Contract No 608224

Deliverable D5.3
Understanding the Societal Cost of Smart Grid Cyber Attacks

AIT Austrian Institute of Technology • Fraunhofer AISEC • The Queen's University Belfast
Energieinstitut an der Johannes Kepler Universität Linz • EMC Information Systems International Ltd
Kungliga Tekniska högskolan (KTH) • Landis + Gyr
United Technologies Research Centre • SWW Wunsiedel GmBH

Document control information	
Title	Understanding the Societal Cost of Smart Grid Cyber Attacks
Editor	K. de Bruyn
Contributors	J. Reichl, K. de Bruyn and M. Schmidthaler
Description	This deliverable outlines the societal costs, in addition to the direct costs incurred by network providers, of smart grid cyber-attacks. This can be used by policy makers in order to set priorities with respect to minimum required security standards.
Requested deadline	30/09/2015

Executive Summary

Smart technology has gained increasing importance in the architecture of electricity grids and will continue to do so within the next decade. New functionalities, real-time metering, and autonomous interventions of the technology promise enhanced operational efficiency and reliability, and open the door to a plethora of new services for the final customers. All of these new capabilities require high interconnectivity between the conventional electricity distribution infrastructure and the information and communication infrastructure. Such unprecedented interconnectivity of two complex systems with essential importance for the vital functioning of our society and economy naturally raises concerns about their technical stability and security. Consequently, research in the technical disciplines intensively addresses the development of measures to protect our power system from cyber threats. However, while the protection from cyber threats requires technical solutions, successful configuration and implementation of these solutions demand the inclusion of socio-economic and legal considerations.

This report thus contains Deliverable 5.3. of the EU FP7 research project SPARKS, which analyses the important factors influencing the public acceptance of various technical protection measures, discusses the economic ramifications of security investment decisions, and outlines the legal prerequisites for the provision of reliable and secure electricity transmission and distribution systems. In doing so, emphasis is put on creating awareness among engineers and developers of security technology to highlight the impact their decisions can have on the economic wellbeing of modern societies. Furthermore the public perception of smart grids and their security measures is evaluated and the societal costs in case of power outages are demonstrated by means of intuitive case study format, which allows the identification of particularly vulnerable societal groups as well as business entities/sectors.

Table of Contents

Table of Figures

1 Introduction

This report summarizes Deliverable 5.3 and presents the main results of the socio-economic analyses carried out in Work Package 5 of the 7th framework research project SPARKS. D 5.3 first and foremost assesses the costs to society which arise in the event of a failure of protection measures. These 'societal costs' not only take into account the damage to energy supply companies and businesses, but fully incorporate the tremendous importance of electricity for modern societies. The knowledge of these cost categories is paramount so that policy makers are able to set priorities with respect to minimum required security standards and to weight the costs of security measures against the overall benefit of successful protection tools. The quantification of opportunity costs in the case of large scale power outages includes a holistic assessment of households' and non-households' expected damages while the analysis of public perceptions and acceptance patterns primarily assesses households' attitudes. Thus, this Deliverable includes a holistic evaluation of different novelties which arise due to an increasingly smart energy system such as privacy and data security concerns. This entails the desired protection of personal data. Definitions thereof are provided and the assessment methodology is explained in detail.

1.1 Motivation Factors for Smart Grid Implementation

The main motivation for the realization of the smart grid vision is its potential to support an enhanced utilization of renewable energy sources (RES, see e.g. Tsoukalas and Gao, 2008). In addition a variety of other reasons exists, but the main smart grid vision is driven by positive expectations about its contributions to solving the challenge of establishing a less polluting energy system, ensuring energy provision at rational costs in the future while simultaneously enhance of the reliability of the power system.

This is particularly relevant for a more sustainable energy system as limited capacities of the power network infrastructure (i.e. most important the distribution grids) due to the intermitting provision of RES represent a major obstacles for a full exploitation of the potentials of decentralized energy production. Since the distribution capacities are reaching their limits only during a very limited number of days or even hours per year, shortages as well as above-average load situations could be handled by targeted interventions at decentralized production sites (e.g. photovoltaic panels at a housing complex). As advanced smart technologies become available, enabling remote switching is significantly cheaper than conventional grid enhancements. So the installation of smart grids can foster economically efficient solutions for electricity transport. In combination with adequate sensor equipment such smart remote systems can timely detect critical situation in grids and counteract. In combination with additional capabilities smart grids could provide a secure and economically efficient operated power grid with larger production volumes of eco-friendly energy at lower costs.

It is important to bear this in mind, especially as these positive effects are only made possible if reliability, privacy and (data) security is not jeopardized. Privacy in this respect encompasses the successful protection of individual data, so as to not render it possible for adversaries to identify a person/household behind energy consumption patterns for instance. This list of normative goals for smart grids, which currently is most prominently discussed with regards to smart metering devices (smart meters) is the main research objective of the SPARKS project and will serve as common thread in this deliverable, which outlines the opportunity costs of not achieving these goals and the associated societal impacts.

1.2 Socio-Economic Challenges for the Smart Grids Vision

In addition to technical, organisational and legal challenges, a number of economic and societal aspects of the smart grid vision require comprehensive consideration for finding long-term beneficial solutions. Among these challenges in particular the aspects which concern and are related to cyber security are still at a relatively early stage. While the possible benefits of smart grids to increasing the efficiency of the overall energy system is unrivalled, their impact on supply security is heavily discussed.

More fundamentally speaking, securing the power grid against malicious attacks and of misuses of consumption and production data of private households and enterprises is a strict obligation considering the devastating effects a pronounced outage of the electric infrastructure would have on all levels of the affected societies. As a matter of fact, measures to prevent such attacks from having impact on the electricity transmission and distribution are intensively researched in the engineering disciplines. This is also reflected by the work carried out in Work Packages 2, 3 and 4 of the SPARKS project.

First and foremost, the aim of the activities in D5.3 is to provide a better public understanding of the value of a proper functioning of the IT infrastructure of the energy system. This is particularly relevant, as for instance, the deployment of information and communication technologies (ICT) in the power grid played only a minor role over the last decades compared to nowadays and expected future levels. The public understanding of the necessity to investigate these issues is thus paramount. However, research has mainly focused on threats evolving from physical manipulations to the infrastructure.[1]

In contrast to the many reported physical attacks on the power system, the list of known successful cyber-attacks on the power system is short. However, it might be the case that the number of unreported incidents is much higher. Companies from all branches are in general reluctant to report security breaches as it might damage their reputation. This behaviour is impeded by an increasing number of countries making reporting of noticed security breaches mandatory, where the US state California has been the first one in 2003. The second reason why the number of cyber-attacks on the power system might actually be underestimated by the public as well as by authorities is a specific feature of cyber security compared to security from physical threats: such attacks potentially happen unnoticed. Physical attacks are being noticed by their nature of affecting the operation of the grid or by leaving clear trails of their occurrence. Cyber-attacks do not necessarily aim at the destruction or interruption of power supply or the corresponding infrastructure.

Experts see one of the emerging data protection issues threats through the area-wide implementation of smart grids their capacity to collect and store consumption data. A better knowledge of the electricity consumption patterns of households allows the inference of consumers' lifestyle and habits. For example a common worry is that potential adversaries can even detect at what times of a day the residents are out of their dwelling. While the last information opens the door to a vision of robbers utilising this knowledge for better planning their raids, more likely exploits are the reselling of this data for more targeted marketing or consumer analyses.

[1] Examples of high impact incidents are the attack on two substations in Florida by dynamite explosions in 1981 (Bompard et al., 2013), or repeated attacks on high voltage lines in Columbia (Sequera, 2012). These attacks have caused significant monetary damage to the power infrastructure and caused power interruptions of different length and severity.

A survey by Capgemini (2007) reveals that the greatest concern of consumers against certain cyber security measures in other fields, i.e. radio-frequency identification of humans, is the fear of being confronted with more direct marketing measures. This shows that not only certain elements of the smart grid, e.g. the smart meters, may have low public acceptance but also the measures intended for their protection need to be put under scrutiny to achieve high levels of acceptance among the users.

The intelligent measuring system, i.e. the smart meter, is a part of the smart grids, yet an important one particularly for security questions and in terms of potential benefits which are attributed to intelligent network components. This system implies that an electronic system is responsible for measuring of the energy consumption whereby more information can be displayed compared to usual meters, and data can be transmitted and received via electronic communication. Due to the available prompt information of the consumer and his consumption patterns, he should be able to control this behaviour better and reduce energy costs. Because of the increasing networking and communication in the electricity sector the risk of ensuring compliance with data protection and data security is increasing which will not be further discussed at this point, as well as the threat of cyber-attacks, which could increasingly cause problems maintaining a certain level of security of electricity supply.

The European Commission (2009) required member states to evaluate the possible economic long-term costs and benefits until 3. September 2012. If a member state evaluated positive at least 80 % of possible consumers shall be equipped with intelligent metering systems by 2020. According to the benchmarking report from 2014 (European Commission), 17 member states plan to meet the 80 % target, while 7 states (including Germany) achieved inconclusive results from the evaluation. In some of the latter 7 countries the possible economic long-term cost/benefits ratio was negative, indicating a low macroeconomic incentive to invest in smart meters. However, these states concluded smart meter roll-out could be economically justified for particular groups of customers.

Remaining countries did not provide input to the benchmarking report. The costs per metering point were estimated from 77 € in Malta to 766 € in the Czech Republic, with an average ranging from 200 € to 250 €. Expected benefits were even more heterogeneous, ranging from 140 € to 1,000 €. The costs are significantly and borne by the customers (at least indirect through their grid tariffs). Such incurred costs are irrecoverable once the meters have been installed. The benefits are mostly not enabled through the existence of the smart meter itself, but through services enabled by the smart meter which are not yet established on the market or have not yet proofed their estimated benefits in large scale rollout. Consequently and opposed to the costs of these customer side smart grid appliances, the benefits are much more indefinite at the time being. The lack of concreteness with respect to the benefits for consumers make public acceptance a critical issue for smart meters besides further concerns about their future role in our daily life.

However contrary to bold political ambitions, low levels of public acceptance continue to hamper the Union-wide installation of smart meters in some European countries. An example of public opinion rejection of technology is the Netherlands, which had to stop the planned mandatory implementation of smart meters in 2009 because the proposal was heavily opposed by many Dutch people. Opponents of the scheme pressed for judicial review where the smart meter legislation was proven to contradict the existing data protection laws. Further examples of low public acceptance with respect to the wide-spread introduction of smart meters are found in Wigan (2014). Even when smart meters are only one element of the smart grid, their role as the interface between the smart grid and the final customers make their public acceptance issue highly viral.

The realisation of the smart grid initiates the most severe change to the power infrastructure and its operational paradigms throughout the last decades. New technologies hardly enter every days life undisputed. Accompanying this severe change by discussing and introducing a plethora of security

measures is necessary, but may have significant impact on the public opinion about smart grids. A low public acceptance of smart grids may induce several problems from an economic point of view: a) delay: as explained along the example of the introduction of smart meters in the Netherlands, public resistance against roll-out plans can force authorities to postpone the achievement of initially ambitious targets. b) costs: such delay is always associated with economic costs. These costs arise at the side of the project developing and implementing agent, and have to be borne also by households and various economic actors. When the smart grid installation would actually increase the economic efficiency of the energy system as intended, then this efficiency gain is also delayed along with the grid measure itself, incurring opportunity costs, and c) the smart grid does not only require acceptance by those affected, for exploiting its full potential in particular with respect to the integration of RES and its ability to foster demand response systems and load shifting, smart grid based technologies require rather engagement than acceptance.

While the smart grids vision is a technological challenge at first, its successful realisation will crucially depend on carefully considering the accompanying social and political challenges. Following from the preceding paragraphs, a successful implementation does not only mean to install and set up the technical system which functions at an acceptable low failure rate, but also requires that its environmental and economic potentials can be exploited, while experiencing a high commitment from the affected society. Additional work carried out in WP 5 thus aims at – for the first time – quantitatively assessing the various factors influencing public acceptance or the lack thereof.

In this report an overview of related challenges and opportunities with respect to smart grids and measures for their protection is thus provided. These challenges and opportunities are discussed in the light of experiences from protective measures of the traditional electric infrastructure such as power lines and facilities for power generation. However, the lessons that can be learned from the traditional infrastructure are limited with respect to protective measures for the smart grid. The open questions are discussed and a research agenda for the socio-economic disciplines is outlined to foster and support a successful realisation of the smart grids vision on the future.

2 Cyber Security Measures: The Socio-Economic and Legal Perspective

Security measures typically share a number of mutual aspects concerning their socio-economic and technological characteristics. Thus, this section discusses the inter-relation between the technological properties and the uptake thereof by the civil population and highlights the necessity to apply interdisciplinary research spanning from the engineering disciplines to legal and socio-economic research to adequately address the plethora of remaining open questions as to how smart grids can be best designed to meet the expectations raised. Security questions in particular deserve higher proportional attention.

In this report, this is done first and foremost by characterising the potential touching points between households and security measures in the power grid. In this respect, it is important to consider that activities addressing the physical security of power grids substantially differ from those addressing cyber security threats. Typically, efforts to increase the physical robustness of power grids frequently incorporate actions involving the construction of new power lines, buses or generation facilities. Such construction measures may interfere with the interests of the neighbouring population in several ways. Constructions like power pylons or wind farms usually have effects on the view shed of surrounding residences, generation facilities based on biomass utilization may spread bad odours, and some technologies for increasing supply security may raise security concerns themselves, such as nuclear power for providing a stable source of electricity to balance the volatile renewable sources (Cohen et al., 2014).

These examples show that some conventional activities to increase the security of power supply serve more than one purpose, as the aforementioned ones are likely to also have impact on the efficiency and capacity of the power system. Thus, even when these effects will never play a role in the actual prevention of a power interruption, still generate benefits through their secondary purpose and compensate (partly or full) the incurred costs. Whether cyber security measures may provide such dual use and thereby disburden respective investment decisions is uncertain in many instances.

Traditional technologies, as the ones named above, are tangible by the affected population. Likewise are the threats themselves, such as bombings or thievery of copper lines. This tangibility does not diminish the potentially catastrophic impact of these threats, nor does it prove the infallibility of the protective measures targeting them. However, discussions between utilities or authorities promoting these developments and the affected population , are reportedly better informed than those dealing with cyber security issues. As the threats through physical attacks are broadly understood, and the effectiveness of the changes against them can be explained vividly, the main points of discussions between proponents and opponents focus on question to what extent these modifications are required and on siting decisions.

2.1 A brief Introduction of Smart Grids and Cyber Security Measures

The first activity for building an advanced power grid was the introduction of smart meters. However, the first installations across Europe already happened before any common understanding of the required functionalities of the smart metering devices was established among the stakeholders, and likewise other technical specifications have not been formulated.

