilities of resilient systems, the central design elements of resilient energy systems must comprise robustness, adaptive capacity, innovation capacity and improvisation capacity. On the design level of components and systems, the resilience-enhancing capabilities can be achieved by first strengthening the identified vulnerable elements (see Preparation and Prevention phase) by increasing redundancy, buffer capacity and energy storage. This will reduce the stress on vulnerable elements in the system and will also act as a precautionary measure for further and yet unknown stressors (Gößling-Reisemann, 2016). In order to prepare for unknown future stressors, principles and elements that enhance the resilience of the system should be implemented in the system.

The principles and elements that are summarized in Figure 9 are derived from a search on design principles and elements with known resilience-enhancing features, e.g., taken from the knowledge of evolutionary processes in ecosystems or socio-technical resilience in energy systems, organizations and other application fields. A brief description of selected elements is given below, a more detailed analysis can be found in (Brand et al., 2017).

**Diversity** contributes positively in the way that a system can respond to stressors. In order to make the concept of diversity more operational and potentially measurable, Stirling suggests to specify diversity in terms of disparity, variety and balance (Stirling, 2007). Disparity is understood as the differences between system elements. Variety characterises the amount or number of different elements with the same functionality in the system. Balance is given by the distribution (mix) of these different elements (Goessling-Reisemann and Thier, 2019). It is also advisable to check existing technologies in the energy system for alternative solutions to enhance diversity.

**Redundancy** describes the multiple availability of elements in a system, either in number or in functional equivalence. These multiple elements are usually not needed in normal operation. Numerical redundancy is understood as the provision of a number of identical elements with the same function, while functional redundancy refers to the situation where the same function is delivered by distinctly different elements (e.g., by different technologies, operating systems, etc.) (Goessling-Reisemann and Thier, 2019).

**Geographical dispersion** plays an important role for resilience. By spreading system elements geographically, all localized stressors, from weather related events to terrorist attacks, have a relatively smaller attack surface (Goessling-Reisemann and Thier, 2019). Distributing system-critical services over a wider geographical range thus enhances resilience.

The implementation of **buffer and storages** in systems will enable the system to maintain its services in case of internal or external resource restrictions. Buffer and storages provide the system with extra capacities that delay critical system states after a disrupted supply. These elements thus serve several functions that enhances a system's resilience; they decouple sub-systems or infrastructures from each other, ensuring functioning of system even after connections have been severed, they also buy extra time for the system's recovery and facilitate the recovery process by itself. If implemented locally, they can help in maintaining a minimum service to a larger number of system users in times of crisis (see (Lovins and Lovins, 2001) for illustrations in electricity grids) Delivering backup power from batteries in cases of disrupted transmission grids is one example (Goessling-Reisemann and Thier, 2019).

A system that can be divided and split into sub-segments is called **modular/cellular**, if the aggregated elements provide full system function in the sub-segments (Goessling-Reisemann and Thier, 2019)**.** Modularity is considered to enhance reparability and lower outage times in technical systems, but it also allows for an enhanced diversity if modules are equipped with well-defined interfaces so as to ease swapping different technological implementations (Huang and Kusiak, 1998) cited in (Goessling-Reisemann and Thier, 2019).

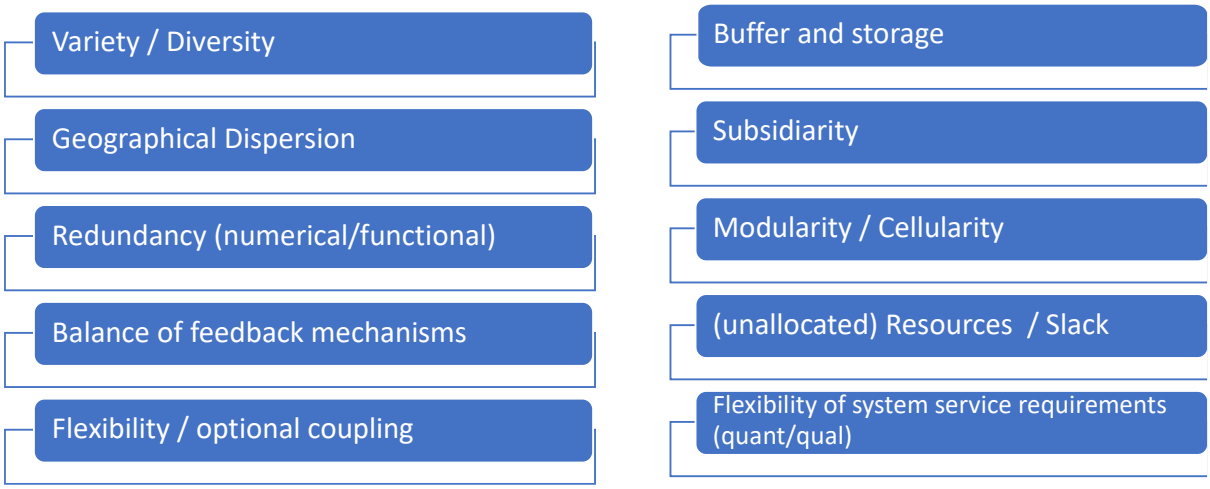


*Figure 9 Overview of principles and elements that enhance the resilience of systems. Source: (Goessling-Reisemann and Thier, 2019)*

### 3.2.3 Manage and recover

If failures of the energy system led to crises, they should be restricted to the smallest possible area or sub-system and be overcome as quickly as possible. To reduce the extent of such crises, emergency planning and respective measures must be implemented on the regional or local level. With the increasing share of renewable energies comes a trend towards decentralization of energy systems, which can be utilized for increased resilience (Gößling-Reisemann, 2016).

### 3.2.4 Learn for the future

Past disasters and avoided disasters should be used to **learn for the future** and thus improve the adaptive capacity of the system. This can be achieved by documenting and analyzing these crises and events thereby identifying the weaknesses that led to their occurrence (vulnerability store), or, respectively, identify the strengths that led to their avoidance or recovery (solution store). Knowledge about crises and potential solutions should then be used to create simulations and business games for system actors on all levels. Improvisation capacity can be increased by confronting actors in these simulations with unforeseen and unlikely developments, like combined external threats and internal failures of equipment (Gößling-Reisemann, 2016).

# 4 Vulnerability Assessment Results

The VA identify a wide range of critical properties, structures and elements coming from the ICT infrastructure that contribute to the vulnerability of CPPS. Based on the qualitative content analysis results, the findings were sorted into four categories and subcategories as shown in Table 2.

*Table 2. Categories and subcategories that reflect critical properties, structures and elements of cyber-physical power systems*

| Category | Subcategory |
|---|---|
| Technology | Insecure endpoints |
| | Insecure communications |
| Organizational security policies and procedures | Improper patch management |
| | Lack of interdisciplinary IT-OT knowledge |
| The human Factor | Lack of security awareness in organizations |
| | Lack of security awareness among consumers |
| Regulations | Lack of effective implementation of standards and regulations |
| | Lack of coordinated effort to improve security |

The vulnerability of each subcategory was assessed individually using the VA methodology described in 3.1 and the results will be explained in the following sections.

## 4.1 Technology

### 4.1.1 Insecure communications

Increasing the number of systems, services and actors involved in the cyber-physical power system means that higher number of interconnections are required. Since power systems use nearly the same TCP/IP based communication technology used in business IT networks, its related cyber-security problems also affects power systems (Interviewee 1, personal communication, 2016; Interviewee 6, personal communication, 2016). However,

security requirements are not the same as in business and industrial networks. Confidentiality is an important aspect of standard IT because of the secrecy associated with companies' information, but hardly a priority in industrial control systems (ICS), where integrity and availability of data is vital to keep systems running (Marin Fernandes, 2012).

If the communications use unencrypted or weakly encrypted network protocols, authentication keys and data payload are exposed. Using clear text protocols may also enable adversaries to perform session hijacking and Man-in-the-Middle (MITM) attacks, allowing the attacker to manipulate the data being passed between devices (NIST, 2014). While some connections may be more secure than others, the weakest link can be used as an attack vector into other domains due to the highly interconnected nature of the cyber-physical power systems (Knapp, 2011).

In order to assess the vulnerability due to insecure communications, the SGAM domains of the power system (see Figure 4) were grouped in three clusters: (a) consumption, (b) distributed energy resources and distribution, (c) generation and transmission.

#### 4.1.1.1 Exposure and sensitivity

**a. Consumption**

In the case of smart meter infrastructure, the majority of the experts mentioned that Germany has a strong encryption communication scheme based on the IT security architecture and security requirements defined by the German Federal Office for Information security (BSI) in their Smart Meter Gateway Protection Profile (see (BSI, 2014)).

According to this security architecture, depicted in Figure 10, the central communication component is a Smart Meter Gateway (SMGW) that is located at customer premises and connects the electronic measuring equipment in the Local Metrological Network (LMN), as well as any controllable consumption, storage, or production devices in the Home Area Network (HAN) with the various market participants (e.g., Smart Meter Gateway Administrator (SMGA) on behalf of the metering point operator, distribution system operator or energy supplier) in the Wide Area Network (WAN) (BSI, 2015a). The SMGW collects, processes and stores the records from meter(s) and ensures that only authorized parties have access to them. Relevant information is signed and encrypted before being sent, using the cryptographic services of a Security Module, which is embedded as an integral part into the SMGW. The Protection Profile (PP) defines the security objectives and corresponding security requirements for a Security Module that is utilized by the Gateway for cryptographic support (BSI, 2014)). To ensure the interoperability of the various components in the smart metering infrastructure, BSI

defined technical implementation guidelines that can be found in the Technical Guideline TR-03109, see (BSI, 2013).

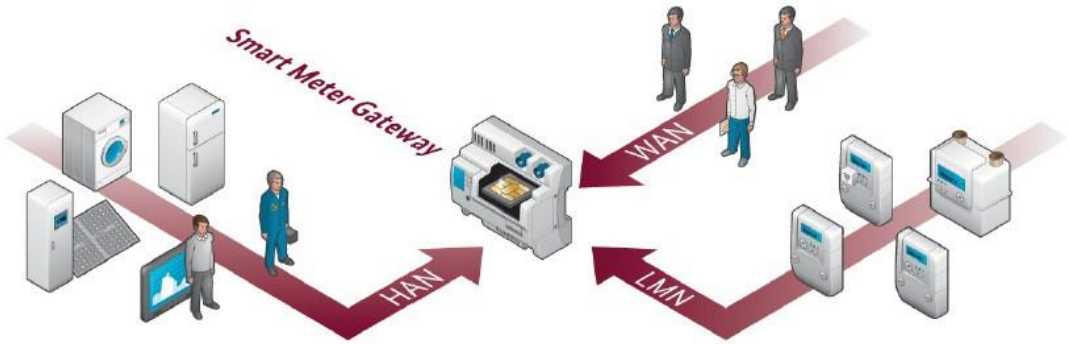


*Figure 10 Smart Meter Gateway Architecture. Source: (BSI, 2015a)*

Despite the fact that this communication scheme aims at ensuring data protection, data security and interoperability, some experts also mentioned that it presents some drawbacks. The scheme is already some years old and the main purpose is to encrypt only the communication between the SMGW and the SMGA. The security requirements for the communication between the SMGW and other actors, i.e. the external market is not regulated in the SMGA certification process, which could imply a potential security gap that could compromise the security requirements of smart metering data (Interviewee 8, personal communication, 2017; Interviewee 19, personal communication, 2017).

An evaluation of the PP and their related technical implementation guidelines were performed by von Oheimb, D. in (von Oheimb, 2012) and several drawbacks were pointed out. It was mentioned that the security scheme required heavy protection mechanism only for SMGW that implies high technical overhead as well as high involved costs for implementation, certification and use. Furthermore, regarding the encryption scheme, the study mentioned that the use of a classical Public Key Infrastructure (PKI) introduces very critical central points of failure, where exploiting any weakness may cause enormous damage to the overall system. This was confirmed by an IT security interviewee, who mentioned that using public key cryptography in the energy sector, power systems would essentially inherit problems of public key cryptography that are currently affecting online security, like websites. Essentially, the problems lie in the overhead for maintaining a PKI, namely, the certificate authorities and key management (Interviewee 13, personal communication, 2017).

Inside the customer's premises, communication protocols used in home or building automation systems (e.g., automated lighting systems, surveillance systems, smart appliances, and other IoT devices.) could represent another entry point for potential data breaches, mainly because some of these protocols are insecure-by-design and not addressed in current regulations. One example of this weakness can be found in the work done by Morgner *et al.* in (Morgner et al., 2017). They performed a security analysis of the network protocol ZigBee Light Link (ZLL), one of the most popular standards used by lighting systems intended for residential, commercial, and industrial buildings. The analysis was targeted at the ZLL *touchlink* commissioning procedure that is used for integrating ZLL devices through close proximity instead of cryptographic authentication. The results showed that the *touchlink* communication relies on communications frames, which are neither secured nor authenticated. Furthermore, the transport of the network key to a joining device is protected solely by a global master key, which was leaked in March 2015 and cannot be renewed due to the backward compatibility demands towards legacy ZigBee Light Link products (Morgner et al., 2017). ZigBee is a popular standard for wireless low-power communication implemented in several Internet of Things (IoT) devices for other applications that includes door locks and intrusion alarm systems, adding more insecure entry points that could compromise security requirements of data inside the HAN.

**b. Distributed Energy Resources (DER) and Distribution**

The growing penetration of distributed energy resources has made the grid more dynamic and complex (Arghandeh et al., 2016), increasing significantly the number of devices (e.g., smart inverters, battery controllers) that are owned and controlled by consumers and third-parties (Qi et al., 2016).

At the local level, DER systems manage their own generation and storage activities autonomously based on local conditions, pre-established settings, and DER owner preferences. However, DER systems are active participants in grid operations and need to be coordinated with other DER systems and distribution grid devices (IEC, 2016). In the work developed by Qi, J., et al. (Qi et al., 2016), a DER system architecture clustered in four domains was proposed that depicts the different actors and interactions (see Figure 11) used for the analysis of cyber-security for DER and smart inverters.

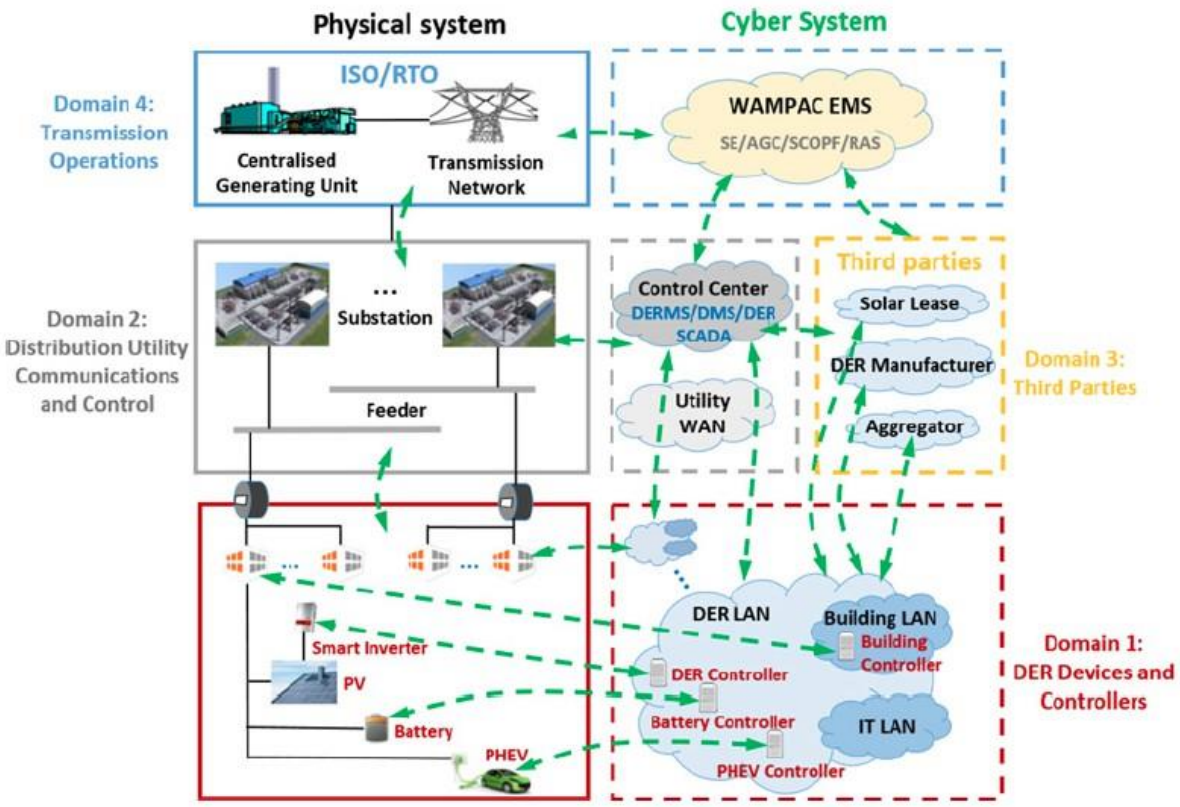


*Figure 11 Generic architecture of power systems with DER. Source: (Qi et al., 2016)*

The following are some critical points related to insecure communication mentioned by the authors (Qi et al., 2016):

- *Domain 1: DER devices and controllers*: The DER owners get the information about the DER by communicating with smart inverters with insecure wireless communication protocols such as ZigBee.
- *Domain 2: Distribution utility communications and control*: The utility interacts with the smart inverters and controllers using communication protocols such as smart energy profile (SEP) 2.0, that should be checked for vulnerabilities.
- *Domain 3: Third Parties:* Most of the third-party entities have the ability to monitor the status of DER, and some may also have the ability to directly control their operation. Furthermore, these entities may have connectivity to a very large number of DER. These interconnections introduce centralized points that could potentially be leveraged by attackers to manipulate and influence a large number of DER across multiple distribution grids.
- *Domain 4: Transmission Operation:* DER operations need to be integrated with the large power grid operations. Communication protocols used for this purpose include Distributed Network Protocol (DNP3) and IEC 61850, which are insecure by design and security improvements could not always be

implemented (see section 4.4.1 Lack of effective implementation of security standards and regulations).

As mentioned by one interviewee from the energy and market sector, the communication infrastructure for DER is partially regulated and external actors such as: manufacturers (e.g., PV inverters or wind turbine manufacturers) or direct marketers can access the controllers of distributed generation units in order to get information for monitoring and controlling purposes. Problems could arise because these actors have their own communication infrastructure to the generation units which could be insecure and be a back door to access the system (Interviewee 2, personal communication, 2016).

**c. Generation and Transmission**

Communication protocols in ICS and Supervisory Control and Data Acquisition (SCADA) Systems have evolved over time from proprietary point-to-point links to open and standard protocols used across distributed systems (McLaughlin et al., 2015). In the beginning, the communication infrastructure of power systems was generally secure because it was isolated from external communication networks (the so called 'air-gap'). Additionally, they were based on custom proprietary hardware and software which conferred them a reasonable level of 'security by obscurity' (Teixeira et al., 2015). However, the extended convergence with ICT networks and the dominant communication based on TCP/IP protocols represent a high security problem for the power systems (Interviewee 2, personal communication, 2016).

Legacy ICS communication protocols were designed without cyber-security in mind therefore, they do not have IT security mechanisms implemented such as encryption or authentication (Interviewee 15, personal communication, 2017). For instance, Modbus is a simple client-server protocol that was originally designed for low-speed serial communication in ICS networks. Given that the Modbus protocol was not designed for highly security-critical environments, Modbus packages are sent unencrypted, therefore it could be easy for an attacker to link to a legitimate network node and manipulate the message that will not be recognized by the receiver (Interviewee 15, personal communication, 2017; Mo et al., 2012), compromising measurement values or control commands which could lead to system malfunction.

Furthermore, industrial control networks in some cases are connected directly to the internet without proper security measures in place thus enabling the access for external threat agents who could infect the industrial networks with viruses or malware (Interviewee 1, personal communication, 2016; Interviewee 15, personal

communication, 2017). Search engines such as SHODAN[4] can be used to easily find internet facing ICS devices. Furthermore, open source and commercial tools for exploiting well-known ICS protocol weaknesses can be easily found on the internet, exposing even more of these systems to potential attacks.

At the station zone from the SGAM model (see section 3.1.2), some sensors or Intelligent Electronic Devices (IED) use wireless communication, which in general tend to be more insecure because of weak protocols, lack of encryption methods or improper device configuration. However, to compromise these devices physical proximity is required, which could be limited for external threat agents inside industrial environments (Interviewee 15, personal communication, 2017). There could be an attack scenario where the initial point of intrusion is located at the substation through wireless devices and spread towards the electrical system operations. If this is not accounted for, it could represent a serious risk (Interviewee 18, personal communication, 2017).

Most of the manufacturers have remote service interfaces for inspection and monitoring of larger components, e.g., a power turbine. Remote access can also get into the controller level or Human Machine Interface (HMI) level for installing updates or patches. If the connection is not properly secured, this remote access could allow access into the system device or further for malicious purposes. Grid operators can also implement remote connections to different devices, e.g., substations equipment, in order to install updates or patches. For this purpose, dedicated communication networks can be used, especially by big operators, but other small operators could use networks leased by telecommunication operators or through the internet. In the latter cases, if the security polices for the communication infrastructure are not properly implemented, data security requirements could be compromised (Interviewee 4, personal communication, 2016; Interviewee 17, personal communication, 2017).

#### 4.1.1.2 Attack mechanisms and stressors

Lack of encryption and authentication implemented for communication protocols enable threat agents to use MITM attacks to perform different actions, such as: a) record communication between nodes and replay packets in order to hide real system behavior without detailed knowledge about the system, b) hijack sessions, when a communication session is taken over by the attacker and used for unauthorized

[4] https://ics-radar.shodan.io

communication with the victim, or c) inject or manipulate data to alter reading and commands in the communication stream in real time (McLaughlin et al., 2015).

In the following section some attack mechanisms and stressors against communication infrastructure at different domain clusters will be described:

**a. Consumption**

Sniffing and eavesdropping attacks can be used by remote or local threat agents to compromise the confidentiality and integrity of privacy-relevant data or billing-relevant data. Remote attackers located in the WAN (see Figure 10) could try to compromise a component of the local infrastructure to cause damage to a component itself or to produce a direct impact on the power grid, e.g., producing grid instability through data manipulation of the smart inverters. Local attackers, including prosumers who have access to the gateway and/or meters, could try to read out or alter assets without authorization while stored or transmitted in the LMN (see Figure 10) (von Oheimb, 2012).

Denial of Service attacks targeting availability of network devices inside the HAN could be done by physical attacks on the communication infrastructure. Wired communication can be affected by 'cutting the wires' and wireless communications can be jammed (McLaughlin et al., 2015). Jamming attack consist of sensing the channels until a communication is intercepted, then overwhelming the channel with illegitimate traffic could be used to affect data availability (Tazi and Abdi, 2015). This kind of attack could be used to prevent meters from connecting with the utility company through stuffing the wireless media with noise. The channel will always be seen as busy by carriers and data packets will be prevented from being received (Baig and Amoudi, 2013) cited in (Lopez et al., 2015).

Morgner and colleagues (Morgner et al., 2017) developed a real-world attack to eavesdrop and packet injection attacks against the wireless communication of ZigBee devices that are commonly used in the smart home domain. The evaluation showed that the protocol security gaps enable the threat agents to compromise the availability of the devices and gain control over all nodes in the network.

**b. Distributed Energy Resources (DER) and Distribution**

Utilities, DER manufacturers or third-party aggregators may need to remotely communicate with DER in order to control the operating points and monitor the status of the devices, which is critical to maintain the reliability of the distribution grid. If the communication is not encrypted or uses insecure network protocols, these weaknesses

could enable threat agents to perform MITM attacks to deny, disrupt, or change the messages. If these attacks occur, they could provide the attacker with the ability to control a large number of DER systems which could produce a serious impact on the distribution grid (Qi et al., 2016).

**c. Generation and Transmission**

The lack of encryption and authentication of many industrial control protocols leaves the system exposed to a range of attacks. For instance, through MITM attacks, a threat agent can intercept communication frames and collect unencrypted plaintext frames that could provide valuable information, such as: source and destination addresses as well as control and settings information (Mo et al., 2012). The attacker can inject or alter readings and commands in the communication stream in real time. While intercepting all packets, some packets can be dropped, altered or new packets can be injected with arbitrary outcome. This attack is very problematic if executed by an experienced user, as it is hard to detect and can potentially have a significant effect. An attacker is able to manipulate measurement values from remote sites as well as to suppress or inject control commands between two communicating nodes (McLaughlin et al., 2015).

