OFFIS NAVIGANT ECOFYS A Navigant Company

Study on the Evaluation of Risks of Cyber-Incidents and on Costs of Preventing Cyber-Incidents in the Energy Sector

final report

Study on the Evaluation of Risks of Cyber-Incidents and on Costs of Preventing Cyber-Incidents in the Energy Sector

Final report

By: Lars Fischer, Mathias Uslar (OFFIS), Doug Morrill (Navigant), Michael Döring, Edwin Haesen (Ecofys, a Navigant company)

Date: 30 October 2018

EC reference: ENER/B3/2017-465
Ecofys reference: ESMDE17665

Reviewer: Edwin Haesen

Ecofys - A Navigant Company
Ecofys Germany GmbH | Albrechtstraße 10 c | 10117 Berlin | **T** +49 (0)30 29773579-0 | **F** +49 (0)30 29773579-99 | **E** info@ecofys.com | **I** ecofys.com
Register Court: Local Court Cologne | **Chamber of commerce Cologne** HRB 28527 | **VAT ID** DE 187378615
Managing Director Scott S. Harper, Julie M. Howard, Monica M. Weed

Executive Summary

The main objective of this study is to provide a **consolidated view on main cyber threats** and **applicable cybersecurity frameworks** in the European energy system, a suggested **energy-focused risk management approach**, and a set of **regulatory recommendations** with **possible cost impact**. This analysis is underpinned by a sound risk assessment methodology and application to the specificities of the European energy system to reasonable level, and benefits from inputs from stakeholders. The results provide a basis for policy makers to discuss this complex topic on national level and within international cooperation. It can also support the European Commission's (EC) strategy building among others on the proposal to call for a network code on cyber security. The study considers various methods of risk management from European and international initiatives and presents approaches to conduct a risk analysis for stakeholders. It strongly integrates earlier guidance and tools from Mandate 490[1] which has already proven its value in the context of standardisation.

The figure below lists the main tasks of the study, which also correspond to the six main chapters of this report. Background information is provided in a set of annexes and an extensive reference list.

Figure 1: Study tasks and chapters of this final report

The European energy system is going through a substantial transition. In the past, discussions mainly focused on physical incidents in energy networks and cyber incidents in information technology (IT) systems. Nowadays and in the future, energy systems consist of integrated energy and communication networks. **This requires an integrated view on physical and cyber requirements**. Current trends in the transition period of the European energy system are the increased **cross-border integration of markets and coordination needs** for system operators, a proliferation of decentralised energy resources, and application of digitised solutions. In contrast to other industry sectors, the energy system includes assets with long lifetimes, which often **were not intended to interact with widespread communication layers**. The currently added interconnectivity in the operational technology (OT) domain requires **urgent cybersecurity solutions** and may expose the system to new threats as it moves from an analogue to a digitized operation mode. The energy system requires also special attention as its vast

[1] M/490 is a standardization Mandate by the European Commission to European Standardisation Organisations (CEN, CENELEC, ETSI) to support European Smart Grid deployment. It includes a European framework to describe smart grids.

interconnectivity of users and **real-time operation** needs to avoid **critical cascade effects** where a single power system outage or cyber-attack may propagate with widespread effects. Cybersecurity solutions need to be deployed **on live systems which need to maintain their integrity for operation at all time** and to ensure the minimum disturbance possible. These specific requirements cannot be addressed by bringing the energy system offline as it might be possible with other IT applications. Therefore, **the European energy system combines unique characteristics of the so-called OT and IT world**.

Chapter 1 of the final report gives a view on recent policy initiatives from the EC on cybersecurity in general and where relevant to the energy sector in specific. It also outlines the main trends the energy sector is experiencing now, including more widespread market/system operation, decentralisation of resources, and digitization. It highlights what is specific in the energy sector beyond usual IT cybersecurity needs, and why dedicated efforts are relevant in this domain.

Energy systems across the globe have experienced cyber-attacks in the past. Examples of existing cases are the often quoted attack on a Ukrainian DSO (2015), the self-inflicted incident in the Austrian TSO system due to a cross-border miscommunication (2013), and the malware targeting industrial control systems at Saudi Arabia energy infrastructure (2017). These cases illustrate how the described trends of **increased cross-border operational coordination, real-time system impact and new communication layers added to legacy assets, increase the need for proper cybersecurity strategies implemented by energy organisations**. The complexity of the European energy system and the historically developing information and communication systems enables a variety of cyber threats. But contrary to pure physical incidents and common approaches in operational planning by system operators, it must be acknowledged that a complete list of potential cyber threats does not exist. Even more the technical grid development and operational procedures cannot ensure absolute resilience, nor can a system be designed which ensures full protection against all future cyber threats. In comparison to pure information technology (IT) systems, additional complication and increased sense of criticality for energy systems comes from operational technology (OT) vulnerabilities which are becoming more prominent.

Chapter 2 of the final report describes examples of (known) cybersecurity incidents in the global energy sector in recent years. A structural framework is presented for threat scenarios. Eleven specific threat scenarios are listed that will feed into the analysis of the next chapters, and which exemplify the priority set of issues the European energy system could face.

To address threats in the European energy system various mitigation measures can be applied. Regulators, standardisation bodies and industry sectors have documented best practices to deal with threats imposed to systems interfaces and business processes. This study presents an overview of basic cybersecurity principles and existing risk mitigation frameworks, describes the relation between various frameworks (e.g. ENISA[2] and NISTIR7628[3]), its system and regulatory context (which differs e.g. in EU and US), and existing gaps when mapping the catalogues. Presently most EU system operators and authorities are triggered to review and implement cybersecurity strategies

[2] ENISA (2012): Appropriate security measures for smart grids, https://www.enisa.europa.eu/publications/appropriate-security-measures-for-smart-grids

[3] NIST (2014): Introduction to NISTIR 7628 Guidelines for Smart Grid Cyber Security, https://nvlpubs.nist.gov/nistpubs/ir/2014/NIST.IR.7628r1.pdf

as a result of the implementation of the NIS directive[4]. This study surveyed European network operators to gain understanding on which practices are applied, which cost and other challenges their cybersecurity strategy faces and which threats and need for action they see. Chapter 3 of the final report explores various cybersecurity best practices and how these interrelate. Facts and viewpoints are presented and analysed on how EU system operators cope with energy cybersecurity. Based on the experience with the strong stakeholder interaction we see a clear need for enhanced monitoring of specific information related to cybersecurity in the energy sector, like costs, implemented measures, maturity levels or incidents. For example, this could be done in national monitoring reports of the energy sector.

To assess risks, this study provides a **blueprint risk management approach** for the European energy sector. The methodology builds on international security standards and guidelines. The objective is to provide a framework which applies maturity levels and prioritises mitigation measures for specific organisations. The approach used covers a so-called **top-down analysis** of logical interface classes based on selected use cases, and a **bottom-up analysis** of the 11 high-priority threat scenarios. This two-fold analysis allows a risk assessment when the limited information is available on attackers and attack modes (top-down view), but also when specific attackers or new (future) attack types are considered (bottom-up). These two analyses **complement each other**. The proposed methodology can be applied by individual organisations or national/European agencies or authorities to identify risks, weakest points and priority mitigation measures (based on the ENISA mitigation catalogues). It can also be used to evaluate expert stakeholder opinions on regular basis. Chapter 4 of the final report presents the above described risk management approach for energy cybersecurity.

Following up the risk management approach, this study performs a high-level EU wide cost projection which states that **currently European electricity TSOs and DSOs are estimated to spend presently about 700 million Euro annually on cybersecurity related measures**. These expenditures account for about 0.02 ct€/kWh, or an average 0.11% of average retail tariffs and bills. **New legislative instruments aiming to advance all grid operators to at least medium or alternatively high maturity level could increase present expenditures by 3 to 6%**. Attention is needed regarding the uncertainty[5] related to these figures. Chapter 5 of the final report lists a set of European policy options that could advance cybersecurity maturity and assesses the cost impact.

[4] The Directive on security of network and information systems (NIS Directive, 2016), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN

[5] Main causes for this uncertainty are confidentiality of expenditure information by organisations on cybersecurity, limited view on present maturity across the large number of energy organisations in Europe all with different legacy, ambiguity within organisation budgets on which part would be attributed to cybersecurity in the OT domain (beyond normal ICT measures), and the difficulty in generalising the additional cost of new measures.

Following up on the main findings, the following main recommendations to increase the maturity level of European energy companies (structured along the objectives of the NIS directive) are derived:

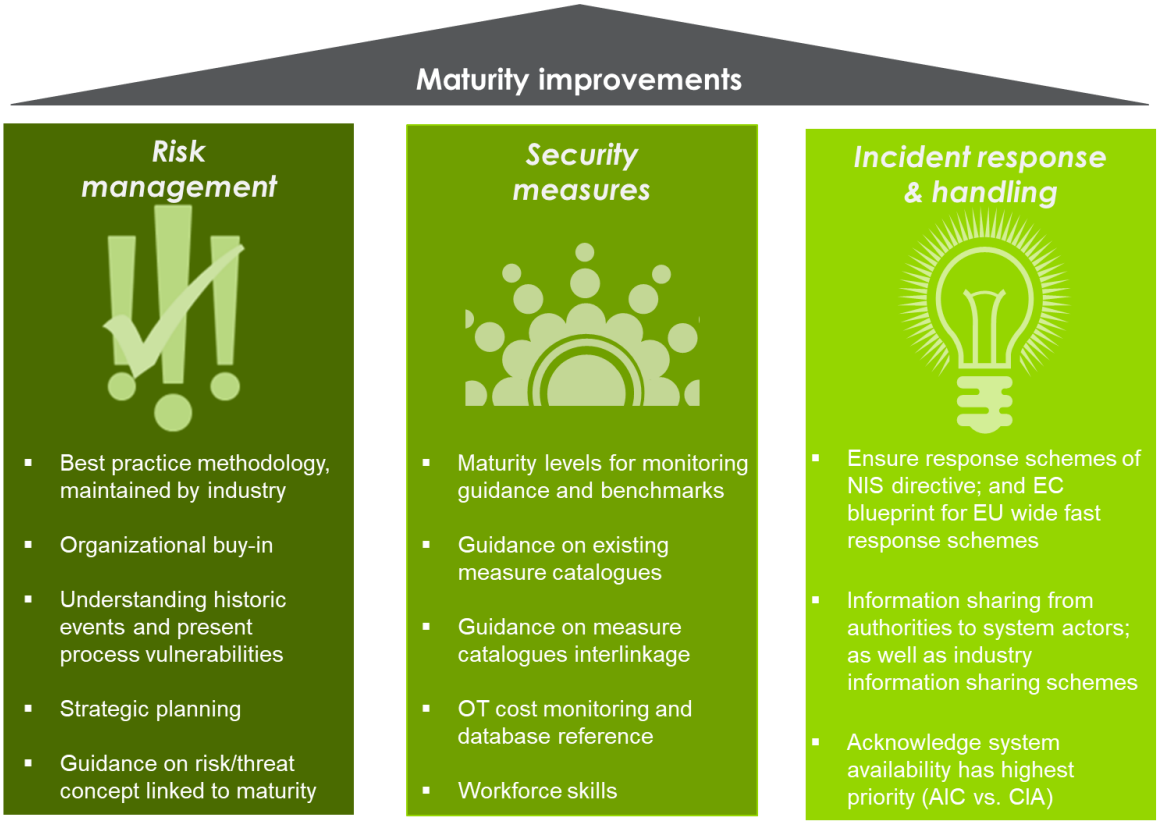

Figure 2: Main recommendations for advancing the objectives of the NIS directive and the Cybersecurity strategy in the energy sector

With further policy instruments it is recommended to bear in mind following key principles for any upcoming cybersecurity regulation: (A) **Avoid lock-in to very specific practices**, which may complicate future legislative updates or national legislation. Cybersecurity threat developments and solutions are highly dynamic. (B) For any instrument, **consider sufficient implementation guidance** and clear monitoring tools. An option could be to have stakeholder implementation committees (in analogy with gas/electricity network codes). (C) **Policy tools can be used to ensure timely progress in industry standardisation**, e.g. via mandate-driven preparatory work and harmonised standards as reference for compliance efforts. Chapter 6 of the final report concludes with a set of recommendations for policy makers, regulatory authorities and industry organisations.

Table of contents

Ecofys - A Navigant Company

Ecofys Germany GmbH | Albrechtstraße 10 c | 10117 Berlin | **T** +49 (0)30 29773579-0 | **F** +49 (0)30 29773579-99 | **E** info@ecofys.com | **I** ecofys.com

Register Court: Local Court Cologne | **Chamber of commerce Cologne** HRB 28527 | **VAT ID** DE 187378615

Managing Director Scott S. Harper, Julie M. Howard, Monica M. Weed

I. Table of Abbreviations

ACER	Agency for the Cooperation of Energy Regulators
AEG	Attack Execution Graph
AIC	Analog Interface Circuit
AMI	Automated Metering Infrastructure
APT	Advanced Persistent Threat
ATM	Asynchronous Transfer Mode
BES	Bulk Electric System
BSI	Federal Office for Information Security (Germany)
CAPEC	Common Attack Pattern Enumeration and Classification
CERT	Computer Emergency Response Team
CIA	Confidentiality-Integrity-Availability
CIP	Critical Infrastructure Protection
COTS	Commercial of The Shelf
CSIRT	Computer Security Incident Response Team
CVA	Cyber Vulnerability Assessments
CVE	Common Vulnerability Enumeration
CWE	Common Weakness Enumeration
DA	Data Access
DCS	Distributed Control System
DDoS	Distributed-Denial-of-Service
DER	Distributed energy resources
DGM	Distribution Grid Management
DIA	Direct Internet Access
DMS	Distribution Management System
DOE	Direct Operational Effect/impact
DSO	Distribution System Operators
EAM	Enterprise Architecture Management
EECSP	Energy Expert Cyber Security Platform
EMS	Energy Management System
ENISA	European Union Agency for Network and Information
EPCIP	European Program for Critical Infrastructure Protection
EPRI	Electric Power Research Institute
EUROSTAT	European Statistical Office
FE	First Energy
FERC	Federal Energy Regulatory Commission
GDPR	General Data Protection Regulation
HAN	Home or Building Area Networks
ICS	Industrial Control System
ICT	Information and Communication Technologies
IDS	Intrusion Detection System
IEA	International Energy Agency
IRC	Internet Relay Chat
IRP	Incident Response Plan
ISMS	Information Security Management System
IT	Information Technology
ITSM	Information Technology Security Manager

KRITIS	Critical Infrastructures (Germany)
LAN	Local Area Network
LI	Logical Interface
LIC	Logical Interface Category
MC	Microgrid controller
MENA	Middle East and North Africa
MIL	Maturity Indicator Level
MP	Market platform
NAESB	North American Energy Standards Board
NERC	North American Reliability Corporation
NESCOR	National Electric Sector Cybersecurity Organization Resource
NIS	Network and Information Systems
NIST	National Institute of Standards and Technology
NISTIR	National Institute of Standards and Technology Interagency Report.
NREL	National Renewable Energy Laboratory
O&M	Operation & Maintenance
OEM	Original Equipment Manufacturer
OFFIS	Institute for Information Technology
OT	Operational technology
OWASP	Open Web Application Security Project
PLC	Programmable Logic Controllers
PMU	Phasor Measurement Unit
PRA	Personal Risk Assessment
RASSA	Reference Architecture for Smart Grids in Austria
RAT	Remote Access Tool
ROC	Regional Operation Centres
RPC	Remote Procedure Calls
RTU	Remote Terminal Unit
SA	Substation Automation
SC	Standards Committee
SCADA	Supervisory Control and Data Acquisition
SEIM	Security Event and Information Management
SGAM	Smart Grid Architecture Model
SGIS	Smart Grid Information Security
SIEM	Security information and event management
SIS	Safety Instrumented System
SL	Security Level
SLA	Service Level Agreement
SME	Subject Matter Expert
SP	Storage Prosumer
SRP	Salt River Project
TSO	Time Sharing Option
UML	Unified Modeling Language
UTM	Unified Threat Management
VBA	Visual basic for application
VPN	Virtual Private Network
VPP	Virtual power plant
XBID	Cross-Border Intraday

1 Towards a European framework for cybersecurity in the energy sector

KEY MESSAGES

The need for appropriate cybersecurity measures in Europe's critical infrastructure, and in particular its energy systems, has been articulated in a number of European policy initiatives of the past 15 years. The recent 2017 EC cybersecurity package provides several regulatory proposals and other communications aiming for a higher cyber resilience. Furthermore, industry expert groups in the energy sector (past Energy Expert Cyber Security Platform (EECSP) and presently the SG TF EG2) investigate various options to strengthen Europe's cybersecurity strategy in energy.