As a consequence interfaces of the different smart meter models at this early stage have not been generally applicable; furthermore the scope of the functionalities differed (and differs) between the

models. However, since legislation did not respond to all offered functionalities by defining official verification protocols for them, some functionalities cannot be exploited in practice due to these legal shortcomings. Additionally, since models with a richer set of functionalities have an up to three times higher autonomous electricity consumption than simpler devices, their rich but unused functionalities can even have adverse effects on their original intention of supporting an energy efficient power grid (Preisel et al. 2012). As a result, part of the smart meters installed in this early introduction stage of smart grids may face replacement before the end of their physical lifetime.

Additionally, installations of smart meters were driven by a desire for innovation partly fostered by politics. The pace of this development precluded a concerted target definition of the smart meter roll out and a careful consideration of its implications beyond the core objectives. It is well known that the lack of a European master plan, including a sound regulatory framework dealing with privacy as well as with other civil rights, at the time of the first realisations of the roll out led to tensions and resistance among the European population.

While cross-regional coordination for technical network development today happens through historically grown cooperation such as European standardization, even when delay may be significant sometimes, such concertation is not a matter of course for socio-economic and legal issues below the level of European Directives (themselves a source of delay sometimes). Summarizing the last paragraphs, enough examples of problems associated with an insufficiently broad development of new network infrastructures exist for deriving a number of determining factors for making the future implementation of the smart grid successful. In addition, legal issues are summarized by means of an analysis of the current European legislation and some ideas for amendments are presented. Subsequently we turn to the socio-economics of smart grid security.

2.2 Socio-Economic Ramifications of Cyber Security Measures

To better define and understand the socio-economic issues related to security considerations within the smart grid it is important to understand the heterogeneity of the term security in this context, or to be more precise: "*what can socio-economic research do to promote secure smart grids?*"

First of all we elaborate what qualifies the decision for a security measure also from a socio-economic perspective. Decisions about investments require that the matter of evaluation first be classified as a private or public good (see Reichl et al. 2013a). These decisions ought to reflect the political commitment and goal setting process as well as the legal framework in adequate ways. A *modus vivendi* for good legislation in energy policy, the legal framework is first to be determined. Subsequent to this step economic efficiency considerations may shed light as to which of the possible alternatives are to be chosen and potentially discern which measure to adopt within the given framework. In the economic literature, a private good or service is traded on the open market (like cars or cinema tickets), while a public good is one whose availability cannot be determined by an individual (non-rivalry and non-excludability). An example thereof is clean air, whose availability results from the environmental politics in an individual's country (if not a larger political scope is relevant). But an individual is not able to obtain air for her or his living environment at another degree of purity than others in the same region. Depending on the judgement whether the good is public or private different requirements apply for being economically efficient. If supply security is classified as a private good, then an efficient level is achieved when the marginal benefit for consumers (i.e. households, companies, establishments, institutions, including the public sector) equals the marginal cost of further improving supply security (Bliem, 2007). If supply security is regarded as a public good, then efficient providing is represented by the Samuelson rule (Jamasb and Pollit, 2005;

Samuelson, 1954). In that case, the sum of marginal rates of substitution between private goods and the public good in question must equal the marginal costs of providing the public good.

In the context of conventional electricity provision the good or service of interest is defined by the availability of electricity at the final customer with a certain degree of reliability. However, smart grids have transformed the provision process. Not only electricity is transported, but its transport is inevitable connected with an information transfer in the smart grids universe. Thus, the good or service is enriched by the integrity of the transferred data and their appropriate exploitation on the technical level (i.e. data for automation purposes) as well as on the socio-economic level (i.e. data with respect to privacy issues). Consequently we define the facilitating service through a smart electricity grid as availability of electricity at the final customer with a certain degree of reliability plus ensuring intentional usage of interrelated data. The socio-economic relevant dimensions of the service provided through a smart grid thus are:

- **Reliability**: smart grids may have an impact on the frequency and duration of power supply interruptions. These may be caused through natural threats such as extreme weather incidents and or insufficient maintenance, or through malicious behaviour such as cyber-attacks. High reliability is understood as one of the core objectives of the power supply system with direct impact on the efficiency of the affected economy.
- **Integrity**: the intertwining of energy transport and information transfer introduced to the power network through smart grids requires assurance of faultless data transfer, consent on intended use, and prevention of misuse through both, agents with authorised access and those without authorisation. Successful operation and credibility of the data transfer process including the defined legal framework decisively impact the acceptance of the smart grid, and the potential success of downstream services built on it (such as automated energy audits enabled through smart metered data).
- **Security**: smart grids interfere with several dimensions of the security topic, where the aforementioned reliability represents but one. These dimensions can be separated into risks potentially addressable through architectural or technical measures and those permeating through other mechanisms. An example of the latter category comes from the possibility of significantly increased volatility of end user prices, with potentially negative impact on grid stability and security. Smart grids remove the technological barriers for a dynamisation of the electricity prices where even households could acquire their momentarily electricity demand directly from the spot market. If storage capacities of electricity become cheap at the same time, electricity could turn into a subject of speculation as other energy carriers already are. Such phenomena may induce problems for the dimensions: reliability and economic efficiency. In addition, a recent report by Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag (2014) finds that: “In addition to questions of reliability and operational safety ("safety") of smart grids, in particular issues of external threats ("security") are to be analyze in greater detail. The strong increase in the scope of the use of IT at all levels - from the control of power generation plants and network operation (especially at the distribution level) for industrial and household consumers (smart home, smart meters) to the increasing networking of components and (sub) systems allows the number of potential entry points for cyber attacks to skyrocket. The safety concepts for preventing or aggravation of such interventions could with this dynamic development not often keep up (eg SCADA)“. Thus, the majority of SPARKS’ initiatives deal with these aspects of smart grid cyber security.
- **Efficiency**: smart grids can have significant impact on the required investments for maintaining a certain level of reliability under the increasingly volatile electricity consumption and production. Additionally, operational costs of smarter electricity grids may be different from those of a traditional grid.

First and foremost, reliability of power supply is one of the most serious concerns when it comes to cyber security. Clearly, a household cannot influence the reliability of the power grid it is connected

to. On the other hand, households and particular businesses can install backup electricity generation, at least for some vital functions, allowing them to somehow assign a private aspect to the good of supply security. Thus, electricity is made available at a higher grade than through the grid. As a consequence, some authors judge supply reliability as a private dimension of the good (see Engerer, 2009 and Keppler, 1996 for discussions). However, the most important services provided by electricity stem from the downstream infrastructures for which electricity is an essential input, such as water supply, telecommunications, or traffic.

In-house backup generation at the final customer cannot prevent the outage of these infrastructures during a blackout, and consequently the reliability of the power system is categorised as public dimension of the good availability of electricity. The security dimension may also have impact on the reliability of smart grids, e.g. when a successful attack triggers a supply interruption. However, security in relation to smart grids incorporates additional dimensions; in the case of natural demand for privacy one aspect has already been mentioned. The security level of none of these dimensions is currently chosen or influenced by the final customer, allowing the classification of security as a public good.

However, future developments might allow a market where different providers offer metering and data handling services with different security levels at different prices. In the case of such a development, the classification of security as a public good might change. Investment and operational efficiency affect the price of a good. The price of the final good supports the efficiency of an economy if the availability of electricity with a certain degree of reliability is realised though investing in the most adequate measures only and if the grid is operated with the minimum expenditures allowing to meet the envisaged reliability. As a consequence it is one core objective of electricity regulation to balance the costs of grid operation and its reliability, largely influenced by respective investments and maintenance expenditures.

Such balancing of investments in protective measures requires particular attention. These reliability enhancing measures do not increase the range of services of grid operators, nor do they necessarily increase the efficiency of their business operations. Additionally, Lohse et al. (2006) highlight the fact that these investments do not benefit consumers directly. Therefore, these capacities are not producing additional value during hours of regular service but are potentially capable of averting or reducing economic losses in the event of a failure. Consequently, it cannot be taken for granted a priori that the market will flawlessly and autonomously provide the macroeconomically optimal level of supply security, which is denoted as a market failure.

While developing the necessary measures to secure grid and supply security (as outlined above) is mainly a challenge to the engineering disciplines, it is the task of economic research to support the development of a system of incentives to counterbalance possible market failure and therefore further the implementation of these technical measures. One central prerequisite for developing an efficient regulatory system is quantifying the value of supply security, and the value of other critical characteristics of smart grids constituting a trade-off between costs, services and security.

The value of electricity supply is usually approximated through the cost of power cuts (see Wolf and Wenzel, 2014, Reichl et al., 2013b, Baarsma and Hop, 2009, De Nooij et al. 2007, or Woo and Pupp, 1992, for instance). A generic software tool for the assessment of power outage costs in the European Union is found under www.blackout-simulator.com (Schmidthaler et al., 2014). This is elaborated on in detail subsequently in a discussion of the practical implications of this software.

As one example thereof and as discussed earlier, the interconnection of traditional power grid and to the information network allows for metering, storing and processing of sensitive end customer data.

Only this interconnection makes the provision of new services possible and supports efficiency gains in the power system. While it is broadly understood that this extension of services and the expected efficiency gains require up-front investments on the hardware and software dimension, costs also arise for the social dimension. One of these costs are potentially negative effects on the privacy of household specific data. In the economic context one considers a change from a certain level of privacy to a lower level of privacy as costs, if this shift is mostly undesired with respect to the affected population. Such negative attitude towards a loss of privacy is expected for a large share of the European population as already discussed in the introduction. However, the costs of the potential loss of privacy may not be higher than the gains in system efficiency or the additional value achieved by the new services enabled through the loss of privacy. Only when these two types of economic quantities are known, losses and added values, rational discussions about the specific design of a certain smart grids feature can start and whether abandoning the present status-quo of privacy is worth it compared to the expected reward. Literature lacks comprehensive theoretical and empirical work on the value of privacy in the power grid. Certainly, there exists an undisputed right to protect individual privacy and data integrity. In terms of empirical evidence however, there exists a plethora of research especially for online-based data, which suggest a rather low awareness of users, which ought to not be confused with a lack of valuation. However, as regards the monetary valuation of someone's data private sphere, we suggest an innovative experiment in D 5.4. We consider this type of benefit-cost analyses particularly important with respect to cyber security, since it can sometimes be the best cyber security measure to simply distract from potentially hazardous components or features than try to fix the vulnerabilities added to the system. However, it is important to state that many currently discussed architectural options of future smart grids including their features and services are expectedly consistent with the exemplarily discussed aim for privacy and other issues underlying some sort of similar trade-off. The key aspect of the foregone discussion is that decisions with respect to a highly security relevant topic as smart grids and the European power system require rational balancing of their benefits and costs. The intention of such balancing is not to stall any promising technology innovations, but to understand what adaptions are required to maximise the outcome for social welfare.

2.3 Legal Provisions for Power Supply Security in the Light of Smart Grid Cyber Security and Renewable Energy

As a result of expected contributions to the timely challenges of the energy systems, the smart grids vision has found its way into several European legal provisions with relevance for their implementation. Each regulation addresses different dimensions of the smart grid.

The functionalities and characteristics of smart grids are defined as political requirements which need careful consideration when developing and implementing measures for its protection. This deliverable briefly discusses legislative aspects, though the main analysis in terms of jurisdiction is presented in Deliverable 5.4. However, it is important to be aware of the status-quo and to show potential conflicts of interests which may arise – or have already done so. Thus as for D5.3 smart grid and energy specific legislation with major societal impacts are briefly outlined and relevant conclusions drawn to support policy makers and stakeholders.

When it comes to the protection of the power grid from cyber threats, disaccord starts at an earlier stage of the discussions. The most wide-spread concerns with respect to smart grids are related to privacy issues (Herold, 2011). More importantly, public acceptance of these new technologies will not be achieved without dealing with these concerns comprehensively. However, the construct of data privacy is not self-explaining and different persons may have different views and concerns about the issue. Herold (2011) divides data privacy into four categories, a) privacy of personal information, b)

privacy of the person, c) privacy of behaviour, and d) privacy of communications. Each of these categories bares its own risk of violations, and which risk is more critical for a certain individual may depend on her or his personal circumstances. As an example for behavioural privacy, fire insurance might reject claims when smart meter data reveals that overuse or misuse of appliances has led to the fire incidence. This raises several questions with respect to smart grid security. The answers to these questions are technical and organisational activities. Legal frameworks and relevant legislation is discussed in detail in Deliverable 5.4. However, as brief introduction, the main research issues from a legal perspective can be summarized as follows:

- First and foremost, what measures are qualified to ensure that the metered data stay at authorised companies and authorised personnel only?
- Secondly, if legally relevant information can be retrieved from the smart metered data, to which extent may it be used as proof in a legal dispute?
- Finally, architects of the smart grid need to answer the questions if the achievement of its environmental and economic targets substantially requires metering electricity consumption detailed enough to draw conclusions about such behavioural aspects.

Again, the identification of legal challenges is paramount in order to ensure a best-possible implementation of smart grids and required security measures. A brief discussion thereof is provided subsequently.

2.3.1 Implementation of Smart Grid Cyber Security in European Legislation

The dependence of European supply security on the preparedness against cyber threats has already been found some response of European policy makers. At this point a short overview with regard to selected Union legislations concerning cyber-attacks is provided. However, it can generally be said that these legislations mainly focus on an underpinning of the importance of the protection from cyber-attacks than on establishing certain standards or procedural requirements for its achievement.

a. Commission Communication for protection of critical information infrastructure COM(2009) 149

Due to the Commission Communication, the information and communication technology (ICT) is always interwoven with the everyday life. Some of these ICT-systems, -services, - networks and infrastructures are an indispensable part of the European economy and society, especially providing essential goods and services or constituting the underpinning platform of other critical infrastructures. Therefore, critical societal functions would be seriously affected in case of a disturbance, they are also considered as critical information infrastructures (CII). However, natural disasters or technical failures resulting risks influenced by human interventions are not completely known or have not been sufficiently analysed. Therefore, cyber-attacks have reached a previously unknown degree of complexity (see also Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag, 2014, p.150). . Especially, viruses, worms and other malicious programs are increasing steadily. Due to strong dependence on CII, regard to the transnational networking and interlinking with other infrastructures as well as their vulnerability and threats make it urgently necessary, to systematically improve security and robustness of these infrastructures to defend themselves at the forefront against outages and attacks. This will require pan-European efforts, because of different strategies and the absence of the transnational networking restrict the effectiveness of national countermeasures. Therefore, the European Commission has named an action plan: Prevention and preparedness, detection and response, mitigation and restoration, international cooperation and criteria for the ICT-sector. This action plan has already achieved successful results and is continuing so.

b. Directive for network and information security COM(2013) 48 final

Furthermore, there is a proposal for a directive on measures to ensure a high level of common network and information security. The objective of the proposal according to the recitals is to improve or ensure the security of the internet, private networks and information systems, so they have to be reliable and safe because they play a key role in the society. Increasing security incidents also due to criminal actions pose a significant threat, which especially affect the exercise of economic activities, produce financial losses and harm the confidence of the users, because personal data could also be affected. To ensure the message of the most serious security incidents it is required to introduce minimum security requirements at Union level and apply this to all communications and information systems.