Protocol specific attacks can be found in the literature. For instance, possible attacks such as: message spoofing, replay attacks, network scanning, and others related to targeting Modbus security issues are detailed in (Mo et al., 2012). Open-source or commercial tools for performing MITM attacks on Modbus networks can also be easily found on the internet[5] (Bodungen et al., 2017). Regarding protocols used for power substation automation, several authors cover the use of DoS attacks on networks running the IEC 60870-5 protocol (Dondossola et al., 2008, 2009) and others present a MITM attack on ICS relying on the IEC 60870-5-104 (Maynard et al., 2014).

The malware known as *'Crashoverride'* (aka *'Industroyer'*) is a real illustration of an advanced and sophisticated piece of malware that combines multiple attack mechanism and leverages the weaknesses of certain industrial protocols used for power substation automation. In Box 1 detail information of this malware is given.

[5] Modbus-VCR (see https://github.com/reidmefirst/modbus-vcr) is an example of a freely available tool that in conjunction with Ettercap, will record Modbus traffic and then replay that traffic so systems appear to be operating as usual for a recorded time period

**Box 1: *'Crashoverride'* malware**

In June 2017, security researchers form ESET and Dragos released a detailed analysis of this malware that was developed to target ICS components. According to the authors, it is very probable that *'Crashoverride'* could have been used to impact a transmission level substation in Ukraine in December 2016 causing power outages (See: (Cherepanov, 2017; Dragos Inc., 2017)).

Threat actors behind the *'Crashoverride'* malware showed a deep knowledge and understanding of industrial control systems used in power systems and targeted industrial communication protocols which were designed some decades ago without security in mind. Therefore, the attackers "didn't need to be looking for protocol vulnerabilities; all they needed was to teach the malware "to speak" those protocols" (Cherepanov and Lipovsky, 2017).

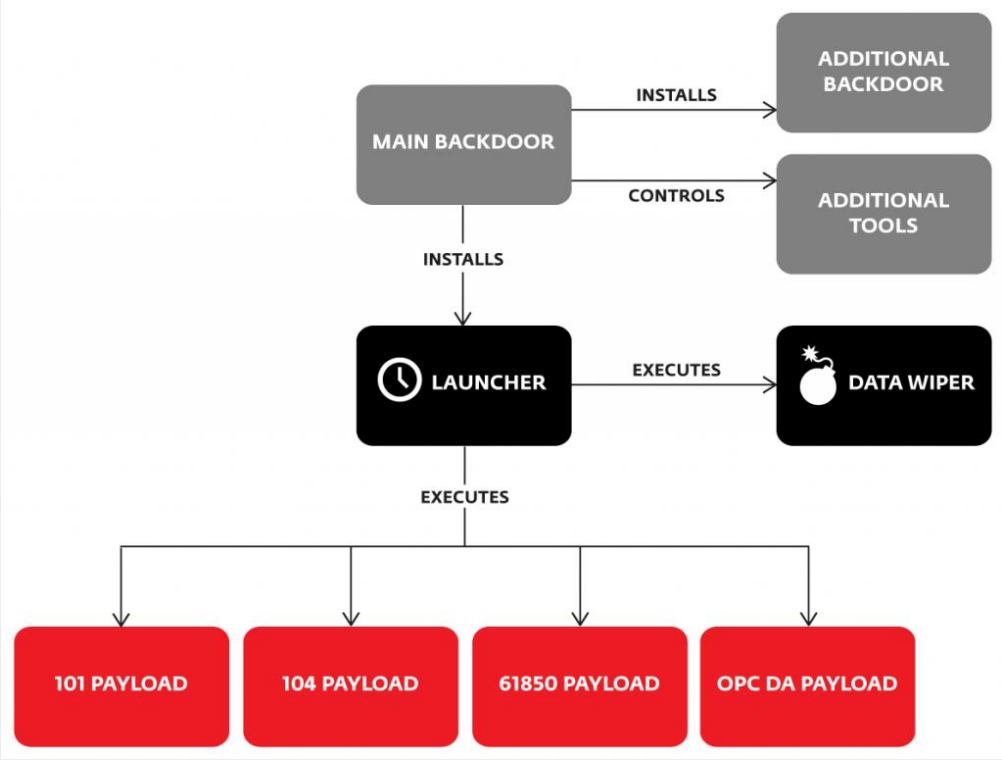


*Figure 12 Simplified schematic of 'Crashoverride/Industroyer' components. Source (Cherepanov and Lipovsky, 2017)*

The *'Crashoverride'* malware is a modular framework that is capable of controlling power substation switches and circuit breakers directly. Figure 12 shows the malware's structure that consists of a main backdoor, an additional backdoor, a loader module and several supporting and payload modules. The backdoor is used by the threat agents to install and control the other components. It connects to a

remote server (command control center, C&C) in order to receive commands and to report to the attackers. The additional backdoor (a *'trojanized'* version of the Windows Notepad application) provides an alternative persistence mechanism that allows the attackers to regain access to a targeted network in case the main backdoor is detected and/or disabled. The launcher module, which contains a specific time and date, loads payload modules and begins an either 1- or 2-hours countdown to launch the data wiper component. The payload components target particular industrial communication protocols specified in the following standards: IEC 60870-5-101, IEC 60870-5-104, IEC 61850, and OLE for Process Control Data Access (OPC DA). The wiper module is designed to erase system-crucial registry keys and overwrite files to make the system unbootable and the recovery harder (Cherepanov, 2017; Cherepanov and Lipovsky, 2017; Dragos Inc., 2017).

Following a brief description of the key feature of each payload module:

- The 101 payload is named after the international standard IEC 60870-5-101 (aka IEC 101) that describes a serial communication protocol for monitoring and controlling electric power systems used for communication between ICS and Remote Terminal Units (RTUs). The 101 payload partly implements the protocol described in IEC 101 and is capable to read a configuration file to enumerate all the RTUs connected to it. The main objective of this payload is to change the on/off state of the underlying RTU (Cherepanov, 2017; Virsec, 2017).
- The 104 payload is a variant of the above 101 payload that runs over a TCP/IP network and can discover RTUs in the network. It was named after the international standard IEC 60870-5-104 (aka IEC 104). The malware 'kills' the original process that performs the normal 104 payload monitoring process and replaces it with a rogue process. In stage 1, the rogue process connects to the target RTUs and iterates through their states. In stage 2, the rogue process continuously flips the on/off state of the target RTUs and logs success so that the operators do not receive an alert (Virsec, 2017).
- The 61850 payload is named after the IEC 61850 standard that describes a protocol used for multi-vendor communication between devices that perform protection, automation, metering, monitoring and control of electrical substation automation systems. Once executed, the module leverages a configuration file to identify targets and without a configuration file, it enumerates the local network to identify potential targets. It communicates with the targets to identify whether the device controls a circuit breaker switch. The payload enumerates the data and creates a log with rich

meta-data about each target for export to the C&C (Cherepanov, 2017; Dragos Inc., 2017; Virsec, 2017).

- The OPC DA payload component implements a client for the protocol described in the OPC Data Access specification. OPC (OLE for Process Control) is a software standard and specification that is based on Microsoft technologies such as OLE, COM, and DCOM. The Data Access (DA) part of the OPC specification allows real-time data exchange between distributed components, based on a client–server model. This payload queries the various OPC Servers it discovers and is looking for items provided by OPC servers that belong to solutions from ABB such as their MicroSCADA range[6]. Once executed, the module will send out a 0x01 status which for the target systems equates to a "Primary Variable Out of Limits" leading operators to misunderstand protective relay status (Cherepanov, 2017; Dragos Inc., 2017; Virsec, 2017).

  The additional tools include Denial-Of-Service (DOS) tool that exploit the vulnerability CVE-2015-5374[7] causing the SIPROTEC digital relay from Siemens to fall into an unresponsive states until it is rebooted manually (Cherepanov, 2017).

#### 4.1.1.3 Potential impacts

The use of insecure communication channels will affect the data security requirements. In the following section, potential impacts for each domain cluster evaluated in the previous section are detailed:

**a. Consumption**

Compromising data confidentiality through MITM attacks is seen as a more relevant security issue in the smart metering infrastructure than in the other power system domains (Interviewee 1, personal communication, 2016). The analysis of energy consumption data can provide significant insight into the privacy of customers (Greveler, 2016). For instance, if a threat agent is able to monitor the power consumption that can be directly related to activity patterns inside the customer premises, this could have implications on household owners' security. Attackers could deduce when the owners are at home in order to perform criminal activities (Interviewee 13, personal communication, 2017).

[6] See: http://new.abb.com/substation-automation/products/software/microscada-pro
[7] See: https://ics-cert.us-cert.gov/advisories/ICSA-15-202-01

The implementation of demand response schemes could also have privacy implications. Demand response requires high frequency measurements of consumption and generation, and the availability of flexible loads. If this privacy-sensitive information gets into the wrong hands, breaching the confidentiality of such information would also have privacy implications (Interviewee 18, personal communication, 2017).

A detailed information about the debate around privacy and data protection for the Smart Meter security scheme in Germany can be seen in (Greveler, 2016).

**b. Distributed Energy Resources and Distribution**

Compromising communication links to DER systems could provide an attacker with access to a large number of DER devices. These impacts maybe minor if the third-party access is limited to only monitoring the state of the DER. However, if the third-party has the ability to change operational set points or software configurations, then attacks against these systems could have serious impacts that may cascade beyond a single distribution grid (Qi et al., 2016).

Some related failure scenarios can be found in the NESCOR catalog (NESCOR, 2015). For instance, the scenario DER.6 illustrates the case when a threat agent compromises DER sequence of commands, possible through a replay attack, causing grid imbalance and power outages. In the scenario DER.14, a threat agent spoofs DER SCADA control commands causing power instability, including outages and power quality problems.

**c. Generation and Transmission**

Data injection attacks against SCADA system or intelligent electronic device (IED) could cause system disruptions. Rogue protocol commands can be sent to force slave devices into inoperable states, shut down services or force resets. Certain commands can be broadcasted to multiple devices at once, thus stopping the flow of network traffic and resulting in Denial of Service (DoS). In addition, malicious codes can be used to erase data from diagnostics (Lopez et al., 2015; Mo et al., 2012).

In the case of the *'Crashoverride'* malware that leveraged weaknesses of industrial communication protocols, the Dragos team described legitimate attacks and impact scenarios that included: de-energized substations and a forced islanding event (Dragos Inc., 2017). In the first scenario, malicious control commands are effectively sent to open closed breakers in power substations in an infinite loop. If a system operator tries to issue a close command on their HMI (Human Machine Interface) the sequence loop will continue to re-open the breaker. This loop maintaining open breakers will effectively

de-energize the substation line(s) preventing system operators from managing the breakers and re-energizing the line(s). The impacts of de-energizing a line or substation will depend on the system dynamics, power flows and other variables. In some circumstances, it may not have an immediate effect while in others it can produce power outages. Furthermore, due to the fact that the control center will lose remote control of the breakers, it will be necessary to send a service crew to the substation for manual operation. This will imply a few hours of outages.

In the second scenario, threat agents target one or multiple RTUs and a control command is sent to begin a loop that toggles the status of the breaker between open and close continuously. Changing the breaker status will invoke automated protective operations to isolate the substation that could produce grid instabilities. If multiple substations are coordinately compromised the impact will be extended power outages.

#### 4.1.1.4 Potential impacts rating

The use of insecure communication channels will compromise integrity and availability and non-repudiation requirements, which could have a direct effect on the delivery of power. Compromising data confidentiality could have an effect on indirect parameters, i.e., public acceptance of smart metering. Therefore, according to the VA methodology, the potential impacts range from Medium to High.

#### 4.1.1.5 Adaptation strategies and implementation

As interviewees stated, in order to preserve the security of the power system, multiple levels of security mechanism should be built on top of each other. First, it is required to implement cryptographic methods on data and communication channels in order to ensure data integrity and prevent unintended disclosure of information in transit. On top of this, the implementation of intrusion detection systems (IDS) is required to have an effective visibility on attacker's activities. (Interviewee 1, personal communication, 2016; Interviewee 13, personal communication, 2017). The advantage of IDS is that they can detect known attacks, there are available databases of patterns and signatures of common attacks that can be download. However, the disadvantage is that these kind of systems are not able to detect unknown attacks, which will require other approaches (Interviewee 1, personal communication, 2016)

The use of encryption is not always the appropriate choice and a full understanding of the information management capabilities that are lost through the use of encryption should be completed before encrypting unnecessarily (NIST, 2014). As experts from IT and automation sector mentioned, data encryption on industrial control networks could

increase the latency. There are solutions from some vendors for encryption devices to be installed before the ICS, e.g., PLC, that encrypt/decrypt the communication. Other solutions providers are developing specific devices to provide secure communication between their devices. Further solutions should go toward encryption directly on industrial controllers. Quantum encryption is a novel solution specially designed to achieve confidentiality, but for industrial networks the most important criteria is availability, and this solution needs to prove that it does not add extra latency and affect the system performance in general (Interviewee 15, personal communication, 2017). In the case where it is impractical to encrypt all measurements, it becomes critical to detect and isolate the measurements which are under attack. Effective attack isolation enables the damage control (e.g., removing attacked measurements for state estimation) to be performed in a timely fashion before the attack can lead to any incident with significant consequences (Teixeira et al., 2015).

In the case of legacy ICS communication protocols, there are already standards to increase the security. For instance the IEC 62351 set of standards provides security improvements for protocols such as IEC 60870-5- 104 and IEC 60870-5-101.However, vendors do not implement them and usually provide only basic functionalities, thus distribution grid providers will not be able to create a secure environment (Interviewee 1, personal communication, 2016) (See section 4.4.1 for more information on lack of effective implementation of security standards as a vulnerability condition).

Furthermore, experts from IT and automation sector mentioned that according to their experience, customers or companies in the industry sector usually do not want state-of-the-art technology, but already tested and robust solutions (Interviewee 15, personal communication, 2017).

Since a large part of today's power grid equipment is old, data encryption can be costly to implement because of the required corresponding update of the equipment. Therefore, it is important to identify which measurements should be encrypted in order to maximize the benefits of the protection resources (Teixeira et al., 2015).

#### 4.1.1.6 Adaptation capacity rating

According to the previous section, there are available adaptation mechanisms (e.g., ICS security protocols) that improve communication security, however, the readiness to implement them could be limited due to preference of ICS owners or related additional costs. Therefore, the adaptation capacity is rated as medium.

### 4.1.1.7 Vulnerability rating

According to the rating assessment of potential impacts in section 4.1.1.4 and adaptation capacity in section 4.1.1.6, high potential impacts and medium adaptation capacity results in High vulnerability due to insecure communication.

Figure 13 summaries the vulnerability assessment due to insecure communications.

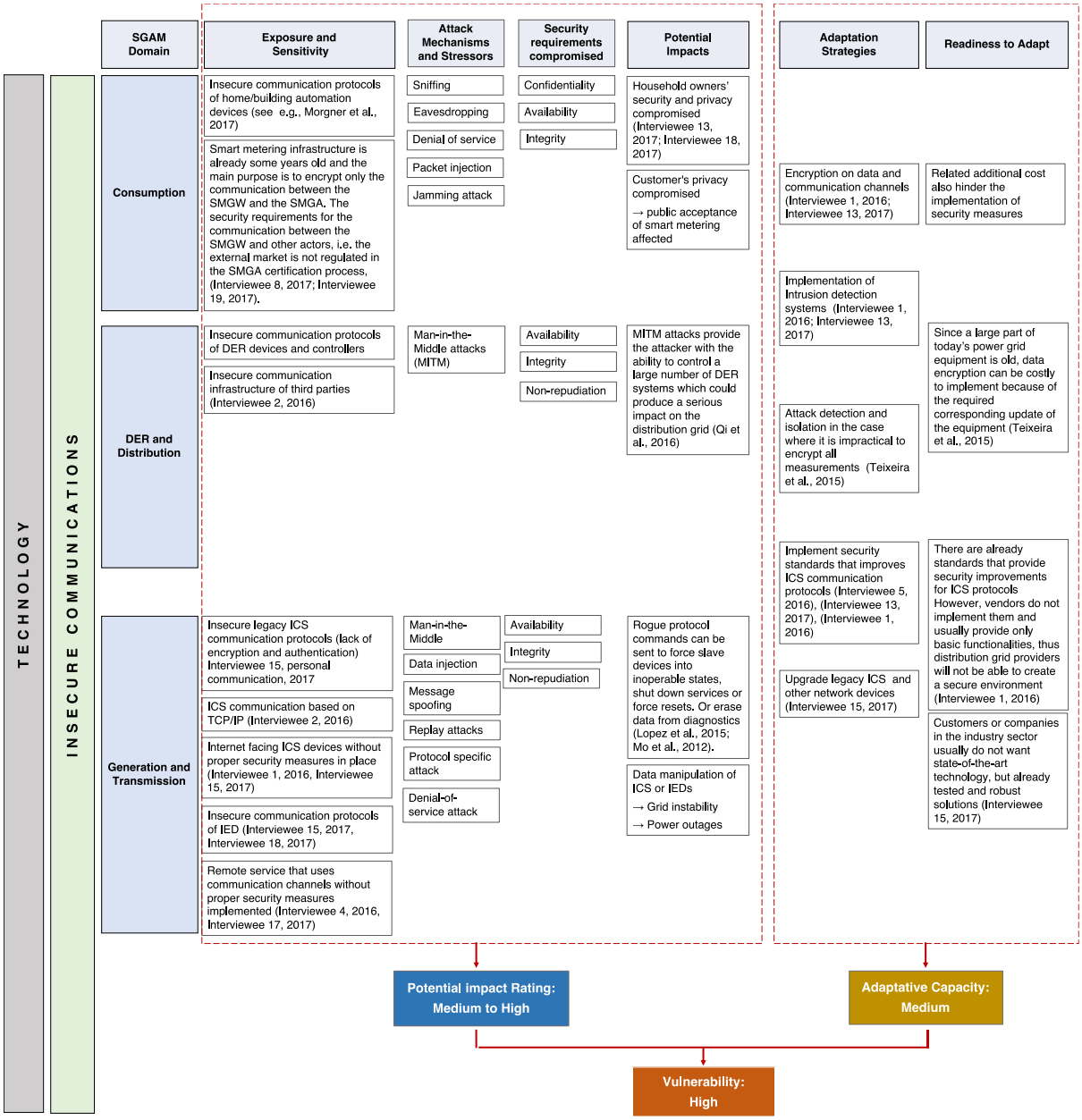


*Figure 13 Summary of vulnerability assessment of cyber-physical power systems due to insecure communications. For the assessment the SGAM domains of the power system were grouped in three clusters (a) consumption, (b) distributed energy resources (DER) and distribution, (c) generation and transmission. Source: Authors' own representation*

### 4.1.2 Insecure endpoints

In network security an endpoint is any device that is network-enabled. Endpoints at different zones and domains from SGAM denote their own challenges. In order to assess the vulnerability due to insecure endpoints, the SGAM domains of the power system (see Figure 4) were grouped in three clusters: (a) consumption, (b) distributed energy resources, (c) generation, transmission and distribution.

#### 4.1.2.1 Exposure and sensitivity

**a. Consumption**

Endpoints located at the customer premises (see Figure 4) (e.g., home automation system, IoT devices mobile phones, laptops) are not regulated by cyber-security measures and they are deployed with poor security features. Therefore, if well-known vulnerabilities of these devices are exploited, they could be used as malicious entry points to conduct further attacks to the power infrastructure. These devices do not have security capabilities such as secure key management and secure credential storage. Also, there is a problem of authentication because in many cases the devices do not have an ID and they do not have good credentials to authenticate. Additionally, there are not enough capabilities to address patch and software management of the devices. Control access to the network are also limited (Interviewee 5, personal communication, 2016; Interviewee 14, personal communication, 2017; Interviewee 18, personal communication, 2017).

Furthermore, the lack of software integrity checks or signed software in IoT devices makes it easy to upload malware on these devices, from where an attack could be launched to perform denial of service attacks (Interviewee 5, personal communication, 2016). Security challenges and threats of smart home devices are further discussed in (Lee et al., 2014).

If the devices are more distributed, there is also a problem of scalability of implementation of security measures to secure them properly, because it is required to monitor, maintain and update not only few end-points, but thousands of them (Interviewee 5, personal communication, 2016). In this aspect, electro mobility will represent a future large attack surface on the customer side (Experten-Workshop 2, 2017).

According to the German regulation, smart meters have to comply with very strict security conditions which aim to increase the security level of the metering infrastructure. However, there are other services or devices equipped with extensive

control possibilities (e.g., smartphones applications), which are not currently regulated (Experten-Workshop 2, 2017)

**b. Distributed energy resources**

A more complex problem mentioned by an expert originates from end-users being prosumers, i.e., being energy producers, while consuming both self-generated power and power delivered by the grid. Previously, in a classic power system generation, transmission and distribution systems were operated by companies and treated as isolated systems. However, the connection of distributed energy resources systems to the grid that are maintained and owned by end-customers is bridging the air gap that previously enabled the achievement of a certain level of cyber security. The problem arises when these distributed systems are connected to insecure networks or to the internet. As a consequence, it has to be assumed that the system would be connected to potentially insecure endpoints, therefore conventional security measures such as authentication or authorization will not be sufficient (Interviewee 14, personal communication, 2017).

Small scale DER systems do not have mandatory regulations to secure these systems therefore representing a potential point for malicious intrusions (Interviewee 2, personal communication, 2016).

**c. Generation, Transmission and Distribution**

Endpoints at station and field zones (see Figure 4) are often installed at remote installation sites without operation or maintenance personnel in place. Therefore, if end-devices at these locations do not have proper security measures, a potential attacker could have the time to try to compromise the insecure devices (computers or network devices), get into the network and launch an attack from there (Interviewee 5, personal communication, 2016).

Even end-points located inside industrial facilities (e.g., power plants, transmission substations), which normally are closed locations, could be compromised. Experts on IT security for industrial automation mentioned that those points where users can interact with the system represent weak points as well, because user or operators could modify or manipulate configuration parameters or control commands. RTUs and PLCs are prone to this kind of stressors (Interviewee 15, personal communication, 2017).

Furthermore, remote access capabilities of systems or devices could also represent potential malicious intrusion points. As mentioned by an interviewee, remote access is not insecure per se, because if there is a secure channel with appropriate measures in

place it is possible to detect attacks like eavesdropping or man-in-the-middle. However, a problem could arise when one of the end-points is potentially insecure (Interviewee 14, personal communication, 2017). For example, if laptops infected with a virus or malware, or connected simultaneously to insecure networks (e.g., the Internet) are used for remote maintenance purposes, these end points could compromise the system (Experten-Workshop 1, 2016).

#### 4.1.2.2 Attack mechanisms and stressors

If the end device is compromised, the adversary does not need to break the cryptography to read or manipulate the data. Different attack mechanisms could be performed in the different SGAM domains:

**a. Consumption**

Threat agents could upload malicious codes or malwares to poorly secured automation devices at customer's premises in order to control them and launch denial of service attacks against the power system or to other infrastructures such as banking systems (Interviewee 1, personal communication, 2016; Interviewee 5, personal communication, 2016).

Smart meters located at the customer premises can be the object of physical tampering attacks, although currently these devices are robust against it. These attacks tend to be more specialized, for example side channel attacks to intercept information (Interviewee 18, personal communication, 2017). A complementary threat analysis of the smart meter gateway was conducted within the research project SPIDER where additional threats were discovered, most of them fall into the tampering and denial of service, affecting integrity and availability of security aspects, see (Becker, 2013) cited in (Detken, Genzel, Hoffmann, et al., 2014).

**b. Distributed Energy Resources**

Another possible attack mechanism can be data manipulation on DER system components (Interviewee 2, personal communication, 2016). DER requires a wide variety of digital devices to control their operation and provide consumers and utilities information about their operation. Most DER include smart inverters and DER controllers; others may also include battery controllers and even electric vehicle (EV) controllers. If attackers can directly access these systems, they will be able to manipulate any of their control functions, or spoof status information to the utilities or owners (Qi et al., 2016).

**c. Generation, Transmission and Distribution**

Some attack mechanisms that could occur against ICS endpoints at station and field zones of the power grid mostly are caused by human failure or misconfiguration. Intentional manipulation of operational parameters could also happen. Devices with wireless interfaces could be another attack vector that could spread towards the electric system operations (Interviewee 18, personal communication, 2017).

USB flash drives that are plugged into the network could also be used as entry point for installation of malware (Interviewee 1, personal communication, 2016; Interviewee 18, personal communication, 2017). During maintenance service (local or remote) technicians could establish a connection through private laptop which could be infected with viruses or other malware, which could be propagated to the industrial network (Experten-Workshop 1, 2016).

Similar to the attack scenarios at the customer's premises, poorly secured industrial control systems located for example in a power substation connected to internet but without a firewall or with one improperly configured could be compromised to be part of a botnet campaign, causing denial of service attacks. Another attack scenario could be that these industrial control systems are used to break cryptographic keys or for bit-coin mining, just like the case of network printers. But this scenario is seen to be unlikely by some IT Security experts (Interviewee 1, personal communication, 2016).