The energy system is going through a substantial transition. Main trends are the increased cross-border integration of markets and coordination needs for system operators, a proliferation of decentralised energy resources, and application of digitized solutions. These energy sector trends are disruptive and provide opportunities, but also demand ever increasing attention for adequate cybersecurity actions. The electricity and gas system include assets with long lifetimes, which often were not intended to interact with widespread communication layers. This added interconnectivity in the operational technology (OT) domain requires urgent cybersecurity solutions and may expose the system to new threats as it moves from an analogue to a digitized operation mode. The energy system (in particular the electricity system) requires also special attention as its vast interconnectivity of users and real-time operation needs to avoid critical cascade effect where a single power system outage or cyber-attack may propagate with widespread effects. In addition, the operation of energy systems is driven by continuous availability needs, while other sectors often prioritise confidentiality with less than 100% availability being acceptable. Cybersecurity solutions need to be deployed on live systems which need to remain their integrity for operation at all time and to ensure the minimum disturbance possible. These specific requirements cannot be addressed by bringing the system offline as in other ICT applications.

Chapter 1 provides further information on these EU policy initiatives and wider energy system trends. The next Chapter 2 provides examples of cybersecurity events in the energy sector and develops a set of high-priority scenarios for the European system that require further analysis and mitigation measures.

1.1 Overview of European policy initiatives

Cybersecurity and the protection of critical infrastructure was first put prominently on the EU agenda in June 2004. The European Commission adopted a green paper on the European Program for Critical Infrastructure Protection (EPCIP) in 2005. This paper resulted in the European Program for Critical Infrastructure Protection in 2007 and in the European Critical Infrastructures Directive in 2008. These first efforts have resulted in a range of activities and

legislation in the last years both at national and EU level, most notably the **Cybersecurity Strategy of the European Union in 2013** and the **Directive on security of Network and Information Systems (NIS) in 2016**. In the perspective of the constant rise of cyber threats the European Commission adopted recently **in September 2017 a new Cybersecurity Package** which proposes further development of the current framework and the introduction of new instruments and legislations (inclusive regulations on ENISA and certification). **Particularly the 2017 revision of the cybersecurity strategy acknowledges the importance of sector specific requirements.**

In this section an overview of the most important legislative actions is provided as well as strategies and programs that aim to improve cybersecurity. The overview below is without prejudice to ongoing national legislative activities in the context of cybersecurity in the energy sector.

Legislation

- The European Critical Infrastructures Directive (Directive 2008/114/EC) [1] from 2008 defines a process for identifying and designating European critical infrastructure for the energy and transport sectors.
- The directive on security of Network and Information Systems (NIS) (Directive (EU) 2016/1148) [2] of 2016 was the first piece of European-wide legislation specifically addressing cybersecurity. It requires Member States to develop national strategies on network and information security. It also triggers European cooperation in this field. While the NIS directive lays down general rules, specific rules can be developed through a network code as foreseen in the Commission proposal of November 2016 [3] (revised electricity regulation as part of the Clean Energy Package), which will offer technical rules for TSOs and possibly DSOs on how to ensure system security in emergency situations while considering new risks resulting from the digitalisation of the energy system.
- A review of the NIS Directive is planned in 2021.

Strategies and Programs

- The European Program for Critical Infrastructure Protection (EPCIP, 2006) [4] sets out the principles and instruments for implementation, aimed at both European and national infrastructure. Within the Program European critical infrastructure and interdependencies between them are defined. Furthermore, expert groups and the Critical Infrastructure Warning Information Network are established to facilitate information sharing and the funding of projects.
- The Cybersecurity Strategy of the European Union (2013) [5] defines overarching principles and priorities for EU cybersecurity efforts to support the internal European market. It emphasises the need to establish a coordinated international cyberspace policy. It stresses the importance to develop capabilities and allocate resources in a way that enhances the Member States' ability to anticipate and handle cyberattacks.
- The European Agenda on Security (2015) [6] and the Digital Single Market Communication (2015) [7] stress the need for a common approach to address cyber threats across Europe.
- In September 2017, the EC and the High Representative published a **Cybersecurity Package** [8] including proposals such as
    - Establishing a EU cybersecurity agency built on a strengthened ENISA and setting up a EU-wide cybersecurity certification scheme for products and services (both elements are outlined in a proposal for regulation)

- A EU response and coordination scheme to large-scale cybersecurity incidents and crises (Commission Recommendation)
- Establishing competence centres in the Member States as well as a European cybersecurity research and competence centre, and setting up a cyber defence training and education platform
- Development of technical guidelines and recommendations for the national implementation of NIS by ENISA in cooperation with relevant stakeholders

Clean Energy Package proposals

- Security of supply is a key component of the legislative proposals given in the November 2016 Clean Energy Package.
  - The package's draft electricity regulation sets out how regional actions (e. g. in risk-preparedness plans and via Regional Operation Centres (ROC)) need to strengthen the reliability of the European energy system.
  - It also suggests several new network codes and guidelines to be developed, complementing the ones established in line with the 2009 Third Energy Package.
  - Next to the decarbonisation and decentralisation, the increasing penetration of information and communication technologies (ICT) in the energy system requires an enhancement of system security solutions. Therefore, as described earlier one of the new network codes will cover the domain of "cybersecurity rules". This builds on a "Security plan for Critical Infrastructure Protection" requirement to all TSOs as already prescribed in the "System Operation Guideline" (Article 26, prescribing a security plan for Critical Infrastructure Protection).

The Clean Energy Package legislative proposal also requests a new EU DSO entity to be established with a mandate to collaborate on various tasks including "data management, cybersecurity and data protection". The package also strengthens the role of DSOs in the development of network codes, together with ENTSO-E, ACER and the European Commission.

1.2 Recommended actions from industry expert groups

The EC set up two industry expert groups to provide recommendations on cybersecurity in the energy sector.

- The Energy Expert Cyber Security Platform (EECSP), active from 2015 to February 2017
- The Smart Grid Task Force Expert Group 2 (SGTF EG2), having a mandate to prepare input for the proposed network code on cybersecurity until end of 2018.

Between 2015 and 2017 the EECSP performed a gap analysis [9] of the current legislation, like the NIS directive, on cybersecurity in the energy sector to secure energy systems against cyber threats and protect the data and its privacy in the energy systems. The analysis covered three main questions:

- *Is energy different from any other sector in respect to cyber security?*
- *What are the challenges in the energy sector to be addressed?*

- *What are recommended actions to be taken in respect of cyber security once the NIS Directive and GDPR are fully implemented?*

In general, the expert group recommends using the existing EU framework, the NIS directive and the GDPR, as a basis for any additional regulation in absence of a real national implementation. The group puts a strong recommendation on establishing rules for a regional cooperation model based on Computer Security Incident Response Teams (CSIRTs) for energy. The approach is aligned to existing best practices from experts. In total the expert group identified 39 gaps which are allocated to four strategic areas indicating areas of generic actions:

- Setup a harmonised, structured and comprehensive **threat and risk management system** to provide an overview on the current and future threat and risk landscape in European energy system, as the current NIS directive focuses on information exchange of current and known incidents. The system should be supplemented by a framework on regional cooperation and information exchange to disclosure of vulnerabilities and incidents.
- Setup a **cyber response and regional coordination framework** focused on the energy sector. In case of cyber incidents, the crisis management should incorporate a strong regional cooperation.
- Improve cyber resilience and develop and implement a specific **European cyber security maturity framework** for the energy sector and to set up contractual public private partnership to **increase resilience of the supply chain** of the energy industry. In this field the expert group recommends incorporating international best practices through extended European and international collaboration.
- **Build-up the required capacity and competences** and promote research in the field of cybersecurity in the energy sector.

As mentioned earlier, in its Clean Energy Package the EC proposed to develop a further network code on cybersecurity rules for the energy system. The EC established in Spring 2017 the Expert Group 2 under the umbrella of the Smart Grids Task Force to provide inputs to the European Commission for this network code focusing on electricity system operators. Final recommendations will be expected end of 2018. A first interim report[6] was delivered end of 2017, including first recommendations, planned activities for 2018 and a list of risk scenarios. Based on the results of the final EECSP report the SGTF EG2 recommends implementing four key elements in the network code:

- Specification of a **European cyber security maturity framework for mitigations** which should take into account specifications of the ISO/IEC 27000 series of standards
- Definition of **minimum cybersecurity requirements for products and systems** to address the supply chain / vendors and covers conformance elements of international standards, e.g. ISO/IEC 27001[7]

[6] smart grid task force expert group 2 (2017): Interim Report, Recommendations for the European Commission on Implementation of a Network Code on Cybersecurity

[7] ISO/IEC 27001 is a specific information security management system which requires certification by accredited external parties in some countries

- Specification of a **European Early Warning System for Cyber Threats** to coordinate the information sharing of incidents between system operators, which may be based on the Computer Security Incident Response Team (CSIRT) established by the NIS directive
- Rules on the **Cross-Border and Cross-Organisational Risk Management** across European system operators

In addition, the SGTF EG2 analyses the impact of several identified cyber risk scenarios. As this study aims to provide input and recommendations for future regulation in the energy sector, a brief comparison of synergies and complementarities to the SGTF EG2 work is given (see also Figure 3). Of the four SGTF EG2 domains, this study links most closely to that of a cross-border/cross-organisational risk management approach and partly to that of a maturity framework.

- This study and the SGTF EG2 work are not overlapping work streams but inspire each other.
- The risk assessment approach in this study is based on the international standard ISO 31000 (risk management guideline), which represents a higher-level abstraction in comparison to ISO 27001. ISO 27001 describes a specific information management system representing one instrument including certification which could be one result or recommendation from an ISO 31000 based assessment. As ISO 27001 focuses on information security, it may be not applicable to all processes included in the energy system. Starting from an ISO 31000 method allows to cover elements due to new risks or domain interfaces of the energy sector, which are not yet specified in the ISO 27000 application series.
- The risk assessment methodology of this study is built to be able to include additional energy domains or energy sub-sectors (e. g. gas transmission system or electricity generation units) whereas SGTF EG2 focuses explicitly on transmission and distributions network of the electricity system as outlined in its terms of reference. As the electricity sector is understood to have more and different critical issues compared to gas, and as system operators have a key role in the domain of cybersecurity control, the application in this study will focus also more strongly on electricity system operators.

This study formulates a few potential EU-wide policy options (set up in close consultation with the EC) to reflect the EU-wide cost drivers per option. Costs are not in the scope of SGTF EG2.

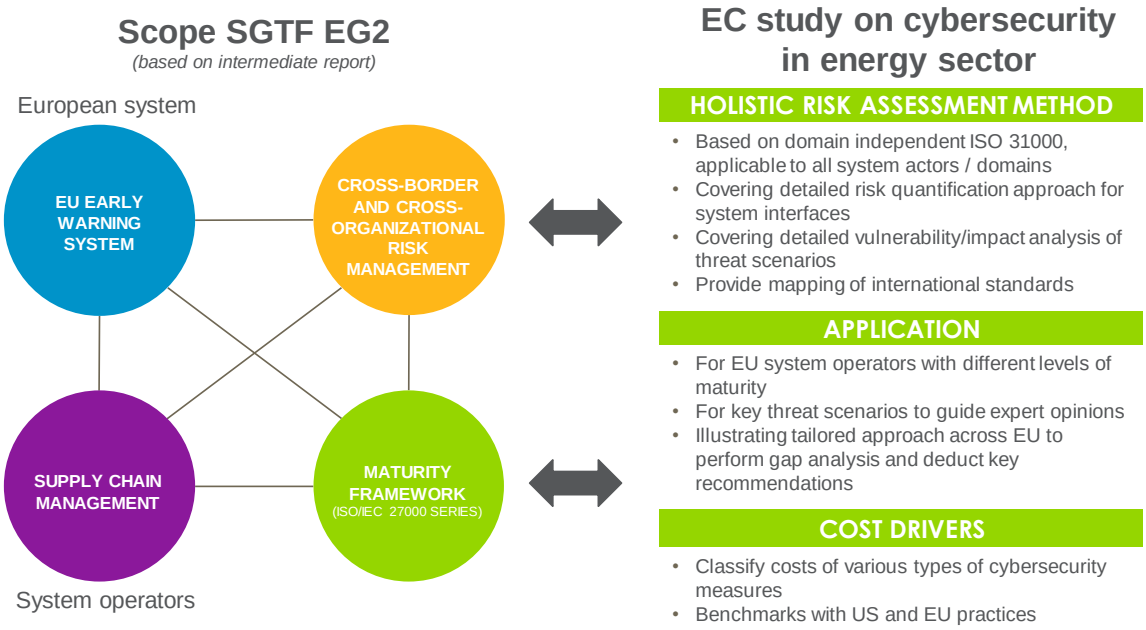

Figure 3: Illustrative comparison of synergies and complementarities of this study to SGTF EG2 work

1.3 Trends in European energy sector

The European energy system is facing a fundamental transformation. The next years will see a massive disruption across the entire energy value chain, impacting core value streams of traditional actors and a broad set of stakeholders. Three main trends are highlighted, which also show cybersecurity risk assessments require evermore attention in the European energy sector.

European market development and integration

Europe has set a clear goal of a fully-integrated internal energy market, which ensures non-discriminatory market access of existing and new actors and facilitates cross-border energy trading. One recent example for market integration is the XBID Market Project, which creates a joint integrated Intraday cross-zonal market to enable continuous cross-zonal trading and complements markets at longer time frames. A first go-live was in June 2018, an extension of the work domain is planned for 2019. The next years will also see various cross-border integration projects of electricity balancing markets. The trend of enhanced cross-border trading results in an increased demand for cross-border coordination and data exchange. In addition, there is a trend towards closer to real-time markets with higher volumes. This requires fast and continuous security analyses and decision-making processes for system operators. Furthermore, new types of actors will enter the market, like aggregators and prosumers, and the overall number of (smaller scale) actors will increase significantly. These actors must incorporate often local (price) signals from new local markets or local flexibility platforms. As such, there will be proliferation of market interfaces for exchanging data close to real-time to enable various market processes.