Summarizing, the electricity networks must not only be modernised or extended as a factor of integration, they also have to be secured against cyber attacks due to the continually growing integration of ICT for communication purposes of the affected actors, because this may also represent a growing risk for the security of supply. In order to achieve this the present EU legislation related to cyber security brings forward two propositions: i) The EU strives for the realization of a uniform level of security by establishing an increased protection of communication channels and therefore the prevention of cyber-attacks on the European energy supply, and ii) the European Commission considers the current status of heterogeneous national legislations insufficient and aims for the establishment of binding standards and guidelines for all member states. While both of these objectives are comprehensible, a unification of national standards takes time, while the viral nature of cyber threats and the corresponding pace of the development of new malicious strategies and technologies is high. The adaption of legal binding standards to these steadily advancing threats might itself require an unprecedented pace considering the sometimes slow-acting European legislative process.

2.3.2 Relevant Legislation to foster Power Provision based on Renewable Sources

The Renewable Energy Directive 2009 shows as goal determination the increasing usage of energy out of renewable sources and accordingly a fast approval for the connection of those plants, which have to be integrated into the transmission and distribution systems. In compliance with article 3 paragraph 1 of the Renewable Energy Directive 2009 a minimum of 20 % of the community's gross final energy consumption must be covered by renewable sources till 2020. The respective national overall target within the meaning of burden sharing far beyond, for example of Austria and Sweden is even ranged by a share of 34 % and 49 % by 2020 ().

The increased feed-in of electricity produced from renewable energy into the traditional electricity grid brings with it a number of changes: In contrast to conventional power plants, smaller generation facilities feed in into the distribution network instead of transmission network due to their plant size. This means a great challenge for a network type which was originally designed as a pure output instead of an input power feed. Moreover, in contrast to conventional power plants there is no possibility of demand driven production, because of the weather dependence of renewable energy sources. RES are typically decentralised and widely distributed over a large geographical area and not centrally concentrated. Therefore article 16 paragraph 1 of the Renewable Energy Directive 2009 provides against the background of the evolution of electricity production out of renewable sources, that the Member States must take steps to expand the overall network infrastructure, intelligent networks and storage systems. According to Article 16 paragraph 2 of the Renewable Energy Directive 2009 the power feed energyout of renewable energy sources needs provision of ensuring the reliability and safety of the grid.

The aim is thereby to continue to ensure supply security, which is quiet high in Europe, despite the increasing feed in of electricity out of renewable sources. With respect to the relevant legislation to foster electricity supply security, the European legal provisions entail among others the following:

- Security of supply directive
- Directive on critical infrastructures
- Internal market in electricity - Directive 2009
- Regulation for trans-European energy infrastructure 2013

In addition to this brief discussion of relevant legal frameworks, a chronological summary thereof is provided in detail in Deliverable 5.4.

3 Applied Socio-Economic Research of Smart Grids Cyber Security Aspects

After describing the challenge mainly related to physical aspects of smart networks, this deliverable elaborates on open questions in the emerging field of cyber security in the smart grids environment, and discusses how an efficient and effective research agenda can look like to foster the security of power grids and maximize societal benefits while being economically sound.

At the beginning, we define and highlight the vital issues of societally and economically sound decision support methods. As a starting point with respect to socio-economic and legal responsibilities, it is usually defined that decision support starts when a thorough problem analysis has revealed shortcomings of a planned or existing construct. However, much excitement of the smart grids vision stems from the vital desire for innovation and the corresponding large scale parallel activities around Europe to realize this vision step by step. Whenever a technological shift touches the security topic, in which a failure would have a fundamental impact on the European society, a methodology based on learning-by-doing drops out as an acceptable strategy for the identification of a system's shortcomings. With respect to the identification of socio-economic shortcomings, these can stem from asymmetric effects of certain measures on individual privacy, lost economic values, or distributional effects. An essential part of the decision support in this respect will come from the formulation of these effects and particularly their quantification. Several functions of the smart grid or measures for its protection potentially impact the non-technical layers or the society, and an illustration of the triangle of relevant disciplines is found in Figure 1. When analysing the impact of changes to the system on the technological level these non-technical effects have to be included in a comprehensive analysis to achieve a systemic view on the measures ramification. Such considerations are debated below to support engineers' understanding for the need to cooperate with scientists from the socio-economic and legal domains at the earliest possible stage of a smart grids project.

As one important question related to the discussion of measure and functionalities in light of smart grids is the issue of cost sharing between those seeking the functionality and those who don't.

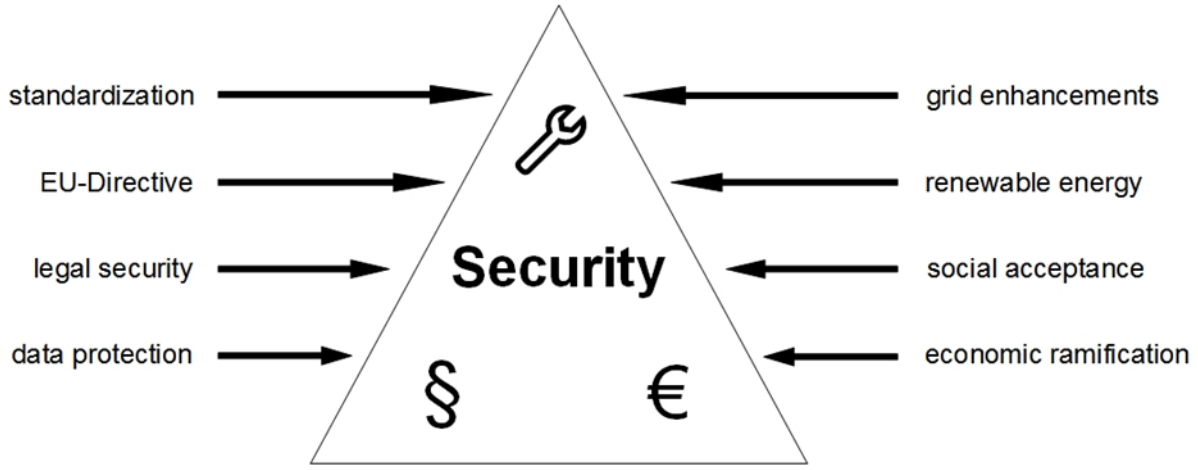

Figure 1: Smart grid security research as comprehensively multidisciplinary approach.

3.1 Cost Sharing between the Individual Consumer and the Collective

The realization of the smart grid vision which includes measures for establishing a certain level of security comes at a price. Starting by the planned - and in many European areas already carried out - installation of smart meters, this vision requires a thorough synchronization of the various national efforts. In addition to the customer side smart grid components (i.e. smart meter devices), smarter switching gears and other new grid components are part of this architecture.

However, in order to facilitate a safe implementation of these technologies, the regular testing of the system's reliability and cyber security is crucial. The first insights into the challenge reveal that the smart grids vision also has a significant impact on investment and operational costs.

Since the electricity grid is a natural monopoly, its costs including the realisation of smart grids are passed on to the final consumers according to a dedicated scheme defined by the regulating authority of each EU member state. These schemes currently link a consumer's specific demand for network services to her or his share of bearing the costs of the overall system mainly based on the required hardware. As one instance, a household may have a dedicated electricity tariff for its heating electricity demand and a dedicated tariff for its regular demand. Such differentiated tariffs require two separate electricity meters, and the respective household contributes to the provision of the metering infrastructure by an additional fee compared to the fee for only one meter. Even when this example shows that demand dependent rates are already applicable in what we termed the conventional grid, the current regulatory practice does not account for heterogeneous demand for specific functionalities of the smart grid. For instance, Austrian national legislation (DAVID-VO, 2012) requires that a household whose electricity consumption is metered by a smart meter is granted access to its load profiles within a delay of only one day. Such access is usually granted through a dedicated web portal or smart phone apps. Costs for the provision of this service are collectively born by all electricity consumers irrespective of their particular interest in such information. Today the vast majority of households does not gain benefits from this service, and scrutinizing the collective cost sharing practise may be required to avoid over-equipping the smart grid without balancing the interests of those demanding its enhanced service capabilities against those not benefitting from it. The intention for this collective cost sharing is obvious, namely to motivate consumers towards its utilization through the argument that it has already being paid by them.

Dwelling upon the necessity to facilitate the smart meter rollout efficiently, it becomes obvious that without them, any smart grid architecture is highly limited. Without smart meters many potentially new services could not be offered to customers, such as load dependent pricing. In this respect cost sharing of its availability is justified as a capacity building measure facilitating future services. Nevertheless, the cost sharing paradigm currently practiced deserves attention of future research. Smart grids may enable services beneficial for some, but the number of those may be small. To find a balance between the needs of some and the society as a whole only a systemic view allows the identification of the first best solution.

Apart from the cost issue, an analysis of the impact of a technical measure should start by identifying potential touch points between technology and the socio-economic layer, and by assessing the technology's costs as well as the expected benefits. Such impacts vary with the specific measure, but exemplary for this issue is the analysis of measures which might support the understanding of the required long-term anticipation in this context.

3.2 New Challenges for Electricity Market Regulation

The regulatory frameworks in place across Europe aim at supporting a cost-efficient distribution of electricity whilst the goal of ensuring a certain levels of reliability of supply has increased substantially in importance. This latter development is clearly visible in the design of European regulatory frameworks, which show a strong tendency to include quality-of-supply aspects into regulation. However, especially in the future, regulation of these services will likely have to include a quantitative measurement for data integrity as an additional dimension once the grids become smart. This is similar to the quantification efforts for supply security which have recently become effective in a variety of countries (see Schmidthaler et al. 2015).

The focus of the regulatory regimes during the last decades was the remuneration of grid operators for transporting the electricity from the centralized producers to the end users and the metering of their consumption. So far regulation has only to some extent addressed the paradigm shift introduced through smart grids. This includes that for instance the costs of area-wide smart meter installations are reimbursed (explicitly or implicitly). However, the current regulatory practice for the most part does not promote for instance discriminatory tariffs dependent on the customers' explicit demand, or the current level of utilization, i.e. the load situation in the moment of consumer demand. Some consumers may actually require metering of 15-minutes load profiles to enable the load dependent electricity and/or for synchronizing their household consumption to the electricity production of their photovoltaic panels, while others main interest may lie in the cheapest possible access to power supply due to their small and inflexible consumption.

In most countries the current regulatory practice is based upon the per unit consumption of electricity from the power grid. This means that if a consumer acquires a part of his electricity consumption from other sources than the grid, e.g. from own production through photovoltaic panels, she or he does not pay any tariffs, which is not optimal from a social welfare perspective (socializing costs, but privatizing benefits). While this approach might have been comprehensible, it bears certain risks for future electricity provision. Costs of the provision of the power grid, i.e. required investments and operational expenses, are to a large extent independent from the amount of electricity it transports. Regulation therefore roughly builds on the paradigm to identify the costs for each grid operator during a year and divide the operator's annual costs (plus some premium) through the expected number of transported kWh. Grid operators' expenses are thus financed through the number of kWh sold over the power grid times the applicable grid tariff. If the number of sold kWh decreases as a result of increased own production and energy efficiency, this will usually not decrease the costs of the provision of the power grid. Consequently, the grid tariff per sold kWh has to increase to ensure financing of grid provision and avoid the risk of a deteriorating grid. Even consumers with a high capacity of own electricity production will require a functioning power grid to ensure supply during hours in which demand exceeds production. Since these producing consumers are responsible for the increase of the grid tariffs while all consumers pay them, questions about fairness and distributional effects arise. Concepts for overcoming these drawbacks of the smart grid enabled embedding of renewable electricity range from the introduction of grid tariffs even for own produced and consumed electricity, to a complete disconnection of charges and consumption through the implementation of fixed costs independently from the consumed amount. Research has not yet addressed this issue of how best to react to this challenge.

Technological progress and capabilities of the infrastructure recondition the paradigms of future electricity market regulation. Not enough research has been done with respect to challenges and opportunities for regulation in light of smart grids. The area of responsibility of market regulation will significantly increase as the service capability of the infrastructures do. Future regulation has not only

to balance the interests of grid operators and consumers, but even varying interests between different consumer groups. Furthermore, additional to the conventional dimensions of regulation, namely affordability and reliability, the target of energy efficiency will become a matter for consideration as the new capabilities of the smart grids suggest some steering competence of the grid. As a part thereof regulation may have to reconsider the provision of incentives for system-friendly consumption behaviour, e.g. through incentivising consumers for shifting their loads towards peak production of renewables. The impact of such load dependent grid tariffs on system stability, required grid investments and operational costs, and the achievable primary energy savings have not been analysed deeply enough to allow the formulation of best practice solutions.

Summarizing, electricity market (network) regulation is a direct policy tool, with which energy politics can directly influence the framework for participants (producers and consumers alike). It is likely that with the increase of complexity in terms of data management and security, the national regulatory authorities will induce standards and regulatory frameworks to ensure that data is collected, stored and transmitted safely.

3.3 Data Granularity and Public Acceptance

The precision with which data is collected will likely influence public acceptance of new ICT based power systems. This is an entirely new dimension in the electricity industry and closely related to data and security questions in social media, (tele-)communication, online banking and other online services.

Closely related to regulatory policy questions in the context of smart grids as well as the question of burden sharing for the provision of the infrastructure prerequisites, is the issue of defining minimum granularity of end consumer representation in the smart grid.

This is best described by a brief example: One named reason for collecting 15-minutes load profiles is to provide grid operators with an almost real-time overview of power demand. Such information could then be exploited for real-time analysing potential countermeasures against load fluctuations or other sources of undesired performance of the grid. However, this information is not required at the household level, but aggregates on certain spatial levels are sufficient. But if load profiles transferred to the utilities which are only containing aggregates instead of household level data, then privacy risks are almost completely prevented. However, such aggregation does then exclude the individual households from advanced services such as the mentioned dynamic pricing. Additionally, information requirements – in the way they are currently formulated e.g. in the Austrian DAVID-VO (2012) – address the individual household level. Nevertheless, it might be one option for increasing the acceptance of smart metering to discriminate between those people with demand of advanced services and being willing to accept a certain degree of privacy risk and those people valuing their privacy more than access to additional services.