Data manipulation could be also performed in the upper zones from the SGAM, e.g., operation, or enterprise (see Figure 4) against database servers (e.g., SCADA historian server), where data is consolidated and approved. Quality bits or the data itself could be manipulated and consequently the information displayed in the HMI at the control center (e.g., frequency) would be different from what is happening in the field (Interviewee 4, personal communication, 2016).

#### 4.1.2.3 Potential impacts on system services

**a. Consumption**

Compromising IoT devices could be used to do ransomware attacks against users. In a future scenario if somebody hacks the smart home environment, the attacker could demand a sum of money to release the control of lighting, heating, car battery charging, etc. (Interviewee 18, personal communication, 2017). Furthermore, as indirect potential impact, public acceptance of new technology could be affected by all security issues related to IoT in the consumer world and reported in the media (Interviewee 5, personal communication, 2016).

Smart meter gateways that are located at the customer's premise could be manipulated to reduce power consumption (Interviewee 1, personal communication, 2016; Interviewee 6, personal communication, 2016; Interviewee 18, personal communication, 2017; Interviewee 19, personal communication, 2017). However, this would be meaningless when the attacker could only impact a single gateway. For an attacker it would be interesting to switch off several gateways at the same time through Trojans or other malware to have a bigger impact (Interviewee 19, 2017). A higher impact could be achieved if a threat agent is able to compromise the IT infrastructure of the smart meter gateway administrator to use the secure communication channel and attack millions of gateways that could be connected to the SMGA (Interviewee 19, personal communication, 2017).

Regarding the function of the SMGW to disconnect the household from the power grid, Greveler, U., in (Greveler, 2016) mentioned that apart from the controllable consumers, the protection profile for the gateway does not provide any function that disconnects the household from the power grid. Such a function carries a special risk, since a successful attack on the gateway would have a considerable effect on the individual consumer (loss of function of almost all electrical devices) as well as on the power grid (potential cascading disconnection of the networks in the event of sudden disconnection of many households).

**b. Distribution Energy Resources**

Attacks that have direct control over the smart inverters could be particularly dangerous because the attack could intelligently manipulate the device's operation based on the state of the grid. This could help the attacker to amplify undesirable grid states (Qi et al., 2016). As a speculative failure scenario, one expert mentioned that in the case a threat agent could be able to manipulate enough decentralized power generation, like PV systems and switch them off simultaneously, this could lead to grid instability and some potential power outages, because the grid itself would not be able to compensate the loss (Interviewee 17, personal communication, 2017). As mentioned, this is a speculative failure scenario, which will require more quantitative analysis to evaluate the potential impact.

**c. Generation, Transmission and Distribution**

At the station and field zones, end points are exposed to potential threats as stated before. However, it will require more effort and a distributed attack in order to have a larger impact on the overall system. According to the control system architecture, the higher the level of the architecture, the more critical it becomes because the information

on one specific layer is gathered from all layers below. Therefore, at the lowest level i.e., station and field zones (see Figure 4), manipulation of the operational limit parameters on industrial equipment would not lead to a big impact on the overall system, but could lead to other impacts such as on the physical integrity of the equipment. For example, if the parameter of maximum work load is modified thus forcing the device to work over the physical limits, this could lead to physical damage producing failures that could have an effect on the performance of the specific system (Interviewee 1, personal communication, 2016; Interviewee 4, personal communication, 2016; Interviewee 15, personal communication, 2017).

In a larger attack scenario, if one substation is compromised and turned off, the effect will be a power outage on the area covered by this substation, e.g., one street or one neighborhood block. Additionally, this kind of attack could have an impact on the overall quality of energy distribution in Germany that could indirectly affect utility companies, due to the fact that they get paid according to the benchmark and these outages could represent an economic impact for them (Interviewee 1, personal communication, 2016). In order to have a larger outage, many power substations would have to be compromised simultaneously (Interviewee 1, personal communication, 2016).

#### 4.1.2.4 Potential Impact Rating

According to the potential impacts mentioned above, the quantity and quality criteria could be affected by different attack mechanisms. The effect on the quality criteria will be higher if simultaneous distributed attacks are performed. Public acceptance would also be affected. Therefore, the potential impact is rated as medium to high.

#### 4.1.2.5 Adaptation strategies and implementation

In general, the implementation of end-to-end security is a challenge. As an IT security expert stated: “It’s probably not realistic or naive to think that we can secure all end-points. But we need to make sure that we find out about the security breach quickly” Very important requirements to improve security is the implementation of security capabilities into the devices in terms of authentication, authorization of usage and control. On top of this, it is important to implement patch management processes including testing to address flaws on software and hardware. Network segmentation and monitoring is also required to prevent attacks and isolate them (Interviewee 5, personal communication, 2016).

Specific adaptation mechanisms for each cluster are mentioned as follows:

**a. Consumption**

If the system is more distributed, more security measures are needed, moreover guidelines and implementation references are needed to support vendors for the implementation of the measures on devices at customers premises e.g., IoT devices. Furthermore, open software would allow getting support from the security community (Interviewee 5, personal communication, 2016).

However, as mentioned before, 100% security cannot be guaranteed. Therefore, it would be necessary to consider these distributed devices as untrusted and verify their inputs. They should be analyzed using statistical tools to detect whether or not these devices are sending manipulated or malicious information. For example, it could be required to analyze the measurements taken from the smart meters installed at customer's premises to ensure that they are not maliciously affecting the grid. However, this analysis could have some privacy concern implications. There are ways of aggregating metering measures at a neighborhood level instead of household levels, but such techniques might involve secret sharing schemes or any other cryptographic protocol or solutions. Therefore, it is necessary to deploy these techniques and find a balance between the perceived granularity by the utility and customer privacy, as well as the overall security of the system (Interviewee 13, personal communication, 2017).

To prevent attacks coming from smart meters, their capabilities should be limited to only reading functionality but control functionalities should not be enabled. Thus they will be less exposed to attacks (Experten-Workshop 2, 2017). Furthermore, as mentioned above, in order to have a larger impact many smart meters or smart meter gateways would have to be compromised. Considering that one SMGA could be connected to about one million gateways, it is highly required that the SMGA has to be certified, which currently is a mandatory regulation in Germany (Interviewee 19, personal communication, 2017).

In order to enhance the SMGA security, the work developed by Detken K. and colleagues (Detken, Genzel, Hoffmann, et al., 2014; Detken, Genzel, Rudolph, et al., 2014) proposes the use of relevant aspects of the Trusted Computing approach, such as: measurement and verification of integrity using Trusted Network Connect (TNC). This security concept complies with the security requirements by generating a trust chain. Integrity verification is first applied at boot time, utilizing secure boot and establishing the trust chain including the TNC software. Integrity verification is also applied at runtime, utilizing the (at boot time) verified TNC software. The measured values of hardware and software components are stored tamper safe in the file system. This leads to an advanced gateway security, which affects all adjacent components.

**b. Distributed Energy Resources**

Regarding the improvement of security for DER systems, experts have mentioned that the smart metering infrastructure that is about to be implemented in Germany could also be used to secure these systems. Although this is currently not the purpose and the development of further regulations would be needed (Interviewee 17, personal communication, 2017).

**c. Generation, Transmission and Distribution**

Prevention mechanism such as bad data detection schemes or data filters can be used. Normally, control systems are designed considering that some data coming from the field could have errors or be wrong, therefore the required dataset is overestimated, enabling the possibility to discard wrong data. The implementation of the mentioned detection schemes, which relies on physical models (e.g., current or voltage, through Ohm's and Kirchhoff's law), will enable further validation of data coming from the field (Interviewee 4, personal communication, 2016; Interviewee 12, personal communication, 2017).

The implementation of these detection mechanism would be limited to the amount of data available. Experts agreed that at the transmission level, there is more data compared to the distribution level where currently there are not many measurement devices posing a challenge for implementing these detection schemes (Interviewee 12, personal communication, 2017).

Furthermore, implementation of better analysis and detection capabilities on industrial routers and switches will improve the security of industrial control systems to be able to detect and prevent attacks from field devices. However, current industrial networks have only basic functionalities, therefore upgrades or new network devices should be considered (Interviewee 15, personal communication, 2017).

#### 4.1.2.6 Adaptation capacity rating

Some adaptation strategies for prevention have been given. However, the implementation of them will be limited due to technical requirements that imply additional costs or the development of further regulations frameworks. Therefore, the adaptation capacity is rated as medium.

#### 4.1.2.7 Vulnerability rating

Considering a combination of high potential impact and medium adaptation capacity. In this case, the vulnerability rating is high.

Figure 14 summaries the vulnerability assessment due to insecure endpoints

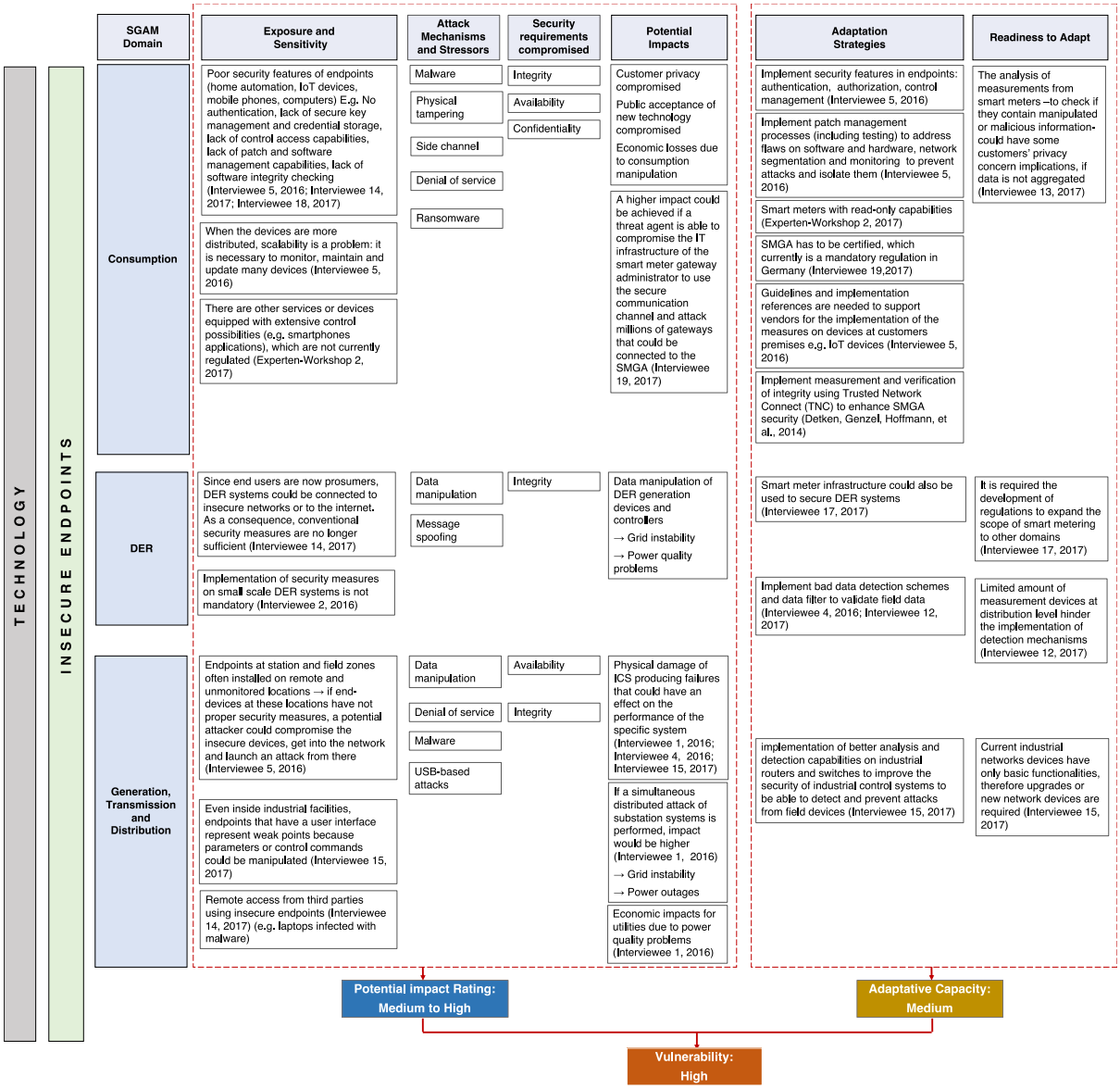


*Figure 14 Summary of vulnerability assessment of cyber-physical power systems due to insecure endpoints. For the assessment the SGAM domains of the power system were grouped in three clusters: (a) consumption, (b) distributed energy resources, (c) generation, transmission and distribution. Source: Authors' own representation*

### 4.1.3 Other technology related conditions

The following further technology related conditions were identified through the interview content analysis. However, due to time constraints a comprehensive vulnerability assessment could not be conducted.

- Insecure interface between components from different vendors or between different systems
- Allowed but unauthorized software and firmware modification
- Systems running in web services, such as virtual power plants

## 4.2 Organizational Security Policies and Procedures

### 4.2.1 Lack of interdisciplinary IT-OT knowledge

#### 4.2.1.1 Exposure and sensitivity

With the increasing number of complexities and interdependencies between IT and OT (Operation Technology) infrastructure of power systems, the needed knowledge to address the new cyber-physical systems have changed. Linkages between both infrastructures have to be examined and protected in specific ways which is difficult for experts with knowledge in only one of those fields. Interdisciplinary knowledge in most of the cases is missing and therefore, it is difficult to properly understand, design, implement and operate the new systems as a whole (Interviewee 1, personal communication, 2016; Interviewee 2, personal communication, 2016; Interviewee 5, personal communication, 2016).

Different stakeholders are involved in the energy sector, namely traditional large-scale commodity providers, distribution network operators, typical consumers, emerging small-scale producers, metering service providers, IT component developers/providers, and several regulatory and standardization institutions. Most of these parties have no strong background in IT security (von Oheimb, 2013). Furthermore, during tender processes the lack of expertise in both infrastructures could lead to mistakes or no comprehensive security requirements description, therefore the systems implemented cannot fulfill minimum requirements (Interviewee 18, personal communication, 2017).

Experts of one domain simply cannot foresee the implications and consequences of their decisions for other domains and parts of the system. For instance, on the one hand, if the IT department considers servers for OT operation (e.g., HMI, historian server) as part of IT-Infrastructure, normal IT security measures (e.g., daily antivirus updates) could have consequences on the operational part of the system, which will affect the availability or performance of the system (Interviewee 4, personal communication, 2016). On the other

hand, a significant portion of OT network are connected, maintained, and operated by IT devices and systems. Normally, these assets are maintained by ICS operators and engineers rather than experienced IT professionals, which can results in common mistakes in maintenance, configuration, and lack of hardening (Bodungen et al., 2017).

Furthermore, the ongoing implementation of ICT into electricity operation system adds new challenges for the system operation. As more ICT functionalities are integrated to electric systems, the operational personnel would require more training to know how to deal with cyber-physical events. Experts state, that these new systems need skilled operators, specifically trained to operate not only the existing electro-technical parts of the system, but also the new IT security systems, e.g., intrusion/anomaly detection systems. Personnel in operation cannot be re-educated to be IT experts within a short period of time to know how to react properly to IT failures (Interviewee 1, personal communication, 2016).

On the one hand, operation control centers normally do not integrate failures or alarms coming from the ICT infrastructure, therefore the operator is not able to distinguish the origin of the failure (Interviewee 1, personal communication, 2016; Interviewee 18, personal communication, 2017). On the other hand, if the IT department manages the anomaly detection systems and IDS, it is unclear how any stressor from IT could be transmitted to the operation center to react on it (Interviewee 18, personal communication, 2017).

#### 4.2.1.2 Attack mechanisms and stressors

The lack of experts in both IT and OT domains opens up many opportunities for attackers to harm the system in several ways. Different approaches for securing ICS from IT and OT measures create security gaps, such as: improper network segmentation, improper change and configuration management, poor local/remote access control, weak generation, use and protection of passwords, amongst others.

If the system is not designed properly due to a lack of knowledge about vulnerable parts of the system, improper revision of newly added software and firmware can cause problems with the system stability. Improper patch management and implementation of IT security measures can also harm the system, as the overall system design gets too complex and leaves systems vulnerable to attacks. Gaps in security or faults in the design and implementation of security measurements can be used by attackers to compromise the system.

An attack scenario could also leverage the lack of IT-OT expertise of operators, when threat agents could flood control centers with errors and alarm signals, to confuse the non-interdisciplinary skilled operators and leading to a loss of overview of the system. Provoking

critical mistakes, controlling errors and wrong control commands, could then lead to system physical damage (Interviewee 4, personal communication, 2016).

#### 4.2.1.3 Potential impacts

The implementation of inappropriate security measurements for cyber infrastructure assets could have unintended consequences for the physical infrastructure, which in turn yield effects on the system performance and stability.

The lack of personnel with expertise in both IT and OT fields will affect the operation of the system. When incidents or events from the IT related to OT are occurring, it would not be possible to react on it. Operators without proper training cannot distinguish between error messages resulting from technical failures, or natural hazards, or those resulting from a targeted attack. If they cannot manage the system properly and according to the real problem, the performance of the system can be affected (Interviewee 4, personal communication, 2016).

#### 4.2.1.4 Potential impacts rating

The implementation of inappropriate security measures due to the lack of interdisciplinary knowledge could compromise data availability that could have a direct effect on the technical parameters. Exploiting security gaps could also lead to system failures and power outages. Therefore, according the VA methodology, the potential impacts range from Medium to High.

#### 4.2.1.5 Adaptation strategies and implementation

As adaptation strategies, experts demand bridging more expert knowledge between IT and OT to help those sectors to understand each other and avoid configuration errors or implementation of inappropriate security measures (Interviewee 13, personal communication, 2017). Having more expertise on cross-sectional and interdisciplinary fields, the industry can be educated towards a better understanding of its own complexity and to develop a holistic view on system architecture (Interviewee 6, personal communication, 2016; Interviewee 17, personal communication, 2017). This view would focus on the connections and interactions between different components and domains.

With more cross-sectional collaborations, better security measurements and system designs can be developed that will consider the complexity and interdependency between IT and OT, and more importantly, the critical operational requirements which are timing and availability. Defining and assessing security responsibilities from development to operation phase will help in addressing specific requirements (Interviewee 9, personal communication, 2017).

Consolidating existing guidelines and sharing them among different fields could be helpful to prepare guidelines for a broader use within the relevant domains and for different actors involved in the system (Interviewee 18, personal communication, 2017).

More specific training for operation is needed, only trained and experienced operators are able to understand specific errors and are able to estimate their impact. They will react accordingly and can operate the system even when errors occur, whereas improperly trained operators might risk damage to components (Interviewee 4, personal communication, 2016). Furthermore, they should work in teams of IT and OT experts for better reactions on system failures of any kind (Interviewee 19, personal communication, 2017).

However, training and education programs for increasing the interdisciplinary knowledge of existing staff or the recruitment of specialists could be hindered due to associated costs (Interviewee 9, personal communication, 2017).

#### 4.2.1.6 Adaptation capacity rating

Adaptation mechanisms were mentioned by the experts, however, as stated from one of them, the implementation of training programs for increasing the interdisciplinary knowledge of existing staff or the recruitment of specialists could be hindered due to associated costs. For this reason, the adaptation capacity is rated as medium.

#### 4.2.1.7 Vulnerability rating

Considering high potential impacts and medium adaptation capacity, in this case the vulnerability due to insecure communication is rated as High.

Figure 15 summaries the vulnerability assessment due to lack of interdisciplinary IT-OT knowledge.

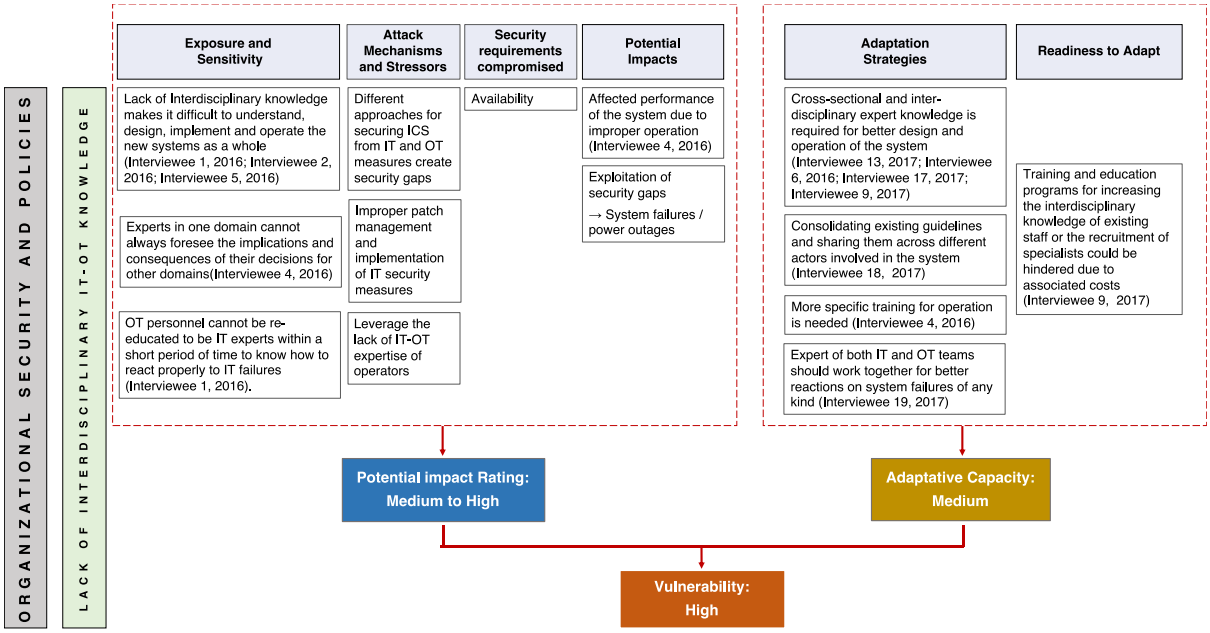


*Figure 15 Summary of vulnerability assessment of cyber-physical power systems due to lack of interdisciplinary IT-OT knowledge. Source: Authors' own representation*

## 4.2.2 Improper security patch management

### 4.2.2.1 Exposure and sensitivity

Software/Firmware patches in some cases are not regularly checked to ensure that they are updated. The consequences of an improper security patch management in the standard IT networks became obvious in the latest global cyber-attacks such as '*WannaCry*'. This attack could have been avoided or mitigated if an adequate implementation of available security patches from corporate and government IT departments would have been performed and more than 10-year-old operating systems would have been upgraded.

Experts agreed that systems connected to the Internet require at least weekly or even daily security patches, in order to maintain their level of security. However, organizations and end-users occasionally fail to see the need to patch their outdated operating systems and network components.

In the case of industrial control systems, expert stated that these systems usually tend to not be well patched, either because vendors do not provide security patches for their devices or because the particular system is critical for the operation and it is not possible to turn it off in order to apply the security measures. As a consequence, the security-gaps are not properly patched and systems are exposed to malicious intrusions.

#### 4.2.2.2 Attack mechanism and stressors

Threat agents will be able to gain access to different system components by exploiting a known security-gap that has not yet been patched. Malware could be installed and used to replace or add any function to a device or a system, such as sending sensitive information or controlling devices (Mo et al., 2012).

#### 4.2.2.3 Potential impacts

Depending on the system domain where the unpatched software or firmware has been compromised, the potential impacts could have different effects.

For instance, the failure scenario AMI.25 from the NESCOR catalog describes the potential impacts due to an attack via an unpatched firewall in the metering systems. This condition could allow the threat agent to shut down the AMI head-end, causing outages due to the utility's inability to implement demand response at peak times (NESCOR, 2015).

If the attack is targeted at industrial control firmware in distribution substations, the threat agent could be able to gain control of the substation and shut down segments of the distribution grid producing power outages. The extent of the outages will depend on the number of substations being compromised (Interviewee 1, personal communication, 2016).

Furthermore, inadequate patch management or a failure in the patching process could also affect the availability of system components being patched, which can cause power outages. (see failure scenario AMI.28 in (NESCOR, 2015)).

#### 4.2.2.4 Potential impacts rating

Based on the detailed analysis above, the quantity and quality criteria could be affected depending on the attack mechanisms and on which domain the attack is target at. The effect on the quality criteria will be higher if simultaneous distributed attacks are performed. Therefore, the potential impacts on the system are rated from medium to high.

#### 4.2.2.5 Adaptation strategies and implementation

Experts mentioned, that proper patch-management is essential for keeping up with technological developments and securing systems with access to the Internet. The management should include a severity rating and timeframes for patching vulnerabilities (NESCOR, 2015).