Growth of decarbonised and decentralised generation

The United Nations Climate Change Conference in Paris 2015 committed to limit global warming to 2 degrees. This commitment is fuelled by multilateral efforts focused on decarbonising the global economy, and adapting to a clean, distributed, intelligent, and mobile energy system. One major driver is the constant growth of renewable energy sources in all European Member States. In 2017, the installed capacity of renewable energy plants in Europe reached almost 500 GW, thereby representing a share of around 30 % of the electricity consumption in the EU. In contrast to the old system with its few larger power plants, this capacity represents millions of fluctuating generation units spread over Europe, reflecting the decentralised character of our future energy system. In the decentralised energy system, the distribution systems and their efficiency become a crucial element to also support system security as evermore of the generation capacity and flexible users will be connected to this system level. Therefore, new and more data interfaces between TSO-DSO and market operators of all flexibility options are becoming widespread. As a next step, these decentralised characteristics could enable new 'regional cell concepts', representing geographically limited but resilient regions (also as a potential measure regarding cybersecurity by means of fast isolations), which can be operated for limited time in case of incidents in the interconnected power systems. However, due to the variable infeed of many renewable energy sources, an extended and robust European power network will remain the crucial backbone of future system security. While local systems may show more intelligence and resilience, the interconnected EU system needs to be able to cope with incidents, including cyberattacks, and be able to avoid a cascade effect across the system. After a critical disturbance in 2006 including massive cascade effects due to a single physical incident (not cyber related), European authorities and system operators have set a key priority in mitigating similar events in future. This objective becomes more challenging with the proliferation of many (smaller) actors in the system, which play an ever more important role in system services (frequency/voltage control) and in some areas are quickly becoming the dominant share of supply.

Another game-changing development is that of average market prices, a higher volatility of those prices and the predominance of capital costs. In various regions worldwide, renewables are cheaper than electricity from new conventional power plants. New renewable energy projects continue to set low-price records, like 5 cents per kWh for offshore wind power in Denmark, less than 3 cents per kWh for onshore wind power in Morocco or 2.6 Cents per kWh for solar power in Chile. This trend raises the question how to argue for more efforts and investments for cybersecurity, especially considering the current cost pressure within energy organisations and from regulators? In contrast to our current power system, all these technologies are capital intensive and have long lifetimes. Operational costs, like fuel costs, are no longer the predominant cost component. The characteristic of high upfront investments from a proliferation of new actors requires new planning reliability criteria and careful reflection of future requirements for central operators and connected parties, e. g. for cybersecurity.

Digitalisation of the energy system

In the energy system, new technologies such as distributed renewable generation, electricity storage and electric vehicles point to the need of the deployment of "smart" technology such as smart meter, virtual power plants, smart home management systems or Internet of Things systems. The decentralisation of the energy system and the inclusion of the consumer and new prosumers across the energy value chain depend upon a far more data-driven

and flexible energy system, also on the consumer side. All these factors lead to a significantly greater use of ICT and a digitalisation of the European Energy infrastructure and market. This trend impacts the full spectrum of infrastructure in the field, market processes, and grid planning/operational procedures. The trend also drives many new activities and opportunities in all of these, but at the same time also asks for more attention to cybersecurity risk mitigation strategies. Figure 4 illustrates current energy sector digitization trends and allocates them to the elements of the value chain.

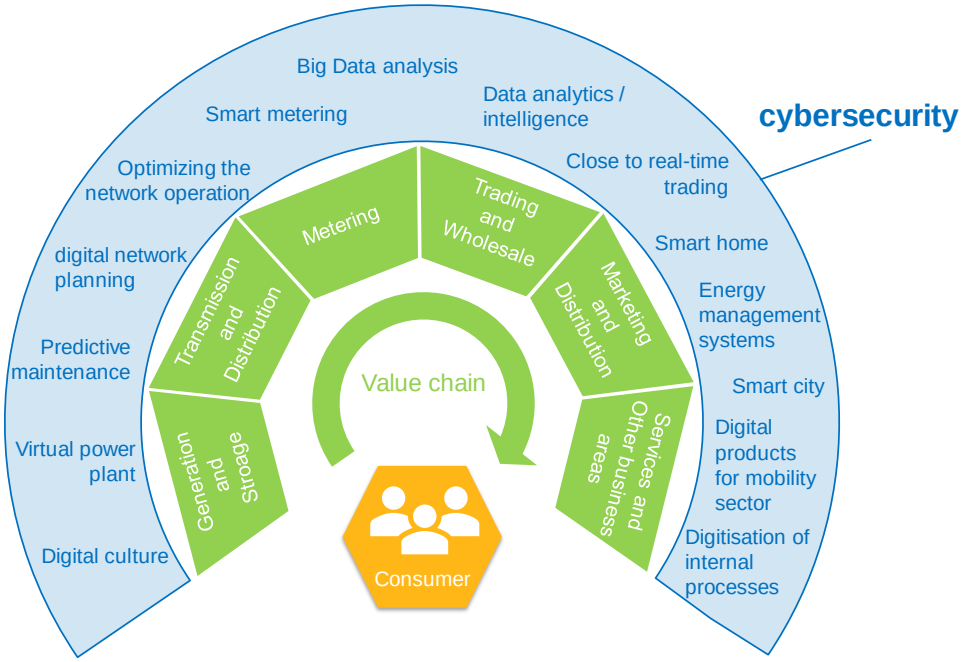

Figure 4: Illustration of the digitalisation along the value chain of our energy system [Source: own illustration based on German energy association (BDEW)]

The digitization in the energy sector is ramping up at impressive pace. The IEA reported that over recent years the expenditures in digitalisation infrastructure and software in the global electricity sector increased by 20% annually and are already surpassing the global investment in gas-fired power generation (>40 billion USD per year). Digitization already is projected to bring benefits of over 80 billion USD per year in direct power system infrastructure efficiencies, including reduced asset investments, reduced O&M costs, reduction of unplanned outages, extended lifetime of assets and lower losses. In addition, digitization is acknowledged as a crucial enabler of renewable integration and distributed energy resources including demand response and electric vehicle integration. This trend brings exposure to three main risks which require concerted actions: data privacy issues, economic disruption and cybersecurity.

1.4 Higher exposure to cyber threats in the European energy sector

Energy sector trends are disruptive and give opportunities, but also demand ever increasing attention for adequate cybersecurity actions

According to recent reports on the level of exposure and threats [10] and [11] various European Member States, like the Netherlands, Germany, France or Great Britain, are in the top lists regarding risks of general cyberattacks. In contrast, no EU Member State is in the Top-5 list of countries best prepared against cyberattacks (top 1 is the U.S.), according to the International Telecommunication Union of the United Nations [12]. While organisational and ICT related cybersecurity issues are common across various sectors, the energy and especially the interconnected power system has several resilience issues, which are particular for this sector. Even more, as the sector is in full transition, all trends listed in Section 1.3 and recent studies show that resilience issues are more pronounced and more urgent to address [13] [14] [15].

A smarter energy system can significantly increase the precision, response time but especially the effectiveness of power generation, transmission network management and market related tasks. These technical advantages make quick responses to outages possible and allow for significant efficiencies in operations and asset management. A smart energy system is constituted by interconnected physical and electronic sensing, monitoring, and control devices. The digitalisation of the energy sector comes with a price: **increased exposure to cyber incidents and attacks**. Ubiquitous connectivity and data collection heighten the already clear need for vigilance with data security for customers, systems or assets. Many energy system assets have been operational since decades in times when communication interconnectivity layers were not considered, or purely monitoring based, or at least tailored for the specific application. Such assets may benefit from security by obscurity. Cybersecurity becomes a prominent issue when transparent industrial standards are applied (and attackers are one step ahead), and when legacy assets are rapidly connected to communication layers. As the decarbonised and digital energy system evolves, widespread, holistic cybersecurity solutions will be critical. Cyber threats apply to all - generation, transmission, distribution and to market services. It raises the question of how to understand and address the risks and threats of cyber incidents affecting personal data and strategic energy infrastructure data, which are crucial for the security of the energy supply and therefore for all underlying sectors.

The EC's DG Connect promotes the concept that three areas of public interest – broadband networks 5G and Big Data, digital service infrastructures (DSIs) and the internet of energy [16], [17], [13] – are the main pillars of a new digitized energy value chain; and that interoperability and standardisation, and cybersecurity, are common issues in all three (Figure 5).

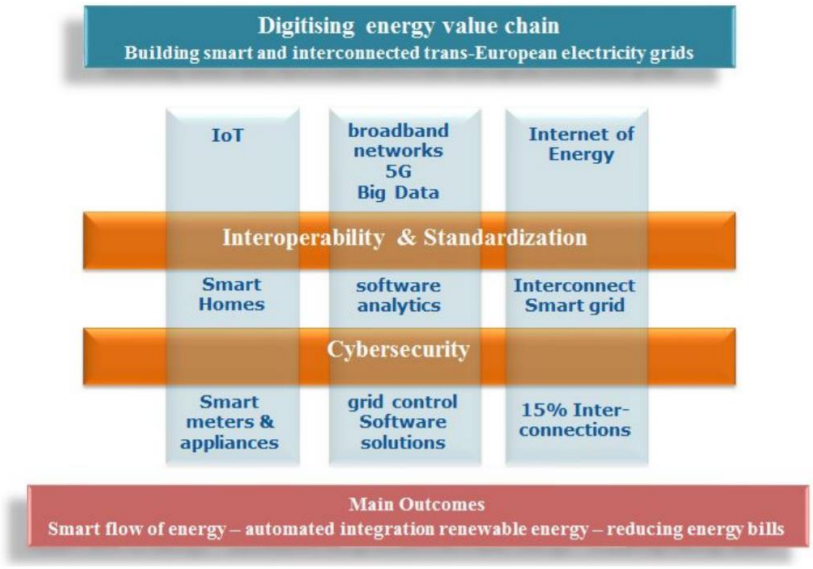

Figure 5: DG Connect view on main pillars in a digitized energy value chain [18]

A recent survey by the German Energy Agency (Dena) of German distribution system operators polled for risk estimates of generic threat types. Figure 6 provides an overview of the results based on feedback of 35 operators. The survey confirms the increasing cyber risk perception due to the interconnection of the IT and OT world and network. The five threats with very high relevance regarding cyber risks for the distribution system operators are also represented by one or more high-priority scenarios as selected in Chapter 2.

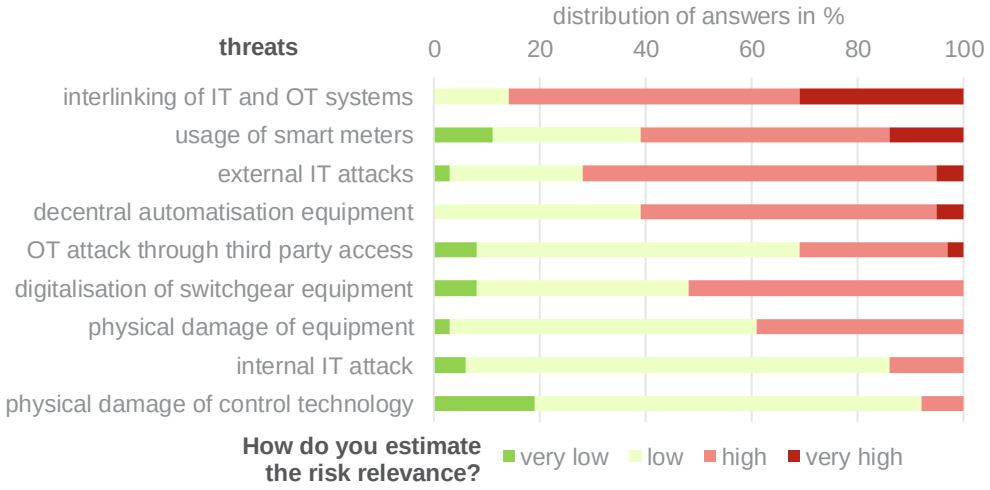

Figure 6: Estimation of risk relevance as regarded by German distribution system operators [Source: Ecofys based on [19]]

Cybersecurity vulnerabilities can be allocated to information technology (IT) networks or operational technology (OT) networks. Most sectors are dominated by IT networks, like the internet, which are open networks. Cybersecurity as a discipline is still often seen as just an IT discipline. In contrast, the energy sector is dominated by OT systems (e. g. remote controlled equipment in distant substations), which are closed networks and therefore used to be characterised by less vulnerabilities. As highlighted earlier, the digitalisation exposes these OT systems to other (open) networks increases the interaction with other domains (e. g. smart home, electric vehicles). Cybersecurity in energy systems faces the specific challenge to secure vulnerabilities of systems, which were originally not designed to be interconnected with open networks. In addition, the strong interaction with other sectors makes it even more challenging to define homogeneous and solid cybersecurity strategies.

A second specific challenge are vast networks of interconnected assets with real-time[8] operational requirements, on which the power and gas systems are based. Historically, the wider transmission system was operated with remote actions, while distribution and end user actions required local manual actions. Decentralisation of generation and flexibility, increase of smart meters and cloud-based platforms all extend these real-time requirements to the edge of the grid. Real-time requirements and industrial control systems in general face specific cybersecurity issues as they are designed to remain 'online' during maintenance, patching and other unusual situations, and the wider energy system needs to remain operational.

In contrast, for example office ICT systems can be shut down during maintenance for a limited period. The high interconnection of, and the frequent data exchange within electricity and gas grids, and its security and reliability criteria, do not always allow for fast isolation of cybersecurity issues nor a pure ICT driven response and restoration of the process after isolation. While these energy system operational measures are designed to ensure high reliability, they are less resilient to cyberattacks.

Apart from a cyberattack cascading effect, the interconnectivity of an energy system also has outage cascading risks. While power and gas systems are built and operated with clear reliability and redundancy criteria, still a large unplanned outage of a specific generation (single big generation unit or large number of distributed generation units across Europe), a substation or a transmission corridor may have a cascading effect with more outages and result in partial or full blackouts. Another cascading risk in energy systems exists due the coupling of different energy carrier systems, e.g. a critical issue in gas supply may impact electricity generation, or a cyberattack in the control system of one may penetrate to the control system of another operator.

Another important difference of the energy system compared to other sectors is that the vast extent of assets with relatively long live times, creates a situation where cybersecurity measures constantly face many legacy systems with weaknesses. The vast amount of historical assets with life times of roughly 30 to 50 years is anyway delaying a fast digitization of the sector. One can assume that in a green-field approach new systems would be designed with state-of-the-art cybersecurity measures in place. In reality, energy systems are populated by 'obsolescent' devices, which for several reasons cannot be replaced easily, and which de-facto could downgrade the cyber resilience of the

[8] Regarding real-time, we mainly refer to the technical operation of the power and gas system. Regarding the applied market design and products, close to real-time markets (day-ahead and intraday) play a major role in power market. Gas markets are in general less close to real-time (days or weeks to delivery), and gas grid operations have more inherent delays in propagating effects.

system. In the energy system cybersecurity should not be seen as an additional operational layer but may require substantive impacts on investment programs as well. It is exactly the transition from an old 'analogue' system to a digitized sector with also new types of users and interfaces that creates a challenge to ensure legacy assets do not create exposures to high cybersecurity risks.

2 Cybersecurity threats in the energy sector

KEY MESSAGES

Energy systems across the globe have experienced cyberattacks in the past. This chapter describes the often quoted 2015 attack on a Ukrainian DSO, a case of a self-inflicted incident in the Austrian TSO system due to a cross-border miscommunication, and a case of malware targeting industrial control systems. These cases illustrate how the trends described in Chapter 1 of increased cross-border operational coordination, real-time system impact and new communication layers added to legacy assets, increase the need for proper cybersecurity strategies implemented by energy organisations.