Such discrimination is currently not addressed in EU legislation making their realisation cumbersome. However, the urgency of the privacy issue calls for concerted research efforts between the legal, sociological and technical disciplines to find an optimum architecture for the representation of the end consumer in the smart grid. In particular we see a great potential for higher acceptance of the smart grid vision among the population if they are offered alternatives for their role within it.

3.4 Example: Spot-Market driven Electricity Prices for Households

With the emerging installation rates of smart meters the technological barriers for introducing load dependent electricity tariffs have fallen, even on the household level. In such a vision households

could be informed momentarily when electricity is available on the spot market at low rates, e.g. from peak production of wind power, and satisfy their demand during these hours from the spot market directly instead from their usual supplier. However, to implement this system, load profiles of the participating households have to be collected and transferred to their standard supplier and a further agent connecting the households to the spot market. Furthermore, information transfer about momentarily spot market prices needs to be ensured through a technical system requiring upfront investments and regular operational costs.

These costs have to be included in the end customers charges the one way or the other. Additionally, security measures have to ensure secure communication between all relevant parties without a gap. Most importantly, these have to ensure that the price information sent to the households is not corrupted. Advanced solutions will exploit the price information not by manual intervention of the households, but by in-home automation steering of the devices and appliances to minimise expenditures for electricity.

Consequently, dedicated security measures will have to ensure that such automated steering cannot result in overuse of appliances or overload of local segments of the power network through malfunction or corrupted signals. Taking all these measures required to facilitate a safe and secure system for spot-market driven electricity prices together as the system's costs, the benefits from such system must outweigh them, at least on the long run.

While the costs for such a bundle of technical and organisational measures are assessable through the system specification analysis as done for a later implementation, socio-economic costs like the aforementioned effects on privacy are not known from such analysis. Additionally, economic benefits from smart grids enabled functionalities are usually neither part thereof. However, individual components of the overall expected economic benefit can be listed:

- a reduction of personnel effort for meter reading,
- a reduction of household expenditures for electricity through shifting consumption towards times of low priced electricity,
- a reduction of the overall electricity consumption in households, as delayed electricity demand is found not to be fully consumed at later times (Kollmann et al., 2013),
- load shifting is considered as a core measure for efficiency increases in grid operation through delaying or even mitigating the necessity of grid capacity enhancements, or reducing costs for balancing energy and operational reserve,
- auxiliary benefits through the customers' more conscious dealing with electricity consumption, such as motivational effects for increasing energy efficiency beyond load shifting,
- systemic benefits through a more balanced electricity consumption, such as the support for a more system-friendly pricing of renewable electricity, or the creating of new businesses operating the dynamic price system while offering additional services exploiting the rich household-level consumption information.

Only parts of the listed benefits are included in the assessment of the European Commission (2014). Quantified benefits there mainly stem from reduced metering effort and gains in energy efficiency, i.e. reduced expenditures for electricity. Assessing economic benefits of less directly assessable categories requires comprehensive economic modelling embedding assumptions on the degree of consumer engagement or even system response. Consequently, evaluated economic benefit may be sensitive to these assumptions, and intervals for the benefits derived from an informed variation of the assumptions may be more supportive than the provision of point estimates only.

Economic theory suggests the possibility to sharing costs of - e.g. security related – system components as the specific benefits will be shared as well. It is not the intention of the SPARKS project to support one position or the other; however we want to illustrate the conflict of burden sharing present in a regulated market when certain services rely on common infrastructure but bring significantly varying benefits to different consumers.

On the other hand an introduction of dynamic electricity pricing for the household sector potentially will mean costs for individual consumers or larger groups of the society as a whole. Such costs can stem from:

- investments which are needed and operational costs will face impact for enabling dynamic pricing,
- the need of privacy varies among the population, the introduction of fine grained consumption metering and data processing therefore induces different costs for different consumers,
- if dynamic prices achieve certain levels of consumer response and load shifting, the electricity market including its pricing will be affected also for those consumer groups still utilizing flat tariffs. These might then experience higher costs to satisfy their inflexible demand,
- if storage for electricity becomes cheap, dynamic end customer prices might increase the exploitability of these storage capacities for speculative electricity trading, as already done for other energy carriers and incurring comparable risks,
- the controllability of the electricity bills will significantly require more efforts from the consumers' side for dynamic prices compared to flat tariffs. As most consumers' might be reluctant to take this effort, the risk of erroneous accounts increases.

Such dynamic pricing system currently exists only on paper and actual implementation is still outstanding. Thus this list is not exhaustive as the actual configuration of such systems is not yet known. However, this offers the great opportunity to design such a system considering its benefits and its costs already during its creation. As achievable benefits are expectedly high and incurred costs may be limited following the outlined systemic view on smart grids and their security. Such system promises an impactful and long-term beneficial service enabled through smart grids. However, finally it will be a matter of the actual process for its implementation if such a system will succeed in contributing towards the formulated environmental and economic targets for Europe's future. Therefore, here, we call for a systemic and collaborative design of new smart grids functionalities incorporating knowledge and views from all affected disciplines to collectively strive for a value adding architecture of the smart grids vision.

Among the most important economic dimensions of smart grid cyber security measures however is the avoidance of societal costs which result from a failure of successful protection from power outages. The various socio-economic aspects thereof are investigated in the subsequent sections.

4 Identification of Societal Costs associated with insufficient Protection Measures

Insufficient protection measures against cyber-attacks may have different consequences ranging from no to only moderate impact to the most severe category of network failure: an interruption of power supply, synonymous for power outage or blackout. This chapter investigates the potential impact a cyber-attack can have on the societal layer of an electricity network and estimates the costs associated with power outages as a worst case scenario of a cyber-attack.

Identifying the full picture of societal ramifications which are to be expected in the event of power outages requires a holistic incorporation of damages to businesses and households at the same time. Making use of the findings from previous research[3] it is possible to analyse damages to businesses, institutions and households in the case of power outages. In this deliverable of the SPARKS project, a brief sketch of these cost categories and magnitudes is presented.

As central cornerstone of the SPARKS project an analysis of different levels of protection technologies is conducted. This is done in a holistic approach taking into account several highly relevant damage categories which include:

- Monetary Losses due to stoppage of productive activities. Interruptions to the value adding process are highly relevant and thus represented in blackout-simulator.com
- Costs due to labour inactivity. As businesses and institutions bear the costs of inactive personnel, these costs are represented in blackout-simulator.com
- Damage costs to productive facilities are incorporated via a general value of lost load approach.

There exists a plethora of literature evidence on power outage cost assessment methods, different approaches and valuations of the value of supply security. For instance Reichl et al (2013a) or Zingman et al. (2000). One valuation approach which was used intensively due to the absence of alternative measurement opportunities was the calculation of backup generation costs. This opportunity cost approach includes the calculation of fixed and variable cost categories for generators, fuel and other expenses. However, recently, research has advanced substantially, thereby making it possible to better measure the monetary and non-monetary changes to utility of affected customers. Thus, subsequently, we briefly explain the methodology which was used to carry out the assessments of the lost energy and monetary damages. Following the methodological explanations, a case study of actual power outage ramifications for the real outage in Italy on 28 September 2003 is provided. We then estimate the so defined societal costs of insufficient protection measures by three case studies of failures in the regional power networks.

4.1 Methodology for the assessment of costs related to service unavailability

Elaborated economic assessments of the value of electricity supply security are valuable inputs especially in the discussions with respect to necessary investments for maintaining and upgrading the current transmission and distribution infrastructure. While developing the necessary measures to

[3] The software was developed in the FP7 Project SESAME. More information can be found in: www.sesame-project.eu. The online tool has been made available for the public at www.blackout-simulator.com. The tool is free of charge and can be used to display the opportunity costs associated with blackouts as well as the amount of electricity not supplied to various (9) economic sectors and households separately.

enhance supply security is mainly a challenge to the engineering disciplines, it is the task of economic research to support the development of a system of incentives to counterbalance possible market failure and therefore further the implementation of these technical measures. One central prerequisite for developing an efficient regulatory system is quantifying the value of supply security. As supply security constitutes a non-market good and can be purchased only in combination with the physical product (electricity), the value of supply security cannot be determined directly. That is why usually the failure of electricity supply, and in particular the cost occurring when electric power cannot be accessed, is used to assess the value of supply security (see Baarsma and Hop, 2009; de Nooij, Koopmans and Bijvoet, 2007; and Woo and Pupp, 1992).

The herewith presented assessment model provides a rationale for electricity supply security enhancing investments and other energy policy decisions. Providing profound knowledge of the damages faced by businesses in the case of power outages and of households' preference structures can assist policy makers and industry to successfully handle the challenges of future electricity systems.

Regulatory frameworks also benefit from such easy-to-use models for quantitative assessments of the value of lost load, the total damage per sector in the EU (at NUTS 2 level), as well as of the energy not supplied in the case of blackouts. The presented model makes it possible for the first time to asses trans-European (as well as nationally or regionally limited) power outages with regards to their socio-economic effects. Depending on the desired level of detail the elicitation of damages with the presented model is now a matter of about two minutes and five to ten mouse clicks.

An efficient level of supply security is achieved when the marginal benefit for consumers (i.e. households, companies, institutions, etc.) equals the marginal cost of further improvements (Bliem, 2007). This is important for a better understanding of supply security as investments in security-related infrastructure are not directly (or always positively) correlated with improvements in the level of supply security. A thorough discussion of the econometric approach and the models used is found in Gutierrez et al. (2013).

Figure 1 displays the easy-to-use application of this tool. The user can simulate self-designed power outages and obtains estimates of the economic impact of the simulated scenarios. These results are then used as input for benefit-cost analyses or further discussions on the efficacy and efficiency of protective measures. While the economic value of power supply reliability has been carefully studied, other services and characteristics of power supply through smart grids have not achieved much attention.

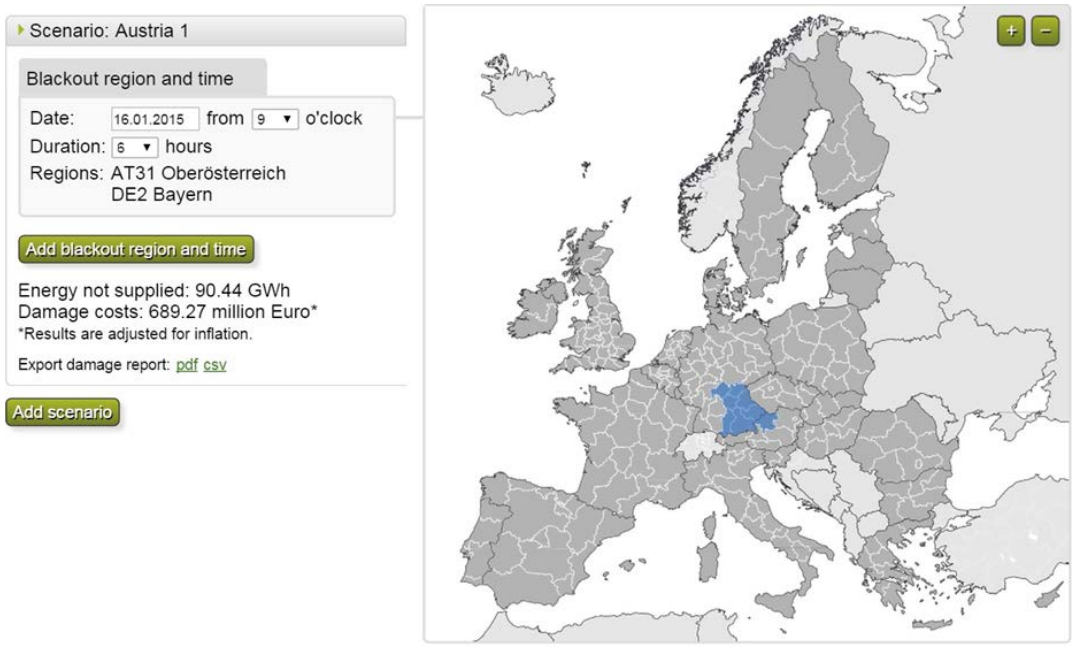

Figure 2: Screenshot of the software tool blackout-simulator.com which enables the customization and assessment of power supply interruptions' economic ramifications.

4.1.1 Damage Assessment I: Non-Households

For the assessment of damages faced by businesses, institutions and administration (non-households) in the case of power outages, the presented model reports the average of two methodologically different assessment approaches for enhanced robustness of the results.

The first methodological approach constitutes a model that assigns the lost value added to every analyzed economic sector, for every incorporated region, and at every. To do so, production data of businesses, industry and public administration are incorporated as central indicator of economic activity. This builds up the first part of the assessment dubbed the production-based approach. The rationale behind this approach is that economic activity is in most cases very closely connected to electricity supply, and details are given subsequently. The second methodological approach applied here exploits earlier work on power outage cost estimations and relates the findings of these studies to the regional and other characteristics of an outage to derive the expected damage of outage scenarios investigated through the presented model. This means, the comparative assessment of sector specific costs is based on a comparison of typical damages per kWh not supplied in certain regions, industries and sectors, which are obtained from earlier studies.

For the first methodological approach of the analysis precise data on the economic activity of businesses in all of the European Union depending on the season, time of the day, country, and other variables were incorporated into the model. The majority of these raw data were gathered from the "World Input-Output Database" (Timmer, 2012). Providing a variety of production and value-added related data this was the central data source fed into the presented model. Other data sources used were regional economic accounts of the regional statistics by NUTS classification (Eurostat, 2012) from Eurostat, which contains the annual value added figures split into geographic NUTS 2 (state or province level) regions.

Data on value added are also available on the level of even more detailed NUTS 3 regions for many EU countries. This NUTS 3 regional definition splits countries into administrative districts below the level of federal states, such that between 150,000 and 800,000 residents fall in every of these regions

(see Eurostat, 2012 for further details on the NUTS classification). However, the value added needs to be joined with other data, in particular those about sectorial electricity consumption. For this reason the regional distribution of the presented model is adapted to the data availability of other sources, and finally returns estimates of economic damage for 266 of the 271 federal states in the EU 27 (NUTS 2 level). The excluded regions are Luxemburg for which the value added of the there important financial sector is not found in official statistics, and Malta, also for the reason of data shortcomings. Additionally, for Germany the areas of Brandenburg-East and Brandenburg-West were combined. In the tool, this generic region is dubbed Brandenburg. The two Nuts 2 regions of Slovenia Vzhodna Slovenija and Zahodna Slovenija have been also merged to Slovenia. Consequently, out of the original 271 Nuts 2 regions in the European Union, 266 remain after the described merging process.

As a next step, the economic losses of non-household sectors are clustered with respect on data availability. In total nine economic sectors were incorporated into the analysis, all of which are based on the "NACE Rev. 2" system, which is explained in the appendix.