However, regular patching for industrial control system, especially SCADA systems represent a challenge because these systems are time-critical. Due to the fact that there is no test environment, patching may introduce new unknown vulnerabilities or ultimately break the system (Cherdantseva et al., 2015). Experts suggest the implementation of

redundant systems to avoid down time. However, the application of this measure would depend on the overall design of the system and can be hindered by associated additional costs.

Even if we keep up-to-date with all patches and mitigations, unknown zero-day exploits and unannounced vulnerabilities are widespread (McLaughlin et al., 2015).

Another solution as some of the interview partners mentioned, would be to establish mandatory regulations to raise the awareness and willingness to implement proper patching and updating.

#### 4.2.2.6 Adaptation capacity rating

From the considerations described above, according to the VA, the adaptation capacity is rated as medium.

#### 4.2.2.7 Vulnerability rating

Considering high potential impacts and medium adaptation capacity, the vulnerability in this case is rated as high.

Figure 16 summaries the vulnerability assessment due to improper security patch-management.

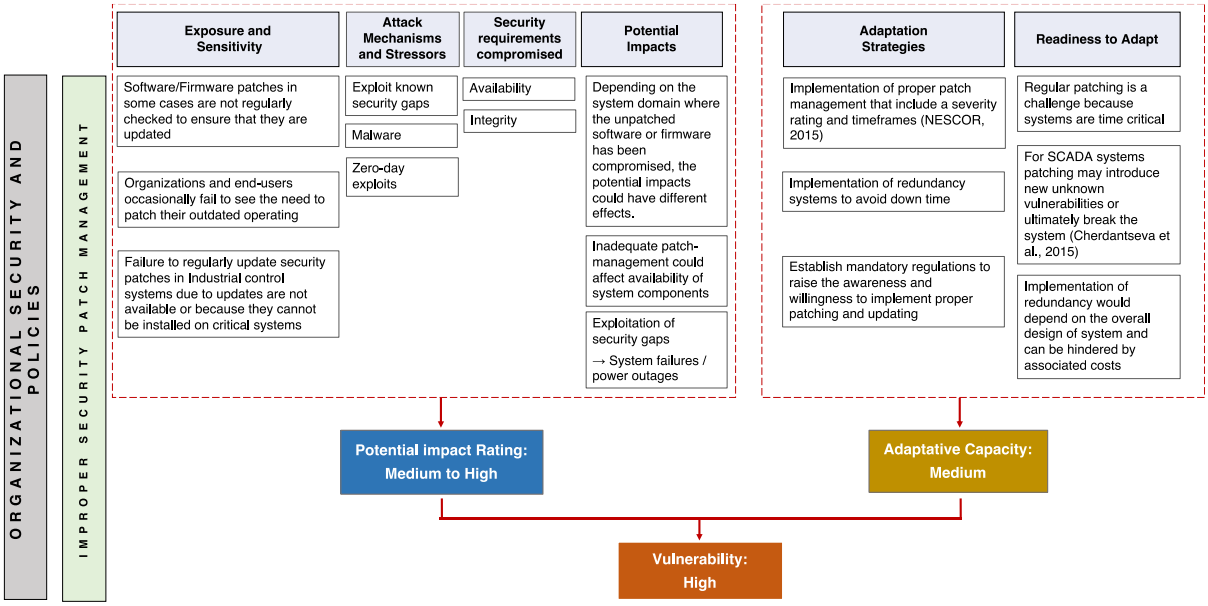


*Figure 16 Summary of vulnerability assessment of cyber-physical power systems due to improper security patch-management. Source: Authors' own representation*

## 4.3 The Human Factor

### 4.3.1 Lack of security awareness or poor response to security policies inside the organization

#### 4.3.1.1 Exposure and sensitivity

The lack of an adequate security training and awareness programs in a power sector organization, e.g., generation power plants, distribution and transmission operators, etc., can lead to inadequately trained personnel, who may inadvertently provide the visibility, knowledge and opportunity for external or internal stressors to execute a successful attack (NIST, 2014).

On the one hand, according to the IT experts, social engineering is one of the fastest growing security problems. This attack mechanism enables the threat agent to exploit one of the weaknesses present in every organization: the human factor. In this case, personnel could be manipulated by external threat agents into helping them get access to the internal system or perform an attack. An inadequately trained workforce will not be aware of the policies and procedures necessary to secure organizational information and equipment, resulting in the potential for weaknesses to be exploited for example: inserting malicious USB sticks into machines in the corporative or operative network, surfing suspicious websites which often contain zero-day exploits, or lack of care with identification badges, which can used to gain partial or complete access to critical systems (NIST, 2014). Furthermore, critical information about system configuration or architecture could be made publicly available through vendors' or asset, owners' website, employee social media sites. Potential threat agents can leverage this information for the attack planning.

On the other hand, further potential threat agents include disgruntled employees with high potential for criminal or malicious behavior, or ex-employees, who were not properly managed when they left (Interviewee 4, personal communication, 2016). They have high knowledge of the systems and access to critical functions or sensitive data (depending on their position), therefore they could be able to identify possible weak internal structures and methods to perform an attack, causing severe damage to the system.

Many lessons about cyber-threats have been learned by organization at their corporative ICT domain, and personnel are made aware of and trained to recognize those threats. However, ICS operators, engineers and other external involved actors such as: ICS vendors, system integrators, contractors and maintenance personnel lack cyber-security training and education (Luiijf, 2016). As stated by the IT security experts, most attacks in the station zone (see smart grid architecture in (IEC, 2020)) come either from human

failure, misconfiguration or social engineering. While networks at operation, enterprise and market zones tend to be secured via firewalls, VPN, IDS and monitoring systems, the station zone is extremely vulnerable to the human factor (Interviewee 1, personal communication, 2016).

#### 4.3.1.2 Attack mechanisms and stressors

Through social engineering, threat agents are exploring new attack mechanisms targeting different levels in the organization. For example, 'spear phishing' is one attack mechanism, where external threat agents send emails containing hidden malicious code to employees to infect the facility's network. In the Ukrainian case in 2015, threat agents developed a malware (*'Blackenergy 3'*) and created weaponized documents to deliver the malware via email. Emails with malicious documents as attachment were sent to people inside the organization in a phishing campaign. Threat actors successfully installed the malware after employees open the weaponized email attachments. The malware included plugin software to collect system access credentials and perform reconnaissance activity on the internal network. Using the stolen credentials, threat agents accessed the industrial control environment and carried out a complex set of actions (Styzcynski and Beach-Westmoreland, 2017).

Another way of breaching the perimeter is through USB-based attacks. USB peripherals have become an attractive tool for launching cyber-attacks, where threat agents take advantage of users who tend to use these peripherals casually, assuming they are safe, when in fact they may carry an embedded malicious payload that can be used to launch attacks (Nissim et al., 2017). USB devices can be used also for attacking specific ICS targets, such as PLCs (Programmable Logic Controllers), as demonstrated by the famous 'Stuxnet' malware against centrifuges at the Iranian uranium enrichment facility outside Natanz. In this case, threat agents performed indirect infiltration via infected mobile devices and USB sticks from contractors who had legitimate access to the most critical system of the facility (Langner, 2013). The Stuxnet worm was an unprecedentedly complex piece of code that attacked in three stages. (1) First, it targeted Microsoft Windows machines and networks, repeatedly replicating itself. Using compromised digital certificates, Stuxnet was able to bypass firewalls as it continued spreading itself throughout the local communication networks of the SCADA system. Stuxnet's peer-to-peer communication capabilities allowed the malware to update itself, even when the compromised device did not have direct access to the Internet. (2) Then, it searched for Siemens Step7 software, which is also Windows-based and used to program PLCs. (3) Finally, once the targeted PLC was infected, Stuxnet changed its operation mode. Using the PLC rootkit, the malware modified the PLC code to perform a disclosure attack and record the received data. After recording data for some

time, Stuxnet began sabotaging the physical system through a disruption attack. While changing the control signal sent to the actuators, Stuxnet hid the damage to the plant by feeding the previously recorded data to the SCADA's monitoring systems (Knapp, 2011; Kushner, 2013; New Jersey Cybersecurity & Communications Integration Cell, 2017). Figure 17 illustrates Stuxnet attack scenario.

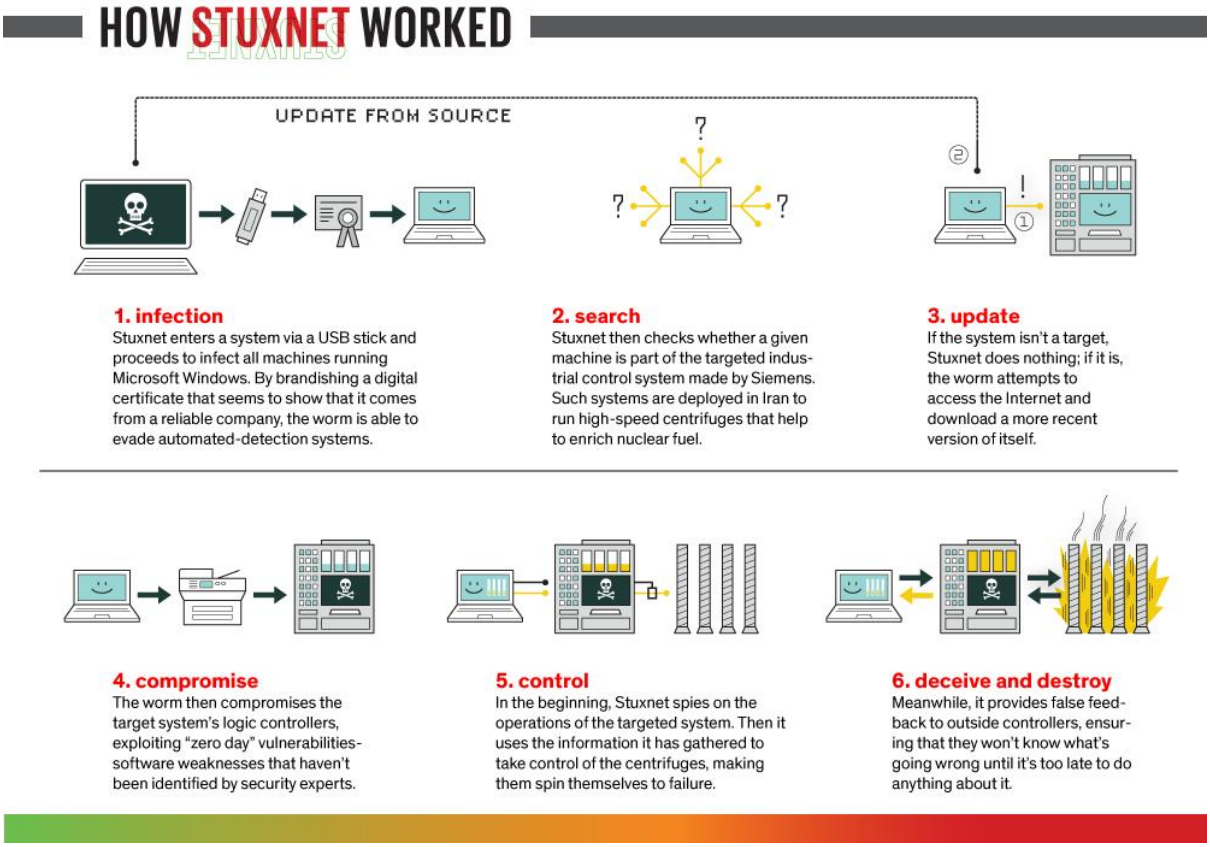


*Figure 17: How Stuxnet Worked. Source (Kushner, 2013)*

An example of an attack performed by insider threat agents is the case of manipulation of smart meters in Malta. Employees of the state-owned energy supplier Enemalta manipulated around 1,000 smart meters against payment of bribes and installed them at customers with high electricity consumption. The smart meters were configured to record up to 75 percent less energy consumption than really consumed. The meters were manipulated without breaking seals or protective mechanisms. There was evidence that meters had been manipulated by other customers to measure higher power consumption in order to keep the total consumption of a district constant and to disguise the fraud (BSI, 2015b).

#### 4.3.1.3 Potential impacts

Depending on the relevance of the compromised data or the privileges the targeted user has, potential impacts could have different ranges. Through information leakage, a threat agent could obtain legitimate credentials to access critical systems. If an attacker passed through a system, it would be possible to compromise the SCADA system infrastructure (e.g., the data historian server). If the situation was aggravated by an improper segregation of corporate and industrial control network, the threat agent could gain control over field devices and perform incorrect or harmful operation control actions causing outages of unknown duration or direct physical damage of the ICS assets. Furthermore, the attack would not only disrupt electricity distribution, but also destroy IT systems, flood call centers and inhibit incident response, like in the Ukraine attack in 2015 (Styzcynski and Beach-Westmoreland, 2017).

In the case of the smart metering infrastructure, compromising the IT infrastructure at the Smart Meter Gateway Administration (SMGA) facilities could allow the threat agent to use the secure communication channel to attack almost one million smart meter gateways, for example switching them off, which will cause grid instability and potential power outages (Interviewee 19, personal communication, 2017).

The NESCOR catalog (NESCOR, 2015) illustrates further potential impacts due to social engineering on: metering infrastructure (see AMI.3, AMI.9), transmission (see WAMPAC.4), distribution (see DGM.10) and generation domains (see GEN.4, GEN.9).

#### 4.3.1.4 Potential impacts rating

Considering the possible range of impacts that could affect both the qualitative and quantitative criteria, in this case the potential impacts on the system are rated as medium to high.

#### 4.3.1.5 Adaptation strategies and implementation

Experts suggest stricter mandatory security measurements on different organizational levels to counter social engineering. Operators and administrative staff must be trained, so that they are aware of conditions that could compromise the system. (e.g., poor password management, improper mail attachments management, unidentified USB-drives, etc.) Employees could be engaged in social engineering exercises, where they receive company generated phishing mails or they find placed rogue USB drives to learn how to react properly to the threat of social engineered attacks. Security training and security awareness programs should be adapted to each member of the staff according to their position. It should include a continuous retraining effort over a specific period of time to reflect new

procedures, new technologies, and reinforcement of the importance of the cybersecurity program (ENISA, 2012; NIST, 2014). Besides this, there should be better personal background checks of new employees to ensure all staff with operational or administrative access to ICS are appropriately screened (ENISA, 2016).

There should be more awareness and willingness towards a harmonized effort from human resources, management, IT-department and regulatory authorities to agree on strict security policies for organizations. Nevertheless, the implementation costs of security policies and training programs can hinder the approval and limit the security level implemented, as stated by an expert. The application of security measures could also be limited to the engagement level of employees.

#### 4.3.1.6 Adaptation capacity rating

Considering that adaptation strategies are given, but their application will depend on the willingness of the involved actors, the adaptation capacities are rated medium.

#### 4.3.1.7 Vulnerability rating

According to the VA methodology, the combination of high potential impact and medium adaptation capacity, yields a high vulnerability rating.

Figure 18 summaries the vulnerability assessment due to lack of security awareness or poor response to security policies inside the organization.

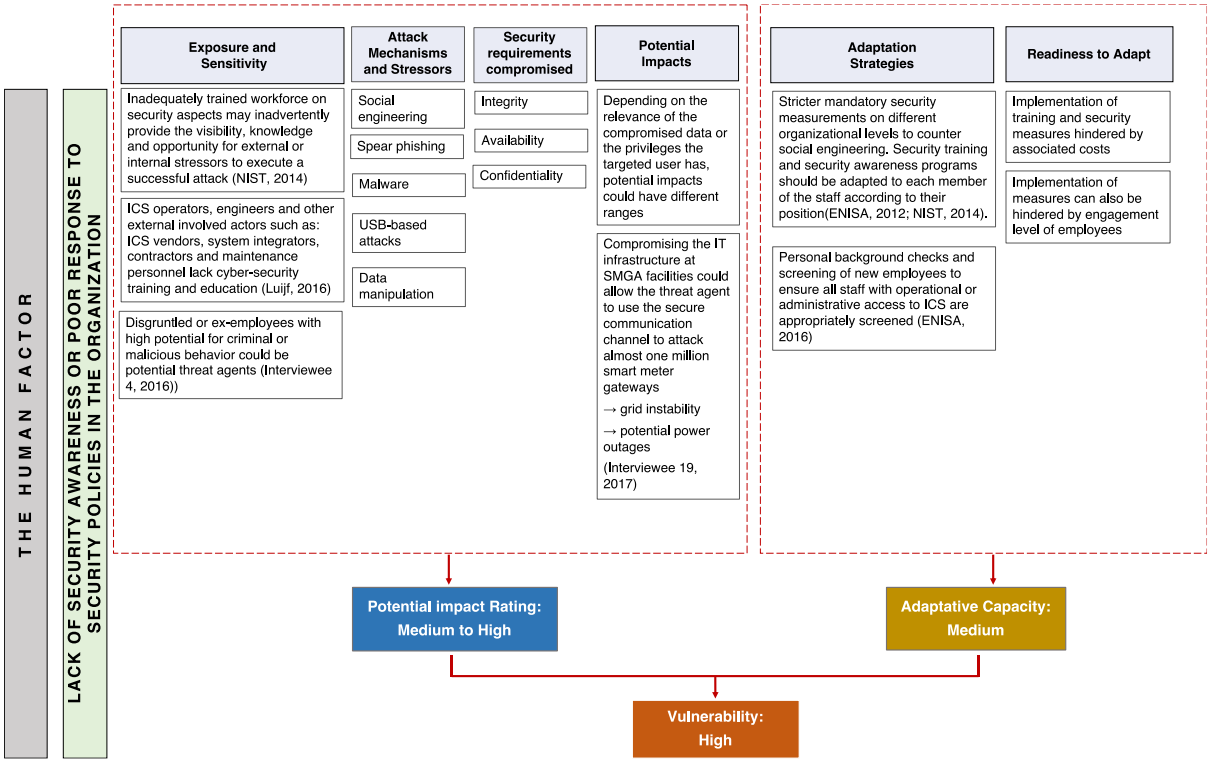


*Figure 18 Summary of vulnerability assessment of cyber-physical power systems due to lack of security awareness or poor response to security policies inside the organization. Source: Authors' own representation*

## 4.3.2 Lack of security awareness among consumers

### 4.3.2.1 Exposure and sensitivity

End users represent another vulnerable point for the system. The lack of awareness or lack of understanding of the consequences of low security from the customer's side could compromise the power system. Experts confirm that the majority of end-users do not have expert-knowledge about their home automation systems and Internet of Things (IoT) devices, thus they are not aware of how to properly secure and maintain their smart devices.

Experts mentioned that on the one hand, IoT and home automation devices, especially off-the-shelf products, have well-known security-gaps that attackers can exploit. On the other hand, end-user devices which are not properly patched or maintained could be connected to the home network, raising the vulnerability of the system by adding more insecure entry points.

A more complex problem mentioned by an expert arises from end-users being prosumers, but yet do not have the expert-knowledge to implement and maintain appropriate security measures for DER systems.

#### 4.3.2.2 Attack mechanisms and stressors

A threat agent can use eavesdropping to access customer data and steal private information including electricity usage through a firewall which intentionally or unintentionally allows direct access from another networks. Besides eavesdropping, threat agents could gain access to smart meter devices to manipulate metering data, or manipulate data on Distributed Energy Resources system parameters. IoT devices could be compromised and used to perform a distributed denial of service (DDoS) attack.

#### 4.3.2.3 Potential impacts

Depending on the attack mechanism, the customer's privacy could be exposed or communication channels could be used as a medium to manipulate data and send incorrect control commands that could lead to power system instability and outages.

The failure scenario DER.2 from the NESCOR catalog (NESCOR, 2015) (NESCOR, 2015) illustrates the case when a large DER system is erroneously connected to a wireless corporative network and thus exposing the DER system to the Internet. The threat agent could gain control and alter the operation of the DER functions. Consequently, the grid could experience damaging reverse power flows, or overloads to substation transformers.

AMI insecure networks or sometimes even protected networks could offer opportunities for a potential breach to compromise customer privacy, which could lead to a loss of customer confidence on AMI.

#### 4.3.2.4 Potential impacts rating

Considering that the security requirements: integrity and confidentiality can be compromised and this could produce an effect on the qualitative criteria, as well as on the delivery of power, the potential impacts due to the lack of security awareness among consumers is rated from medium to high.

***Adaptation strategies and implementation***

To prevent breaches with potentially large impacts, interview partners recommended that education regarding cyber-security for the end-user side is needed to reach a higher security level. Better knowledge of their own smart systems raises awareness among end-users. It further enables end-users to properly operate and maintain their system, so that they could ensure a certain degree of security on their own. Mandatory security measurements for home devices and their maintenance would help to reach a minimum security for home automation systems. However, these strategies are not in place yet and there is no policy enforcement for their application.

Achievement of higher security level will be in conflict with a short-term economic rationale, as experts mentioned. Therefore, in most cases, the implementation of higher security measures on the customer or prosumer side will be limited by their willingness to pay for security.

Furthermore, experts stated that most of the security measures that are currently in place, are trying to keep the malicious attackers outside of the system, therefore one of the biggest challenges is to go further from prevention or detection of cyber-attacks towards recovery mechanism after a successful attack. Together with better monitoring and detection systems, this could offer better possibilities to react on attacks and manipulated data. But it is important to be aware of customer privacy when applying more monitoring systems.

#### 4.3.2.5 Adaptation capacity rating

Considering that the mentioned adaptation strategies are not in place yet and that the willingness of customers for adaptation is limited, the current adaptation capacity in this category is rated low.

#### 4.3.2.6 Vulnerability rating

Following the VA methodology, medium to high potential impacts combined with a low adaption capacity rate leads to a high overall vulnerability concerning the lack of security awareness from the customer´s side.

Figure 19 summaries the vulnerability assessment of cyber-physical power systems due to lack of security awareness among consumers

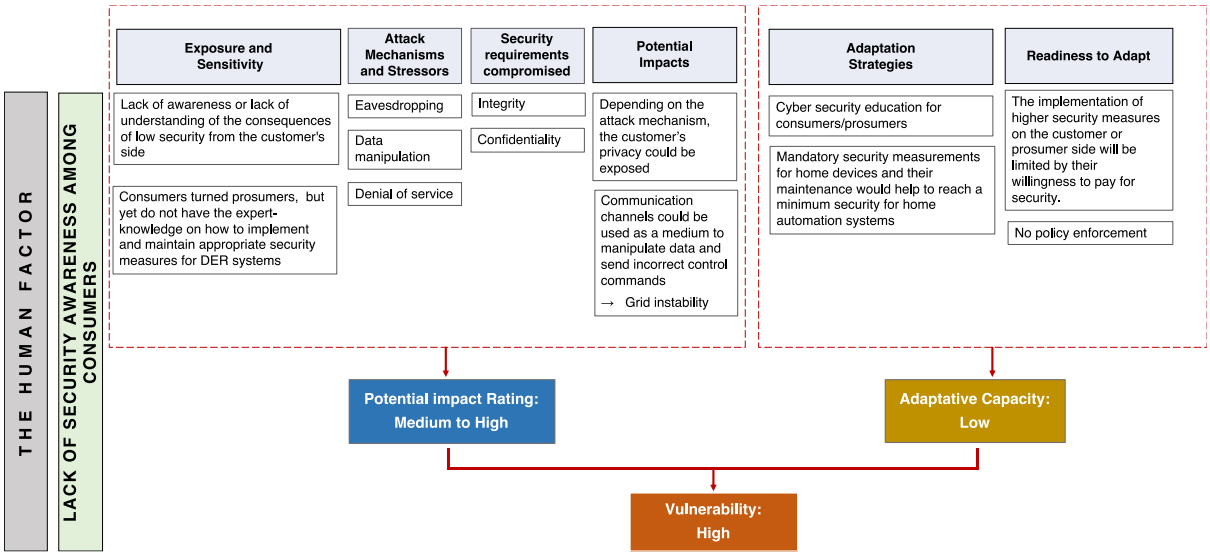


*Figure 19 Summary of vulnerability assessment of cyber-physical power systems due to lack of security awareness among consumers. Source: Authors' own representation*

## 4.4 Regulations

### 4.4.1 Lack of effective implementation of security standards and regulations

#### 4.4.1.1 Exposure and sensitivity

Different technical and organizational standards have been developed to address cyber security requirements in smart grids. However, as experts have stated, in most of the cases, they are only recommendations and their implementation is not obligatory.

For instance, the IEC 62351 set of standards was developed to address security for substation infrastructure and provides a framework for end-to-end security for the communications between software applications. It relies heavily on the use of TLS to protect power system against different attack mechanisms (International Electrotechnical Commission (IEC), 2007).