This Chapter 2 further provides an overview of how cyber threats can be classified. Especially attackers with a high amount of available resources (mainly nation state and large criminal organisations) play an important role regarding threats to our energy system. In this study 11 high-priority threats are developed and clearly described. This list is based on events which have already occurred in the past or which could become relevant given the transition the energy sector is going through (see trends in chapter 1). In contrast to pure information technology (IT) systems, additional complication and increased sense of criticality for energy systems comes from operational technology (OT) vulnerabilities which are becoming more prominent. The selected scenarios serve as further illustration of the type of threats the energy system has been and in future still can be susceptible, too.

Due to the complexity of our energy system and the historically developing information and communication systems a variety of cyber threats are possible. Main limitations are the creativity and the available resources of the attackers. Contrary to physical incidents and common approaches in operational planning by system operators, it must be acknowledged that a complete list of potential cyber threats does not exist. Even though reliability in the European energy system has remained at very high level over the past decades, technical grid development and operational procedures cannot ensure absolute resilience. Nor can a system be designed which ensures a full protection against all future cyber threats.

In Chapter 4 a risk management analysis is performed using these 11 high-priority scenarios which allows individual organisations or authorities to link threat scenarios to system impact and recommended mitigation categories.

2.1 Case studies of known incidents

Three recent incidents are used to illustrate typical cyber threats. A more elaborate list of publicly known incidents in the energy sector can be found in Annex 8.1.

Example 1: Attack on the Ukraine distribution system operator in 2015

The electric power sector was forced to take a more aggressive approach to cybersecurity following the 2015 attack on the Ukrainian power grid, affecting 27 substations and approximately 225,000 end customers. Target was the Ukrainian electricity distribution company Kyivoblenergo. The attack can be classified as an advanced persistent threat (APT) and resulted in a disruption of service and blackout.

The attackers used targeted emails carrying weaponised visual basic for application (VBA) Microsoft Word and Excel attachments. Opening the files by employees installed a specific remote access tool (RAT) / malware, BlackEnergy3, on the workstations. From there the attackers got access privileges for at least 6 months until they fully deployed specially crafted malware to the SCADA and field system enabling them to affect multiple substations. Finally, they were able to open a series of breakers of multiple substations, triggering the blackout. Seven 110 kV and twenty-three 35 kV substations were disconnected. This incident received global attention and helped spread public awareness to the vulnerabilities of electric power systems. A subsequent attack in December 2016 further exasperated industry concerns, with the country's power grid quickly becoming a test bed of sorts for cyberattacks.

Example 2: Self-inflicted information overload of the Austrian control centre due to cross-border miscommunication in 2013

In 2013, a misconfiguration in the control system of the Austrian electricity transmission grid operator led to the situation that a single counter value query from the Bavarian gas system triggered a domino effect and an overload or temporary non-availability of the crucial services of the Austrian control centre. The incident was an accident due to misinterpretation of a data signal at the interface of two domains in different energy sectors and resulted in temporary non-availability of relevant system functions.

More specifically, a status request command packet, which was broadcast from a German gas company as a test for their newly installed network branch, found its way into the systems of the Austrian energy power control and monitoring network. Due to misinterpretation the data message from the gas system generated thousands of reply messages in the power system, which generated even more data packages, which in turn flooded the control network. To stop this self-inflicted Distributed-Denial-of-Service (DDoS) 'attack', part of the monitoring and control network had to be isolated and disconnected. Fortunately, the situation was resolved without any power outages.

Example 3: Destructive industrial control system malware targeted at Saudi Arabia energy infrastructure in 2017

While responding to an incident caused by malware acting on critical safety systems, the analysts found that the malware seemingly aimed at causing physical damage [20]. The attackers were able to deploy the attack framework, named TRITON, custom-made for Schneider Electric's Triconex safety instrumented system. Subsequent analysis found that it has been part of a larger campaign aimed at disrupting industrial safety systems in Saudi Arabia [21].

The Triconex safety instrumented system is used for different applications to ensure safety of personnel and infrastructure in various sectors including oil and gas. While the attackers seemingly where not able to execute their

final attack, due to a mistake that lead to a failure of the system, the attack however succeeded in all stages of a full industrial control system intrusion [22].

Later analysis indicated that the attackers gained sufficient knowledge of the Triconex Safety Instrument System Controllers to re-develop parts of the proprietary communication protocol. They were able to reverse engineer sufficient parts of the closed-source communication and controller software to actively participate in safety control communication and trigger emergency operations [23].

The initial vector / source of infection has not been disclosed or remains unknown. The attackers most likely invested significant amounts of time to learn about the attacked operational technology (OT) system. Neither secrecy of the software nor the proprietary communication protocol could prevent the attack that, most likely, was aimed at capabilities to cause physical damage.

2.2 Selection of threats in the European energy system to assess risks

Due to the complexity of our energy system and the corresponding information and communication system a variety of cyber threats are possible. Main limitations are the creativity and the available resources of the attackers. Hence, a complete list of threats does not exist, nor does any full protection against it. The risk analysis in this study covers a selection of most relevant threat scenarios that will be used in a risk assessment bottom-up analysis (see chapter 4.3).

2.2.1 Overview of threat categories in energy systems

Energy infrastructure provides a distinctively different threat landscape as compared to non-physical ICT threats, although attack patterns on ICT components are naturally similar. From observed incidents in literature ([24], [25]) follows a classification of general threat agents and a set of threat categories / high-level scenarios (Figure 7). In comparison to non-physical ICT threats, attack agents with a high amount of available resources (mainly nation state and large criminal organisations) play an important role regarding threats to our energy system. Threat categories help to identify and distinguish threat scenarios to provide coverage of — at least — the most important threats. Based on the classification of threat agents, threat categories and observed incidents in literature a list of threat scenarios is developed in the following paragraph as a basis for the further analysis. The list of scenarios aims to cover a variety of identified categories and high-priority threats for the energy system.

Figure 7: Classification of threat agents / attackers and threat scenarios (high-level scenarios)

2.2.2 High-priority scenarios in the European energy system

A selection of high-priority threat scenarios in the European energy sector is developed taking into account inventories of published incidents, considering available documents from ENISA [26], EECSP [9], SGTF EG2 [27], CERT-EU [28] or NESCOR [29] on threats.

The selection covers current threats and incidents, but also future developments and a variety of affected systems. Table 1 shows the proposed list of threat scenarios. It gives a concise description and provides a mapping to real past incidents where possible.

ENISA's Threat Taxonomy [30] provides an extensive list of threats to power systems, including a broad selection ranging from environmental hazards to intentional malicious behaviour. Classification of below high-priority threat scenarios in Table 1 is provided down to threat detail level. Detail levels missing in the ENISA Threat Taxonomy are denoted by "-". Extending this selection towards a complete enumeration of threat scenarios is beyond the scope of this study as the relation between threats and threat scenarios is very complex. Further current taxonomies that have been used for ideation of threat scenarios can be accessed in [31] or [32].

The objective in this study is to identify threat scenarios for which there either is historical precedence, or for which there are consequences with upcoming technologies and are not yet considered sufficiently. Scenarios 1 to 6 are derived in this study to close obvious gaps on novel or standard threat scenarios. Scenarios 7 to 11 are important scenarios selected from [33] and [29]. The NESCOR scenarios are considered the only source for complete and structured threat scenario descriptions in the energy sector. It is recommended that future research adapts the complete list of 127 threat scenarios for European energy systems.

Novel technologies considered for threat scenarios are based on emerging ICT-based technologies increasingly deployed in the industry. The technologies considered are mobile computing and remote access, security measures (intrusion detection and prevention systems used for zone protection), dynamic software updates, and finally cross-sector communication.

In the bottom-up risk analysis of Chapter 4, the selection is transformed into a systematic and logical description to perform the risk assessment. Through the analysis risks can be estimated, and appropriate mitigation strategies for the selected threat scenarios recommended.

Table 1: Overview of selected high-priority scenarios in the European energy sector, further description and references in the Annex 8.1

ID	Title	System
1	**Infection through intrusion detection system (IDS)**	ICT-System

Description

Intrusion Detection or Prevention Systems (IDS or IPS), applied as ICT protection system, for example on firewalls, usually require to be executed on very high-privilege levels with wide access throughout the system. They are also most often outward-facing. This makes them a very interesting target for intrusion themselves[9]. To infect the general ICT protection systems of power system equipment enables the attacker to get access rights for all crucial elements and subsystems of the infected system, e. g. substation or generation unit. A threat agent exploits the security vulnerability in out-facing interfaces of a protection measure (e.g. firewall or IDS) to gain access to the internal network. Access then is extended laterally throughout the distribution or transmission grid operators enterprise network. This scenario is an instance for a general type of scenario where the (often necessarily) higher access rights of protection software and devices make them an interesting entry vector to compromise the control system of the system operator. This is especially interesting in industrial control systems, more so in power systems, where often only such perimeter security is deployed. One example are legacy systems that commonly are integrated through virtual private networks. Another reason for perimeter-only security is ease-of-use in a corporate culture deeply rooted in physical systems.

Impact

The compromise has no direct impact to the power system but provides a high-privilege entry-point for threat agents. There is a very high probability that sensible corporate data will be disclosed to the attackers or could be manipulated by them. Attackers could significantly disrupt the communication abilities of the attacked company, affecting for example customer service or the ability to monitor wide area energy controls. The scenario carries a high potential of lateral movement, i.e. allowing the attackers to extend their foothold deeper into all connected systems.

Example

Real incidents: Vulnerabilities in IDS/IPS systems are known. It is reported, that this type of vulnerabilities has been exploited in the field.[10] No real incident description public available

Classification

Nefarious Activity [Malicious Code [*]]

[9] See, for example, the length of vulnerabilities found in the Common Vulnerability Enumeration https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=intrusion+detection (last visited 2018-09-12)

[10] "Cisco is aware of the Proof of Concept code, which can result in either a DoS or RCE. The PoC is publicly available on the internet and it has been reported to the Cisco PSIRT team that attempted exploitation using the PoC occurred." [https://www.securityweek.com/cisco-aware-attacks-exploiting-critical-firewall-flaw]

ID	Title	System
2	**Virus/Trojan infiltrates industrial control system**	IT/OT-System

Description
In this scenario the attacker infiltrates the equipment via a virus, worm or trojan. An existing virus, worm or trojan without special targeting the industrial control system (ICS) is infecting an ICS system disrupting or threatening to disrupt the process and to take over the control the attacked equipment.

Example
Real incidents: Gundremmingen/Germany 2016 (two viruses infiltrated industrial control systems of a cargo crane in Gundremmingen via USB-sticks), Integral Energy/Australia 2009 (A virus infiltrated the network and equipment of a Utility)

Impact
The scenario has an overall low impact. Main damage comes from loss of productivity and recovery of system software on devices, e.g. IT-servers or desktop computers.

Classification in ENISA Threat Taxonomy
Nefarious Activity [Malicious Code [*]]

ID	Title	System
3	**Social engineering: phishing employees on enterprise level propagates to field level manipulation or introducing a remote access tool kit to human machine interface**	Office ICT-System (affecting OT-System)

Description
In this indirect attack, the attacker first infiltrates the general office ICT-System of the network operator or manufacture and secondly gets access to control systems of the attacked organisation. This attack does not address individual power system equipment but allows access to all control systems of the organisation.
Remote Access Toolkits (RAT) are injected to workstations in the Enterprise Zone through spear phishing employees through emails carrying weaponised attachments (e.g. scripts embedded in text processor macros). The attacker then laterally extends its foothold in the Enterprise Zone and collects intelligence on access codes and structure of the company network. This information is then used to vertically extend access by deploying RAT in the Operations and Field Zone using legitimate credentials. The threat agent operates an external command and control service to execute control on the infected devices. The gained access is then used to change the behaviour of field devices, e.g. to disrupt power or gas distribution or to damage equipment.

Example
Real incident: Ukraine 2015/16. On Dec. 23rd in 2015 nearly 225,000 customers in three areas of Ukraine had to endure 3 hours of blackout due to (likely) the first cyber attack on the control system of a power grid. The perpetrators had entered the enterprise IT through targeted emails carrying weaponised VBA Word or Excel attachments. Opening the files installed the RAT "Black Energy 3" on the workstations. From there the attackers extended their foothold and access privileges for at least 6 month until they deployed specially crafted malware to the SCADA and field system enabling them to affect multiple substations [34].

Impact
Although the immediate impact is comparatively low and limited to the operation of a single DSO, the follow-up threats are highly critical, e.g. power disruption within a city or region, including potential long-term damage to equipment, emission of flammable gas, or compromise of sensor, company or customer data. The attack vector “phishing” is easily exploited and is one of the most often and most successfully used. Knowledge on the development of RATs is widely spread and not very complicated. Detection of custom-made tools is usually difficult, which means the likelihood of detection of an ongoing attack is low.

Classification
Nefarious Activity [Receive of unsolicited e-mail [unsolicited infected E-Mail]]

ID	Title	System
4	**Malicious update to firmware in the field to influence single substation**	Substation (OT-System)

Description
This scenario focuses on the security of the manufacturers / supply chain and affects all equipment having regular firmware updates. A threat agent uses access to the update service for OEM firmware to inject malicious code to influence, by injection of communication to the field bus, the behaviour of other devices at the substation of the power system. The attacker may aim at damaging individual devices by blocking (i.e. jamming) communication for protection functions or disrupt service by issuing single commands.

Example
Real incident: Siberian Gas Pipeline 1982. The USSR used a pipeline control software from a Canadian company. This software included a Trojan Horse from the United States that caused a major explosion of the Trans-Siberian gas pipeline. The Trojan ran during a pressure test on the pipeline but doubled the usual pressure, causing the explosion.

Impact
Local disruptions of distribution that likely affects only a limited number of customers until re-construction of the site. Targeted attacks on a single facility depend on in-depth knowledge of the system and may require special vulnerabilities for delivery. Execution, as in the example, thus is difficult, and requires time or resources.

Classification in ENISA Threat Taxonomy
Nefarious Activity [Unauthorized Activities [Unauthorized use or administration of devices and systems],
Unauthorized installation of software [-]

ID	Title	System
5	**Cross-sector, cross-border message flooding**	Control centre (TSO, DSO)

Description
See description case study 2

Example
real incident: Germany-Austria 2013

Impact
Low probability of short term disruptions, that are unlikely to leave persistent compromise of any device. The scenario describes an accident that is, given proper procedures, unlikely to repeat frequently.

Classification
Nefarious Activity [Misuse of information/ information systems (including mobile apps)]

ID	Title	System
6	**Compromise equipment through SCADA apps**	IT/OT-System (IT-System Attack)

Description
This scenario focuses on security of regular maintenance via so-called SCADA apps (business clients) and smart home applications (end consumer). Mostly generation units are affected in this scenario.
A threat agent exploits the established relation between a (legitimate) SCADA app on a dual-use (private and business) smart phone of a control room engineer to gain privileged access to a distribution SCADA system (e.g. of a generation unit or transformer station) and establishes a persistent remote access there.

Example
No real incident description public available

Impact
Threat agents gain access to the control room with the potential to manipulate the system. Unless secondary attacks are executed, manipulations should be obvious to personnel, yet may have drastic consequences ranging from disruption of service to damage to facilities. Mobile devices are usually not in the sphere of physical protection, can easily be stolen and many vulnerabilities exist in common mobile devices. Likelihood of such an attack relates to the utilisation of the technology.