As outcome of these steps, a database was generated that includes the annual gross value added for 266 European regions and per branch cluster within these regions. To facilitate an assignment of value added to the 8,760 hours of a (non leap) year a twofold approach was undertaken. First, the synthetic load profiles of available branches published by distribution system operators (BDEW, 2014) were used as base input. This allows estimating the ratio between electricity consumption during productive hours of a sector and non-productive hours of a sector in a certain branch. Since these synthetic load profiles have originally been constructed considering German and thus central European production schedules only, the productive hours in a certain country and branch were adapted according questionnaires completed by employees of the Austrian Economic Chambers located in the respective other countries. Thus the thereby developed load profiles of each country keep the ratio of electricity consumption between hours of high and low productivity, while the respective hours themselves vary between the countries. Finally, imprecisions from this approximations that lead to aggregated electricity consumption over all 8.760 annual hours not exactly equal to the annual electricity consumption reported in Timmer (2012), and these approximation errors were smoothed by scaling the load profiles upwards or downwards to equal these annual consumption values.

Based on these load profiles the annual gross value added per economic sector and per region was broken down from the aggregate figures into an approximated hourly value for the years. The underlying assumption here is that electricity is an essential input for value added, and that hours without electricity supply deal damage even when happening during non-productive hours. Such damages stem from e.g. inoperable cooling appliances or safety facilities. Additionally, the presented model automatically checks the input date of simulated power outages for national holidays, while it was impossible to account for all regional and sometimes geographically very limited holidays.

The production-based approach is then complemented by the second methodical approach of the assessment of non-households, which is based on a comparison of typical damages per kWh not supplied in certain industries and sectors. This value of lost load (VoLL) approach is capable of assigning every unit of electricity not supplied a damage for a certain country and sector. In total 360 Values out of 57 independent studies were used to elicit sector-specific damage indicators, these are fully listed in the appendix. These allow the identification of region and branch specific effects which were fed into the data base to form the basis for the assessment of businesses' damages in the case of power outages. This VoLL approach requires the standardization of electricity demand patterns and damage figures. To do this, all values were adjusted for inflation and corrected for changes in exchange rates. The differences between elicitation methods, countries, affected entities, etc. are important and are thus accounted for. The sources utilized in this procedure are presented in the appendix. Given the fact that the range of calculated businesses' damages (range of 65-85 per cent of

the overall damages), is very well in line with international studies, see e.g. Reichl et al., (2013) for a comparison of international studies, the validity of this approach is strongly supported.

A distinction of the damages based on the economic activity (NACE nomenclature) is the cornerstone of the analysis software For each sector different economic evaluations are carried out:

1. Electricity not supplied (in GWh)

In this category the amount of electricity that cannot be supplied to the consumers due to the power outage is provided (in MWh).

2. Total damage (in €)

In this category indirect damages in the economic sectors are presented. Indirect monetary damages are referred to as negative monetary damages that arise as a consequence to the non-availability of energy in a certain sector. For example the costs for personnel still arise even after the halt of production. Although these productive capacities lay idle, employees receive pay with significantly reduced or halted production and significantly less value added. Accordingly, the indirect damages shown here include the amount of the foregone value added, lost inputs, and the part of personnel costs, which still occur in the absence of electrical power.

In addition to this, the Value of Lost Load is calculated wherever this can be done objectively. This figure allows the comparison of damages across countries and for different (research) approaches.

4.1.2 Damage Assessment II: Households

The assessment of damage occurring to households due to power outages is more difficult than for non-households. The majority of damages to households is indirect and not material or monetary as it is in the case of businesses and public administration. An adequate assessment must therefore also incorporate the negative consequences to a household, such as diminished value of leisure and the mental stress that occurs when the household does not know when it will be able to receive power again. (See also the definitions in the Annex). The following values were obtained using a willingness to pay analysis method (WTP) of roughly over 250 households in every of the 27 (in year 2012) member states. The damage assessment (including the mentioned intangible damages) was thus provided by the households themselves. Some literature sources point out that households tend to underestimate their willingness to pay to avoid power outages. These values are therefore to be considered a lower boundary of the actual damage.

For any comprehensive analysis of the household sector's vulnerability in the case of power outages it is necessary to include non-monetary effects alongside material losses. Thus, for the analyses carried out in WP 5, a model was used which includes a class-leading survey approach conducted in a FP7 research project[4]. To incorporate households' willingness to pay (WTP) to avoid power outages a total of 8,336 participants were evaluated in depth as regards their preferences in terms of supply security. This is central for assessing the majority of losses experienced by households in the case of power outages. The interviews were carefully designed and conduced to account for all relevant social, geographic and demographic groups of society.

While an individual household will usually not be able to give a precise estimate of its WTP, the large number of households which stated their preferences in the SESAME household survey ensures

[4] The empirical field work was conducted in SESAME, which were partly included in the quantification process of Del 5.3. The model adaptation and testbed definitions are a based on the intensive stakeholder interaction processes in SPARKS.

excellent WTP estimates. Details of the characteristics of the survey, of the economics involved and the econometric modelling can be found in chapter 5 of (Garcia Gutierrez, et al. 2013). Table 1 provides a descriptive summary of the household survey. For comparison, the average figures for the whole of the European Union are also provided. The sample of survey participants is considered representative of the European population.

4.1.3 Example – Power Outage affected all of Italy on 28 September 2003

A prominent example of a large power outage in Europe occurred on September 28th 2003 in Italy. It provides a vivid example for the demonstration of the assessment procedure with the presented model. The outage was due to a transmission failure and subsequently affected all of Italy (with the exception of Sardinia). Figure 2 shows the extent of this power outage and the average time needed to fully restore the supply with electric power to different parts of the country. The economic losses are modelled for the period from 3am until full recovery. The total duration was 3 hours in the north, 9 hours in the center, 12 hours in the south, and 16 hours in Sicily.

Table 1 depicts the characteristics of this outage scenario which the user selects in the presented model. The affected areas are selected by means of an interactive map function.

Table 1: Case Study Power Outage in Italy on September 28th 2003

Date of start of outage 28th September 2003	
Start time of outage	03:00 am
Duration in hours	3-16 depending on the region
Provinces affected	Italy (except Sardinia)
Public holiday	Yes (Sunday)

The different restauration times which followed this power outage are displayed in Figure 3.

Figure 3: Example of affected areas during the Italian power outage of September 28th 2003

The economic losses and effects associated with this power outage are presented in Table 2. First and foremost, the overall damage to businesses is calculated with 897.5 million €. This is equivalent to .08 per cent of the annual Italian GDP. In terms of households' change of utility, it can be concluded that material as well as non-material losses amounted to 285 million €.

Table 2: Total losses across all regions and sectors, Summary of the presented model

	Primary sector	Secondary sector	Tertiary sector	Total losses three sectors	WTP Households	Total losses in region
Region North	5.3	136.7	60.8	202.8	43.0	245.8
Region Center	20.6	217.6	154.6	392.8	98.2	491.0
Region South	20.9	82.8	97.5	201.2	94.3	295.5
Region Sicily	12.4	33.7	54.6	100.7	49.5	150.2
Total	59.2	470.8	367.5	897.5	285.0	1182.5
% of GDP	0.004%	0.031%	0.025%	0.060%	0.019%	0.079%

A specifically introduced board of Italian experts and scientists (Commissione di Indagine, 2003) conclude that this outage caused costs of approximately 640 million € and was responsible for a loss of load of 160 MWh. This only takes into account non-households' damages, which diverges very little from the independently calculated damages of businesses and the public sector. International comparability is nevertheless paramount. Figure 4 presents the selection process by means of the blackout-simulator.com.

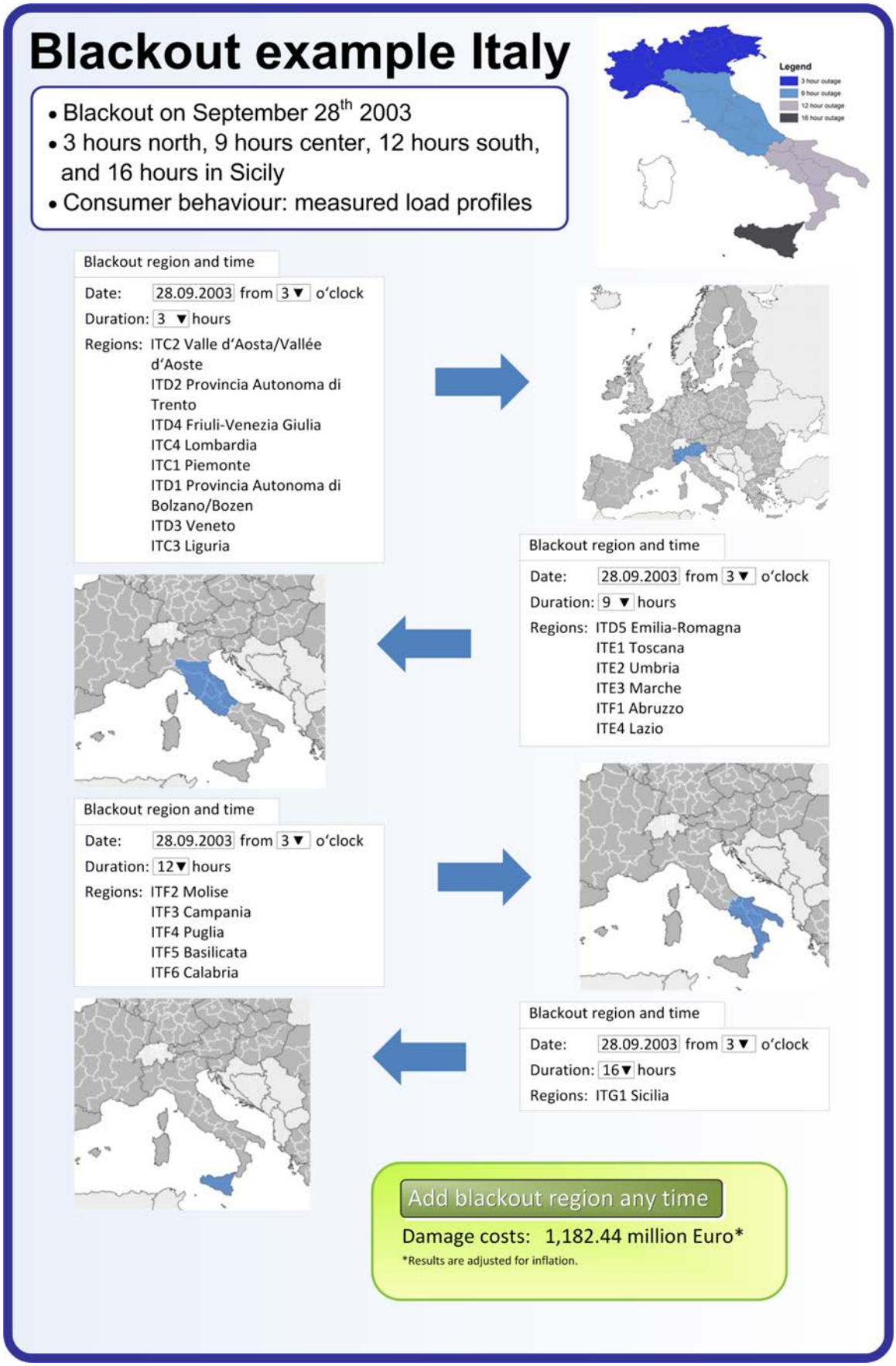

Figure 4: Implementation of the assessed power outage in Italy on September 28th 2003 using the presented model7

4.2 Economic Testbeds - Case Study of Smart Grids Networks

This section presents the analytics applied to investigate the dimension of the societal costs for several smart grids of different sizes.

This is done in strict accordance with state-of-the-art in applied research and allows stakeholder from policy, industry and the public to objectively value the amenity of providing sufficient protection levels in the ICT and subsequently physical electricity infrastructure.

However, since the societal costs reveal the vulnerability of the service area under investigation, this information is considerably sensitive. The estimated societal costs are not related to the probability of the causing incident in this section, and events with high costs are not necessarily likely to occur. Thus, using specific system operators as objects of the investigation, and reporting the societal costs for the case that a cyber-attack leads to a disruptive incident, may result in disproportionate concerns about the vulnerability of the named system operator. In contrast, the objective of this section is to demonstrate the impact an insufficient protection of smart grids against cyber-attacks can have *in general*. As a consequence, this section shows the scale of the associated costs for realistic but synthetic service areas not representing an actual system operator.

For the political debate, and in particular as input for regulatory decisions, such indicative information is sufficient for starting the related discussions and demonstrating the importance of cyber security protection. If more detailed information is required for certain service areas, these can be provided by the SPARKS team upon request, while produced information may then require non-disclosure to the public.

The synthetic service areas are defined to represent northern (North), southern (South), western (West), and eastern (East) European regions, respectively. For each of these regions, we assume three synthetic network operators each with a different scope of their related service area. The service areas are constructed to represent a typical small municipal utility (S), a medium sized regional utility (M), and a large transregional network (L). Hence, we refer to the, say, northern medium sized economic testbed by ETB-North-M. Economic activity and its beak down into branches is chosen is such a way that it reflects the typical economic structure of the corresponding region.

Summarizing, the use of these proto-typical economic testbeds allows for DSO of various sizes, areas and number of customers to identify similarities in terms of potential damage as result from unsuccessful cyber protection measures and help identify potential vulnerabilities.

Furthermore, the careful choice of these Economic Testbeds enables policy makers and industry alike to put a value on the availability of supply thus making it possible to compare costs and benefits of cyber security protection measures. The key figures of each economic testbed, which represent a large part of the European electricity industry are thus presented in Table 3.

Table 3: Key figures of the investigated synthetic economic testbeds

		North	South	West	East
Small	no. of residents	20,000	20,000	20,000	20,000
	gross regional product in mio. €	557	357	700	235
	annual electricity consumption in GWh	137	83	155	62
Medium	no. of residents	200,000	200,000	200,000	200,000
	gross regional product in mio. €	5,584	4,369	8,341	2,815
	annual electricity consumption in GWh	1,102	886	1,549	698
Large	no. of residents	2,000,000	2,000,000	2,000,000	2,000,000
	gross regional product in mio. €	76,501	58,599	83,907	53,387
	annual electricity consumption in GWh	12,350	7,120	14,920	7,429

For the case studies of cyber-attack-induced power outages, we demonstrate the impact of three outage scenarios on the economic testbeds. The most decisive factor for the severity of a power outage is its duration, and we define the outage scenarios for three different durations, respectively. Firstly, a short outage is analyzed lasting for 30 minutes only. Such duration reflects the average time per year for which electricity consumers experience unplanned supply interruptions in countries with very high reliability, such as Austria. Secondly, we simulate a power outage of 8 hours duration.