Despite the fact that this standard provides security improvements for protocols such as: IEC 61850 (GOOSE, SV and MMS), IEC 60870-5- 104 and DNP3, and IEC 60870-5-101 and serial DNP3, in practice it is not always applied (Basagiannis et al., 2015; McLaughlin et al., 2015) and experts mentioned that often vendors do not implement the recommended security measures in their products. IT experts considered that the absence of mandatory regulations to enforce power system operators to implement minimum required security standards or vendors to provide the necessary security requirements in their products expose the system to possible cyber-attacks.

#### 4.4.1.2 Attack mechanism and stressors

A threat agent could exploit known weaknesses due to the lack of authentication or encryption in certain standard protocols, get unauthorized access to the system, manipulate and compromise communication sessions.

Some examples of possible stressors can be found in the literature for attacks, such as: DoS attacks (Dondossola et al., 2008, 2009) or man-in-the-middle (Maynard et al., 2014) on networks running the IEC 60870-5 protocol. The work from (Kush et al., 2014) also demonstrated a practical attack by exploiting weaknesses in authentication and encryption in GOOSE (Generic Object Oriented Substation Event) to spoof messages with incorrect data between each valid message.

#### 4.4.1.3 Potential impacts

Depending on the attack mechanism, the impacts could differ. For example, if a threat agent intercepts unencrypted plain text SCADA frames (such as Distributed Network Protocol 3.0, DNP3) that contains valuable information, like control and setting information

for intelligent equipment devices (IED), the threat agent could be able to shut down device services, send incorrect commands and cause disruptions (Kush et al., 2014).

#### 4.4.1.4 Potential impacts rating

Considering that the IT security requirements, compromise could lead to power system instability and outages. According to the VA methodology, the potential impacts on the system are rated from medium to high.

#### 4.4.1.5 Adaptation strategies and implementation

There are good practice guidelines that recommend the implementation of higher security standards to secure device communications protecting messages and ensuring integrity within power systems management and substation automation. However, according to experts, they are not mandatory and the compliance of minimum-security levels is not enforced by regulations.

Furthermore, the decision to upgrade legacy systems in order to implement the security measures could be delayed until the next planned lifecycle equipment replacement, due to different factors. The critical level of the process or economic constraints in the organization could hinder the application. As a consequence, currently installed legacy devices using legacy protocols will ensure that many vulnerable systems will remain in the field, waiting to be exploited (Knapp and Samani, 2013).

#### 4.4.1.6 Adaptation capacity rating

Considering that there are already adaptation mechanisms to improve security in the smart grids but the willingness to apply them could be limited, the adaptation capacity is rated as medium.

#### 4.4.1.7 Vulnerability rating

Considering high potential impacts and medium adaptation capacity, in this case the vulnerability is rated as high.

Figure 20 summaries the vulnerability assessment due to lack of effective implementation of security standards and regulations.

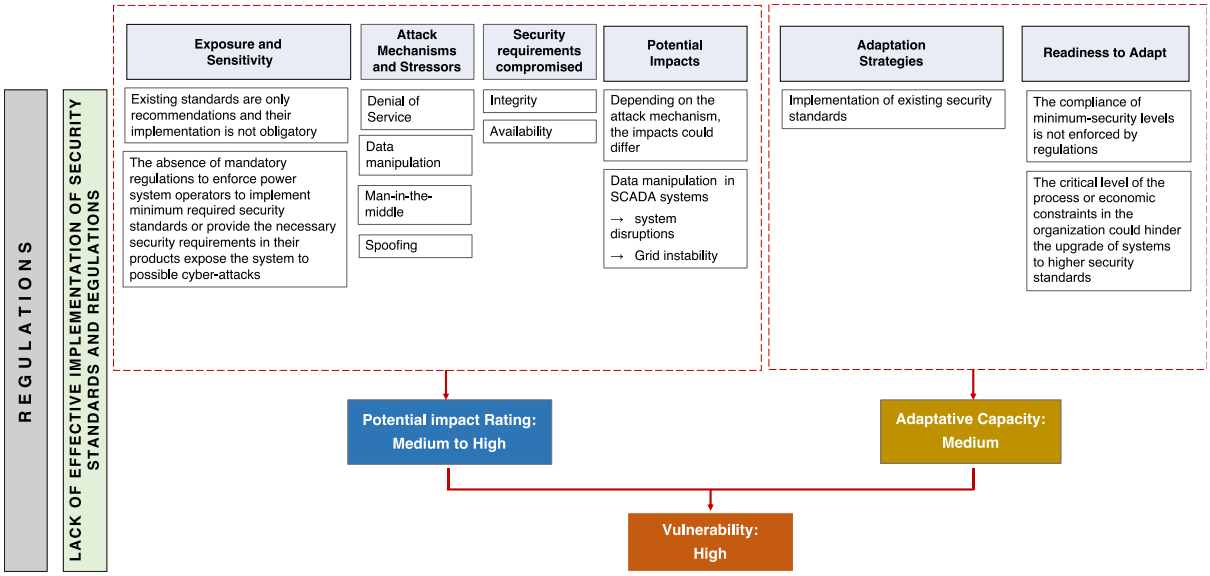


*Figure 20 Summary of vulnerability assessment of cyber-physical power systems due to lack of effective implementation of security standards and regulations. Source: Authors' own representation*

### 4.4.2 Lack of coordinated effort to improve security

For this category a comprehensive assessment accordingly to the VA methodology was not conducted due to time constraints. But the main findings from the interview analysis are presented below.

In the case of Germany, security regulations are mainly focused on smart metering and critical infrastructures. However, the experts mentioned that an effective coordination to improve security for the overall system is missing. According to the German legislation, electricity network operators have to establish and certify an Information Security Management System (ISMS) based on IEC/ISO 27001. However, currently[8] there are no mandatory regulations to secure small scale DER systems (Interviewee 2, personal communication, 2016) which according to the VA performed in section 4.1 and 4.3.2, have critical points that can be exploited by threat agents causing significant impacts to the power system.

Similarly, in the case of the smart metering infrastructure, the security measures based on Protection Profiles (PP) and technical guidelines (TR-03109) do not include regulations for other services or devices equipped with extensive control possibilities that could be connected to the home automation network.

Furthermore, improving the security from power generation and grid operators' side would imply additional economic investments and this could be transferred to the customers via

[8] By the date of the interviews, i.e. 2016 and 2017

electricity bills. An expert on the power sector mentioned, that customers are not willing to pay a higher price for better security. They prefer to choose their power supplier based on the lowest price and thus will not accept a new power system which offers no major direct benefits compared to the old system (Interviewee 6, personal communication, 2016). Experts on IT security stated that, customers were not asked nor included in the process of the energy transformation and this could be the case of digitalization transformation as well. Therefore, lack of awareness on the importance of new technologies and the related security on customer's side could hinder the willingness to invest in more secure power solutions, as customers do not know the many advantages gained from a secure power system (Interviewee 1, personal communication, 2016).

## 4.5 Illustration of the Event-based Vulnerability Assessment methodology

This section shows examples that illustrate the application of the methodology used for the event-based vulnerability assessment EVA. Here, the vulnerability level was identified for four specific stressors from ICT: (1) GPS signal spoofing, (2) insider threat against SCADA systems, (3) manipulation of ICS firmware in substations, and (4) Advanced Metering Infrastructure data eavesdropping. These stressors were mentioned by the experts during the interviews and identified through the content analysis method.

Each stressor was categorized according to the domain and layer of the power system where it could take place. Figure 21 shows the location of each stressor on the reference architecture model.

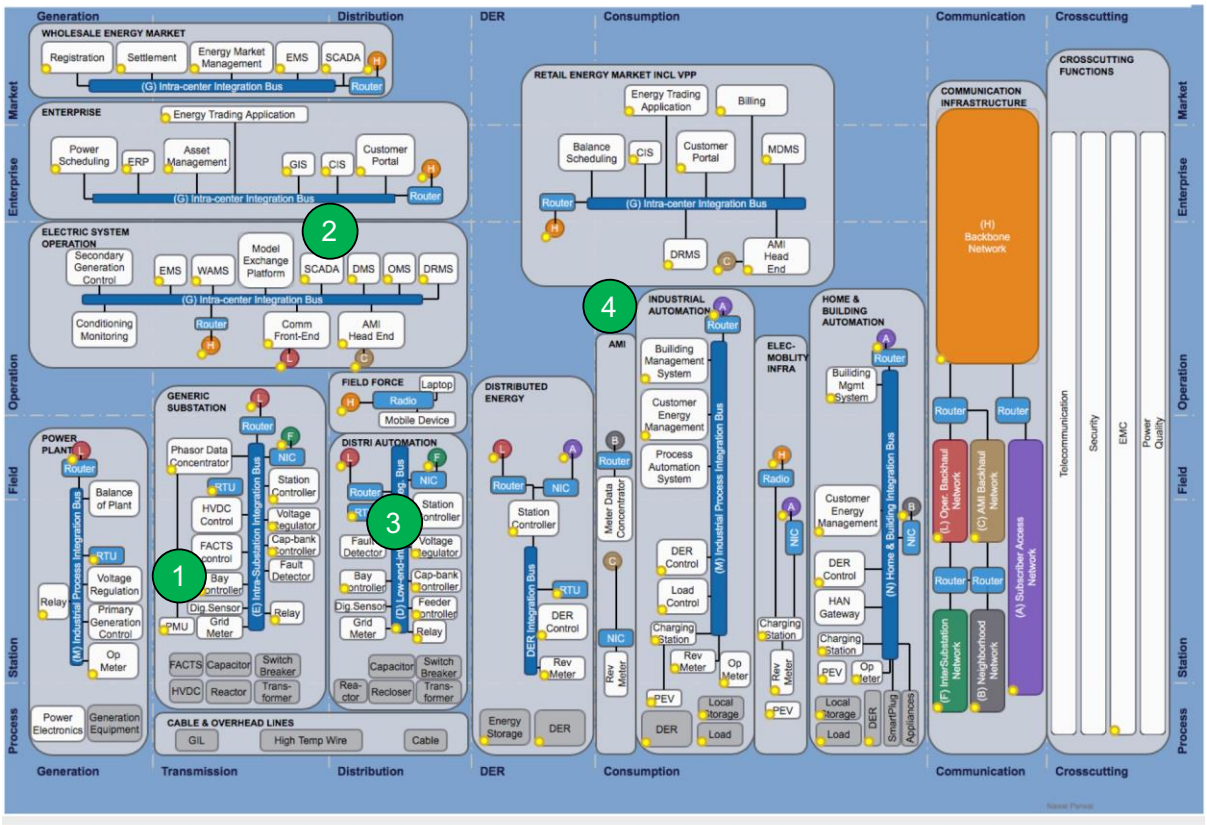


*Figure 21 Location on the reference architecture model of stressors used as example for the application of the Event-based VA. The stressors are numbered as: (1) GPS signal spoofing, (2) insider threat against SCADA systems, (3) manipulation of ICS firmware in substations, and (4) Advanced Metering Infrastructure data eavesdropping.*

The EVA methodology (see Figure 1) was applied to evaluate the vulnerability due to each specific stressor and the results are depicted in Figure 22, Figure 23, Figure 24 and Figure 25.

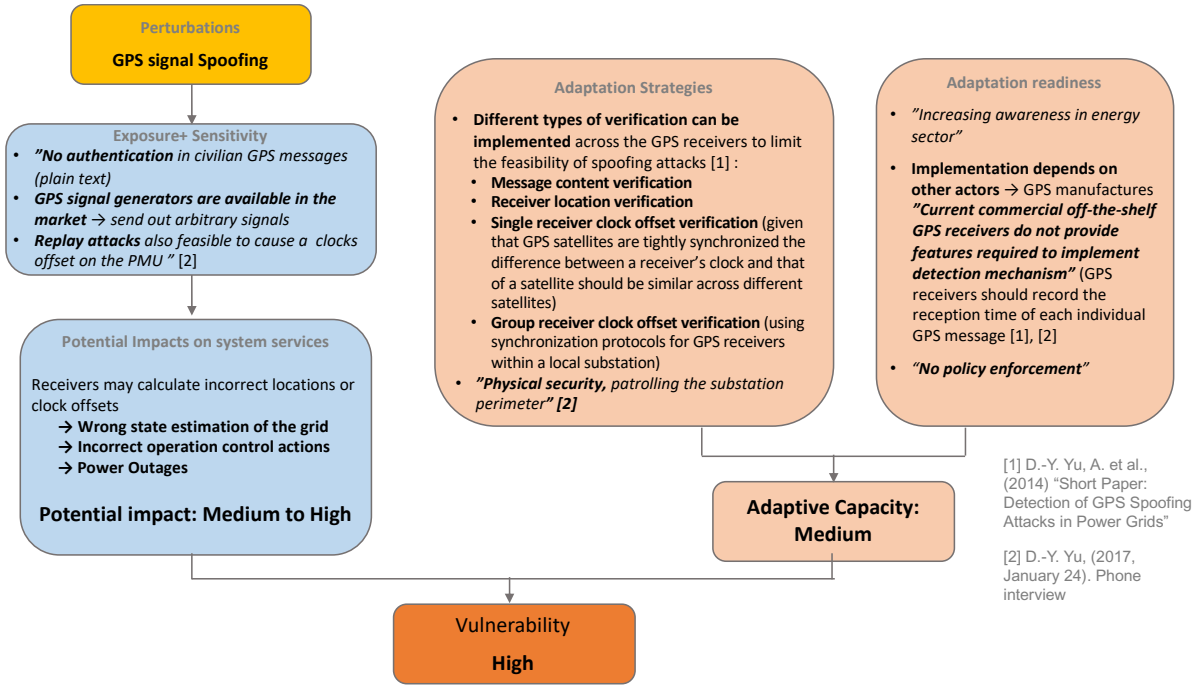


*Figure 22 Vulnerability assessment of CPPS due to stressor (1) GPS signal spoofing. Source: Own representation.*

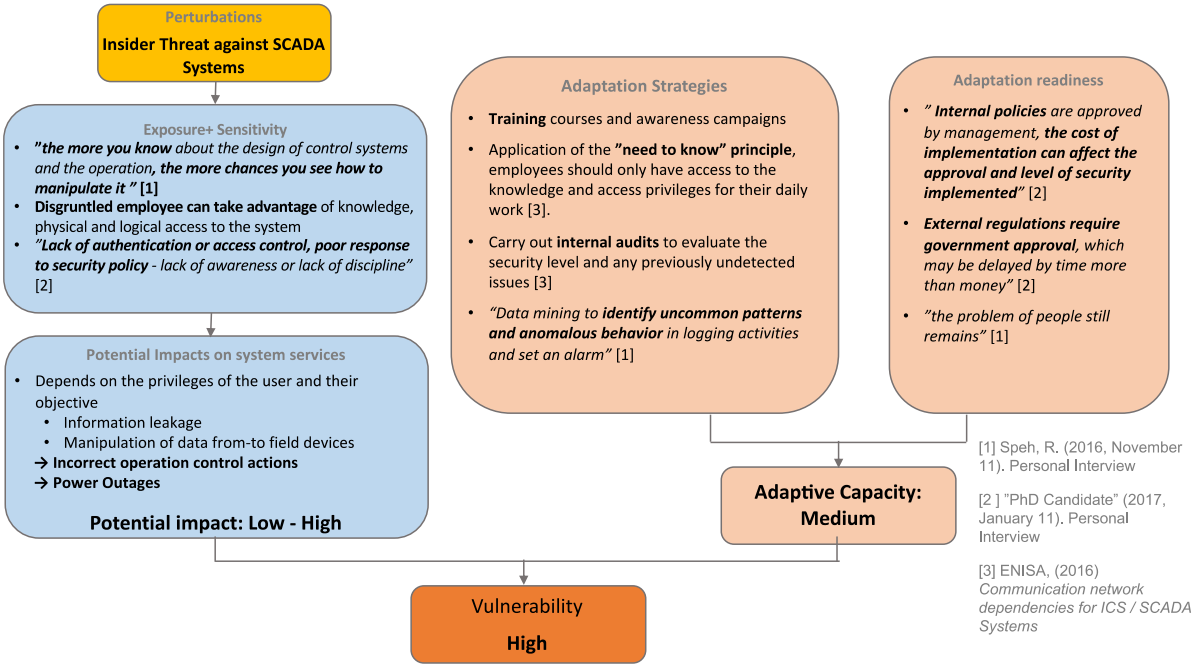


*Figure 23 Vulnerability assessment of CPPS due to stressor (2) Insider threat inside SCADA systems. Source: Own representation.*

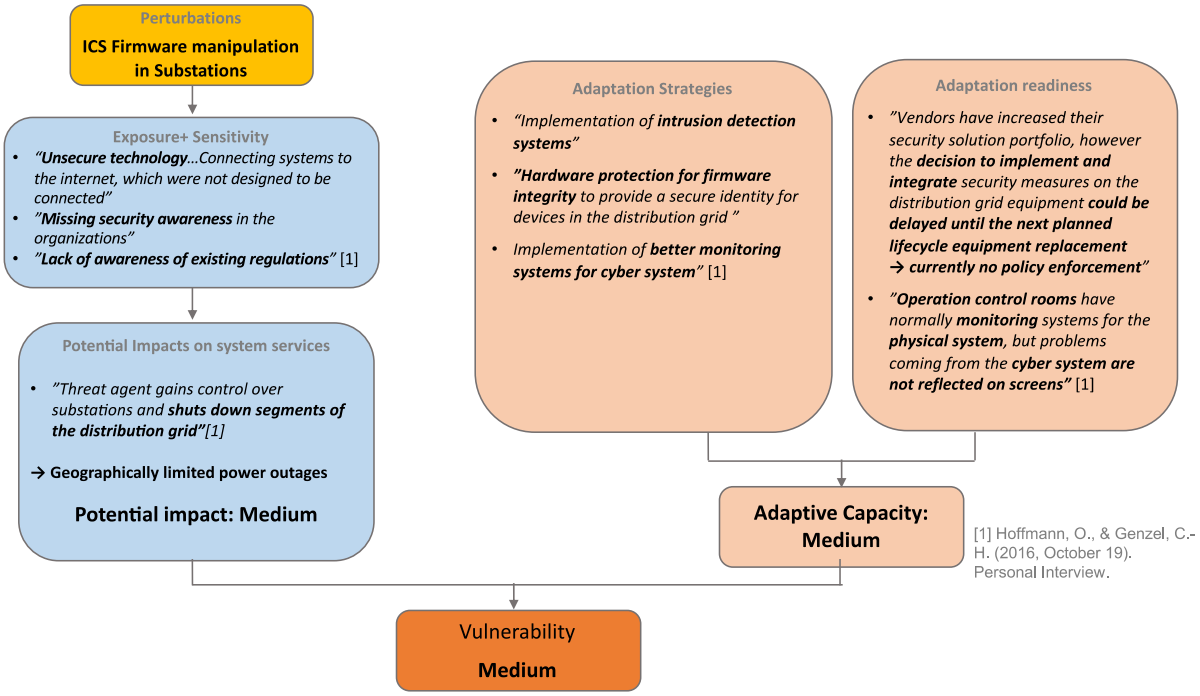


*Figure 24 Vulnerability assessment of CPPS due to stressor (3) ICS firmware manipulation in power substations. Source: Own representation*

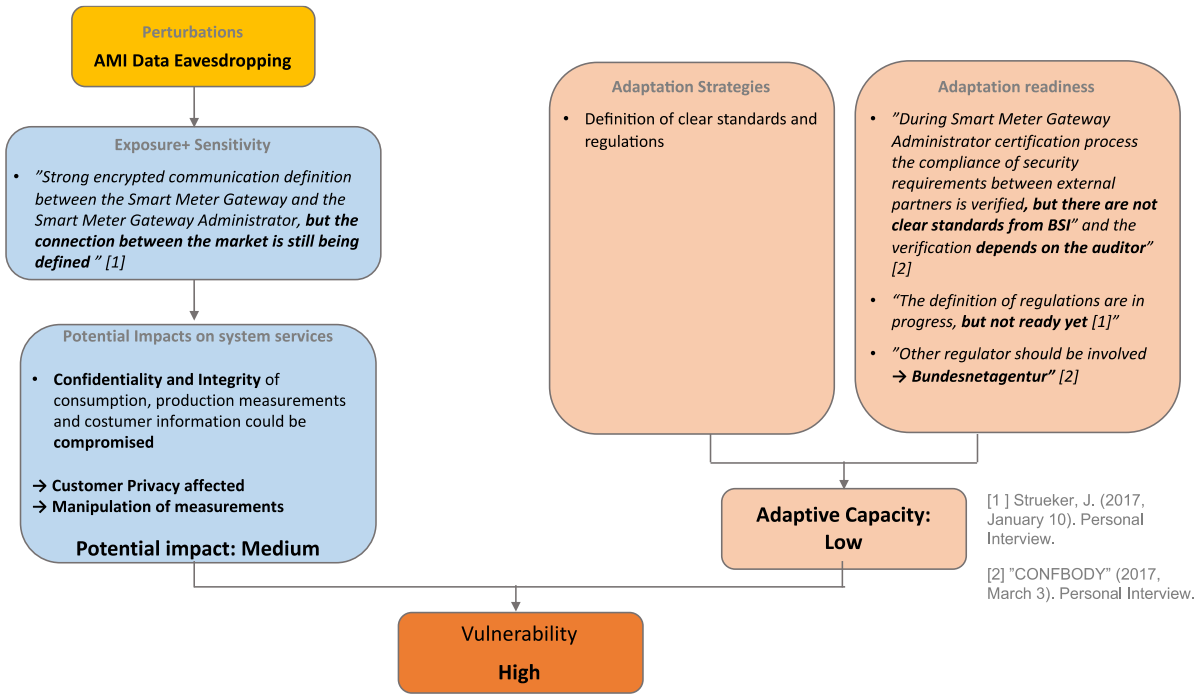


*Figure 25 Vulnerability assessment of CPPS due to stressor (4) Advance Metering Infrastructure data eavesdropping. Source: Own representation*

## 4.6 Vulnerability Assessment Summary

Table 3 summaries the results of the vulnerability assessment for each category and subcategory described in detail above. As it can be seen according to the assessment, all the identified conditions in the different categories make the cyber-physical power system more vulnerable. Data security requirements will be compromised if threat agents exploit one or more of the identified critical points. Depending on the attack mechanism this will lead not only to grid instability or power outages, but also the privacy of customers could be affected. In case of power outages, their magnitude and duration will depend on the system architecture. On one hand, centralized operations will always be more attractive to attackers because they represent a single point of failure and a successful attack could result in a wide-extended blackout. On the other hand, a more distributed architecture formed by smaller units in a cellular structure could lessen the impact of the attack because they have the capacity to run independently and isolate themselves in the case of grid failures.

In spite of the existence of adaptation mechanisms that could minimize the impact, it was found that their implementation could be hindered by the lack of policy enforcement or the un-readiness of the involved actors to implement these measures. Therefore, the challenge is to define an appropriate regulatory landscape without adding complex procedures and monitoring its effective implementation.

*Table 3 Categories and subcategories that reflect critical properties, structures and elements of the cyber-physical power and the corresponding ratings of Potential Impacts, Adaptive Capacity and Vulnerability on the scale L: Low, M: Medium, H: High.*

| Category | Subcategory | Potential Impacts | Adaptive Capacity | Vulnerability |
|---|---|---|---|---|
| Technology | Insecure endpoints | M-H | M | H |
| | Insecure communications | M-H | M | H |
| Organizational security policies and procedures | Improper patch management | M-H | M | H |
| | Lack of interdisciplinary IT-OT knowledge | M-H | M | H |
| The human Factor | Lack of security awareness in organizations | M-H | M | H |
| | Lack of security awareness among consumers | M-H | L | H |
| Regulations | Lack of effective implementation of standards and regulations | M-H | M | H |
| | Lack of coordinated effort to improve security | M-H | M | H |

# 5 Resilience management strategy

The VA unveiled the critical vulnerable points of cyber-physical power systems. Security measures, if applied, have great potential to reduce some vulnerabilities. However, there are further challenges. First, security measures focus mainly on trying to keep the malicious attackers outside of the system, focusing less on recovering mechanism after a successful attack. Second, the dynamic characteristic of ICT systems, as well as the complex interconnections and interdependencies with power systems, make it infeasible to analyze all possible stressors coming from the cyber domain that could threaten the power system. Further stressors of unknown nature commonly referred to as 'black swans', such as: unanticipated information system failures (e.g., bugs, 'zero-days exploits) or more innovative and highly sophisticated attack mechanisms (i.e., advanced persistent threats), and the unknown frequency of these (probability of occurrence) pose significant challenges on developing preventive security methods.

Examples of these uncertain events with low probabilities, yet destructive tendencies are the '*WannaCry'* ransomware and the *'NotPetya'* cyber-attacks occurred in 2017. The cyber-attack against the Ukrainian energy infrastructure in 2016 caused by the highly customized malware *'Crashoverride / Industroyer'* (see more details about *'Crashoverride'* malware in Box 1 from section 4.1.1 Insecure communications) is another example of a 'black swan' against cyber-physical systems.