Classification in ENISA Threat Taxonomy
Nefarious Activity [Manipulation of Hardware and Software [Abuse of vulnerabilities, 0-day vulnerabilities, Access to device software], Targeted Attacks [*]

ID	Title	System
7	**Advanced persistent threat (APT) to DSO flexibility management system**	DSO (IT/OT-convergence threat)

Description

A threat agent performs reconnaissance of utility communications, an electrical infrastructure, and ancillary systems to identify critical feeders and electrical equipment. The threat agent gains access to selected elements of the utility distribution management system (DMS) - that includes all distribution automation systems and equipment in control rooms, substations, and on pole tops - via remote connections. After gaining the required access, the threat agent manufactures an artificial cascade through sequential tripping of select critical feeders and components, possibly causing automated tripping of distribution level generation sources due to power and voltage fluctuations. A blackout of varying degree and potential equipment damage ensues. Remote connections to the DMS might be established using a variety of methods or combination of methods.

Example

Real incidents: See description case study 1 (Ukraine 2015),

In addition, the US-CERT Threat Alert TA18-074A describes in detail current government cyber activity targeting management systems of energy companies

Impact

This the most prominent and most consequential scenario that has repeatedly been observed at various stages of execution in real-life systems. Consequences include long-term compromise of IT- and OT systems, with often undetected changes of system behaviour, ranging from increased disruption rates to increased failure rates of components or productivity loss. APT attacks are designed to stay undetected for a long time and to deeply penetrate and compromise the whole system laterally and vertically. This also means that restoration can be very costly and may take a lot of time and effort until the whole system (field, operation, and enterprise) can be considered clean.

Classification

Nefarious Activity [Unauthorized Activities [Unauthorized use or administration of devices and systems], Unauthorized installation of software [-]

ID	Title	System
8	**Plant tripped off-line through compromised vendor (software update by manufacturer) and remote connection to generation unit or equipment**	Generation

Description

This scenario focuses on the security of the communication channel of the manufacturer to upload software updates on power system equipment in the field (in general generation units) per remote access. A threat agent uses compromised authorisation credentials to access a secured remote maintenance network-interface. The interface provides access to a vendor-maintained asset controllable through a distributed control system (DCS). The network access must correlate with a separate call from the vendor to the utility to open a conduit to the interface. The threat agent then drops a modified system file that further attacks the local DCS network, either by flooding the network, or by compromising further devices within the network. In order to affect a large area, multiple similar attacks have to be executed in parallel. The threat otherwise affects only a single DCS and all attached assets.

A variant of the scenario establishes a foothold in a DCS and uses this access to further progress into different parts of the system. The elevated trust potentially assigned to a utility's "own" devices is exploited and used to access larger control structures, for example through an uplink to a control room. The threat might also be the first stage of a coordinated load-changing attack that potentially affects the whole system [35].

Example

Real incidents: No real incident description public available

Impact

The vulnerability underlying this scenario is very common and often a result of misconfiguration or "shortcuts" around security measures. The impact is usually limited to a single generation unit but depending on the capacity of the unit and the destruction effected, the impact can be substantial. Effect may be long lasting due to extensive restoration necessary. The threat is difficult to detect because the most common attack vectors imply circumvention of detection mechanism and provide pretext for unusual interaction and behaviour of the components involved.

Classification in ENISA Threat Taxonomy

Nefarious Activity [Manipulation of Hardware and Software [Alternation of Software, Rogue Hardware]]

ID	Title	System
9	**Compromised distribution grid management through supply chain vulnerabilities**	Supply Chain

Description

Lifecycle attacks against equipment (in general generation units) during development, production, shipping, and maintenance can introduce deliberate errors that will result in failure under special conditions. For example, a threat agent might upload modified firmware in a relay during production that introduces a back door for changing relay settings and set points. This could render the relay inoperable or cause it to operate unexpectedly.

The functional integrity of digital systems is based on functional assumptions of the whole hardware and software stack. This implies, that the whole supply and maintenance chain, starting from the design process, is protected against code injections. Any modification potentially has a catastrophic impact that not be detected for a long time. The recently publicized vulnerabilities "Meltdown" and "Spectre", which affected whole design series of microcontrollers [Kocher 2018], provide an example of the possible scale of the number of involved devices in case of such issues. Large-scale industrial

installations are considerably vulnerable if they rely on a very limited number of manufacturers of parts and sub-parts of the system.
This scenario addresses also infiltrated hardware from third-party countries.

Example

Real incidents: In 2016 United States of America Department of Defence issued a warning to refrain from using Lenovo Microcomputers due to the threat of these devices being compromised on the microcontroller level. Similar warnings have been issued in Great Britain by the intelligence agencies. [11]

Due to the complexity of validating — especially hidden — extra functionality in microcontrollers, as well as firm- and software, the threat poses a substantial risk if nation states are considered as potential threat agents.

Impact

Compromise to the integrity of a supply chain is subverting the fundamental assumption of defined behaviour and attributes of components, which may enable the attacker to gain arbitrary access, depending on the component and the deployment of the component. This access can be used for large-scale disruption, damage and will most likely be undetectable except for the effect. Effects will often be attributed falsely to other causes, because the usually high trust that is attributed to fundamental components. This specific scenario limits the impact to a single component, but the attack vector could impact a large number of components that use common sub-components and thus could lead to a widespread disastrous impact.

Classification in ENISA Threat Taxonomy

Nefarious Activities [Unauthorized Installation of Software [-]]

ID	Title	System
10	**Weakened Security during Disaster**	IT/OT-System

Description

A threat agent could take advantage of the confusion, lack of security, and hasty reconstitution of the distribution grid after a disaster. For example, a threat agent could delay the recovery effort by leveraging temporary communications with low security to access a DMS towards switch breakers. Likewise, this objective could be achieved by subverting weak physical security at substations (due to damage or communication outages) to access engineering or console ports or relays to change settings and render them inoperable. Further, the interception of temporary communications with low security might support reconnaissance of high-priority vulnerabilities to aid in future attacks.
Physical or remote access must be enabled for personnel to access facilities and assets. Especially in times of emergency, access points may stay open for a prolonged time with little access control due to strained resources. Opportunistic threat agents can use this lowered access control to physically or remotely access consoles and remote interfaces to persistently compromise the system by deploying remote access toolkits of various designs.
Compromise results in unauthorized remote access to individual systems that may stay undetected for a prolonged time, which would allow the attacker to extend his access to various parts of the system.

[11] DOD Issues Cybersecurity Warning Against Lenovo Computers, Handheld Devices, FEDmanager on 25 October 2016, https://www.fedmanager.com/featured/9-general-news/2608-dod-issues-cybersecurity-warning-against-lenovo-computers-handheld-devices

Example
Real incidents: No real incident description public available

Impact
Persistent remote access is likely gained that may be used for long-term objectives or as a foothold for consecutive operations. Immediate threat extension may turn a critical emergency into a catastrophic event. The likelihood of a successful operation thus is limited, due to the time available for the actual attack and potentially limited capabilities of predicting the emergency situation.

Classification in ENISA Threat Taxonomy
Nefarious Activities [Unauthorized Installation of Software [-]]

ID	Title	System
11	**Unauthorized Mass Remote Disconnect Through Firmware update**	Smart Meter

Description
A threat agent prepares smart meter firmware containing malware and manually installs it on a target smart meter in each neighbourhood. The single insertion point in each neighbourhood becomes the bot master for a smart meter based botnet. The bot master acquires the IP address for the neighbourhood's headend at the utility and spoofs that address. As other smart meters attempt to connect to the headend, the bot master sends a firmware update command to the smart meters and transmits the malicious firmware to each victim. Individual bots propagate the malicious firmware throughout the neighbourhood and use them to achieve a mass remote disconnect scheduled at the same time.
This threat scenario extends the more generic threat of malicious firmware updates onto a widely distributed, high-volume set of homogeneous, low-criticality devices. Even considering strict diversity requirements as given, a threat agent could gain access to a large number of smart metering devices with only a single, widely distributed vulnerability found in the system. In the near future this might provide the threat agent with control over high load capacities. The wide distribution thus increases the impact of small attack capacities, i.e. capabilities to exploit a limited number of vulnerabilities in a small number of device classes.

Example
Real incidents: No real incident description public available

Impact
Wide area sensor and billing functionality is lost to the utility, compromising market participation but also system stability depending on the size of the loss. Immediate revenue loss may be buffered and reserves may be available for secure system management, but reputation of utility is severely damaged.

Classification in ENISA Threat Taxonomy
Nefarious Activity [Manipulation of Hardware and Software [Alternation of Software]]

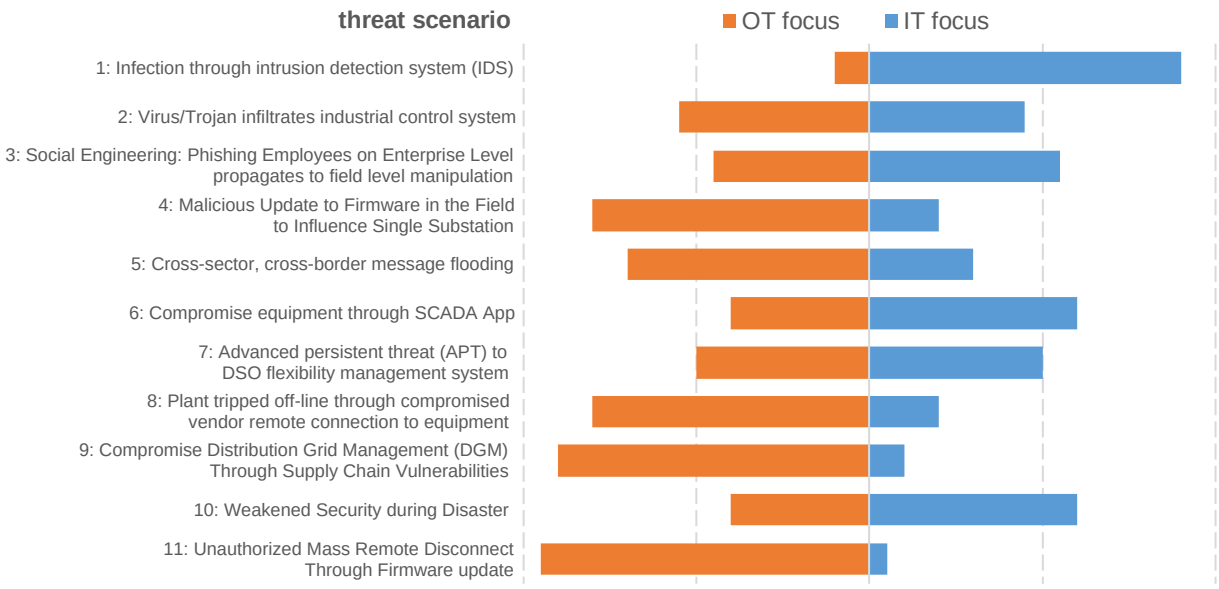

Figure 8: Relative OT versus IT focus of developed threat scenarios

Cybersecurity is a discipline that covers many sectors in modern society and economy and is often seen as an IT discipline. For energy systems the additional complication and increased sense of criticality comes from possible OT domain vulnerabilities which are becoming more prominent and are more time consuming to address. Figure 8 provides a qualitative view on how much each of the selected high-priority threat scenarios focuses on either IT or OT vulnerabilities. This classification is an own estimate from experts in the study team. The estimations consider a general classification of involved systems that are compromised in the threat scenario. The graphic also clarifies that this study covers both OT and IT aspects in the scenario generation, though more predominantly the OT domain which is a specific criticality in the energy sector.

3 Existing measures for cybersecurity

KEY MESSAGES

Various mitigation measures can be applied when handling threats in the European energy system. Over time the discipline has gained maturity. Regulators, standardisation bodies and industry sectors have documented best practices to deal with threats imposed to systems interfaces and business processes.

This Chapter 3 presents an overview of basic cybersecurity principles and existing risk mitigation frameworks to support safe and secure operations in the energy sector. Also, the relation between various frameworks (e.g. ENISA and NISTIR7628) is addressed to clarify its structure, its system and regulatory context (which differs e.g. in EU and US), and existing gaps when mapping the catalogues.

Presently most EU system operators and authorities are triggered to review and implement cybersecurity strategies as a result of the implementation of the NIS directive which is cross-sectoral. This study surveyed European electricity and gas TSOs and DSOs to gain understanding on which practices are applied, which cost and other challenges their cybersecurity strategy faces and which threats and need for coordinated national/European action they see. Input from 20 organisations is synthesized. First and foremost, the limited response to this survey demonstrated the challenge in collecting data from a large set of operators on a topic which is strategically sensitive, complex and in some cases bound by legal confidentiality obligations. The response rate and aggregated results are in line with surveys from other studies and reports highlighting the uncertainty of present strategies, maturity and expenditures. The feedback from this set of operators shows how organisations across Europe are at a different maturity level still, and face common challenges of applying existing frameworks, getting organisational buy-in and attracting expert staff. The chapter discusses how maturity models can be used to identify weak points in an organisation's processes, to setup longer term roadmaps to advance its cybersecurity effectiveness and link it to needed budget.

In Chapter 4 a risk management analysis is performed using the ENISA mitigation catalogues. In Chapter 5 projections are made for how maturity of organisations across Europe can advance depending on different policy options, and how their budgetary efforts relate.

Main sources that guided the analysis of this project are the following:

- **Existing guidelines and standards:**
  - ENISA: Appropriate security measures for Smart Grids - Guidelines to assess the sophistication of security measures implementation
  - NISTIR 7628: Guidelines for Smart Grid Cyber Security

  - NIST SP 800-53: Security and Privacy Controls for Federal Information Systems and Organisations
  - ISO/IEC 27019 series on Information technology -- Security techniques -- Information security controls for the energy utility industry
- **Recent studies and surveys:**
  - European Smart Grids Task Force Expert Group 2, Interim Report 2017 [27]
  - European Smart Grids Task Force's Best Available Techniques for cyber security and privacy of the smart metering system [36]
  - The RASSA Initiative – Defining a Reference Architecture for Secure Smart Grids in Austria [37]
  - Protection and security analysis as part of the development of smart grids in Switzerland [38]
  - SIKT – Secure information and communication technologies for an intelligent energy network [39]
  - NREL: States of Cybersecurity: Electricity Distribution System Discussions, 2017 [40]
- **Feedback from system operator survey and expert interviews** conducted in this project (Section 3.3)

3.1 Basic cybersecurity principles

This section provides a short overview of basic principles and existing frameworks for cybersecurity measures. General cybersecurity principles describe how cybersecurity measures can be understood and approached to protect cyber assets. In addition to the basic principles various international frameworks exist. Each framework addresses a unique aspect or specific domains, like the energy system, of cybersecurity implementation and maintenance.

Cybersecurity measures cover the practice of defending information from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction. Cybersecurity is a general term that is used indifferent of the representation of data (e.g. electronic, physical). Cybersecurity is an adoption of the terminology of computer systems, which in turn, goes back to three fundamental objectives defined early in NIST Handbook 1995, also referred to as CIA-Model:

- ***Integrity:*** Information is timely, accurate, consistent, and complete.
- ***Availability:*** Services are provided to authorised users in a prompt manner.
- ***Confidentiality:*** Information is only disclosed to authorised entities.

Various more detailed security sub-objective categorisations of these main principles exist of course. Integrity of information especially ensures authenticity, i.e. information is genuine, as provided by the source of the information. While cybersecurity in typical IT domains often puts more attention on confidentiality, for reliable system operation of energy systems the integrity of data exchanges may be considered most crucial.

ICS security reverses the prioritisation of the three objectives compared to classical IT security. In the IT world, usually confidentiality is the primary security objective as data and information make up the primary items-of-interest and confidentiality cannot be re-established once it is compromised. Confidentiality in communication or storage of data needs to be established before transmission and storage and ensured continuously over the whole lifetime of the protected (data-)object. Integrity protection, including authentication, can be established a posteriori and outside

the explicit context of storage or transmission. Compromised or unavailable authentication usually can be re-established, making it less critical as compared to confidentiality assuming there are no temporal availability requirements. Generally temporal requirements in IT-applications are less strict than within ICS-application (or other cyber-physical applications).