A power outage of such a duration is an exceptional event, and, for example, only 2.7% of German residents have experienced a power outage of such a length during a period of 5 years (2008-2012), while this share amounts to 31% for Lithuania (Garcia Gutierrez et al., 2013). As a third duration we investigate the impact of a 24 hours outage on the economic testbeds. Such incidents are rare across the EU and the only three countries were more than 10% of the population have experienced outages of at least 24 hours between 2008 to 2012 are Finland, Latvia, and Estonia (Garcia Gutierrez et al., 2013).

To enrich the set of outage scenarios, we simulate that the incidents happen during two seasons, winter and summer. As starting time of the outages we define 9 am on a workday, and 9 pm on a holiday, which allows the intuitive identification of particularly vulnerable periods as well as society and business groups. Table 4 presents the results from a proto-typical assessment of expected damages for a small-scaled supply area in Northern Europe. This is highly relevant for understanding the difference and time-dependencies of power outages.

Table 4: Case study results; economic impact for different scenarios in ETB-North-S

		30 min	8 h	24 h
Summer, workday, 9am	economic damage in mio. €	0.15	1.67	3.56
	unserved electricity in MWh	7.47	60.11	159.72
Summer, holiday, 9am	economic damage in mio. €	0.07	0.80	2.61
	unserved electricity in MWh	7.08	55.31	152.48
Summer, workday, 9 pm	economic damage in mio. €	0.07	0.76	3.56
	unserved electricity in MWh	6.92	45.71	159.72
Summer, holiday, 9pm	economic damage in mio. €	0.07	0.76	3.56
	unserved electricity in MWh	6.77	45.48	159.56
Winter, workday, 9am	economic damage in mio. €	0.15	1.61	3.60
	unserved electricity in MWh	10.94	87.02	219.20
Winter, holiday, 9am	economic damage in mio. €	0.08	0.84	2.47
	unserved electricity in MWh	7.00	57.36	171.99
Winter, workday, 9 pm	economic damage in mio. €	0.07	0.81	3.60
	unserved electricity in MWh	8.58	54.29	219.20
Winter, holiday, 9pm	economic damage in mio. €	0.07	0.79	2.48
	unserved electricity in MWh	7.95	54.29	185.68

The tendency to underestimate the damage potential of unsuccessful smart grid protection measures becomes clearly visible when calculating the damage per unit of energy not supplied. This value of lost load (VoLL in €/kwh) is highly relevant when comparing protection measures against one another. Especially for this test bed – which is prototypical for Northern Europe, a VoLL between 8.2 €/kWh (30 minute interruptions on a winter holiday) to 22.3 €/kWh (24h interruption on summer workdays) demonstrates the urgent necessity to invest in protection measures, particularly as this relates to the price of electricity by a factor of 80-100. Table 5 presents the intuitive case of a medium sized supply area in Northern Europe with 200,000 inhabitants living there.

Table 5: Case study results; economic impact for different scenarios in ETB-North-M

		30 min	8 h	24 h
Summer, workday, 9am	economic damage in mio. €	1.14	12.62	27.11
	unserved electricity in MWh	61.22	491.02	1291.83
Summer, holiday, 9am	economic damage in mio. €	0.54	6.02	19.69
	unserved electricity in MWh	58.78	461.63	1239.18
Summer, workday, 9 pm	economic damage in mio. €	0.50	5.73	27.11
	unserved electricity in MWh	57.55	357.55	1291.83
Summer, holiday, 9pm	economic damage in mio. €	0.49	5.71	27.10
	unserved electricity in MWh	55.10	355.10	1289.38
Winter, workday, 9am	economic damage in mio. €	1.11	12.49	28.01
	unserved electricity in MWh	85.71	684.49	1717.95
Winter, holiday, 9am	economic damage in mio. €	0.57	6.46	19.03
	unserved electricity in MWh	56.33	472.65	1354.28
Winter, workday, 9 pm	economic damage in mio. €	0.53	6.19	28.01
	unserved electricity in MWh	67.35	411.43	1717.95
Winter, holiday, 9pm	economic damage in mio. €	0.52	6.07	19.03
	unserved electricity in MWh	63.67	411.43	1449.79

The same picture applies to interruptions in ETB NORTH M for medium sized supply areas. The opportunity costs of not having electricity is thus up to 100 times larger than the cost of electricity in the first place. This is already the case for short (30 min) interruptions, but expands substantially for longer periods. The VoLL is calculated between 7.8 €/kWh (30 minute interruptions on a winter workday) and 20.9 €/kWh (24h interruption on summer workdays). This is in the medium to upper range of comparable VoLL values.

Table 6 displays the analysis of the economic test bed ETB-North-L which is proto-typical for a large supply are (2 m inhabitants) in Northern Europe.

Table 6: Case study results; economic impact for different scenarios in ETB-North-L

		30 min	8 h	24 h
Summer, workday, 9am	economic damage in mio. €	14.13	161.98	344.06
	unserved electricity in MWh	686.11	5540.31	14654.09
Summer, holiday, 9am	economic damage in mio. €	6.25	72.82	242.26
	unserved electricity in MWh	634.65	5054.32	13847.91
Summer, workday, 9 pm	economic damage in mio. €	6.15	70.95	344.06
	unserved electricity in MWh	640.37	4110.92	14654.09
Summer, holiday, 9pm	economic damage in mio. €	5.98	70.63	343.75
	unserved electricity in MWh	617.50	4082.33	14625.50
Winter, workday, 9am	economic damage in mio. €	13.85	161.32	354.52
	unserved electricity in MWh	1012.01	8090.34	20148.66
Winter, holiday, 9am	economic damage in mio. €	6.52	77.14	227.50
	unserved electricity in MWh	628.93	5214.41	15323.04
Winter, workday, 9 pm	economic damage in mio. €	6.42	75.65	354.52
	unserved electricity in MWh	783.30	4837.05	20148.66
Winter, holiday, 9pm	economic damage in mio. €	6.25	73.95	227.50
	unserved electricity in MWh	720.41	4808.46	16500.86

The largest testbed in area in ETB North shows a similar tendency as regards relative and absolute damage values. This is due to the fact that similarities are present not only in terms of economic and residential structure, but as regards protection measures and coping (i.e. restoring) strategies.

The VoLL lies between 8.2 €/kWh (30 minute interruptions on a winter workday) and 23.5 €/kWh (24h interruption on summer holiday).

Table 7 presents the calculations for ETB-South-S, which is exemplary for a smaller supply area (20,000 inhabitants) in the South of Europe.

Table 7: Case study results; economic impact for different scenarios in ETB-South-S

		30 min	8 h	24 h
Summer, workday, 9am	economic damage in mio. €	0.05	0.61	1.33
	unserved electricity in MWh	4.51	36.94	98.33
Summer, holiday, 9am	economic damage in mio. €	0.03	0.34	1.02
	unserved electricity in MWh	4.86	40.06	102.84
Summer, workday, 9 pm	economic damage in mio. €	0.02	0.30	1.33
	unserved electricity in MWh	4.51	29.48	98.33
Summer, holiday, 9pm	economic damage in mio. €	0.02	0.30	1.33
	unserved electricity in MWh	4.68	29.83	98.68
Winter, workday, 9am	economic damage in mio. €	0.05	0.65	1.46
	unserved electricity in MWh	5.72	44.22	110.12
Winter, holiday, 9am	economic damage in mio. €	0.03	0.38	1.09
	unserved electricity in MWh	3.64	34.68	97.64
Winter, workday, 9 pm	economic damage in mio. €	0.03	0.34	1.46
	unserved electricity in MWh	4.86	27.05	110.12
Winter, holiday, 9pm	economic damage in mio. €	0.03	0.34	1.09
	unserved electricity in MWh	4.68	29.48	100.59

The smallest ETB in area “South” is quite different when compared to ETB in area North and West.

The VoLL lies between 5.3 €/kWh (30 minute interruptions on a summer holiday) and 13.5 €/kWh (24h interruption on summer workdays).

Table 8 shows the impact of various outage scenarios on ETB-South-M, which affects a medium sized supply area of 200,000 residents in Southern Europe.

Table 8: Case study results; economic impact for different scenarios in ETB-South-M

		30 min	8 h	24 h
Summer, workday, 9am	economic damage in mio. €	0.73	7.98	17.11
	unserved electricity in MWh	58.56	480.48	1285.29
Summer, holiday, 9am	economic damage in mio. €	0.37	4.17	12.71
	unserved electricity in MWh	61.56	501.50	1323.57
Summer, workday, 9 pm	economic damage in mio. €	0.34	3.86	17.11
	unserved electricity in MWh	57.06	395.65	1285.29
Summer, holiday, 9pm	economic damage in mio. €	0.34	3.86	17.11
	unserved electricity in MWh	59.31	401.65	1291.29
Winter, workday, 9am	economic damage in mio. €	0.71	8.24	18.23
	unserved electricity in MWh	74.32	580.33	1451.95
Winter, holiday, 9am	economic damage in mio. €	0.39	4.57	13.35
	unserved electricity in MWh	46.55	427.93	1267.27
Winter, workday, 9 pm	economic damage in mio. €	0.37	4.26	18.23
	unserved electricity in MWh	61.56	365.62	1451.95
Winter, holiday, 9pm	economic damage in mio. €	0.37	4.26	13.35
	unserved electricity in MWh	61.56	400.15	1307.81

The VoLL lies between 5.7 €/kWh (30 minute interruptions on a summer holiday) and 13.3 €/kWh (24h interruption on summer workdays).

Table 9 presents the expected monetary damage and the amount of electricity not supplied for three distinct interruption scenarios for ETB-South-L, which stands for a large economic testbed in the South of Europe.

Table 9: Case study results; economic impact for different scenarios in ETB-South-L

		30 min	8 h	24 h
Summer, workday, 9am	economic damage in mio. €	6.52	74.61	158.19
	unserved electricity in MWh	490.59	3957.11	10580.11
Summer, holiday, 9am	economic damage in mio. €	3.03	37.47	116.00
	unserved electricity in MWh	521.25	4316.53	11116.69
Summer, workday, 9 pm	economic damage in mio. €	2.80	33.79	158.19
	unserved electricity in MWh	480.37	3180.33	10580.11
Summer, holiday, 9pm	economic damage in mio. €	2.80	33.79	158.19
	unserved electricity in MWh	497.41	3217.81	10617.58
Winter, workday, 9am	economic damage in mio. €	6.69	83.73	177.05
	unserved electricity in MWh	640.50	4974.06	12188.16
Winter, holiday, 9am	economic damage in mio. €	3.27	41.36	119.21
	unserved electricity in MWh	393.50	3705.00	10501.75
Winter, workday, 9 pm	economic damage in mio. €	3.04	37.68	177.05
	unserved electricity in MWh	516.14	2929.93	12188.16
Winter, holiday, 9pm	economic damage in mio. €	3.04	37.68	119.21
	unserved electricity in MWh	514.44	3197.37	10828.81

The VoLL lies between 5.6 €/kWh (30 minute interruptions on a summer holiday) and 14.9 €/kWh (24h interruption on summer workdays). This is in the low to medium range of applicable VoLL comparisons.

Table 10 shows the calculations for ETB-West-S, which is a small scale supply area in Western Europe.

Table 10: Case study results; economic impact for different scenarios in ETB-West-S

		30 min	8 h	24 h
Summer, workday, 9am	economic damage in mio. €	0.10	1.12	2.40
	unserved electricity in MWh	6.61	53.96	142.40
Summer, holiday, 9am	economic damage in mio. €	0.05	0.51	1.74
	unserved electricity in MWh	6.98	56.14	144.56
Summer, workday, 9 pm	economic damage in mio. €	0.05	0.52	2.40
	unserved electricity in MWh	6.34	41.29	142.40
Summer, holiday, 9pm	economic damage in mio. €	0.05	0.52	2.39
	unserved electricity in MWh	6.23	41.02	142.13
Winter, workday, 9am	economic damage in mio. €	0.09	1.10	2.48
	unserved electricity in MWh	9.62	76.82	201.95
Winter, holiday, 9am	economic damage in mio. €	0.05	0.58	1.72
	unserved electricity in MWh	6.78	56.17	167.94
Winter, workday, 9 pm	economic damage in mio. €	0.05	0.57	2.48
	unserved electricity in MWh	8.16	54.64	201.95
Winter, holiday, 9pm	economic damage in mio. €	0.05	0.56	1.72
	unserved electricity in MWh	7.63	55.13	171.49

The VoLL lies between 6.1 €/kWh (30 minute interruptions on a winter workday) and 16.9 €/kWh (24h interruption on summer holiday).

Table 11displays the expected damages in case cyber security protection measures are not successful for the case of a medium sizes (200,000 residential customers) in the West of Europe (ETB-West-M).

Table 11: Case study results; economic impact for different scenarios in ETB-West-M

		30 min	8 h	24 h
Summer, workday, 9am	economic damage in mio. €	1.32	14.62	31.02
	unserved electricity in MWh	79.45	651.86	1680.78
Summer, holiday, 9am	economic damage in mio. €	0.63	6.92	22.49
	unserved electricity in MWh	79.83	641.10	1671.36
Summer, workday, 9 pm	economic damage in mio. €	0.62	6.79	31.02
	unserved electricity in MWh	72.03	483.54	1680.78
Summer, holiday, 9pm	economic damage in mio. €	0.61	6.78	31.00
	unserved electricity in MWh	71.36	481.16	1678.40
Winter, workday, 9am	economic damage in mio. €	1.23	13.92	31.27
	unserved electricity in MWh	117.41	939.20	2419.51
Winter, holiday, 9am	economic damage in mio. €	0.66	7.39	21.94
	unserved electricity in MWh	78.12	643.29	1965.75
Winter, workday, 9 pm	economic damage in mio. €	0.65	7.29	31.27
	unserved electricity in MWh	94.77	651.38	2419.51
Winter, holiday, 9pm	economic damage in mio. €	0.64	7.19	21.94
	unserved electricity in MWh	89.15	657.66	2008.94

The VoLL lies between 6.8 €/kWh (30 minute interruptions on a winter workday) and 18.5 €/kWh (24h interruption on summer holiday). This is in medium range of applicable VoLL comparisons.

Table 12: Case study results; economic impact for different scenarios in ETB-West-L presents the expected damages for ETB-West-L.