Therefore, one of the biggest challenges to secure the power system is to find a way to broaden the horizon in handling known and unknown stressors by including recovering, adapting and learning mechanism after successful attacks, instead of only focusing on prevention and detection. This was the objective of the second part of the study. Our main concern was to investigate how to increase the resilience in CPPS. For this purpose, a resilience strategy was developed by using the resilience management approach presented in section 3.2 to identify how CPPS can be better prepared for any kind of stressor.

In the following sections the results of the resilience management strategy and related measures will be described for each phase.

## 5.1 Preparation and Prevention

As a first step during the preparation and prevention phase, weak points in the system need to be identified and effective preventive measures and guidelines must be derived from the results (Acatech et al., 2017). When vulnerabilities, attack vectors and system impacts are known, countermeasures must be developed based on traditional risk assessment and management procedures. For these tasks, a shared effort and cooperation between IT and

operation technology (OT) is needed. Typically, IT cyber security is based on providing confidentiality, integrity and availability to cyber assets, while power system security is based on engineering design and operational strategies. Therefore, IT and power system security should be combined to provide the resilience of the cyber-physical power system (IEC, 2016).

Improvements in security analysis, threat modeling and overall system design will aid the goal of building a resilient system (Interviewee 13, personal communication, 2017). Risk management and risk assessment based on models and simulations will help to figure out the necessary security measures (Interviewee 18, personal communication, 2017; Interviewee 19, personal communication, 2017). A holistic and comprehensive risk assessment that involves reviewing policies and procedures, as well as identifying assets and systems, communication paths and attack vectors, weaknesses, and threat sources will help to determine the level of risk to assets and systems. The evaluation of attack scenarios and attack trees will provide a much more accurate accounting of their likelihood of occurrence, which will produce a risk mitigation strategy that is better prioritized, more targeted, and cost-effective (Bodungen et al., 2017).

Frameworks for risk assessment and management must specifically focus on cyber-physical systems and account for the complex interconnections between both infrastructures considering potential cascading effects between both infrastructures. Some examples of risk management tools designed for ICS or for utility networks can be found in (Bodungen et al., 2017; Schauer et al., 2017). Understanding attacks is essential for planning and evaluating defenses. Using an approach based on example attacks can help in enabling the communication of risks effectively to business decision-makers. See for example the approach that uses the top 20 cyber-attacks on ICS developed by(Ginter, 2017).

In order increase further the resilience of ICS's, some of the standards and common measures from business IT security, such as robust programming and the application of security standards, are also applicable. However, in the case of CPPS, it would be necessary to have more specific security standards, which facilitate the design of this kind of networks (Interviewee 15, personal communication, 2017). For this purpose, a shared effort and cooperation between IT and physical system operators is required to oversee the possibilities and necessary standards for a specific system, as some security standards for computer system networks are not suitable for ICS. For instance, unsupported protocols issues must be addressed in this phase to avoid further related problems (Interviewee 1, personal communication, 2016).

As mentioned in the VA section, there are already available security standards and regulations for ICS. However, an effective implementation of them is still missing (Interviewee 1, personal

communication, 2016). As IT experts in ICS mentioned: "We consider that (*the current security standards)* for industrial control systems are not weak, but probably their actual implementation within the companies could have some weaknesses." (Interviewee 15, personal communication, 2017). Therefore, an effective implementation of existing security standards and regulations is thus an important issue in this phase.

Furthermore, the continuous deployment of IoT devices in the power sector will require the development of more guidelines, references and open source software to support the implementation of adequate security requirements (Interviewee 5, personal communication, 2016). The consolidation, as well as evaluation of existing guidelines and best practices will help utility companies or grid operators to find the suitable security measurements for their specific system. For instance, the whitepaper developed by BDEW (Bundesverband der Energie- und Wasserwirtschaft e.V.) in (BDEW, 2015) provides recommendations for all newly procured control and telecommunication systems for power industry organizations. Also, the report developed in the framework of the research project SPARKS (Smart Grid Protection Against Cyber Attacks) project (see (SPARKS Consortium, 2016) provides recommendations regarding existing and new standards relevant to securing Smart Grid and identifies critical gaps in existing standards and in standards under development.

From another point of view, more effective and engaging security training and awareness programs targeted at corporate staff and IT / OT personnel is of paramount importance. Better awareness and engagement of personnel will contribute to addressing attacks mechanism such as social engineering.

Technology-wise, the implementation of additional measures for data storage and preserving unused resources - operational slack - to better deal with surprises are helpful (Fischer and Lehnhoff, 2019).

### 5.1.1 IT Prevention Mechanism

There are specific IT prevention mechanisms that contribute to preparation and prevention of CPPS. For instance, security driven design ("security by design") should be the standard instead of just adding security features via updates and patches (Interviewee 13, personal communication, 2017). Furthermore, multiple levels of security should be used and security mechanisms should be built on top of each other to preserve the overall security of the system. Firstly, the implementation of cryptographic methods for data and communication channels is required in order to ensure data integrity and prevent unintended disclosure of information in transit. On top of this, the implementation of intrusion detection systems (IDS) is required to have an effective visibility of attacker activities. (Interviewee 1, personal communication, 2016; Interviewee 13, personal communication, 2017).

However, even if the communication channel is secure, the endpoints could still be compromised. Therefore, to address the challenges of end-to-end security, as an IT-security expert stated, it is necessary to make sure that it is possible find out about the security breaches quickly (Interviewee 5, personal communication, 2016). Very important requirements to improve security is the effective implementation of security capabilities into endpoints in terms of authentication, and authorization of usage and control (Interviewee 5, personal communication, 2016). From the perspective of security engineering, one special requirement is scalability for monitoring, maintaining and updating endpoints, due to the increasing number of connected devices, which must be monitored, updated, and maintained (Interviewee 5, personal communication, 2016).

The implementation of trusted computing features is also important for software/firmware integrity. As one of the interviewees mentioned, there is no secure software and security should be hardware based. A trusted platform should be used, which is a hardware device integrated with the systems that cannot be removed without destroying the system, thus assuring integrity (Interviewee 1, personal communication, 2016).

Furthermore, device hardening which refers to different techniques to reduce the attack surface of the system components should also be implemented. In the first place, reducing available services and functionalities to the strict required ones. Closing unwanted service ports and removing non required libraries helps reducing the probability of a device being vulnerable to security exploits (Fischer and Lehnhoff, 2019). The second part of hardening is to keep the software and firmware up-to-date and establish patch management processes that include testing to address flaws on software and hardware. Device hardening increases the ability of a system to absorb ongoing cyber-attacks by increasing the complexity of finding and exploiting vulnerabilities within a system's devices (Fischer and Lehnhoff, 2019).

Regarding access control to software or equipment, a common way to reduce complexity in order to make access control manageable is role-based access control (RBAC), where subjects are not representing individual persons but functional roles. A person is then allowed to act in defined roles and each role has rights attached to it as a subject in the access control matrix (Fischer and Lehnhoff, 2019). The standard IEC 62351-8 provides guidelines for architecture and implementation of RBAC in energy systems. Time-constraints and computational limits of devices make it impossible to have full access control mechanisms down to the field layer. It is necessary to define areas of mutual trust, where no authentication or access restrictions are implemented. Nonetheless, the system design should explicitly specify the context and rationale of access control decisions, especially under what circumstances should no specific access control mechanism be implemented on a device (Fischer and Lehnhoff, 2019).

In order to be able to have better control of the flow of data between groups and prevent an attack that could be spread through the whole network, segmentation into different functional groups is vital. In ICS, the most fundamental separations are between ICS, SCADA and the business network, because each one has different security requirements (Fischer and Lehnhoff, 2019).

## 5.2 Implementation of robust and precautionary design

As mentioned above, the unknown nature of potential future stressors acting on cyber-physical systems make the definition of measures for prevention or preparation difficult. Therefore, the second phase of building resilience must focus on the implementation of a robust and precautionary system design. This will empower the system to maintain its services even under stress or disturbances.

In section 3.2 the resilience design principles were introduced briefly. In this section the design principles will be operationalized for CPPS.

- Diversity contributes positively to the way a system can respond to stressors. On a technological level, the **diversity** of IT components manufacturers, operating systems or communication protocols should be increased in structures and functions of the system.
- Redundancy describes the multiple availability of elements in a system, either in number or in functional equivalence. In CPPS, **Redundancy** of communication channels and devices should be ensured.
- In cyber-physical systems, **geographically distributed** control architectures, possibly extended by virtualization (Mangharam and Pajic, 2013), or based on multi-agent control (Lehnhoff and Krause, 2013) are favourable.
- In terms of buffers and storages, experts suggested the **usage of backups** on several levels in CPPS. Besides the trivial case of energy supply backups (UPS), backups or exact copies of digital systems as well as data and hardware backups are required. Both should be stored offline in a secure manner (Interviewee 2, personal communication, 2016; Interviewee 13, personal communication, 2017). Snapshots of systems before critical software updates should be available to mitigate the impact from manipulated patches and allow for a quick recovery.
- Implementing the **subsidiarity** principle reduces the workload and data flows in the hierarchical higher structures. This can contribute to a higher efficiency and a more appropriate response in case of attacks hitting the structure.
- For cyber-physical systems, **modularity** can be achieved by strictly standardizing interfaces and using open protocols. An example of standardization approaches for

power grid distribution management systems (DMS) is the work developed by the consortium called OpenKONZEQUENZE[9] (oK), which brings together German and Netherlands Distribution System Operators (DSOs), software vendors, service providers and researchers. The oK drives modularization of DMS functionalities, establishing a reference architecture and quality standards to overcome the existing vendor lock-in and system complexity. The goal is to ensure interoperability and make software development vendors independent and faster, while keeping software quality at a high (Goering et al., 2016).

- Based on the analyzed interviews, strongly centralized structures with large power plants, central control units and centralized data processing are seen as less resilient, because they represent a single point of failure and are more attractive to attackers. However, a strongly decentralized structure is not considered resilient either, because it requires a higher level of coordination and synchronization in order to not compromise the performance and reliability of the grid. Furthermore, if coordination in a decentralized system is heavily automated, this adds a new layer of complexity and extends the attack surface even further. A better way to achieve more resilience would be achieved with a **cellular structure**, e.g., the cellular approach, as suggested in (VDE, 2015), where generation and consumption are balanced within adequately sized cells. In Germany, the utility company SWW Wunsiedel GmbH has developed a solution based on this concept applying the segmentation into smaller units consisting of integrated micro-power plants, intelligent consumers and energy storage capacities in order to manage renewable energy volatility and increase cyber-security (see (Kleineidam, Jung, et al., 2016; Kleineidam, Krasser, et al., 2016).
- As discussed with the experts, **decentralized physical backup systems** are needed, which can maintain a stable power supply within decentralized structures, even when there is a blackout in central IT and communication systems. They should be able to conduct adaptations for system loads, frequencies and reactive power compensation based on physical network parameters in cases where digital communication fail.

In general, resilience design measures may cause technical (i.e. efficiency) or economic conflicts. Therefore, design measures must be assessed with a systematic cost-benefit analyses that includes long-term effects and the evaluation of damage cost from rare, but possible, extremely damaging events (Gößling-Reisemann, 2016).

[9] https://www.openkonsequenz.de

### 5.2.1 Detection Mechanism

Cyber-security focuses on keeping the malicious attackers outside of the system. Cyber-resilience involves measures to detect and recover if the system has been compromised by a threat agent. Different algorithms (e.g., machine learning, statistical or Bayesian networks methods among others) should be used to identify manipulated data and flag them as untrustworthy, in order to be treated as suspicious or to be ignored (Interviewee 14, personal communication, 2017).

For the physical systems, existing security algorithms in the energy management systems (EMS) such as power system state estimation or bad data detection can be used to trigger alerts in the case of unexpected behavior (Friedberg et al., 2015). For the detection of intentional attacks directed at disrupting the functioning of state estimation, (e.g., see false date injection attacks in (Liu et al., 2011)), additional measures to detect the malicious data need to be taken into account. Some detection solutions can be found in the literature. For instance, in (Kosut et al., 2010), the authors studied the problem of adversarial false data injection in power system state estimation and presented a novel formulation for the bad data detection problem. They introduced a heuristic method for the detectability of a particular attack by the adversary, which allows particularly bad attacks to be easily computed for any set of compromised measurement. In (Gaber et al., 2015), a strategy is discussed for detecting the presence of bad data and simultaneously estimate it, in order to be able to separate the bad data from the power system observations.

For the ICT systems, existing security solutions such as intrusion detection system (IDS) should be used. The specific means of detection used by an IDS may be, for example, rules similar to those used by firewalls that allow network traffic that violates security policies to be detected. An IDS can also be configured to identify reconnaissance activities, such as host and port scans, which may indicate that an attack is imminent (McLaughlin et al., 2015) If systems or components cannot be updated or patched, the implementation IDS is therefore important to detect if and when systems have been compromised (Interviewee 18, personal communication, 2017). An open source network-based intrusion detection system (NIDS) called Snort[10] is one of the most widely known and used IDS in the research community. It can perform protocol analysis, content searching, and content matching on network traffic in real-time (McLaughlin et al., 2015).

Anomaly-based detection systems over communication channels will enable the detection and distinction of process disturbances from related cyber-attacks. They compare definitions of

[10] https://www.snort.org/

what is considered normal for an activity against observed events to identify significant deviations. The definition of what is normal can be: (a) threshold-based or (b) profile-based. (a) A threshold-based process can monitor the frequency of occurrence of certain events and raise an alarm when violation of the threshold occurs. Examples in the communications could be the number of packets per second, the size of certain packets or flows, etc. (b) Profile-based anomaly detection focuses on characterizing the past behavior and detection of any change. This normally requires a training period, and careful selection of meaningful characteristics to observe (McLaughlin et al., 2015). A study regarding solutions for anomaly detection and diagnostic systems based on Multivariate Statistical Process Control (MSPC), that aims at distinguishing between attacks and disturbances can be found in the literature (see (Iturbe et al., 2016)).

Another method to detect attackers trying to take over the system could rely on examining usage patterns of operators and the connected data history, as an expert suggested. Analyzing those usage patterns could show how individual operators use the system. If someone is using illegitimately acquired login credentials from another user and is operating the system in a different way than the legitimate operator, those deviations could be detected. Regarding this, proper password management is key to avoid unauthorized usage of login credentials (Interviewee 4, personal communication, 2016).

## 5.3 Manage and recover from crises

In case of a successful attack, it is necessary to manage the crisis by restraining it to the smallest possible area or sub-system and recover the system services as quickly as possible. The most critical consequences are long-term power failures and in order to reduce the extent, business continuity planning, emergency planning and respective measures must be implemented on the regional or local level (Acatech et al., 2017; Gößling-Reisemann, 2016).

Furthermore, to be able to react and to recover the system, it is necessary to quickly identify where the failure is located. ICT monitoring systems integrated or coupled to OT monitoring systems is needed to detect failures in IT system parts. Experts on both IT and OT are needed in the grid control centers, and they need to be able to handle different IT and physical infrastructures together. Reaction on possible failures should be planned and trained or implemented in advance, not just as a reaction to attacks and failures (Interviewee 1, personal communication, 2016; Interviewee 4, personal communication, 2016). This requires active emergency planning and exercises with realistic cyber-attacks. Also, monitoring and dynamic segmentation enables the identification and isolation of a compromised endpoint (Interviewee 5, personal communication, 2016). Segmentation capabilities are related to the modular design principle and the loose (or optional) coupling paradigm.

Moreover, it is beneficial to improve the ability of the system to be operated with or without a minimum of ICT, in this way, it could be possible to control it manually or at least secure a soft landing of the system in case of an attack to the ICT infrastructure.

Recovery mechanisms required also depend on the attack as well as the resulting impact. In the case of an attack on the software system, reinstallation of the program logic is required. Therefore, an uncompromised backup of the control logic is necessary. Furthermore, updating the program logic to address/correct the flaws is required (Interviewee 15, personal communication, 2017). Backups on any software level are needed to recover computers and terminals after an attack. Again, offline backups provide better security, as they cannot be compromised by attackers (Interviewee 13, personal communication, 2017), although installing these backups is work intensive.

In case of failures in a centralized system, it is necessary to identify the failing parts and it might be helpful to reconfigure the system in a more distributed fashion. The concept of multi-agent based decentralized control consensus could improve stability and security in the case of failures (see (Lehnhoff and Krause, 2013)). Once the recovery mechanism has been performed and compromised components have been set-up from backups, the former centralized configuration can be re-established. A system would thus be able to gradually go from centralized to more decentralized in the case of failures and then go back again. Concerning this approach, an expert mentioned that working "in smaller cells could be less efficient, because every cell has to provide backup and ancillary services, but it is doable and workable as long as this doesn't become the general case". As soon as possible, the system should go back to a more central configuration that provides more efficient backup and provision of ancillary services (Interviewee 14, personal communication, 2017).

## 5.4 Learn for the future

Past disasters and avoided disasters should be used to **learn for the future** and thus improve the adaptive capacity of the system. This can be achieved by documenting and analyzing these crises and events to identify the weaknesses that led to their occurrence (vulnerability store). In this sense, digital forensic would allow investigating incidents and near incidents in-depth and identify lessons learned. Conversely, identifying strengths that contributed to prevention or recovery (solution store) can be used as a basis for planning strategies and emergency scenarios (Acatech et al., 2017; Gößling-Reisemann, 2016).

Learning from previous attacks could reveal the attack surface that threat agents used, the mechanisms of the attack and it will help to learn how to secure these surfaces or address flaws. For example, the lesson learned from attacks like Stuxnet is that companies need better preparation for social engineering attacks. This includes better security training for employees

as well as proper isolation of business and control system networks (Interviewee 1, personal communication, 2016; Interviewee 13, personal communication, 2017).

When a flaw in the system is discovered and announced, this alerts not only potential attackers, but also vendors who can then take countermeasures. If flaws are not announced, vendors are not aware of them and cannot perform any countermeasure (Interviewee 15, personal communication, 2017). Also, information of successful or unsuccessful attacks could be shared between companies to learn from incidents, comparable to the work done by CERT-Bund (Computer Emergency Response Team for federal agencies) (Interviewee 19, personal communication, 2017). Especially averted attacks should be a very good source for learning. Current practices of “don’t tell” would need to be replaced with a transparency rule, which allows for learning from past mistakes and success stories while maintaining the energy system operator’s right to protect their critical business data.

## 5.5 Summary of Resilience Management Strategy

Several resilience enhancing measures were discussed in the previous sections according to the four phases of the resilience management approach. Now, we will summarize them by sorting the different measures by the categories used in the VA. This enables one to have a better overview of the resilience-enhancing measures and connect them to the critical points identified in the VA.

Table 4 summaries the suggested measures for the category Technology, Table 5 summaries measures for the category Organizational Security Policies and Procedures, Table 6 summaries measures for the category the Human Factor and Table 7 summaries measures for the category Regulations.

*Table 4: Resilience-enhancing measures and elements for the category Technology organized by the phases (1) Prepare and prevent, (2) Implement robust and precautionary design, (3) Manage and recover, and (4) Learn for the future. Source: Own representation.*

| Technology | | | |
|---|---|---|---|
| **Prepare and prevent** | **Implement robust and precautionary design** | **Manage and recover from crises** | **Learn for the future** |
| Implement **security measures at endpoints** e.g. encryption, authentication and authorization (Interviewee 5, 2016) | Increase the **diversity** of IT components (at least in respect to manufacturing, operating systems and communication protocols) | **Multi-agent based control** with decentralized consensus findings could enhance stability and security during crises (Lehnhoff & Krause, 2013) | Make use of **digital forensics**, to draw conclusions from 'near failures' and learn from them them (Gößling-Reisemann, 2016; Acatech et al., 2017) |
| Implement **test routines for patch management** in order to counteract compromised hardware and software with manipulated updates (Fischer and Lehnhoff, 2018). | Ensure **redundancy** in communication channels and devices. | Improve the ability to **operate the system without ICT**, i.e. manually, or to at least secure a *soft landing* | Implement additional measures for data storage (Interviewee 9, 2017; Interviewee 15, 2017) |
| Use a holistic security approach between IT and OT, considering complex interconnections and interactions (International Electrotechnical Commission (IEC), 2016) | Maintain the ability to rely only on decentralized **physical parameters for** operation and hardware-based security, in order to secure a minimum and stable power supply, in case of a failing central ICT infrastructure ("discussed by the interviewed experts") | | |
| Organize the system in a way that security breaches and gaps can be found out quickly (Interviewee 5, 2016) | **Cellular structure** can improve resilience (Verband der Elektrotechnik Elektronik Informationstechnik), 2015 | | |
| Use of a trusted platform, in form of a hardware device integrated with the system that cannot be removed without destroying the system (Interviewee 1, 2016) | Implement intrusion and anomaly **detection systems** (McLaughlin et al., 2015; Interviewee 18, 2017) | | |
| Keep uncompromised backup of the control logic and updating of the program logic (Interviewee 15, 2017) | | | |
| Use of role-based access control (RBAC) in order to make access control more manageable (Fischer & Lehnhoff, 2018) | | | |

*Table 5: Resilience-enhancing measures and elements for the category Organizational Security Policies and Procedures organized by the phases (1) Prepare and prevent, (2) Implement robust and precautionary design, (3) Manage and recover, and (4) Learn for the future. Source: Own representation.*

| Organizational Security Policies and Procedures | | | |
|---|---|---|---|
| **Prepare and prevent** | **Implement robust and precautionary design** | **Manage and recover from crises** | **Learn for the future** |
| Use **security by design** taking into account new threats and vulnerabilities, e.g. bug bounty programs (Interviewee 13, 2017) | Implement **adaptive mechanisms allowing for real-time monitoring**, intrusion and anomaly detection in communication channels (Interviewee 14, 2017) | Provide **business continuity and emergency plans** on a regional and local level, e.g. 'supply islands' at least in and around public properties/ buildings (Acatech et al., 2017a; Gößling-Reisemann, 2016) | Identify strengths in avoided failures that in the past or enhanced recovery as the basis for planning strategies and emergency measures (**Solution Store**) (Gößling-Reisemann, 2016) |
| Apply **energy-focused risk assessments and management approaches** (Interviewee 18, 2017; Interviewee 19, 2017) | Perform periodic **backups of the complete systems** (control logic and updating of the program logic) for quick recovery. (Offline backups prevent manipulation) (Interviewee 13, 2017 ; Interviewee 15, 2017) | Restrict crises to the smallest possible area or sub-system and overcome them as quickly as possible (Goessling-Reisemann and Thier, 2019) | Learn from mastered crisis by documentation and analysis, i.e. learn from previous attacks, e.g. Ukraine, Wannacry or Stuxnet. (Interviewee 1, 2016; Interviewee 13, 2017 |
| **Less is more**: reduce services and function-nalities in terms of data, ports, libraries, group permissions, (Fischer and Lehnhoff, 2018) | **Proper password management** is key to avoid unauthorized usage of login credentials (Interviewee 4, 2016) | **Monitoring and dynamic segmentation** enables the identification and isolation of a compromised endpoint (Interviewee 5, 2016). | Identify weaknesses and document them in a way that the information is accessible to everyone (**Vulnerability Store**) (Gößling-Reisemann, 2016) |
| Develop more and **better guidelines and references** to support the implementation of adequate security requirements (Interviewee 5, 2016) | **Security by obscurity**: intentionally implement a system in a way that is not consistent with conventions and standards in order to confuse attackers and force them to invest more time in system reconnaissance (Fischer & Lehnhoff, 2019) | Identify failing parts and reconfigure the system in a more distributed fashion during a crisis. (Interviewee 14, 2017) | Make use of digital forensics, to draw conclusions from 'near failures' and learn from them (Gößling-Reisemann, 2016; Acatech et al., 2017) |
| Obtain evidence of trustworthyness from manufacturers and suppliers, ensure product integrity, **avoid monocultures** (BSI, 15.10.2019) | Use existing security algorithms in the energy management systems (EMS), such as power system state estimation or bad data detection, to trigger **alerts in the case of unexpected behavior** (Friedberg et al., 2015) | | |
| **Examine usage patterns** of operators and the connected data history (Interviewee 4, 2016 ) | | | |
| **Evaluation of attack scenarios and attack trees** will produce a risk mitigation strategy that is better prioritized, more targeted, and cost-effective (Bodungen et al.,2017). | | | |
| Reaction on possible failures should be planned and **trained or implemented in advance**, not just as a reaction to attacks and failures (Interviewee 1, 2016; Interviewee 4, 2016) | | | |

*Table 6: Resilience-enhancing measures and elements for the category The Human Factor organized by the phases (1) Prepare and prevent, (2) Implement robust and precautionary design, (3) Manage and recover, and (4) Learn for the future. Source: Own representation.*

| The Human Factor | | | |
|---|---|---|---|
| **Prepare and prevent** | **Implement robust and precautionary design** | **Manage and recover from crises** | **Learn for the future** |
| Implement more effective and engaging security training and awareness programs for IT and OT personnel | Enable a tight cooperation between IT and OT for operating and monitoring cyber-physical systems (Interviewee 1, 2016; Interviewee 4, 2016) | Prepare for active emergency planning and exercises based on realistic cyber-attacks | Preserve unused resources - operational slack – will improve the learning. |
| Preserve unused resources - operational slack - to better deal with surprises (Fischer and Lehnhoff 2018) | | | Provision of security training for employees, and proper isolation of business and control system networks (Interviewee 1, 2016; Interviewee 13, 2017) |

*Table 7: Resilience-enhancing measures and elements for the category Regulations followed by the phases (1) Prepare and prevent, (2) Implement robust and precautionary design, (3) Manage and recover, and (4) Learn for the future. Source: Own representation.*

| Regulations | | | |
|---|---|---|---|
| **Prepare and prevent** | **Implement robust and precautionary design** | **Manage and recover from crises** | **Learn for the future** |
| Implement effective guidelines and best practices e.g BDEW (Bundesverband der Energie- und Wasserwirtschaft e.V., 2015) | Make it mandatory to implement resilience principles: Diversity and Redundancy in structures and function, Buffer and Storages. Decentralize management with subsidiarity principle, Modular components, flexible Couplings. (Acatech et al., 2017), (Gößling-Reisemann and Thier, 2019) | | Use the understanding of attacks to plan and evaluate defenses and share this information (Solution store) |
| Ensuring effective implementation of existing Intrusion detection systems(IDS) (Interviewee 1, 2016) (Interviewee 15, 2017) | | | Make documentation regarding failures, attack mechanisms and implement countermeasures publicly available between companies mandatory. (Interviewee 19, personal communication, 2017) |
| Make the monitoring and the effective implementation of a minimum security requirement mandatory. | Strengthen resource efficiency and flexibility, increase participation and burden sharing (Acatech et al., 2017) | | |

# 6 Conclusions and Outlook

It is widely accepted that the power system is rapidly evolving to a large and complex cyber-physical power system which is vulnerable to cyber-physical attacks. At the same time, the attack variants are also becoming more complex, resulting in a necessity to change the existing defense mechanisms that are usually based on lessons from past events and are not effective for protecting the system against unknown threats. Therefore, an approach that goes beyond knowledge about past events and attack mechanisms is needed to aid in protecting the power system against known as well as unknown threats. This was the focus of this study. We assessed existing and known vulnerabilities of the power and cyber infrastructure, and developed a resilience management strategy to prepare cyber-physical power systems for unexpected threats.