Security priorities in the ICS world are usually the other way around. Many applications require prompt and reliable response, while service downtime could often mean interruption of the whole production process, irreversible damage to goods or machinery or even health and safety issues. Availability generally is of the highest priority. A similar argument prioritises availability next in line, as acting on wrong information, e.g. maliciously injected commands, may even have worse results than no action. Confidentiality is important but relatively less critical. Most information transmitted and stored within a typical ICS control process are not confidential, or disclosure of this information has no immediate substantial impact to processes, products or personnel.

The objective of any specific cybersecurity framework is to provide mitigation in-depth. A typical applied cyber-environment at the energy system uses many different threat mitigation technologies to be able to minimize the success of a cyberattack at multiple levels (see Figure 9).

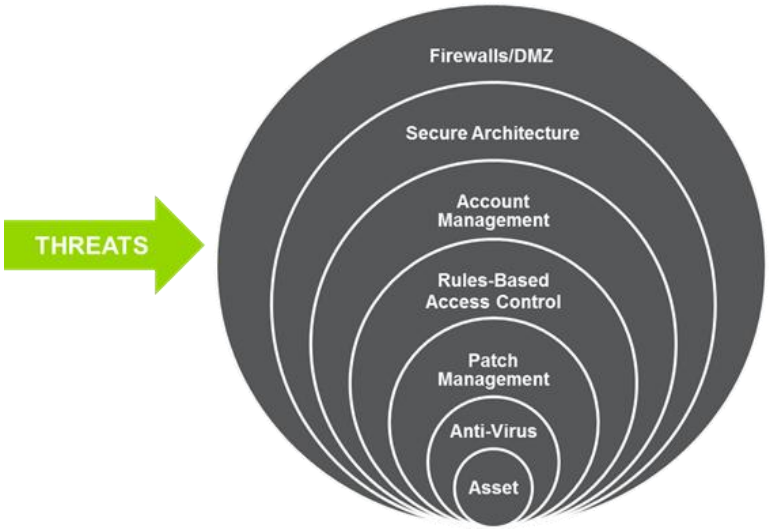

Figure 9: Illustration of mitigation layers, source: Navigant

3.2 Existing frameworks and guidelines for cybersecurity in the energy domain

A number of cybersecurity frameworks and guidelines are applied in energy systems worldwide.

- **ENISA guidance:** The European Union Agency for Network and Information Security (ENISA) developed specific security measures for smart grids. The document provides a set of minimum security measures for smart grids which enhance the minimum level of the addressed cybersecurity services. The proposed

measures are organised into ten domains (see overview in Table 3). Though ENISA is not only focusing on energy, the related guidelines and reports are still very much relevant for the energy sector and cover the monitoring of information sharing, and guidance on industrial control systems.

- **NISTIR 7628**: The National Institute of Standards and Technology (NIST) is a non-regulatory federal agency within the US Department of Commerce. NISTIR 7628 is a specific NIST guideline for cybersecurity of IT/OT systems in smart grids. The guideline describes an approach to identify cybersecurity aspects for classified system interfaces and to map and adapt specific security requirements / mitigation measures.
- **NIST SP 800-53:** NIST provides a generic cybersecurity framework applicable to various sectors. It consists of five concurrent and continuous functions: Identify, Protect, Detect, Respond, and Recover. These functions are a high-level summary of the lifecycle of cybersecurity risk management. Each core element is developed to identify associated key categories and subcategories for each function. For each subcategory, there are associated standards, guidelines, and practices.
- **NIST Framework for Improving Critical Infrastructure Cybersecurity** (Version 1.1, 2017/12): The NIST CIC Framework focuses on using business drivers to guide cybersecurity activities and considering cybersecurity risks as part of the organisation's risk management processes. It can be used in any domain and is independent. The framework consists of mostly three parts: (I) Framework Core, (II) Framework Profile, and (III) Framework Implementation. The Framework Core is a set of cybersecurity activities, outcomes, and informative references (domain-independent) that are common across sectors and critical infrastructure. Elements of the Core part provide detailed guidance for developing individual organisational profiles. Using profiles, the framework will help an organisation to align and prioritise its cybersecurity activities with its business requirements, risk tolerances, and resources. It provides a mechanism for organisations to view and understand the characteristics of their individual approach to managing cybersecurity risk, which will help in prioritising and achieving cybersecurity objectives for their specific organisation.
- **ES-C2M2 Framework:** The Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2) was developed as a tool to enhance the security and reliability of the electrical grid (see also section 3.7). The intent of a C2M2 exercise is like the use of NIST framework profiles, but C2M2 is intended to be a comprehensive and enterprise-wide measurement tool centred upon ten areas. The ES-C2M2 evaluation is designed to assist organisations in identifying specific areas of competency to strengthen their cybersecurity program, prioritise cybersecurity actions and investments, and maintain the desired level of security throughout the IT/OT systems' life cycle.
- **NERC CIP:** The Critical Infrastructure Protection (CIP) standards from the North American Electric Reliability Corporation (NERC) was established by the electric utility industry in the US and Canada, as well as Mexico through a Memorandum of understanding. The CIP lifecycle approach is segmented into six areas of activity: Analysis and Assessment, Remediation, Indications and Warnings, Mitigation, Incident Response and Reconstitution. The first three activities take place prior to any actual event or incident. The last three activities take place during and after a cybersecurity event. Where most measures focus on the practical 'what to do' aspects, NERC CIP focuses on 'how' organisations should organise themselves.
- **BDEW and Oesterreichs Energie** Whitepaper from 2011 and its recent update in 2018 [41], which is widely used by German utilities and manufacturers of power system equipment, provides a selected subset of ISO 27002 / ISO 27019.
- **UK NCSC Guidelines:** The National Cyber Security Centre in UK provides an exhaustive collection of guidance documents addressing generic cyber security recommendations, regular and current threat

intelligence analyses as well as specific guidance for selected industrial sectors. The documents span the complete risk management and security process. Structure is provided by “collections” which curate contents for specific industrial sectors or topics, e.g. “10 Steps to Cyber Security” or “NIS Guidance Collection” [25].

- **IEC 62351** on ‘Information Security for Power System Control Operations’ provides a set of documents describing best-practise technologies for implementing selected security solutions in power systems. The document series is not providing a taxonomy for mitigations but recommendations how to implement recommended security systems.
- **ISO 27019** on ‘Information security for process control in the energy industry’ (based on ISO27001)
- **IEC 62443** is a series of standards and reports on cybersecurity for Industrial Automation and Control Systems (IACS)

3.3 Focus on European system operators

Most current studies on cybersecurity cover general overviews of generic threats, actual incidents or available frameworks. A comprehensive European or international overview of the status of applied cybersecurity measures and best practices of implementation does not exist. This can mostly be attributed to the high dynamics in this domain, the wide diversity of maturity, and the sensitivity (and thus low incentive for transparency) on applied measures and strategies.

The main direction for many energy system actors in Europe is set by the European NIS directive, covered in section 3.3.1. To assess how organisations address cybersecurity risk management, this study used an own survey and extended expert interviews to get more insights on the specific measures and best practices in the field, covered in section 3.3.2. This complements the public information on best practices. As experienced in other published surveys on cybersecurity in the energy sector, also this survey had a limited response rate (20 in total) despite communication support from system operator associations.

Note: Responses were received from across Europe, though mostly from TSOs (17) and larger DSOs (3). The written responses and conducted interviews did confirm large diversity in maturity and main organisational challenges. Nevertheless, it is emphasized that the sample size to present an overview of measures in place is very limited compared to the total number of operators active in EU28. When the sector or authorities seek in future more substantiated monitoring info on measures, costs and barriers, it deserves further attention how to incentivize or oblige data sharing (see also Chapter 6 on regulatory recommendations).

The survey invitation was sent via sector organisations to all European TSOs (electricity and gas) and a group of DSOs. In addition to the written survey, additional expert interviews were conducted to further assess the national status on cybersecurity organisation given the NIS directive implementation, as well as main experiences from the organisations over past years. Engagement with the operators and clarification on the objective of the approach was

done via the European sector organisations ENTSO-E, GIE and ENCS[12]. This report does not make reference to individual responses and provides overall responses and anonymized individual experiences.

3.3.1 Building on the NIS directive

Most operators indicated that the legislative basis for cybersecurity is mostly driven by national implementations (done or anticipated) of the NIS directive, which assigns TSOs and part of the DSOs as operators of essential services. Though not explicitly covering cybersecurity, also the GDPR, and to some extent the older Critical Infrastructure Protection directive have driven national and organisational cybersecurity strategies. Also, regulators give increasing attention to cybersecurity governance.

At present the NIS directive is still not transposed in all EU countries (see Figure 10). Nevertheless, in many countries where no transposition is done yet, authorities have engaged with national system operators and sometimes set out national strategy or vision documents.

[12] ENTSO-E was addressed as being the single association of all European TSOs in electricity. Communication was facilitated via ENTSO-E's dedicated Expert Group on cybersecurity which has points of contact with all members. For gas TSOs the engagement ran through GIE who has cybersecurity taken up in its internal work streams; note that ENTSO-G has no dedicated activity in this domain. To collect input from DSOs, the survey was addressed via ENCS. Presently ENCS covers 16 DSOs in electricity and/or gas among its members from Continental Europe, Baltics and Scandinavia and from various sizes. It is assumed that given their membership these are more advanced in cybersecurity implementation, considering also that Europe's power system covers more than 2,000 DSOs (in electricity) with strongly differing legacy and size.

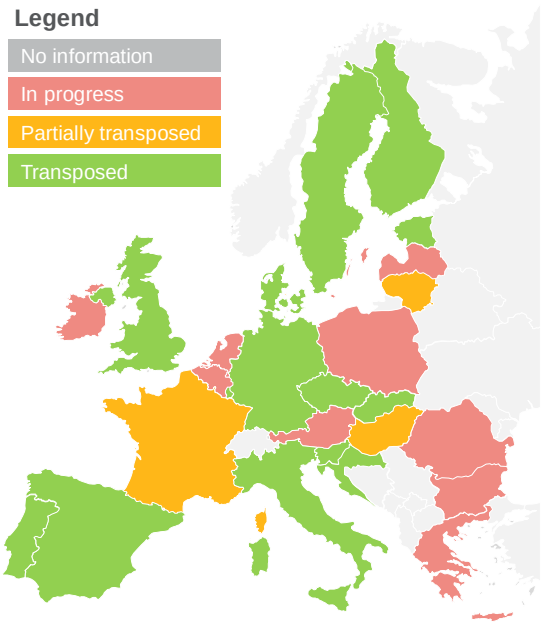

Figure 10: Overview of present national implementation progress of the NIS directive (status September 2018). Not depicted: Malta (in progress), and Cyprus (transposed) [source: Ecofys based on EC]

The situation of two countries having not transposed the NIS directive, but having national strategy or vision documents in place, are given as example cases:

- In the Netherlands the Raad voor Leefomeving en Infrastructuur published a report on "Stroomvoorziening Onder Digitale Spanning" in 2018. This policy recommendation from the Dutch governmental advisory council on Environment and Infrastructure considers that a full system view is needed to cope with cybersecurity in the energy sector. It urges for more research on the impact of digitization of the energy sector, to cope with preventive measures in standards, more joint fact finding, and European-wide rules in product certification and network codes [42]. The council's recommendation also consider the call of the Dutch cybersecurity council [43] for a clear legislative framework on responsibilities of all actors in a more digitized economy (not restricted to energy) e.g. via liability measures for vendors, more awareness via information campaigns and product labelling, and clear certification of products. If EU measures do not provide sufficient clarity soon, then national measures on procurement should be enacted to provide this clarity.
- In Portugal the government adopted a resolution on a "Estratégia Nacional de Segurança do Ciberespaço" in 2015. The Portuguese national strategy does not provide specific measures or energy specific analyses. It enforces main principles to guide further measures, including subsidiarity between authority and individuals, complementarity roles of various actors, need for cooperation, proportionality and sensibilization. This strategy guides discussions between regulator, ministry and system operators.

The impact of the NIS directive differs by country as some relied on existing legislation already, while for others this domain had no clear framework yet. In any case, all interviewed stakeholder experts agreed one of the main

contributions of the NIS directive is the awareness it creates, either within the organisation to give high-priority (resources/budget) to cybersecurity as a cross-organisational domain, as well as in discussions with national authorities. Across countries where the NIS directive has been transposed, the national guidance takes a cross-sectoral approach (as the directive itself) which thus not capture the peculiarities of the energy sector.

A selection of countries which have implemented the NIS directive illustrate the variety in application:

- Germany: The NIS Directive was implemented in Germany mid-2017, building on the 2015 national IT security law. A legislative framework on cybersecurity for critical infrastructures (KRITIS) includes among others the following:
    - Suppliers of critical infrastructure are required to apply the technology which is commonly used ("Stand der Technik") for IT security and are required to inform the Federal Office for Information Security (BSI) of severe incidents.
    - An expanded role of the BSI is foreseen with more enforcement and supervisory powers.
    - The implementation is a complement to the existing law on IT security. Providers of cloud-computing-services, online market platforms etc. need to comply with minimal standards and reporting obligations. It is anticipated between 500 and 1.500 enterprises are affected by the new rules
    - The BSI is implementing Mobile Incident Response Teams (MIRTs) of cybersecurity experts which can be dispatched to investigate and resolve severe cyber attacks on-site if the supplier of critical infrastructure asks so.
    - The German IT security act makes ISO27001 certification mandatory for energy and gas system operators as well as large generation plants. The regulator also published a catalogue with further IT standards for energy companies ("IT Sicherheitskatalog").
- UK: The NIS directive was implemented in May 2018 in UK. Non-compliant organisations can be fined up to 17 million pounds depending on the specific sector. Businesses operating in critical industries must comply with 14 high-level security principles including
    - Managing security risk: Governance, risk management, asset management, supply chain
    - Protecting against cyberattack: Service protection policies and procedures, identity and access control, data security, system security, resilient network and systems, staff awareness and training
    - Detecting cyber security events: security monitoring, anomaly detection
    - Minimizing the impact of cyber security incidents: response and recovery planning, improvements

  Operators of essential services will be monitored through audits by the competent authorities. Digital service providers will not be audited but can be subject to investigations. The UK NSCS published an extensive set of guidance documents (see section 3.2). Note that the UK also builds on a longer track record of public guidance, most notably with the 2014 Cyber Essentials Scheme which gives practical steps for small and large organisations (not energy specific) and accreditation tools.

3.3.2 Measures in place

This section summarizes applied practices at European TSOs and DSOs based on feedback from a survey conducted in this study. For a full list of questions see Annex 8.12. Further interviews were conducted with experts to clarify provided data and gain more understanding. As stated before it is emphasized that the response rate in the

survey conducted in this study was very limited, despite active support of and engagement with the sector organizations. The low response rate is also observed in other public cybersecurity related reports and underline the sensitivity of sharing information on this topic and the challenge for regulatory authorities and policy makers to have a view on common practices and efforts. The results cannot be considered accurate in terms of statistical distribution of practices across all European TSOs and DSOs in electricity and gas. Nevertheless, the response do already underline diversity in practices. Also a hypothesis is that respondents willing to share information have an above average cybersecurity maturity level and experience. This is especially relevant considering the few thousands smaller DSOs active in Europe for which factual information on present practices is lacking.