Table 12: Case study results; economic impact for different scenarios in ETB-West-L

		30 min	8 h	24 h
Summer, workday, 9am	economic damage in mio. €	11.92	135.23	286.68
	unserved electricity in MWh	720.26	5889.07	15151.13
Summer, holiday, 9am	economic damage in mio. €	5.57	62.61	205.54
	unserved electricity in MWh	722.67	5804.66	15037.78
Summer, workday, 9 pm	economic damage in mio. €	5.45	61.21	286.68
	unserved electricity in MWh	652.73	4282.15	15151.13
Summer, holiday, 9pm	economic damage in mio. €	5.35	61.03	286.50
	unserved electricity in MWh	643.09	4255.63	15124.60
Winter, workday, 9am	economic damage in mio. €	11.33	131.30	292.83
	unserved electricity in MWh	1056.27	8435.69	21627.01
Winter, holiday, 9am	economic damage in mio. €	5.87	67.29	199.39
	unserved electricity in MWh	703.38	5810.29	17440.51
Winter, workday, 9 pm	economic damage in mio. €	5.74	66.11	292.83
	unserved electricity in MWh	843.25	5685.69	21627.01
Winter, holiday, 9pm	economic damage in mio. €	5.64	65.02	199.39
	unserved electricity in MWh	790.19	5733.12	17811.09

The VoLL lies between 6.8 €/kWh (30 minute interruptions on a winter workday) and 18.9 €/kWh (24h interruption on summer holiday).

Table 13 highlights the effects on ETB-East-S if cyber security protection fails to prevent three distinct power outage scenarios.

Table 13: Case study results; economic impact for different scenarios in ETB-East-S

		30 min	8 h	24 h
Summer, workday, 9am	economic damage in mio. €	0.02	0.26	0.64
	unserved electricity in MWh	3.51	27.88	74.71
Summer, holiday, 9am	economic damage in mio. €	0.02	0.19	0.56
	unserved electricity in MWh	3.67	28.71	76.29
Summer, workday, 9 pm	economic damage in mio. €	0.01	0.16	0.64
	unserved electricity in MWh	3.17	21.95	74.71
Summer, holiday, 9pm	economic damage in mio. €	0.01	0.16	0.63
	unserved electricity in MWh	3.17	22.12	74.96
Winter, workday, 9am	economic damage in mio. €	0.03	0.28	0.72
	unserved electricity in MWh	4.59	36.23	95.66
Winter, holiday, 9am	economic damage in mio. €	0.02	0.22	0.65
	unserved electricity in MWh	3.51	29.38	85.31
Winter, workday, 9 pm	economic damage in mio. €	0.02	0.19	0.72
	unserved electricity in MWh	3.76	25.21	95.66
Winter, holiday, 9pm	economic damage in mio. €	0.02	0.19	0.65
	unserved electricity in MWh	3.59	26.38	86.56

The VoLL lies between 4.2 €/kWh (30 minute interruptions on a summer holiday) and 8.5 €/kWh (24h interruption on summer workdays).

The VoLL in at EBT East – S is thus different to ETB in areas North and West and similar to South.

The issue of whether or not to implement protection measures can be evaluated by means of a weighted opportunity cost approach. This includes the necessity to analyze the weighted risk (product of damage and incident risk p.a.) to best-possibly approximate opportunity costs which can then be compared to the expenses associated with protection measures. Table 14 presents the results for ETB-East-M.

Table 14: Case study results; economic impact for different scenarios in ETB-East-M

		30 min	8 h	24 h
Summer, workday, 9am	economic damage in mio. €	0.25	2.77	6.49
	unserved electricity in MWh	38.25	313.95	843.33
Summer, holiday, 9am	economic damage in mio. €	0.15	1.76	5.38
	unserved electricity in MWh	38.25	312.42	845.78
Summer, workday, 9 pm	economic damage in mio. €	0.14	1.65	6.49
	unserved electricity in MWh	36.72	257.96	843.33
Summer, holiday, 9pm	economic damage in mio. €	0.14	1.64	6.48
	unserved electricity in MWh	37.33	260.71	846.08
Winter, workday, 9am	economic damage in mio. €	0.25	2.91	7.32
	unserved electricity in MWh	51.10	413.40	1089.35
Winter, holiday, 9am	economic damage in mio. €	0.18	2.12	6.22
	unserved electricity in MWh	36.72	320.38	947.67
Winter, workday, 9 pm	economic damage in mio. €	0.17	2.01	7.32
	unserved electricity in MWh	44.98	300.18	1089.35
Winter, holiday, 9pm	economic damage in mio. €	0.16	1.99	6.22
	unserved electricity in MWh	41.92	312.73	962.06

Similar to ETB in other areas, size is not determined to being the primary sources of distinctiveness. The question whether or not to invest in security measures almost entirely depends on the quantification of risk, given a consistent approximation of the costs involved with protection technologies. This is a cornerstone of thes SPARKS project.

The VoLL lies between 3.8 €/kWh (30 minute interruptions on a summer holiday) and 7.7 €/kWh (24h interruption on summer workdays).

Finally, Table 15 displays the effects three different scenarios for large scale power outages would have on a large supply area in the South of Europe (ETB-East-L).

Table 15: Case study results; economic impact for different scenarios in ETB-East-L

		30 min	8 h	24 h
Summer, workday, 9am	economic damage in mio. €	2.98	33.14	77.33
	unserved electricity in MWh	411.51	3368.54	8954.84
Summer, holiday, 9am	economic damage in mio. €	1.82	20.91	63.46
	unserved electricity in MWh	402.40	3297.52	8878.37
Summer, workday, 9 pm	economic damage in mio. €	1.58	18.52	77.33
	unserved electricity in MWh	376.91	2638.38	8954.84
Summer, holiday, 9pm	economic damage in mio. €	1.53	18.43	77.24
	unserved electricity in MWh	373.27	2658.41	8974.87
Winter, workday, 9am	economic damage in mio. €	3.00	34.57	85.37
	unserved electricity in MWh	569.92	4566.64	11811.73
Winter, holiday, 9am	economic damage in mio. €	2.02	24.25	70.20
	unserved electricity in MWh	391.48	3392.21	9956.30
Winter, workday, 9 pm	economic damage in mio. €	1.78	21.89	85.37
	unserved electricity in MWh	464.31	3086.31	11811.73
Winter, holiday, 9pm	economic damage in mio. €	1.73	21.66	70.20
	unserved electricity in MWh	424.25	3201.02	10114.71

The VoLL lies between 3.8 €/kWh (30 minute interruptions on a winter workday) and 8.6 €/kWh (24h interruption on summer workdays).

This is the lowest VoLL value in this comparison.

4.3 Summary of Economic Testbed Analyses

This report contains an innovative analytical methodology which can be used by stakeholders and the public to assess the effects of protection measures failing to prevent a power outage in terms of economic costs and energy not supplied.

Using innovative economic testbeds allows stakeholders from policy, industry and research to identify vulnerabilities and potential enhancements as regards cyber security protection measures. This is crucial as every technical solution comes at a cost, which can now be compared with the potential pay-off and macroeconomic benefit.

The format was chosen so as to comply with the needs of stakeholders from different regions, areas and size of respective regions. Thus – in total – 12 economic test beds were evaluated which corresponds to four primary regions, North, East, South and West as well as three region sizes respectively.

The results yield detailed insights into the economic ramifications associated with a failure to protect the currently high levels of supply security – Detailed information on the precise damage expectations are presented in Table 4 to Table 15.

While the supply of electricity is relatively reliable in Europe, maintaining this degree of reliability in the future involves a number of challenges. Decisions on investing in infrastructure are possible only if the value of electricity supply security to households and businesses can be determined.
To obtain an understanding of the benefits of successful cyber security measures, this report presents a model approach to assess the opportunity costs of not achieving successful protection. This approach furthermore accounts for damages of businesses, administration and public institutions using a split accounting approach. As a result, not only particularly vulnerable sectors, such as the semiconductor industry, papermaking or data-generating processes, but all branches of the economy as per NACE 2008 (economic classification) scheme can be modeled.

The wide range of blackout scenarios which can be assessed using the presented model last from one to 48 hours and covers many different conceivable outages for most of the provinces of the EU. Thus, it is possible for the first time to judge subsectors of the European economy province by Nuts 2 level as regards their degree of dependence on a reliable supply of electricity. Part of the work is an efficient utilization based on research conducted in the 7th framework program project SESAME. In fine-tuning the power outage assessment model (blackout-simulator.com) outages due to not successful cyber protection measures can be modeled in detail.

We exclude interruptions cuts lasting longer than 48 hours, with their hard-to-assess socio-economic impacts, and outages in the second to minute range, which cannot be represent objectively in economic terms. The presented model draws upon the estimation of country-specific valuations of uninterrupted power supply which take into account the variables season (of the outage), size of the outage area, participants' gender, education, household income and previous experience of power cuts. This ensures that the sample used in the presented model closely resembles the actual European population.

In order to provide a vivid example of the capabilities of the tool, this report contains the evaluation of economic test beds and presents a case study which is capable of analyzing for instance the effects of the large 2003 power outage in Italy, which affected over 55 million people. This prominent example of an outage lasted for three hours in the north, nine hours in the center of Italy, 12 hours in the south and up to 16 hours in Sicily. The macroeconomic damage of this power outage in the entire was calculated to be 1.18 billion € (in 2003 €). The level of detail is unprecedented and includes economic damage data for every sector (897.5 million €) and for households (285.0 million € respectively).

Summarizing, the costs associated with power interruptions are an important corner stone in the assessment of cyber security protection measures. The presented model for the first time provides an intuitive, easy-to-use tool for the assessment of the economic damages caused power outages. The outage properties can entirely be chosen by the user and include multiple connected (or individual scenarios). Applications of this tool are expected to be helpful for policy makers, for regulatory authorities, industry, utilities and other interested private/professional users.

4.4 Data integrity valuation

The societal and economic benefits of successful protection measures against cyber security threats include individual valuations for secure collection, storage and transmission of energy related data. This becomes obvious in the current debate regarding the Union-wide smart meter implementation. This roll-out can only be successful if protection of data is ensured and the financial means to DSO are granted to implement costly protection measures.

The EU-wide roll-out of Smart Metering technology[5], which primarily entails intelligent power metering devices, capable to bi-directionally transmit near-real-time information on electricity consumption data, has experienced noticeable opposition from household customer groups in various countries. A major public concern is found to be rooted in peoples' concerns with regards to data security and privacy. Empiric evidence for this type of concern – and how to best possibly address the issue of lack of confidence for the data management processes – is scarce. However, precise information on data security and privacy preferences with special regard to smart meter technology is found to be of high practical relevance. Deriving a better understanding the importance of ensuring data security and privacy has been endorsed by the highest authorities of the European Union (European Commission Vice-President Andrus Ansip for the Digital Single Market, and Věra Jourová, Commissioner for Justice, Consumers and Gender Equality):

"New technologies are emerging fast and have enormous potential for our society and economy. This potential can only be fully realised if people can trust the way their personal data is used. Ensuring trust will allow the European Digital Single Market to live up to its full potential. EU data protection reform, which will cut red tape for business and ensure a single set of rules, is part of the solution."

The SPARKS project and its stakeholders have understood this necessity and fill the related knowledge gap by conducting an empiric assessment of peoples' preferences in terms of data security and privacy with respect to smart grids. This is done in D5.4. and will be presented in the relevant deliverable report in detail.

The cornerstones of this task, is the conduct of a *beyond-state-of-the-art* assessment of security and privacy's monetary value. According to stakeholders such monetization has become necessary to learn about the importance of these issues to EU and national authorities and foster their thorough and rational consideration when deciding on related next steps. In SPARKS this monetization is done by means of an economic experiment, which assesses the preference structures of Europeans in terms of data protection (security) and privacy.

Knowledge about households' preferences with respect to data security and privacy in the smart grids environment becomes particularly relevant as various initiatives pursue the standardized collection, transmission and storage of energy consumption data. New market participants, henceforth aggregators, are expected to emerge at the European level. In the light of these (largely market based) developments, the necessity to precisely define required data protection standards, which best-possibly take into account consumers' preferences[6], becomes urgent. In particular, the D5.4 investigates consumers' preferences with regards to the collection, transmission and storage of power consumption data captured in 15 minute intervals by installed smart meters. The results of this analysis are presented in D5.4 which we refer to.

[5] The roll out strategy implies that by 2020 80 percent of European households ought to be equipped with ?intelligent meter technology. In countries such as Austria, this benchmark was raised to 95%.
[6] In economic terms, this is referred to a maximizing consumers' utility in terms of the data protection. This is followed throughout by means of a discrete-choice-like econometric modelling approach.

4.5 Sustainability dimensions of smart grid cyber security protection measures

In addition to the benefits associated with successful security measures in current and future electricity grids as outlined in previous chapters, high levels of data security, supply security and energy efficiency contribute to social stability and non-material benefits, which remain to be assessed.

In the future, these aspects will receive even greater attention making the increasing implementation of smart grid technology a necessity.
Especially the conversion from a strict division into consumers and producers is likely to affect the energy system as a whole. To make this transition possible, it is important to carefully alter the relationship between electricity generating, transmitting and distributing units on the one hand and customers on the other hand. Furthermore, this concerns the personal engagement opportunities for – in particular – residential consumers. In order to being able to participate in this "energy market 4.0", the customer needs to be equipped with the tools to monitor her consumption pattern, to interact with the energy markets and to engage in new generation processes.
The latter is particularly important for households which possess generative facilities based on renewable energy such as photovoltaic panels.

These important aspects of future smart grids give rise to the necessity of (i) better understand the various dimensions of electric energy by the public as well as to ensure that these services can be provides safely. The latteris a duty of the technical sciences to support by means of security measures.

The socio-economic dimensions of these future energy interactions are heterogeneous, though of high importance. Consumer benefits are to be assessed in terms of saved money as a consequence of shifting loads to low-price periods (load shifting), in terms of additional income opportunities based on energy provision as well as in terms of *ad hoc* savings due to efficiency improvements.

Summarizing, there is a variety of benefits to customers associated with smart grid implementations. For these to be realistic however, the security of power supply, the integrity of data and the provision of privacy in terms of energy-related consumption patterns need to be ensured. These protection measures come at a cost, but as indicated here, the benefits are likely to vastly outweigh the costs of these measures.

5 Summary and Conclusion

The understanding of socio-economic and legal aspects of smart grids cyber security is the cornerstone of the applied field work in D 5.3 of the SPARKS project. Furthermore, the aim of "Understanding the Societal Cost of Smart Grid Cyber Attacks" (D5.3) within the research project SPARKS is to create awareness and understanding of the non-technical implications smart grids and measures for their protection may have.

This report outlined that any planed measure or functionality of the smart grid should be scrutinized with respect to the incurred costs and the expectable benefits. Particular emphasis was given to the broader understanding of costs and benefits including those from a welfare economic point of view.