In the first part of the study, critical properties, structures and elements that increase the vulnerability of cyber-physical power systems were identified using the vulnerability assessment approach based on (Gößling-Reisemann et al., 2013; von Gleich et al., 2010). Two assessment methodologies were applied, an event-based vulnerability assessment (EVA) and a structural based vulnerability assessment (SVA). The input for the assessment were obtained from experts from power and IT sectors during semi- structured interviews and two expert workshops. The expert statements were evaluated by means of a comprehensive qualitative content analysis methodology. Review of relevant literature on the topic was included for the assessment. The results were grouped under the categories: (1) Technology, (2) Organizational security policies and procedures, (3) The human factor and (4) Regulations. For each category, further subcategories were defined that matched the focus of the assessment on stressors coming from the ICT infrastructure. Some of the identified conditions that contribute to a high vulnerability rating include: insecure communications or poor security features on end points, especially at the customer premises that could compromise data integrity, availability and confidentiality. Social engineering was identified as a critical attack mechanism, which is a rapidly growing security problem that enables threat agents to exploit one of the weaknesses present in every organization: the human factor. In spite of the existence of some adaptation mechanisms that could improve the security level and minimize the impact of these threats, it was found that their implementation could be hindered by the lack of policy enforcement or the unreadiness of the involved actors to implement these measures. From the VA results it was concluded that in order to address these cybersecurity challenges, an integrated assessment consisting of a physical, cyber and social perspective should be used.

In the second part of this study, a resilience management approach was developed in an attempt to give answers to the question of how to prepare cyber-physical power systems to the unknown unknowns. The resilience management approach comprise four phases (1) Prepare and prevent, (2) Implement robust and precautionary design, (3) Manage and recover from crises, and (4) Learn for the future. These phases must be run through iteratively.

In the proposed strategy, resilience-enhancing measures were sorted by the same categories used for the VA and allocated to each phase. The measures were built on the VA results and were derived from the expert interviews, literature research and own judgments. The resilience management strategy focuses on structuring resilience-enhancing measures which include mechanism to prepare for the unexpected, implementation of a precautionary design, adaptation mechanisms and the ability of the system to learn for the future.

In the first phase - Prepare and prevent -, known vulnerabilities and weak points must be identified and effective preventive measures must be implemented. For instance, the implementation of authentication and encryption at endpoints, performing backups of the control and program logic, reducing the services to only the necessary ones and developing better guidelines. Besides, adequate cyber security regulation frameworks should be established and its implementation should be effectively monitored. In the second phase, the focus shifts to implementing a robust and precautionary design. The main focus here is using and applying resilience design principles such as diversification of components and protocols, establishing redundant and modular structures and communications, and implementing anomaly detection systems, amongst other. If the above measures fail and the system is subjected to stress, e.g., as the result of a successful attack, it is necessary to manage the crisis by restraining it to the smallest possible area or subsystem and recover the system services as quickly as possible. This leads to the third phase of the resilience management strategy which is the provision of adaptation mechanisms. In order to manage and recover from crises, the system's architecture should be flexible, e.g., through a cellular structure with multi-agent-based control with decentralized consensus. Additionally, offline physical backups should be built to provide better security and ICT independent recoveries in cases of successful attacks. For the last phase – Learn for the future - suitable measures include establishing a vulnerability store, in which identified weaknesses are documented along with a solution store, in which strengths in avoided failures from the past are recorded. This information should be shared between organizations in order to learn from incidents or near misses.

The resilience-enhancing measures are summarized in Table 4, Table 5, Table 6, Table 7 of section 5.5. The suggested measures do not intend to be comprehensive and it can be seen that for some phases or categories not many measures have been derived. For instance, for

the ‘manage and recover’ and ‘learn for the future’ phases, as well as ‘the human factor’ and ‘regulations’ categories, only few measures are proposed, although these phases are highly relevant for a resilient behavior of the system. We therefore conclude that more effort has to be put into finding adequate measures for these phases and categories taking non-technological and organizational aspects into consideration.

Regarding the applied methodologies, we consider that the vulnerability assessment approach was straight forward, easy to apply and can successfully deliver results, however, it can be time consuming. Whereas deriving the resilience management strategy was a more challenging process. The results from the VA and the resilience design-principle-theory supported the definition of measures for phase one and two. However, for the other two phases, which are strongly related to resilience building and are not included in traditional risk management approaches, it was challenging to give generalized advice that would help to mitigate any kind of stress. This is reflected on the limited measures listed for these phases.

We consider that the use of resilience principles and elements, as well as the establishment of a resilience management approach can support stakeholders and users on preparing the evolving power systems for the unexpected. However, further work is needed to proof this assumption and to improve the knowledge in this area. We therefore propose that the next steps should be to implement the suggested measures described in this manuscript, monitor the behavior of systems under stress and iteratively add further measures for the different phases. Procedures and results should be documented and openly accessible, thus making it possible for joint contributions and for learning from previous experiences. This will enable a continuous improvement of the resilience management strategy, as well as the knowledge of resilience itself.

# 7 References


Acatech, Leopoldina, and Akademienunion. (2017). *Das Energiesystem resilient gestalten: Maßnahmen für eine gesicherte Versorgung*. Acatech, Leopoldina, Akademienunion.

Arghandeh, R., von Meier, A., Mehrmanesh, L., and Mili, L. (2016). On the definition of cyber-physical resilience in power systems. *Renewable and Sustainable Energy Reviews*, *58*, 1060–1069. https://doi.org/10.1016/j.rser.2015.12.193

Baig, Z. A., and Amoudi, A. R. (2013). An analysis of smart grid attacks and countermeasures. *Journal of Communications*, *8*(8), 473–479. https://doi.org/10.12720/jcm.8.8.473-479

Basagiannis, S., Chabukswar, R., Yang, Y., McLaughlin, K., and Boubekeur, M. (2015). Chapter 10—Implementation Experiences from Smart Grid Security Applications and Outlook on Future Research. In F. Skopik and P. Smith (Eds.), *Smart Grid Security* (pp. 283–306). Syngress. https://doi.org/10.1016/B978-0-12-802122-4.00010-9

BDEW. (2015). *Whitepaper Anforderungen an sichere Steuerungs- und Telekommunikationssysteme White Paper Requirements for Secure Control and Telecommunication Systems*. https://www.bdew.de/internet.nsf/id/232E01B4E0C52139C1257A5D00429968/$file/OE-BDEW-Whitepaper_Secure_Systems V1.1 2015.pdf

Becker, C. (2013). *Bedrohungsanalyse für Smart Grids und Anpassung des Sicherheitskonzeptes*. Hochschule Bremen.

BNetzA. (2019). *Bundesnetzagentur—Sicherheitsanforderungen*. https://www.bundesnetzagentur.de/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Anbieterpflichten/OeffentlicheSicherheit/KatalogSicherheitsanforderungen/aktualisierung_sicherheitsanforderungen/aktualisierung_sicherheitsanforderungen-node.html

Bodungen, C., Singer, B., Hilt, S., Shbeeb, A., and Wilhoit, K. (2017). *Hacking Exposed Industrial Control Systems: ICS and SCADA Security Secrets & Solutions* (1st ed.). McGraw-Hill Education.

Brand, U., Giese, B., von Gleich, A., Heinbach, K., Petschow, U., Schnülle, C., Stührmann, S., Stührmann, T., Thier, P., Wachsmuth, J., and Wigger, H. (2017). *Resiliente Gestaltung des Energiesystems am Beispiel der Transformationsoptionen „EE-Methan-System“ und „Regionale Selbstversorgung“: Schlussbericht des vom BMBF geförderten Projektes RESYSTRA (FKZ: 01UN1219A-B)*. Universität Bremen. https://doi.org/10.2314/KXP:1667649884

BSI. (2013). *TR-03109 Anforderungen an die Interoperabilität der Kommunikationseinheit eines intelligenten Messsystems für Stoff- und Energiemengen*. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03109/TR03109-1.pdf?__blob=publicationFile&v=1

BSI. (2014). *Protection Profile for the Security Module of a Smart Meter Gateway ( Security Module PP )*. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/Reporte/ReportePP/pp0077V2b_pdf.pdf?__blob=publicationFile&v=1

BSI. (2015a). *Das Smart-Meter-Gateway*. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Smart-Meter-Gateway.pdf?__blob=publicationFile&v=2

BSI. (2015b). *KRITIS-Sektorstudie Energie*. https://www.dqs.de/fileadmin/files/de2013/Files/Standards/Informationsmanagement/IT-Netzbetreiber/KRITIS-Sektorstudie_Energie.pdf

Cellan-Jones, R. (2018, July 24). *Russian hackers penetrate power stations*. BBC News. https://www.bbc.com/news/technology-44937787

CEN-CENELEC-ETSI Smart Grid Coordination Group. (2012). *Smart Grid Reference Architecture*. https://ec.europa.eu/energy/sites/ener/files/documents/xpert_group1_reference_architecture.pdf

Cherdantseva, Y., Burnap, P., Blyth, A., Eden, P., Jones, K., Soulsby, H., and Stoddart, K. (2015). A review of cyber security risk assessment methods for SCADA systems. *Computers & Security*, *56*, 1–27. https://doi.org/10.1016/j.cose.2015.09.009

Cherepanov, A. (2017). *WIN32/INDUSTROYER A new threat for industrial control systems*. ESET. https://www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf

Cherepanov, A., and Lipovsky, R. (2017, June 12). *Industroyer: Biggest threat to industrial control systems since Stuxnet*. WeLiveSecurity. https://www.welivesecurity.com/2017/06/12/industroyer-biggest-threat-industrial-control-systems-since-stuxnet/

Cleveland, F. (2016). *IEC 62351 Security Standards for the Power System Information Infrastructure*. http://iectc57.ucaiug.org/wg15public/Public%20Documents/White%20Paper%20on%20Security%20Standards%20in%20IEC%20TC57.pdf

Department of Homeland Security. (2018, March 15). *Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors | CISA*. https://www.us-cert.gov/ncas/alerts/TA18-074A

Detken, K.-O., Genzel, C.-H., Hoffmann, O., and Sethmann, R. (2014). Security concept for gateway integrity protection within German smart grids. *3rd ASE International Conference on Cyber Security, ASE (Academy of Science and Engineering)*. https://www.spider-smartmetergateway.de/cms/upload/pdf/ECSaR2014_Stanford.pdf

Detken, K.-O., Genzel, C.-H., Rudolph, C., and Jahnke, M. (2014). Integrity protection in a smart grid environment for wireless access of smart meters. *2014 2nd IEEE International Symposium on Wireless Systems within the Conferences on Intelligent Data Acquisition and Advanced Computing Systems*, 79–86. https://www.spider-smartmetergateway.de/cms/upload/pdf/IDAACS-Wireless2014_SMGS-Integrity_final.pdf

Dondossola, G., Garrone, F., Szanto, J., and Gennaro, F. (2008). A laboratory testbed for the evaluation of cyber attacks to interacting ICT infrastructures of power grid operators. *CIRED Seminar 2008: SmartGrids for Distribution*, 54–54. https://doi.org/10.1049/ic:20080459

Dondossola, G., Garrone, G., Szanto, J., Deconinck, G., Loix, T., and Beitollahi, H. (2009). ICT resilience of power control systems: Experimental results from the CRUTIAL testbeds. *2009 IEEE/IFIP International Conference on Dependable Systems & Networks*, 554–559. https://doi.org/10.1109/DSN.2009.5270292

Dragos Inc. (2017). *CRASHOVERRIDE Analyzing the Threat to Electric Grid Operations*. https://dragos.com/blog/crashoverride/CrashOverride-01.pdf

ENISA. (2012). *Smart Grid Security: Security Related Standards Guidelines and Regulatory Documents*. https://www.enisa.europa.eu/topics/critical-information-infrastructures-

and-services/smart-grids/smart-grids-and-smart-metering/smart-grid-security-related-standards-guidelines-and-regulatory-documents/view

ENISA. (2016). *Communication network dependencies for ICS / SCADA Systems*. https://www.enisa.europa.eu/news/enisa-news/attacks-on-ics-scada-how-to-protect-critical-infrastructures

Experten-Workshop 1. (2016). *Strom-Resilienz Experten-Workshop 1 Protokoll*.

Experten-Workshop 2. (2017). *Strom-Resilienz Experten-Workshop 2 Protokoll*.

Fischer, L., and Lehnhoff, S. (2019). IT-Security for Functional Resilience in Energy Systems. In M. Ruth and S. Goessling-Reisemann (Eds.), *Handbook on Resilience of Socio-technical Systems* (pp. 316–340). Edward Elgar Publishing Limited.

Fischer, L., Uslar, M., Morrill, D., Döring, M., and Haesen, E. (2018, October 30). *Study on the Evaluation of Risks of Cyber-Incidents and on Costs of Preventing Cyber-Incidents in the Energy Sector. Final Report*. https://ec.europa.eu/energy/sites/ener/files/evaluation_of_risks_of_cyber-incidents_and_on_costs_of_preventing_cyber-incidents_in_the_energy_sector.pdf

Friedberg, I., McLaughlin, K., and Smith, P. (2015). Towards a cyber-physical resilience framework for smart grids. In S. Latré, M. Charalambides, J. François, C. Schmitt, and B. Stiller (Eds.), *9th IFIP WG 6.6 International Conference on Autonomous Infrastructure, Management, and Security, AIMS 2015, Ghent, Belgium, June 22-25, 2015. Proceedings* (Vol. 9122, pp. 140–144). Springer, Cham. https://doi.org/10.1007/978-3-319-20034-7_15

Gaber, A., Seddik, K. G., and Elezabi, A. Y. (2015). Joint estimation-detection of cyber attacks in smart grids: Bayesian and non-Bayesian formulations. *2015 IEEE Wireless Communications and Networking Conference (WCNC):-Track 4 - Services, Applications, and Business Joint*, 2245–2250. https://doi.org/10.1109/WCNC.2015.7127816

Ginter, A. (2017). *The Top 20 Cyberattacks on Industrial Control Systems*. https://static.waterfall-security.com/Top-20-ICS-Attacks.pdf?submissionGuid=1817532c-9229-4b7f-987e-5288b36b017d

Goering, A., Meister, J., Lehnhoff, S., Jung, M., Rohr, M., and Herdt, P. (2016). Architecture and Quality Standards for the Joint Development of Modular Open Source Software for Power Grid Distribution Management Systems. *D-A-CH+ Energy Informatics 2016*, 36–39. http://www.energieinformatik2016.org/wp-content/uploads/2016/09/Proceedings_DACH-Energy-Informatics_ComForEn-2016-Web.pdf

Goessling-Reisemann, S., and Thier, P. (2019). On the difference between risk management and resilience management for critical infrastructures. In M. Ruth and S. Goessling-Reisemann (Eds.), *Handbook on Resilience of Socio-technical Systems* (pp. 117–135). Edward Elgar Publishing Limited.

Gößling-Reisemann, S. (2016). Resilience – Preparing Energy Systems for the Unexpected. In I. Link and V. Florin (Eds.), *IRGC Resource Guide on Resilience*. EPFL International Risk Governance Center (IRGC).

Gößling-Reisemann, S., Wachsmuth, J., Stührmann, S., and von Gleich, A. (2013). Climate change and structural vulnerability of a metropolitan energy system: The case of Bremen-Oldenburg in Northwest Germany. *Journal of Industrial Ecology*, *17*(6), 846–858. https://doi.org/10.1111/jiec.12061

Greveler, U. (2016). Die Smart-Metering-Debatte 2010–2016 und ihre Ergebnisse zum Schutz der Privatsphäre. *Datenbank-Spektrum*, *16*(2), 137–145. https://doi.org/10.1007/s13222-016-0219-4

Hirschl, B., Aretz, A., Bost, M., Tapia, M., and Gößling-Reisemann, S. (2018). *Vulnerabilität und Resilienz des digitalen Stromsystems. Endbericht des Projekts „Strom-Resilienz“* (p. 111). Institut für ökologische Wirtschaftsforschung (IÖW) und Universität Bremen, Fachgebiet Resiliente Energiesysteme. https://www.strom-resilienz.de/data/stromresilienz/user_upload/Dateien/Schlussbericht_Strom-Resilienz.pdf

Huang, C.-C., and Kusiak, A. (1998). Modularity in Design of Products and Systems. *IEEE Transactions on Systems, Man, and Cybernetics - Part A: Systems and Humans*, *1*, 66–77.

IEC. (2016). *Power systems management and associated information exchange—Data and communications security- Part 12: Resilience and security recommendations for power systems with distributed energy resources (DER) cyber-physical systems* (1.0). IEC. https://webstore.iec.ch/preview/info_iec62351-12%7Bed1.0%7Den.pdf

IEC. (2020). *Smart Grid Standards Map*. Architecture View. http://smartgridstandardsmap.com

International Electrotechnical Commission (IEC). (2007). *Technical IEC Specification TS 62351-1. Power systems management and associated information exchange—Data and communications security Part 1: Communication network and system security—Introduction to security issues*.

Interviewee 1. (2016). [Personal communication].

Interviewee 2. (2016). [Personal communication].

Interviewee 4. (2016). [Personal communication].

Interviewee 5. (2016). [Personal communication].

Interviewee 6. (2016). [Personal communication].

Interviewee 8. (2017). [Personal communication].

Interviewee 9. (2017). [Personal communication].

Interviewee 12. (2017). [Personal communication].

Interviewee 13. (2017). [Personal communication].

Interviewee 14. (2017). [Personal communication].

Interviewee 15. (2017). [Personal communication].

Interviewee 17. (2017). [Personal communication].

Interviewee 18. (2017). [Personal communication].

Interviewee 19. (2017). [Personal communication].

Iturbe, M., Camacho, J., Garitano, I., Zurutuza, U., and Uribeetxeberria, R. (2016). On the Feasibility of Distinguishing Between Process Disturbances and Intrusions in Process Control Systems using Multivariate Statistical Process Control. *Proceedings of the 46th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshop (DSN-W 2016), 2016*, 155–160. https://doi.org/10.1109/DSN-W.2016.32

Jesse, B.-J., Heinrichs, H. U., and Kuckshinrichs, W. (2019). Adapting the theory of resilience to energy systems: A review and outlook. *Energy, Sustainability and Society*, *9*(1), 27. https://doi.org/10.1186/s13705-019-0210-7

Kleineidam, G., Jung, G., Krasser, M., and Koch, B. (2016). The Cellular Approach—Security of Micro Smart Grids. *SPARKS Workshop Nov 2016*.

https://www.researchgate.net/publication/301231063_The_Cellular_Approach_-_Security_of_Micro_Smart_Grids

Kleineidam, G., Krasser, M., and Reischböck, M. (2016). The cellular approach: Smart energy region Wunsiedel. Testbed for smart grid, smart metering and smart home solutions. *Electrical Engineering*, *98*(4), 335–340. https://doi.org/10.1007/s00202-016-0417-y

Knapp, E. (2011). Chapter 3 – Introduction to Industrial Network Security. In *Industrial Network Security* (pp. 31–54). https://doi.org/10.1016/B978-1-59749-645-2.00003-3

Knapp, E., and Samani, R. (2013). Chapter 3—Hacking the Smart Grid. In *Applied Cyber Security and the Smart Grid* (Syngress, pp. 57–86). https://doi.org/10.1016/B978-1-59749-998-9.00003-7

Kosut, O., Jia, L., Thomas, R. J., and Tong, L. (2010). Limiting false data attacks on power system state estimation. *44th Annual Conference on Information Sciences and Systems, CISS 2010*, 1–6. https://doi.org/10.1109/CISS.2010.5464816

Kush, N., Ahmed, E., Branagan, M., and Foo, E. (2014). Poisoned GOOSE: Exploiting the GOOSE Protocol. *AISC '14 Proceedings of the Twelfth Australasian Information Security Conference*, *149*, 17–22.

Kushner, D. (2013, February 26). *The Real Story of Stuxnet*. IEEE Spectrum: Technology, Engineering, and Science News. https://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet

Langner, R. (2013). *To Kill a Centrifuge—A Technical Analysis of What Stuxnet's Creators Tried to Achieve* (November; pp. 1–36). The Langner Group. https://www.langner.com/wp-content/uploads/2017/03/to-kill-a-centrifuge.pdf

Lee, C., Zappaterra, L., Kwanghee Choi, and Hyeong-Ah Choi. (2014). Securing smart home: Technologies, security challenges, and security requirements. *2014 IEEE Conference on Communications and Network Security*, 67–72. https://doi.org/10.1109/CNS.2014.6997467

Lehnhoff, S., and Krause, O. (2013). Agentenbasierte Verteilnetzautomatisierung. In P. Göhner (Ed.), *Agentensysteme in der Automatisierungstechnik* (pp. 207–223). Xpert.press Springer-Verlag. https://doi.org/10.1007/978-3-642-31768-2_12

Liu, Y., Ning, P., and Reiter, M. K. (2011). False data injection attacks against state estimation in electric power grids. *ACM Transactions on Information and System Security*, *14*(1), 1–33. https://doi.org/10.1145/1952982.1952995

Lopez, C., Sargolzaei, A., Santana, H., and Huerta, C. (2015). Smart Grid Cyber Security: An Overview of Threats and Countermeasures. *Journal of Energy and Power Engineering*, *9*(7), 632–647. https://doi.org/10.17265/1934-8975/2015.07.005

Lovins, A. B., and Lovins, L. H. (2001). *Brittle Power -Energy Strategy for National Security*. Brick House Pub. Co.

Luiijf, E. (2016). Threats in Industrial Control Systems. In E. J. M. Colbert and A. Kott (Eds.), *Cyber-security of SCADA and Other Industrial Control Systems* (pp. 69–93). Springer International Publishing. https://doi.org/10.1007/978-3-319-32125-7_5

Mangharam, R., and Pajic, M. (2013). Distributed Control for Cyber-Physical Systems. *Journal of the Indian Institute of Science*, *93*(3), 353–388.

Marin Fernandes, P. (2012). Chapter 11: Introduction to Smart Grid Cyber Security. In L. Berger and K. Iniewski (Eds.), *Smart Grid Applications, Communications, and Security* (pp. 229–320). John Wiley & Sons.