Most respondents have an organisational cybersecurity risk management approach and incorporate cybersecurity in their Enterprise Architecture Management. At least half of the system operators perform annually an enterprise level risk assessment, some have more regular reviews, some only do this every few years.

All respondents having a sound approach in place do apply multiple frameworks. The majority applies ENISA guidance, NIST SP 800-53 and NERC CIP measures (Figure 11). Note that while the ISO27000 series is by several used as guiding strategy, only few operators pursued or are intending to pursue certification.

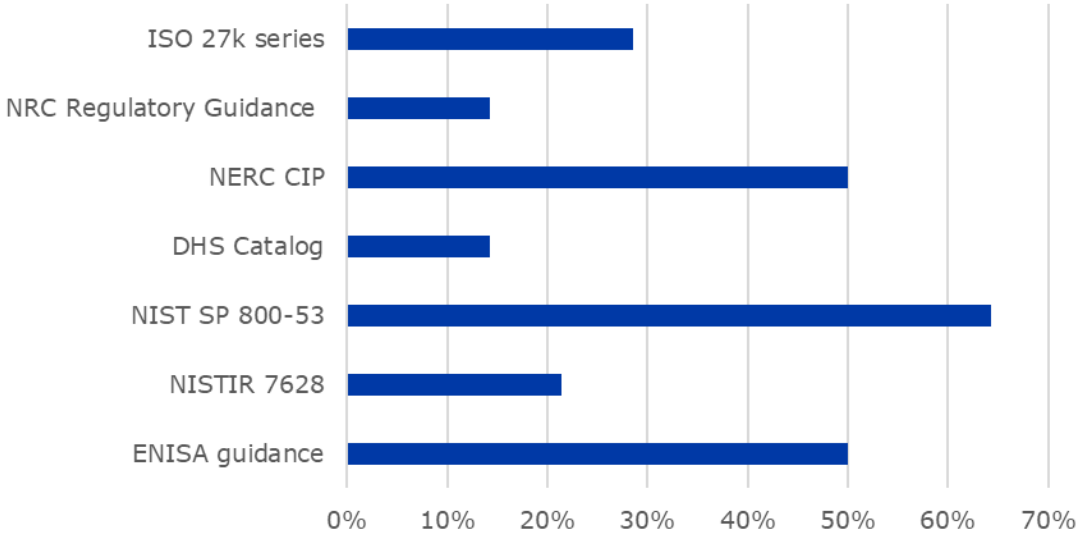

Figure 11: Ratio of system operators applying cybersecurity standards or reference documents in industry [project survey]

The earlier European work in M/490 is not directly used by the surveyed operators for cybersecurity mitigation guidance. However, the M/490 Smart Grid Architecture Model (see also Annex 8.3) is used by some to outline their OT architecture.

All surveyed system operators confirm application of measures that are generic to industrial control systems (e.g. IEC 62443).

The majority of the operators have experienced attempts by phishing, malware and ransomware (which are not unique to the energy system) to be still the most common cyber-attack modes. About half also state attacks possibly occur unnoticed and therefore place great value in forensics analyses.

The main mitigation measures focused on by European system operators can be summarized in following clusters:

1. Awareness and Training
2. Authentication and Access
3. Threat Intelligence and Vulnerability Assessment
4. Firewall (IDS/IPS), Malware Detection

A more detailed view on measure classes applied is given in Figure 12. This list is based on NISTIR 7628. For more information on the context of these classes, and their link with the mitigation classes of ENISA, please refer to Section 3.5 and Annexes 8.4 and 8.5.

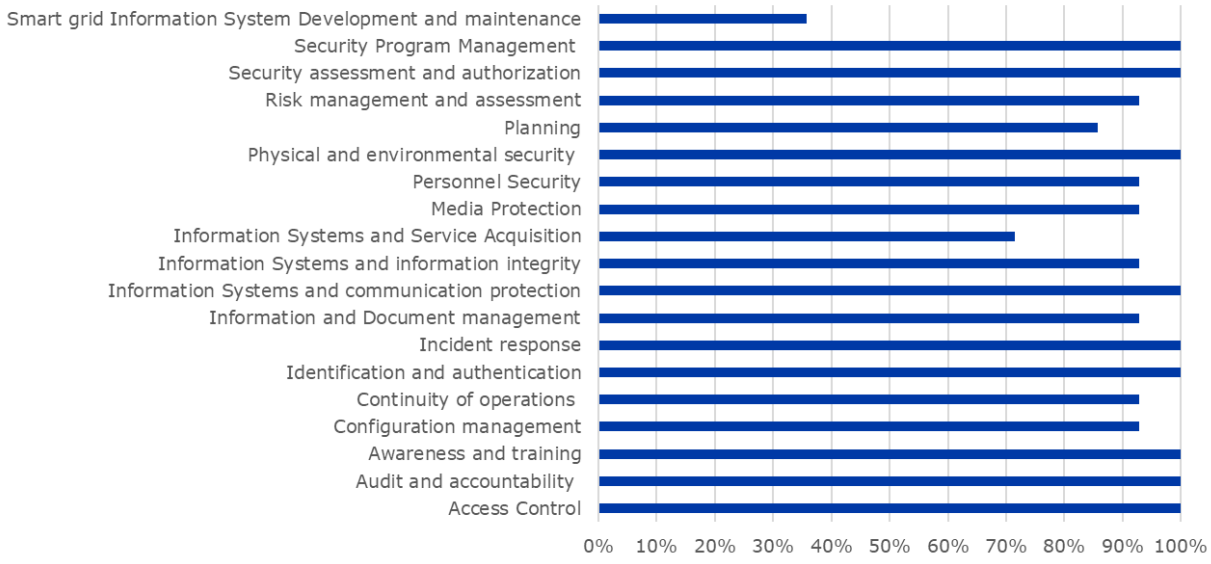

Figure 12: Type of measure classes applied by system operators [project survey, based on NISTIR 7628 classification]

The most recurring priority challenges in stakeholder interviews include the complexity of asset inventories, information system security and the need to ensure safe continuity of operations.

Most operators indicated the risk exposure of cyber threats and the needed annual expenditures have increased over past years. Only few respondents (5) gave insight in the total organisation expenditures for cybersecurity measures. These figures are largely in line still with expert views from the industry, and with market sizes reported by vendors of cybersecurity solutions for TSOs and DSOs. See Section 5 for more info on cost projections. The survey responses and interviews highlighted that most of the costs relate to continuity of operations, SCADA security, and physical security. The number of staff member FTEs involved in compliance checks ranges from one (part-time) for

smaller operators to about ten for larger ones, though the relation with total organisation staffing is not straightforward proportional. Various operators indicated that the main issue with staffing is not just internal budget, but mostly the availability of skilled people with energy OT experience who often opt for other career opportunities then with a system operator.

Also challenges which are common in cybersecurity in various sectors beyond energy, are all deemed very present in the energy sector (Figure 13). This relates specifically to the implementation of new technology and systems, a company-wide shift in mindset across all activities, dedicated training and development for operational and support staff, and as stated earlier most importantly the scarcity of skilled cybersecurity experts.

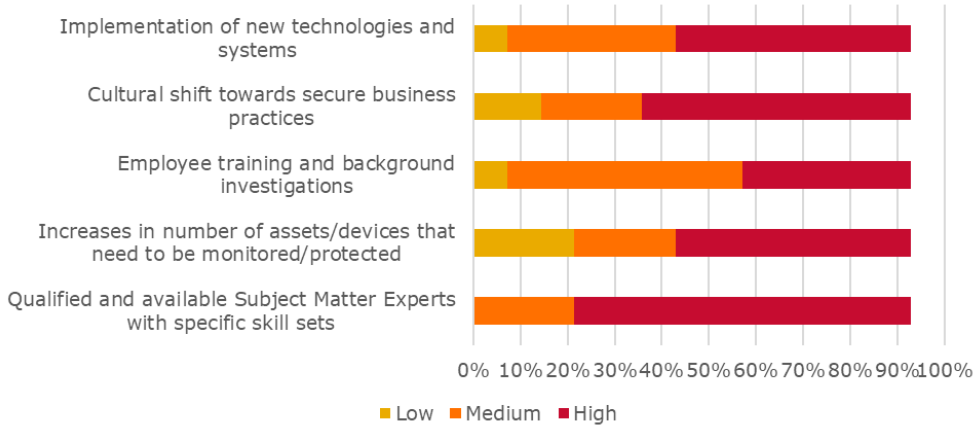

Figure 13: Cybersecurity challenges perceived from low to high by system operators [project survey]

Some experiences from individual organisations are listed which shape the complexity of advancing in cybersecurity maturity:

- All interviewed experts acknowledged the need for senior organisation level buy-in for cybersecurity strategies and for company-wide awareness and cultural shifts. This was raised as a particular concern since cost reduction pressure is high, and cybersecurity programs are often difficult to motivate to senior management or regulators.
- Few organisations have set out long-term roadmaps to accelerate a rise in cybersecurity maturity. Typically, those cycles take several years, e.g. to set up appropriate measures in the SCADA/EMS/DMS, to have an effective usage of a security information and event management (SIEM), to roll out OT security measures in substations including O&M practices, to implement secure lifecycle processes etc.
- Many actors struggle with implementing best practice measures, e.g. due to the unclear link with their existing infrastructure and the unclear link with their normal business processes. All highly value industry knowledge sharing platform and implementation guidance of international standards and national/EU legislations.

3.4 Status of cybersecurity of non-EU system operators

The status of cybersecurity practices in other parts of the world needs to be seen in context of its energy system characteristics and applicable legislation. In literature and wider industry reference is sometimes made to US practices where the system has different reliability performance and other regulatory frameworks compared to EU. This section addresses some practical challenges and experiences from US utilities regarding cybersecurity measure implementation, without linking it to high or low maturity and without assigning best practices which would partly be specific for its system and regulatory context. Further background on US NERC CIP implementation experiences are given in Annex 8.9.

In 2017, the National Renewable Energy Laboratory (NREL) performed a survey [40] on the status of cybersecurity at utilities in the US. NREL prepared a questionnaire of 33 questions segmented in the categories: Demographics, Standards and Governance, Oversight, Planning, Execution and Performance, Support. In total, 250 utilities in the US were contacted. The results are based on a complete set of answers from 22 utilities. Key findings and conclusions for the participants are the following:

- The **biggest challenges** for utilities are the installed equipment basis, budget, skilled workforce, technology availability and maturity. In terms of budget, utilities reported challenges to clearly identify how to account for the costs and the benefits of cybersecurity expenses. Clear regulation or guidelines on accountable costs or types of costs for cybersecurity could address this issue.
- Various number of cybersecurity frameworks and guidelines (e. g. NISTIR 7628, NIST Cybersecurity Framework, ES-C2M2) are used, but NREL sees a **lack of cohesive use of cybersecurity guidelines** and unclear reasons for selecting one instead of another. The authors propose to enhance capacity building via workshops or trainings to identify and clarify publicly available standards and guidance.
- They conclude that **utilities have the tendency to rely on national or local associations**. These authorities and agencies play a key role as first contact for utilities and to provide effective guidance and spread best practices regarding risk assessments and technical implementation from more advanced utilities to less advanced utilities.
- All the participating utilities reported having a cybersecurity team. But **most do have small to very small cybersecurity teams** of 1 to 5 persons (see Annex 8.9). In terms of budget, the majority reported to spend less than 100k USD/year on cybersecurity. In general, this amount represents not more than 10% of the overall IT budget, as a higher IT budget does not necessarily imply a higher cybersecurity budget (see Annex 8.9). Furthermore, costs for IT and OT cybersecurity are often managed differently and result in a **lack of clarity on overall costs for cybersecurity**.

3.5 Understanding the correlations between various mitigation classifications

NIST provides an extensive list of resources on industrial security counter-measures. The risk analysis method proposed in this study (Chapter 4) is rooted in the NISTIR 7628 Guidelines for Smart Grid Cyber Security [44] and the measure class catalogue of ENISA. The NISTIR guidelines provide an extensive and well-structured taxonomy of mitigations that can be used to derive security concepts tailored to individual systems. The NISTIR 7628 is

complemented by further documents as, for example the NISTIR 7628 User's Guide. It is important that the interface architecture underlying the NISTIR 7628 analysis method is adapted to fully suit European power systems (terminology and actors), but still the security counter-measures or mitigations are sufficiently general to be considered directly.

The NISTIR 7628 mitigation taxonomy is part of a history of NIST publications on security mitigations. Most categories for mitigations can already be found in SP 800-12 "An Introduction to Computer Security: The NIST Handbook" dating back to 1995 [45]. Notable as well is the SP 1108 Framework for improving critical infrastructure (2010), which provides a different categorisation of mitigations focused more on security management [46].

Table 2 gives exemplary non-technical and technical measures, categorised by the five main NIST categories.

Table 2: Illustration of exemplary non-technical and technical measures allocated to NIST categories

NIST category	Examples of non-technical measures	Examples of technical measures
Identify	- Cybersecurity audit and maturity study	- Inventories
Protect	- Cybersecurity standards for demand, generation or network equipment communication devices - Supply chain management - Policy enforcement	- Whitelisting - Next-generation firewalls - Network access controls - Encryption - Communication monitoring
Detect	- Security Operations Centre - Vulnerability assessments / cybersecurity testing	- Audit logs - Network behaviour anomaly detectors - Network intrusion detection system - Antivirus/malware protection
Respond	- Incident response plan	- Configuration manager
Recover	- Recovery planning	- System recovery

ENISA has a different history and uses another categorisation for smart grid related cybersecurity. Table 3 shows an overview of applied categories for the NISTIR 7628 and ENISA guidelines for completeness. An injective mapping from ENISA onto NIST can be found in Annex 8.4.

Table 3: Comparison of covered categories of mitigation measures in NISTIR 7628 and ENISA guidance

Categories of NISTIR 7628	- Access Control (SG.AC) - Awareness and Training (SG.AT) - Audit and Accountability (SG.AU) - Security Assessment and Authorisation (SG.CA) - Configuration Management (SG.CM) - Continuity of Operations (SG.CP) - Identification and Authentication (SG.IA) - Information and Document Management (SG.ID) - Incident Response (SG.IR) - Smart Grid Information System Development and Maintenance (SG.MA) - Media Protection (SG.MP) - Physical and Environmental Security (SG.PE) - Planning (SG.PL) - Security Program Management (SG.PM) - Personnel Security (SG.PS) - Risk Management and Assessment (SG.RA)
Categories of ENISA guidance	- Security governance & risk management - Management of third parties - Secure lifecycle process for smart grid components/systems and operating procedures - Personnel security, awareness and training - Incident response & information knowledge sharing - Audit and accountability - Continuity of operations - Physical security - Information systems security - Network security

In [47] ENISA provides a hierarchical taxonomy for security mitigations. The taxonomy covers 39 mitigations ordered into 10 groups of mitigation classes. ENISA further provides a mapping of mitigations onto subsets of the 197 mitigations provided in NISTIR 7628. The analysis conducted in this study concluded that the ENISA mapping is not complete, as it lacks crucial mitigations from the NIST IR 7628, most notably the category “Identification and Authentication”. No mitigation from the ENISA taxonomy includes the missing NISTIR 7628 mitigations sufficiently. The gap between the coverage of mitigation measures provided by ENISA and NIST deserves further research. It may be also necessary to extent the provided list of measures by ENISA to reach the level of coverage of NIST.