While engineers and project planners understand as costs only those identifiable through bills and accounts, the effects of smart grids projects will usually have broader impacts on the well-being, perceived risks and satisfaction of consumers beyond the accounting perspective but with macro- and microeconomic relevance. As an example thereof we emphasised the change of current privacy levels introduced through the interconnection between power grid and information network. Such changes manifested in privacy levels, e.g. through smart metered electricity consumption, have to be considered as costs if associated with welfare losses for parts of the society. When policy decision about architectural aspects of the smart grid or its functionalities have to be taken, these welfare losses (or gains in welfare) require incorporation for having a complete information base.

More broadly speaking, electricity markets are regulated, which means that consumers have no direct possibility to signal the responsible companies for grid operation and how they value certain aspects of the infrastructure or offered services through their purchasing behaviour. The magnitude of investments in the smart grids vision is thus widely shaped by politics, not by users of the grid. Considering efficient energy market regulation this condition for the operation of a natural monopoly is not decreasing cost-efficiency of power grids per se, but comprehensive weighting of possibly diverging interests of stakeholders is required for approving new investments and changes in operational practice. For the conventional grid such decisions in most cases were about the approval of investment in new – but well understood – infrastructure, such as new power lines. With the emergences of smart grids, the decisions have become more complex. For the frequently smart grid protection measures no well-established knowledge exists about the welfare economic costs and the expected benefits. As over-equipping our power grids may be result in as negative consequences as underinvestment does, we urgently call for future research as input for regulation.

Summarizing, the smart grids vision promises significant support for the envisaged transition to a low carbon society. It is yet unclear whether this promise holds, and whether its achievement comes in an economically efficient way bringing benefits to a large portion of the society while respecting the heterogeneous requirements of the population. This deliverable was set up to contribute to a better understanding of special smart grid aspects, yet it particularly also highlights the need for further research.

The valuation of the worst case of failing protection measures – i.e. power outages – are discussed in detail in this report. This is done by means of innovative economic test beds, which allow the identification of anticipated damages on the basis of 12 proto-typical regions in Europe. These span from small areas with 20,000 inhabitants to larger regions with 2 million people. To ensure European representativity, this assessment is carried out for four distinct geographically identified cases spanning from Northern to Eastern, from Southern to Western Europe. Results indicate that damages

are highest in the North and West, while adequate cyber security protection is certainly justified in Eastern and Southern Europe as well. [7]

Analyses of this kind are among the first globally to assess ramifications of failing infrastructures. This is increasingly important as every protection measure comes at a cost, which has to be compared to potential benefits by means of quantitative methods.

The main findings show the great importance of uninterrupted power supply to European societies. This, in turn, gives rise to the necessity of implementing protection measures which address looming threats even in the light of substantial efforts needed to develop and implement them.

In addition to the investigation of physical effects – i.e. power outages – we refer to D5.4 which conducts a *beyond-state-of-the-art* empirical assessment of security and privacy's monetary value in collaboration with stakeholders from the industry and policy making. The monetization of Europeans' need for data security and privacy will significantly support the weighting of investments for security measures compared to their benefits for the European population. This is considered as important input for decision processes and policy making targeting an efficient allocation of resources, considering the existing lack of quantitative measures thereof in light of energy consumption data. In line with costs associated with traditional threats - i.e. opportunity costs from power outages - from a macroeconomic perspective, the costs of data protection ought to reflect the demanded security level.

The societal dimensions of smart grids thus incorporate security related aspects which have to be addressed by science. The SPARKS project develops sophisticated technologies in various tasks and work packages. This deliverable is the accompanying socio-economic research, which is relevant as it assesses the monetary benefit of successful protection measures.

[7] Parts of the economic assessment model were used in collaboration with the FP7 research project SESAME. To ensure objectivity, the analysis was conducted in each of the 27 (in 2012) member state of the European Union. It was done in strict accordance with the recommendations of best practice methodology for contingent valuation methods (Arrow, et al. 1993).

6 References

Arrow, Kenneth, Robert Solow, Paul R. Portney, Edward E. Leamer, Roy Radner, and Howard Schuman. "Report of the NOAA Panel on Contingent Valuation." Tech. rep., National Oceanic and Athmospheric Administration, Washington, D.C., 1993, 4601-4614.

Baarsma, B., P. Hop (2009). Pricing power outages in the Netherlands, Energy, 34, pp. 1378-1386

Baarsma, Barbara E., and J. Peter Hop. "Pricing power outages in the Netherlands." Energy 34, no. 9 (2009): 1378-1386.

BDEW. Standardlastprofile Strom. BDEW. 8 22, 2014. http://www.bdew.de/internet.nsf/id/DE_Standartlastprofile (accessed 8 22, 2014).

Bliem MG. (2007). Ökonomische Bewertung der Versorgungsqualität im österreichischen Stromnetz und Entwicklung eines Modells für ein Qualitäts-Anreizsystem. Dissertation, Alpen-Adria-Universität Klagenfurt.

Bliem, Markus Gilbert. "Ökonomische Bewertung der Versorgungsqualität im österreichischen Stromnetz und Entwicklung eines Modells für ein Qualitäts-Anreizsystem." Ph.D. dissertation, Alpen-Adria-Universität Klagenfurt, Klagenfurt, 2007.

Bompard, E., T. Huang ,Y. Wu and M. Cremenescu (2013). Classification and trend analysis of threats origins to the security of power systems. Electrical Power and Energy Systems 50, pp. 50-64.

Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag (2014): Moderne Stromnetze als Schlüsselelement einer nachhaltigen Energieversorgung, report, available at: http://www.tab-beim-bundestag.de/de/untersuchungen/u9700.html, last accessed on 28 October 2015.

Capgemini (2007). RFID and Consumers: Understanding Their Mindset. Capgemini; consulting, technology, outsourcing. Availible at: http://www.us.capgemini.com

Centolella, Paul and Farber-DeAnda, Mindi and Greening, Lorna A. and Kim, Tiffany. "Estimates of the Value of Uninterrupted Service for The Mid-West Independent System Operator." Tech. rep., SAIC, 2006.

Cohen J.J., J. Reichl and M. Schmidthaler (2014). Re-focussing research efforts on the public acceptance of energy infrastructure: A critical review. Energy, 76, pp. 4-9.

Commissione di Indagine. "Black-out del sistema elettrico italiano del 28 settembre 2003 Rapporto della Commissione di Indagine." Rome, 2003.

Database, World Input-Output. World Input-Output Database. n.d. http://www.wiod.org/new_site/data.htm (accessed 08 12, 2014).

DAVID-VO 2012 der E-Control, BGBl. II Nr. 313/2012

De Nooij, M.,C. Koopmans, C. Bijvoet (2007). The value of supply security: The costs of power interruptions: Economic input for damage reduction and investment in networks. Energy Economics, 29, 277-295.

de Nooij, Michiel, Carl Koopmans, and Carlijn Bijvoet. "The value of supply security. The costs of power interruptions: Economic input for damage reduction and investment." Energy Economics 29 (July 2007): 277-295.

Engerer, H. (2009) Security Economics: Definition and Capacity, Economics of Security Working Paper 5, Berlin: Economics of Security.

Engerer, Hella. "Security Economics: Definition and Capacity." Economics of Security Working Paper Series, DIW Berlin, German Institute for Economic Research, 2009.

European Commission (2009). Directive 2009/72/EU of the European Parliament and of the Council of 13 July 2009 concerning common rules for the internal market in electricity and repealing Directive 2003/54/EC.

European Commission (2014). Report from the Commission: Benchmarking smart metering deployment in the EU-27 with a focus on electricity.

European Commission. "Directive 2003/54/EC concerning common rules for the internal market in electricity." Official Journal of the European Union, 2003: L 176.

Eurostat. "17 Millionen Studenten an den Hochschulen der Europäischen Union." Dezember 12, 2005. http://epp.eurostat.ec.europa.eu/cache/ITY_OFFPUB/KS-NK-05-019/DE/KS-NK-05-019-DE.PDF (accessed Juni 21, 2013).

Garcia Gutierrez, F., M. Schmidthaler, J. Reichl, S. Voronca, and T.E. Roman. Securing the European electricity supply against malicious and accidental threats: Public effects knowledge data base, European Union Seventh Framework Programme, Project # 261696. Madrid: Deloitte & Transelectrica & Energy Institute at the Johannes Kepler University Linz, 2013.

Herold, R. (2011). Ensuring Smart Grid Social Acceptance by Securing Data Privacy. Grid Talk – Power Utilities Communcations e-Zine. July, pp. 2-3.

Jamasb, T. and Pollitt, M. (2005). Electricity Market Reform in the European Union: Review of Progress toward Liberalization and Integration, Working Paper of the Center for Energy and Environmental Policy Reserach: Joint Center of the Department of Economics, Laboratory for Energy and the Environment and Sloan School of Management.

Jamasb, T., and M Pollitt. "Electricity Market Reform in the European Union: Review of Progress toward Liberalization and Integration." Tech. rep., Joint Center of the Department of Economics, Laboratory for Energy and the Environment and Sloan School of Management., 2005.

Kariuki, K.K., and R.N. Allan. "Evaluation of reliability worth and value of lost load." Generation, Transmission and Distribution, IEE Proceedings- 143, no. 2 (mar 1996): 171-180.

Keppler, J. "Public Goods, Infrastructure, Externalities and Subsidies: A Conceptual Framework for the “IEA Questionnaire on Government Interventions in the Energy Sector”. Subsidies and Environment – Exploring the Linkages." OECD Documents (OECD Documents), 1996: 193-200.

Keppler, J. (1996). Public Goods, Infrastructure, Externalities and Subsidies: A Conceptual Framework for the “IEA Questionnaire on Government Interventions in the Energy Sector”. Subsidies and Environment – Exploring the Linkages. Series: OECD Documents, p. 193-200.

Kollmann, A., S. Moser, K. de Bruyn, M. Schwarz, and K. Fehringer (2013). Smart Metering im Kontext von Smart Grids. Technical report commissioned by the Austrian Ministry for Transport, Innovation and Technology.

Lohse, T, Robledo JR, and Schmidt U. "Self-Insurance and Self-Protection as Public Goods." Journal of Risk and Insurance, 2010: 57-76.

Lohse, T., J.R. and U. Schmidt (2006). Self-Insurance and Self-Protection as Public Goods. Hannover Economic Papers (HEP) dp-354

Munasinghe, M, and A Sanghvi. " Reliability of Electricity Supply, Outage Costs and Value of Service: An Overview." IAEA Special Issue Electricity Reliability Issue, no. 9 (1988).

OECD. "Family size and household composition." Juli 1, 2010. http://www.oecd.org/els/soc/41919509.pdf (accessed Juni 27, 2013).

Perakslis, C., and R. Wolk (2005). Social acceptance of RFID as a biometric security method. IEEE Technology and Society Magazine, DOI:10.1109/MTAS.2006.1700020.

Preisel M., W. Wimmer, D. Frey and A. Huser (2012). Smart Metering Consumption. Schriftenreihe of the Austrian Ministry for Transport, Innovation and Technology: Berichte aus Energie- und Umweltforschung 44/2012. http://download.nachhaltigwirtschaften.at/edz_pdf/1244_smart_metering_consumption.pdf

Reichl, J., M. Schmidthaler and F. Schneider (2013a). Power Outage Cost Evaluation: Reasoning, Methods and an Application. Journal of Scientific Research & Reports. 2(1), pp. 249-276.

Reichl, J., M. Schmidthaler and F. Schneider (2013b). The value of supply security: The costs of power outages to Austrian households, firms and the public sector. Energy Economics. 36, pp 256-261.

Reichl, Johannes, Michael Schmidthaler, and Friedrich Schneider. "The value of supply security: The costs of power outages to Austrian households, firms and the public sector." Energy Economics 36, no. 0 (2013): 256-261.

Samuelson PA. (1954). The Pure Theory of Public Expenditure. Review of Economics and Statistics, 36, pp. 387–389.

Samuelson. "The Pure Theory of Public Expenditure." The MIT Press, 1954: 387-389.

Schmidthaler M., J. Reichl and J. Cohen (2014). Economic Valuation of Electricity Supply Security / Ad-hoc cost assessment tool for power outages. Electra. 276, pp. 10-15.

Schmidthaler, M., Cohen,J.J., Reichl, J. and Stefan Schmidinger (2015). *The effects of network regulation on electricity supply security: A European analysis*. Journal of Regulatory Economics (http://tinyurl.com/JRE-Schmidthaler).

Sequera, V. (2012). Colombian rebels attack energy systems. The Washington Times online, September 17 2012, http://www.washingtontimes.com/news/2012/sep/17/colombian-rebels-attack-energy-systems/?page=all

Sforna, M., and Maurizo Delfanti. Overview Overview of the of the events events and and causes causes of the. Atlanta: Politecnico de Milano, 2006.

Timmer, Marcel P. (ed). "The World Input-Output Database (WIOD): Contents, Sources and Methods." WIOD Working Paper Number 10. 1 1, 2012. http://www.wiod.org/publications/papers/wiod10.pdf (accessed 6 27, 2013).

Tsoukalas, L. H. and R. Gao (2008). From Smart Grids to an Energy Internet: Assumptions, Architectures and Requirements. Third International Conference on Electric Utility Deregulation and Restructuring and Power Technologies. DOI: 10.1109/DRPT.2008.4523385

Wacker, G, and R Billinton. " Customer Cost of Electric Service Interruptions. Proceedings of the IEEE." 1989: 919-939.

Wigan, M. (2014). User Issues for Smart Meter technology. IEEE Technology and Society Magazine, pp. 49-53. DOI: 10.1109/MTS.2014.2301856

Wolf, A. and L. Wenzel (2014). Regional diversity in the costs of electricity outages: Results for German counties. Utilities Policy. DOI: 10.1016/j.jup.2014.08.004

Woo, C., R. Pupp (1992). Costs of service disruptions to electricity consumers, Energy,17, pp. 109-126.

Woo, Chi-Keung, and Roger L. Pupp. "Costs of service disruption to electricity consumers." Tech. rep., Department of Economics and Finance, Hong Kong, 1992.

Zhu, B., A. Joseph, and S. Sastry (2011). A Taxonomy of Cyber Attacks on SCADA Systems. IEEE International Conferences on Internet of Things, and Cyber, Physical and Social Computing. pp. 380-

Zingman, Craig, Robert J. Thomas, Ian Hiskens, Kevin Stamber, Thomas J. Overbye, Richard Schuler, Philip N. Overholt, Paula Scalingi, John D. Kueck, Paul Carrier, Fernando L. Alvarado, Anjan Bose, Vikram S. Budhraja, William Buehring, Anthony Como, Chris DeMarco, Joseph H. Eto, Regina Griego, and John F. Hauer (2000), Findings And Recommendations To Enhance Reliability From The Summer Of 1999, available at https://emp.lbl.gov/sites/all/files/final-doe-pwr-outage-study-team%202000.pdf last accessed 28 October 2015.