Maynard, P., Mclaughlin, K., and Haberler, B. (2014). Towards Understanding Man-In-The-Middle Attacks on IEC 60870-5-104 SCADA Networks. *2nd International Symposium on ICS & SCADA Cyber Security Research 2014 (ICS-CSR 2014)*, Pages 30-42. https://doi.org/10.14236/ewic/ics-csr2014.5

Mayring, P. (2014). *Qualitative content analysis: Theoretical foundation, basic procedures and software solution*. https://nbn-resolving.org/urn:nbn:de:0168-ssoar-395173

McCarthy, J., Powell, M., Stouffer, K., Tang, C., Zimmerman, T., Barker, W., Ogunyale, T., Wynne, D., and Wiltberger, J. (2018). *Securing Manufacturing Industrial Control Systems: Behavioral Anomaly Detection. NISTIR 8219*. https://www.nccoe.nist.gov/sites/default/files/library/mf-ics-nistir-8219.pdf

McLaughlin, K., Friedberg, I., Kang, B., Maynard, P., Sezer, S., and McWilliams, G. (2015). Chapter 5—Secure Communications in Smart Grid: Networking and Protocols. In F. Skopik and P. Smith (Eds.), *Smart Grid Security* (pp. 113–148). Syngress. https://doi.org/10.1016/B978-0-12-802122-4.00005-5

Mo, Y., Kim, T. H.-J., Brancik, K., Dickinson, D., Perrig, A., and Sinopoli, B. (2012). Cyber–Physical Security of a Smart Grid Infrastructure. *Proceedings of the IEEE*, *100*(1), 195–209. https://doi.org/10.1109/JPROC.2011.2161428

Morgner, P., Mattejat, S., Benenson, Z., Müller, C., and Armknecht, F. (2017). Insecure to the touch: Attacking ZigBee 3.0 via Touchlink Commissioning. *Proceedings of the 10th ACM Conference on Security and Privacy in Wireless and Mobile Networks - WiSec '17*, 230–240. https://doi.org/10.1145/3098243.3098254

NESCOR. (2015). *Electric Sector Failure Scenarios and Impact Analyses – Version 3.0*. http://smartgrid.epri.com/doc/NESCOR Failure Scenarios v3 12-11-15.pdf

New Jersey Cybersecurity & Communications Integration Cell. (2017). *Stuxnet*. NJCCIC. https://www.cyber.nj.gov/threat-profiles/ics-malware-variants/stuxnet

Nissim, N., Yahalom, R., and Elovici, Y. (2017). USB-based attacks. *Computers and Security*, *70*, 675–688. https://doi.org/10.1016/j.cose.2017.08.002

NIST. (2014). *National Institute of Standards and Technology Interagency Report 7628 Rev. 1*. https://doi.org/10.6028/NIST.IR.7628r1

Qi, J., Hahn, A., Lu, X., Wang, J., and Liu, C.-C. (2016). Cybersecurity for distributed energy resources and smart inverters. *IET Cyber-Physical Systems: Theory & Applications*, *1*(1), 28–39. https://doi.org/10.1049/iet-cps.2016.0018

Rossebo, J. E. Y., Wolthuis, R., Fransen, F., Bjorkman, G., and Medeiros, N. (2017). An Enhanced Risk-Assessment Methodology for Smart Grids. *Computer*, *50*(4), 62–71. https://doi.org/10.1109/MC.2017.106

Rubin, H., and Rubin, I. (2005). *Qualitative Interviewing (2nd ed.): The Art of Hearing Data*. SAGE Publications, Inc. https://doi.org/10.4135/9781452226651

Schauer, S., König, S., Latzenhofer, M., and Rass, S. (2017). *Identifying and Managing Risks in Interconnected Utility Networks*. 79–86. http://www.thinkmind.org/index.php?view=article&articleid=securware_2017_5_20_30042

Sobczak, B. (2019, May 6). *Experts assess damage after first cyberattack on U.S. grid*. Security. https://www.eenews.net/stories/1060281821

SPARKS Consortium. (2016). *Deliverable D3.3 Smart Grid Security Standards Recommendations*. https://project-sparks.eu/wp-content/uploads/2014/04/D-3-3_SmartGridSecurityRecommendations.pdf

Stirling, A. (2007). A general framework for analysing diversity in science, technology and society. *Journal of the Royal Society Interface*, *4*(15), 707–719. https://doi.org/10.1098/rsif.2007.0213

Strauss, A. L., and Corbin, J. M. (2010). *Grounded theory: Grundlagen qualitativer Sozialforschung* (Unveränd. Nachdr. der letzten Aufl). Beltz.

Styzcynski, J., and Beach-Westmoreland, N. (2017). *When the lights went out. A comprehensive review of the 2015 attacks on Ukrainian critical infrastructure*. https://www.boozallen.com/content/dam/boozallen/documents/2016/09/ukraine-report-when-the-lights-went-out.pdf

Tapia, M., Thier, P., and Gößling-Reisemann, S. (2020). Building resilient cyber-physical power systems. *TATuP - Zeitschrift Für Technikfolgenabschätzung in Theorie Und Praxis*, *29*(1). https://doi.org/10.14512/tatup.29.1.23

Tazi, K., and Abdi, F. (2015). Review on Cyber-Physical Security of the Smart Grid: Attacks and Defense Mechanisms. *3rd International Renewable and Sustainable Energy Conference (IRSEC)*, 1–6. https://doi.org/10.1109/IRSEC.2015.7455127

Teixeira, A., Kupzog, F., Sandberg, H., and Johansson, K. H. (2015). Chapter 6 – Cyber-Secure and Resilient Architectures for Industrial Control Systems. In F. Skopik and P. Smith (Eds.), *Smart Grid Security: Innovative Solutions for a Modernized Grid* (pp. 149–183). https://doi.org/10.1016/B978-0-12-802122-4.00006-7

VDE. (2015). *Der Zellulare Ansatz: Grundlage einer erfolgreichen, regionenübergreifenden Energiewende*. VDE ETG (Energietechnische Gesellschaft im VDE). http://www.vde.com/de/fg/ETG/Arbeitsgebiete/V2/Aktuelles/Oeffenlich/Seiten/VDEETG-StudieDerZellulareAnsatz.aspx

Virsec. (2017, May 7). Virsec Hack Analysis: Deep Dive into Industroyer (aka Crash Override). *Virsec Systems*. https://virsec.com/virsec-hack-analysis-deep-dive-into-industroyer-aka-crash-override/

von Gleich, A., Gößling-Reisemann, S., Stührmann, S., Woizeschke, P., and Lutz-Kunisch, B. (2010). Resilienz als Leitkonzept – Vulnerabilität als analytische Kategorie. In K. Fichter, A. von Gleich, R. Pfriem, and B. Siebenhüner (Eds.), *Theoretische Grundlagen für erfolgreiche Klimaanpassungsstrategien. Nordwest2050 Berichte Heft 1* (pp. 13–49). Projektkonsortium ‚nordwest2050'.

von Oheimb, D. (2012). IT Security Architecture Approaches for Smart Metering and Smart Grid. *Smart Grid Security*, 1–25. https://doi.org/10.1007/978-3-642-38030-3_1

von Oheimb, D. (2013). IT Security Architecture Approaches for Smart Metering and Smart Grid. In J. Cuellar (Ed.), *Smart Grid Security* (pp. 1–25). Springer Berlin Heidelberg. https://link.springer.com/chapter/10.1007/978-3-642-38030-3_1

# Appendix A: Interview Analysis Methodology

## Expert interviews

To gain adequate data from relevant sources in the field, expert interviews were chosen as the optimal method to generate data (Rubin and Rubin, 2005). The aim was to find interview partners whose long-term expertise in the IT or energy sector can provide a well-founded overview of relevant topics in the field. In the end, 19 interviews were conducted with experts from IT, energy, and automation fields, and public bodies. Each of those interviews were conducted in English, transcribed and then further analyzed based on (Mayring, 2014).

## Questionnaire

The questions used for the semi-structured interviews are listed below:

**Professional information**

1. What is your educational and professional background?
2. Which job position do you have at the moment? Since when?
3. Could you describe your current job position?
   3.1. How is it related to smart grids?
   3.2. How is it related to smart grid cyber security?
4. Are you involved in any R&D project on cyber security of smart grids in your organization?
   4.1. If yes, could you briefly describe it?

**Knowledge about studies on cyber security in Smart Grids and risk assessment**

5. Several standards, guidelines and recommendations have been addressing smart grid cyber security and risk assessment in particular. One example is the report developed by the U.S. National Institute of Standards and Technology (NIST): "Guidelines for Smart Grid Cyber Security (NIST-IR 7628)".
   5.1. Are you familiar with some of these initiatives?
   5.2. Do you know about any other study dealing with smart grid cyber security issues in Germany, Europe and/or worldwide?
      5.2.1. If yes, could you name and briefly describe them?

**Cyber security vulnerabilities in Smart Grids**

Considering the following smart grid reference architecture model *(see (IEC, 2020)) and assuming a complete implementation of the smart grid functionalities:

6. In your opinion, which are the main cyber security challenges for the smart grid that need to be addressed? Why?
7. In the reference architecture model, could you identify which components (power equipment or information assets) are potentially most vulnerable?
   7.1. Which of them represent special interest in your field of expertise?
   7.2. For what reasons?
8. Which are the perturbations / events that could have an effect on the system services?
9. What could be the potential impacts from these perturbations/events?
10. Which are the relevant stressors / aggressors for the occurrence of these perturbations / events?
    a) people

b) organizations
c) hazards
d) others: please name

11. What conditions in each of the following fields facilitate the occurrence of these perturbations / events?
    a) technology
    b) organization/structure
    c) economy/regulations
    d) culture/society
12. In case of intentional perturbations, what is the feasibility of putting these perturbations / events in practice, either in present or in future power systems?
    12.1. What would be the attack mechanisms?
13. What is required or has to be modified in order to prevent the occurrence of these intentional or unintentional perturbations / events?
14. What are the existing (or prospective) adaptation options to recover the system services?
    14.1. What could be done on the technical and organizational level for such a recovery?
15. How can we learn from past events and from the so called “near misses”?
16. When and to what extent can the identified adaptation measures be implemented?
17. Who are the actors and institutions involved in the development and regulation of the implementation of these adaptation options? From:
    - energy sector
    - IT sector
    - regulatory authorities
    - the market

**System Granularity**

Considering the evolution of the power systems, in terms of production, consumption and control, which goes from a totally centralized system towards a more granular or decentralized system:

18. How would the granularity of the system affect the exposition and sensitivity to the previous perturbations identified?
19. How would the granularity of the system affect the identified measures to cope with them?

## Overview of content analysis methodology

The main focus of the qualitative content analysis methodology is to construct a code system, which is systematically derived out of the interview data while working along a set of methodological rules (Mayring, 2014). Qualitative content analysis put an emphasis on constructing and founding codes based on the data from previously conducted expert interviews (Mayring, 2014). Code systems are both starting point and result of the first analytical steps while contributing to the reliability of this methodological approach. As this methodology is also very theory driven, these codes serve as theoretical categories, oriented on thematic aspects of the data, prior knowledge and previous studies. These codes were filled with text passages from the material, which contain relevant content, matching the thematic orientation or the topic of the categorical code. More information about the coding

process, which addresses open coding as analytical tool (Mayring, 2014), is provided in the next section.

It is also important to include current research and theoretical aspects in every step of the content analysis (Mayring, 2014). In this project, the results of both literature review and vulnerability assessment methodology, including the ideas behind this method took a significant part in conducting the content analysis. Another criterion for content analysis is objectivity. This can be achieved by the inter-coder reliability which is a research tool designed to compare the codes from different researchers and look for differences in the way the content was coded. This tool affords multiple researchers and addresses the problems of site boundary and too different interpretations of the text material (Mayring, 2014). Furthermore, an exact determination of the basic data material in use, as well as its origin has to be regarded. The basic material which has to be analyzed can consist out of every linguistic data, pictures and even videos. The most common source of data is presented in form of transcribed interviews (Mayring, 2014). After the determination of a precise research issue, the rest of the analytical process has to be agreed upon. During this, analytical steps can vary depending on the research topic and the chosen special method of a content analysis (Mayring, 2014). Those special techniques focus on different forms of processing textual data: structuring, explication and summarization.

For this project, the technique of summarization was chosen. The goal here was to reduce the initial material while keeping the main content and meaning intact. The standard summarization procedure proposed by (Mayring, 2014) which was used in this study, will be shortly described:

- After an initial coding, the coded text passages were paraphrased in order to reach a consistent linguistic level. Here, the initial text material was reduced for the first time, as the passages which were transcribed as they were spoken were transformed to grammatical abbreviations. The main content and structure were still maintained in those paraphrases while unimportant elements which do not contain meaning or relevant contents were deleted (Mayring, 2014).
- After paraphrasing, the material was condensed once more. For this step, the level of abstraction was agreed upon to edit those paraphrases. Everything under the desired level was kept for further abstraction and generalization, anything above that level was kept as it was. Paraphrases with the same content were integrated and those containing no relevant meaning were left out (Mayring, 2014).
- In a second round of summarization, paraphrases were integrated into each other. In this way, categories on the desired level of abstraction were generated. In combination with this, a preliminary system of categories including summaries for each relevant

topic was derived from the material. Following this, it was checked if the basic material was still represented accordingly by reviewing the initial code system, categories and paraphrases. If the representation of the initial data was satisfying, the summaries were further reduced and integrated until the desired level of concentration was achieved (Mayring, 2014).

Concerning the construction of the code system, the methodology proposes that this could be done in different ways: either inductive, deductive or as a mixture of both. Inductive construction means that a code system will not be existing when stating the coding process. Instead, it will emerge out of the data during the coding process and the successive bundling of the material. Codes are generated directly through the material by first deriving selective criteria concerning the desired level of abstraction and then, selecting content which is relevant for the topic of interest. The research issue should be kept in mind at this step. During the coding, the material will be viewed completely and codes are constructed and filled with coding. Another round of checking and revisiting the codes after the first round of coding will be necessary, to have all codes coded with the whole material (Mayring, 2014).

Deductive construction of codes implies starting off with a previously generated code system which take into account all the theoretical background, literature reviews and the research topic. This preliminary code system will then undergo the processes of coding and summarizing as described above (Mayring, 2014).

The last way of generating codes is deductive-inductive. It combines the advantages of a preliminary code system, constructed alongside the theoretical background, research hypothesis and previous knowledge with the advances of revisiting, reviewing and reworking the code system during the coding process (Mayring, 2014). This method was chosen to be the right starting point in this study, as the elements of the VA could be used as codes for the first code system. Then the statements from expert interviews were categorized by those codes and then reviewed accordingly.

To meet the demands of this interdisciplinary and mixed methods project, the standard procedure of content analysis had to be altered. Therefore, the process of paraphrasing and reducing was shortened as the experts' statements were very specific and thematically focused. This led to larger text segments being coded. These segments were then paraphrased keeping a focus on the delivered meaning in order to achieve a constant level of articulation. But instead of transforming the segments of direct speech into abbreviations, whole sentences were constructed to keep the structure of arguments intact and to prepare them for later summarizations. The paraphrases then underwent a round of checking by every

researcher, in order to make sure that content and meaning were correctly extracted and condensed.

With those more comprehensive paraphrases, the first summaries were constructed for the VA methodology. The reason for choosing paraphrases which were in full sentences and more comprehensive was so that it would be easier distinguish between statements from different experts.

Later on, as the phases for the resilience strategy were developed and included in the code system the material was once more coded with these new categories and paraphrased. Those paraphrases were also summarized to achieve a comprehensive text from every major code. These summaries include different statements which were unbundled and reduced as described above.

The paraphrased statements from the coding system were ordered by their topic. Statements concerning the same topic but from different interviewees were integrated into each other. Emphasis was laid on keeping the specific structure and meaning of statements intact, so that it can be differentiated between statements of different experts.

### Coding content

In this section, the process of open coding will be described in more detail to show how documents were initially analyzed and thus prepared for the content analysis methodology.

Open coding based on the Grounded Theory methodology is very well suited to open a material in an early analysis phase and for forming the first categories. This is done by classifying, conceptualizing and categorizing the original data (Strauss and Corbin, 2010). Through constant comparison during the process, the data is given specificity and precision during which questions are also posed to the material - what is conveyed, how is it expressed, why was that very word chosen, in what context is the passage described, what is the meaning conveyed? (Strauss and Corbin, 2010). Thus more and more concepts are gradually being determined from the data, which are then combined into groups from which phenomena can be derived (Strauss and Corbin, 2010). The concepts must therefore be appropriately named. This can either be done by yourself, or by in vivo codes that are derived directly from the text passage and adopted (Strauss and Corbin, 2010). After concepts and phenomena have been derived, the first categories are created which contain dimensionalities and reflect the properties of the concepts they contain (Strauss and Corbin, 2010).

There are different methods for open coding. Thus, the material can be viewed line by line, or even more precisely, word by word. This is the most detailed and at the same time most effective approach since the largest possible number of categories can be filtered out of a text

(Strauss and Corbin, 2010). This is particularly important in early analysis phases in order to generate a wealth of categories which can be checked and revised in the further procedure.

The next coding method focuses on the text passages per sentence or paragraph. Here the main ideas of sections are filtered out and compared with the other concepts. This is particularly suitable if some categories already exist and are to be encoded in their thematic environment (Strauss and Corbin, 2010).

A third approach is to consult entire documents. The main aim is to identify differences to other documents or to differentiate the overall context of the document (Strauss and Corbin, 2010). According to this, open coding leads in a special way to deal with the source material in order to derive first theoretical building blocks in the form of categories filled with content. This is precisely why the method is suitable for analyzing interview data for its content and categorizing it in such a way that further analysis steps can follow.

Another way to code documents is axial coding. Content analysis affords this step after an initial round of coding, to check data with a focus on an existing code system. But it is also possible, to conduct only axial coding, if a preexisting code system has to be validated. This is important, to ensure that existing codes are sufficient as relevant categories and contain enough meaning. The material is viewed alongside the code systems and is constantly compared with it. Keeping strictly focused on existing codes to enhance and fill them is especially needed when a preexisting code system is used. In this case, the first round of coding makes sure that existing codes are sufficient, otherwise new ones have to be created. A second round of coding makes sure that all documents are included in the newer codes and confirms if existing codes are still in the right categories. After completing the second round of coding, the code system should be more precise and structured. If not, additional rounds of coding and recoding can be conducted, until a satisfactory level of structuration and saturation is reached (Mayring, 2014).

The following describes the coding process performed in this study:

- Text segments from the interview transcription were coded with categories which contained a specific topic mentioned. Those topics could be: general information about professional information, or it could be content that was relevant for categories of the VA or for the resilience strategy. The whole text segment containing a specific topic was sorted into the respecting category.
- The first round of coding combined perks of open coding with the focus of an axial coding.
- Like open coding, new codes were derived out of the material and the material was initially broken up into coding. Axial coding with the preliminary code system (Table 8)

ensured, that codes in this code system were filled accordingly, thus gaining reliability and validity.

- It also was important, that every researcher in charge of the content analysis had completed a full round of coding, including all documents. After this, the code system underwent a complete run of recoding by every researcher. During this step, every coding inside of a code was reviewed with a focus on checking the following points: (a) if coding belongs to the right code, or whether more structuring was needed, (b) if the code still conveys its initial thematic orientation, (c) if enough content was conveyed by the code in order to keep it a category or (d) if the code has to be a sub-code of another major code.
- The research team together revisited the resulting code system, which underwent major changes during this analytical step as it was decided to change the structure and to include the phases of the resilience strategy and some structuring for parts concerning elements of the VA. With this new code system, another round of coding and recoding followed.

The resulting code system (Table 9) proved to be reliable to capture the content, which was delivered by interviewed experts.

*Table 8 Initial code system derived from the expert interview and workshops*

| List of codes |
|---|
| Code system |
| Working domain |
| Challenges |
| Open category |
| Professional and educational background |
| Current job position |
| Research project |
| Regulations |
| Vulnerable assets |
| Human resources |
| Administrative staff |
| Electrical Operators |
| IT operators |
| Cyber infrastructure assets |
| Electrical infrastructure assets |
| Perturbations |
| External perturbation |
| Internal perturbation |
| Potential impacts |

- Cyber infrastructure
  - Confidentiality
  - Non-repudiation
  - Availability
  - Integrity
- Electrical infrastructure
  - Power outages
    - Large power outage
    - Small power outage
  - Qualitative Criteria
    - Indirect Parameters
      - Public acceptance
      - Economic impacts
    - Impacts on technical parameters
- Stressors
  - Other
  - Hazards
    - Degradation
    - Human errors
  - Organizations
  - People
    - External stressor (P)
    - Internal stressor (P)
- Conditions
  - Other
  - Society
  - Regulations (conditions)
  - Economy
  - Organization
  - Technology
- Attack mechanisms
- Feasibility
  - Motivation
  - Level
  - Effort
  - Knowledge
- Adaptation strategies
  - Preparation
    - Challenges (Prep)
  - Prevention
    - Challenges (Prev)
  - Detection
    - Challenges (Det)
  - Response
    - Challenges (Resp)

| |
|---|
| Recovery |
| Challenges (Rec) |
| Learning |
| Challenges (Lear) |
| Implementation of adaptation strategies |
| Willingness to implement |
| Readiness to implement |
| Actors involved |
| Market |
| Others |
| Regulatory authorities |
| IT sector |
| Energy sector |
| Granularity of the system |
| Low granularity |
| High granularity |

*Table 9 Final code system that captures the content delivered by interviewed experts and was used for the assessment of vulnerabilities and for deriving resilience-enhancing measures*

| **Final list of codes** |
|---|
| Code system |
| New Categories |
| Insecure communications |
| Exposure and Sensitivity |
| Attack mechanism and Perturbations |
| Potential impacts |
| Adaptation strategies, implementation |
| Insecure End-Points |
| Exposure and Sensitivity |
| Attack mechanism and Perturbations |
| Potential impacts |
| Adaptation strategies, implementation |
| Insecure interface between components of different vendors |
| Exposure and Sensitivity |
| Attack mechanism and Perturbations |
| Adaptation strategies, implementation |
| improper change and configuration management |
| Incorrect settings damage the system or allow to get access |
| Software and firmware allows unauthorized modification |
| Exposure and Sensitivity |
| Attack mechanism and Perturbations |
| Potential impacts |
| Adaptation strategies, implementation |
| Systems running in web services |
| Exposure and Sensitivity |

| |
|---|
| Attack mechanism and Perturbations |
| Potential impacts |
| Adaptation strategies, implementation |
| Lack of “expert” operators |
| Exposure and Sensitivity |
| Attack mechanism and Perturbations |
| Potential impacts |
| Adaptation strategies, implementation |
| Lack of IT-OT experts in the organization |
| Exposure and Sensitivity |
| Attack mechanism and Perturbations |
| Potential impacts |
| Adaptation strategies, implementation |
| Improper network segregation |
| Exposure and Sensitivity |
| Attack mechanism and Perturbations |
| Potential impacts |
| Adaptation strategies, implementation |
| Improper security patch management |
| Exposure and Sensitivity |
| Attack mechanism and Perturbations |
| Potential impacts |
| Adaptation strategies, implementation |
| Lack of effective implementation of security standards |
| Exposure and Sensitivity |
| Potential impacts |
| Adaptation strategies, implementation |
| Lack of security awareness in the organizations |
| Exposure and Sensitivity |
| Attack mechanism and Perturbations |
| Potential impacts |
| Adaptation strategies, implementation |
| Lack of security awareness among consumers |
| Exposure and Sensitivity |
| Attack mechanism and Perturbations |
| Potential impacts |
| Adaptation strategies, implementation |
| No economic incentives to invest / lack of coordinated effort |
| Exposure and Sensitivity |
| Attack mechanism and Perturbations |
| Potential impacts |
| Adaptation strategies, implementation |
| System malfunctions |
| Exposure and Sensitivity |
| Potential impacts |

| |
|---|
| Adaptation strategies, implementation |
| Failure scenarios |
| Resilience Strategies |
| Implementation of adaptation strategies |
| Willingness to implement |
| Readiness to implement |
| Challenges for Resilience |
| Challenges (Prep) |
| Challenges (Prev) |
| Challenges (Det) |
| Challenges (Resp) |
| Challenges (Rec) |
| Challenges (Lear) |
| Adaptation strategies |
| Prepare and prevent |
| Preparation |
| Prevention |
| Implementation of robust and precautionary design |
| Detection |
| Manage and recover from crisis |
| Response |
| Recovery |
| Learn for the Future |
| Learning |
| Granularity of the system |
| Failures and Malfunctions |
| Attacks and Impacts |
| Security Solutions and Response Mechanisms |
| Cells and Micro Grids |
| Centralized Architectures |
| Decentralized Architectures |
| General Codes |
| Actors involved |
| Open category |
| Challenges |
| Regulations |
| Experts Information and Research Projects |
| Research project |
| Professional and educational background |
| Working domain |