It may be discussed whether individual mitigations are crucial for providing security, but Identification and Authentication can be deemed fundamental to many other security mitigations and should be included in any security

recommendation. Arguably these mitigations could be covered by ENISA *SM9.2 Account management*, however this is not mentioned and should be considered in an updated document-map using ENISA mapping plus additional category. The Annex to this study provides a starting point on the mapping of specific measures from these two guidelines (see Annex 8.4 – mapping of NISTIR and ENISA).

A general view on how various guidance sets link together and refer to each other is shown in Figure 14

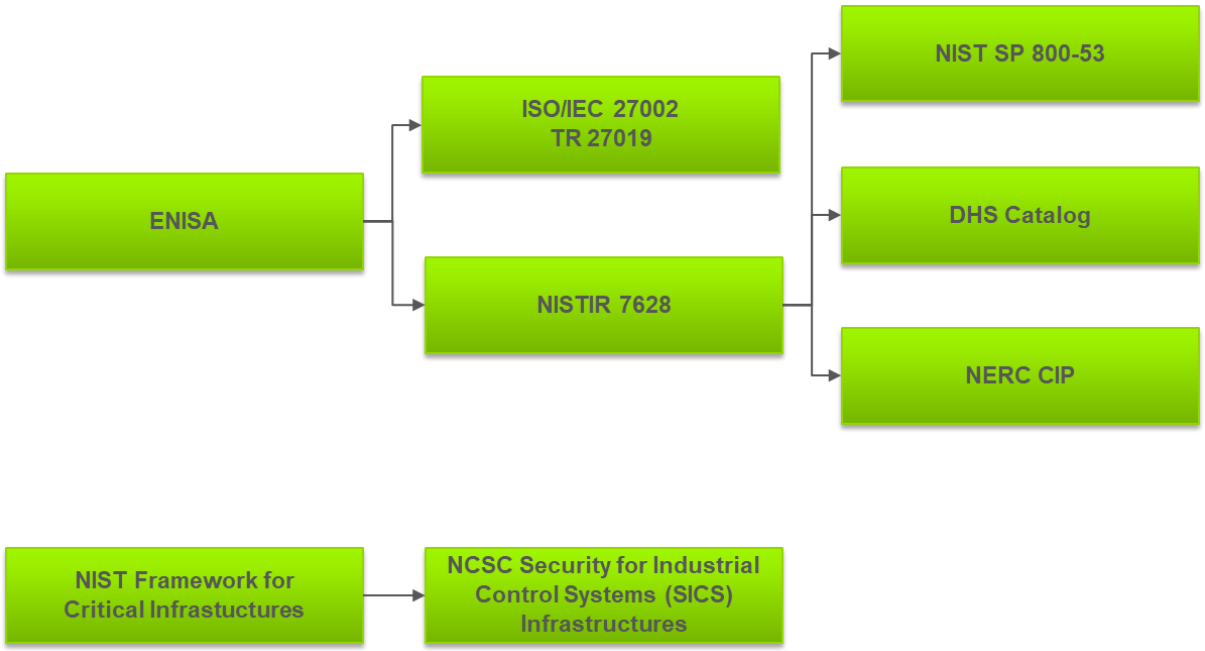

Figure 14: Mapping of mitigation taxonomies from different catalogues

It is important to note that the survey conducted in this study showed that about half of the responding EU system operators tend to refer to US based NIST measures among others for guidance. Also, in various cybersecurity reports from the industry, the US terminology and approach is often a point of reference, although the applied terminology between US standards and EU standards is quite different. Mapping of global standards vs NIST vs ENISA guidance does show that NIST measures are at least more complete as a package. Nevertheless, these NIST measures, as well as the NERC CIP compliance assessments, have in practice suffered issues especially related to proper understanding and lack of focus for smaller utilities. The mitigation list recommended by ENISA has less requirement classes and can be more suitable to non-experts assigning mitigations and prioritising them, e. g. for organisations with lower maturity level. Also, a share of the NIST mitigations are generic and not specific to a certain interface, which should be in place anyhow. Focusing on the more specific ones of ENISA might lead to a better overview for the user. Lastly, specifically for NERC CIP it needs to be emphasised these measures apply only to the electricity transmission system. While it aims to enforce a strong level of maturity, it may not necessarily provide best risk hedging against the weakest links in the system, such as the few assets types which a deemed mature organisation could still not cover, or mass tripping effects in distribution grids.

See also the Annex 8.10 for more background on the US NERC CIP experience. In this study many of the measures considered in the risk assessment methodology do take inspiration from the NIST catalogue. This should not be read as this study advocating to take the NIST catalogue as reference for EU industry or policy. The objective of this study is precisely to identify which aspects pose higher vulnerabilities in the EU energy sector (technical or organisational), and how to mitigate these via several policy options. The analysis in this study will refer to cybersecurity measures in a general manner, and where possible ENISA guidance or international standards.

3.6 Organisational maturity

3.6.1 Type of models

Maturity models are a widespread instrument for the **assessment of processes** (e.g. Process and Enterprise Maturity Model), **software development** (see Capability Maturity Model Integration model from Carnegie Mellon University), business skills (see Organisational Project Management model), **cybersecurity in the energy sector** (see ES-C2M2), and many more relevant issues for applying metrics to. The SGTF EG 2 interim report also highlights the relevance of such model for the European energy system [27].

Overall, more than 100 maturity models and more than 1000 academic papers can easily be found which analyse, refine or develop maturity models. For the scope of this study, focus is put on maturity models in the very context of

- Smart Grids and Critical Infrastructures
- Assessing mitigations (e.g. ENISA recommended ones) based on known best practices
- Addressing technology, organisation and legislation
- Non-compliance driven processes
- Self-assessment for utilities

Despite the diversity of existing maturity models in terms of their objectives, across most of them a lot of similarities can be found, which shows the models aim for more than just assessing a status in a harmonised manner.

Maturity models are step-based models for specific objects, which are decomposed into further units in the concrete analyses. Most of the maturity models measure or evaluate each unit or technology separately. The maturity level provides information about the current state of the observed object. Maturity models serve as evaluation models but can additionally function as explanatory and optimizing models – e.g. what to do when aiming for a higher maturity for a certain process or technology in your utility.

Maturity models can be basically distinguished in two different types of models.

- Related to enterprise cross-cutting issues such as processes or business skills
- To evaluate specific issues such as the Smart Grid or interoperability in energy systems

3.6.2 Benefits of Maturity Models

The benefits of maturity models are that they allow establishing comparable assessments of a present and future status for a certain scope. For cybersecurity, one wants to assess how mature an organisation is in the context of a possible (but still fictional) threat or attack scenario. A maturity can be assessed for both the present level or assessed for a future needed level which needs be achieved by an organisation to cope with future likeliness of a threat. Migration paths between levels must be documented to trigger the organisation to advance its maturity.

An advantage of maturity models is that they inform the enterprise about the current state of development concerning a specific issue. In the case of cybersecurity that implies how mature and cost-effective mitigations to threats must be for risk management according to ISO 27019 or ISO 31000 in general.

Based on these analysis results, optimizations can be deduced. The level of detail for these requirements vary in the different kinds of models. A uniform documentation is compiled during the evaluation process. This documentation can be used for internal communication and coordination, as well as for the communication with external parties. The results of the maturity evaluation are often used in benchmarking processes.

Certain assessments can be done for compliance with a maturity level defined (a profile of an organisational capability to fulfil certain requirements imposed) or could be formally certified as with ISO 27019 certifications. This has relevance in case of a legal framework, but certainly also when no such framework exists. Certain mitigations are very basic protection or organisational governance and provide the very basic level for protection. The C2M2 model proposes to help with a self-assessment facilitator's guide, thus limiting costs and efforts needed by users to implement the use of a maturity model. The mitigations proposed for lowering risks can show how maturely an organisation deals with risks and threats. It also shows how effective the measures taken are in comparison to the costs of lowering the risks, as opposed to accepting a higher risk for an incident to happen.

Another advantage of maturity models manifests when they are being used for individual process improvement initiatives. The main benefit lies in the elicitation of single maturity levels that can be performed and should be performed as a regular process for improvement of the governance of the security processes for operations, planning and strategy at a given utility.

The changes (positive and negative ones) and the overall developments of the company can be consistently recognized by deploying the same procedure, thus keeping track on the implementation of e.g. an ISMS dealing with IEC 27019. This helps to form long-term targeted positioning of organisations and fosters transparent and comparable information needed to cope with threats, risks and incidents taking place.

Depending on the governance, maturity models can also support the identification of weak points or gaps, the introduction of new processes, and the quality control by introducing them. When the model e.g. proposes one type of mitigation to a generic interface in a process, the mitigation shall also be applied to all comparable interfaces. The ENISA list covers a broad range of mitigations which can be applied jointly. This leads to the operator of the infrastructure getting new expert knowledge from the documented state-of-the-art on how specific mitigations should be implemented jointly.

One of the central elements of maturity models, which as well explain the popularity of these models, is the inclusion of experience or best practice procedures of other companies into the concept of the model. This gives each utility the advantage to benefit from the experience of others by using a single model. Still, the greatest benefit is still the identification of existing potential and how these can be used in the future to further transform an organisation.

4 Risk analysis methodology

KEY MESSAGES

This Chapter 4 is the cornerstone of this study and gives a blueprint risk management approach for the European energy sector. The methodology builds on the ISO31000 process, the NISTIR 7628 methodology, as well as the Smart Grid Architecture Model and security levels developed in M/490. The objective is to provide a framework which applies maturity levels and prioritises mitigation measures for specific organisations. Also a high-level pan-European application is done, the recommendations of which feed into a cost projection analysis in Chapter 5.

The approach covers a so-called top-down analysis of logical interface classes based on selected Use Cases, and a bottom-up analysis of threat scenarios. This two-fold analysis allows for a risk assessment when the limited information is available on attackers and attack modes (top-down view), but also when specific attackers or new (future) attack types are considered (bottom-up). It is important to underline that the two analyses complement each other and can be applied as a single integrated risk assessment by a specific organisation.

The top-down approach focuses on pre-defined interfaces, i.e. the entry points of potential attacks. As this step is based on standardised interfaces which are mapped to required mitigation classes, it shows priorities for a full system or specific Use Cases.

It does not show all insight in how new vulnerabilities can be exploited and attacks propagate. The bottom-up analysis does cover full attack trees, but only covers specific defined scenarios and may thus miss vulnerabilities if the list of high-priority scenarios is incomplete. The bottom-up analysis is applied in this Chapter for the high-priority threat scenarios developed in Chapter 2 and covering the ENISA mitigation categories described in Chapter 3. It results in a ranking of ENISA mitigation classes for four highest priority scenarios.

A ranked list of mitigations or mitigation classes can be used as guidance for organisations or authorities. While all potential mitigations of existing mitigation catalogues have their value evidently, a ranking may be useful in case of budget, resource or monitoring prioritisation. The proposed methodology can be applied by individual organisations or national/European agencies or authorities to identify risk profiles, weakest points and priority recommendations. A simple maturity framework based on so-called generic utilities is proposed in this Chapter for European energy companies, which allows to estimate in Chapter 5 how policy objectives to advance cybersecurity maturity to a certain level necessitate specific additional implementations if measures and carry costs.

4.1 Applying a holistic approach to specific parts of the European energy system

This study proposes a risk assessment methodology tailored to the energy system based on ISO 31000. The assessment approach can be applied at various scales:

- By individual energy companies to understand their risk exposure and analyse their cybersecurity strategy;
- By authorities to assess vulnerabilities or threat scenario impacts on national/regional system by analysing an average system, a possible weakest link system, or comparing a number of systems with different maturity; or
- At European level as common framework for risk mitigation.

For the first two uses, the following chapter is relevant in terms of methodology explanation. Further information on specific points is provided in Annex 8.3 to 8.8 and listed references. The third point fits with the scope of this study. This section provides for an application of part of the methodology (bottom-up analysis), taking into account assumptions and simplifications, that serves as risk assessment of the wider European energy system infrastructure.

The methods described and further developed in this study stem from electricity grid security analyses (e.g. the European work on M/490). Given the technical nature of OT devices and processes, various attack scenarios can be considered similar across electricity and gas infrastructure, such as manipulating data on a meter, hacking an IED or RTU. Therefore, the vulnerability of the control infrastructure (communications overlay) has a strong similarity across both domains, while impact in gas systems may be considered less taking into account cascading effects and proliferation of decentralised solutions in the electricity system as highlighted in Chapter 1.

The outcome of this analysis and the recommended measures, will also feed into the cost projections of various European policy options in Chapter 5.

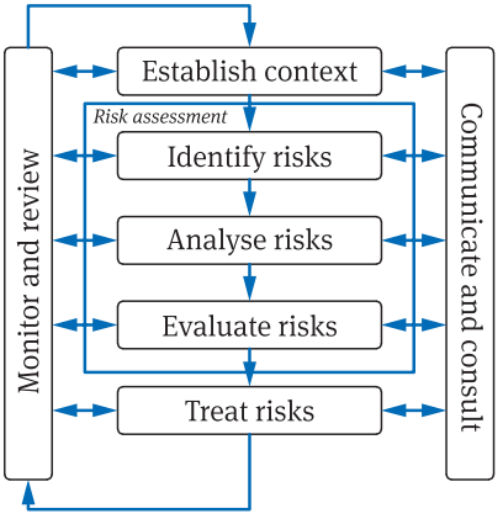

Figure 15: ISO 31000 risk management process

Considering the experience of NISTIR 7628, the risk assessment approach combines a top-down analysis of relevant system interfaces and a bottom-up analysis of vulnerabilities based on threat scenarios. The **top-down analysis** derives security requirements based on the description of Use Case scenarios and security classification of interfaces using a standardised Logical Interface Model (NISTIR). This allows a risk assessment even when the attacker or its operational mode is less known. If on the other hand the attacker is known to a detailed degree, the attack scenario descriptions provide a **bottom-up approach** by analysing existing attack conditions and the potential attack paths towards the critical infrastructure.

- The **top-down analysis** provides a structured approach to derive recommendations for security measures based on documented Use Cases (e.g. in the IEC 62559 or 62913 format) and pre-defined mappings onto logical data interface and their impact categories. Key characteristics are
    - mitigation is based on archetype systems and interfaces;
    - basic protection is achieved implementing those measures;
    - no capture point for an attack is given;
    - basic budget spending can be allocated;
    - integration with M/490 SGIS-SL assessment is possible.
- The **bottom-up analysis** provides additional insights in vulnerabilities of systems and assets, and recommendations taking into account key threat scenarios, emerging attacks and zero-day exploits. Key characteristics are
    - threat scenarios for specific types of attacks are considered;
    - it provides more in-depth information on the attack vector;
    - it relies on knowledge that attack has happened or will likely happen;
    - it provides detailed prioritisation of mitigation needed;
    - capture Information is provided.

An alternative approach could be to assess the application of specific standards like IEC/ISO 27019 which focus on the governance of an information security management system (ISMS). The specific measures of this ISO standard are taken up in the mitigation measure catalogue of the proposed risk assessment methodology.

It is important to underline that the two analyses complement each other and can be applied as a single integrated risk assessment when applied by a specific organisation. Each of the two analyses could also be applied without the other. The top-down approach focuses on interfaces, i.e. the entry points of potential attacks. It does not show all insight in how vulnerabilities can be exploited and attacks propagate. The bottom-up analysis does cover full attack trees, but only cover specific defined scenarios and may thus miss particular vulnerabilities if the list of high-priority scenarios is incomplete. The application of the risk assessment in this study focuses on the bottom-up analyses, as the main objective is to understand the impact and recommended mitigations related to a clearly defined set of priority threat scenarios (Section 4.3).

Both assessments include the existing system architecture and applied cybersecurity measures, as well as existing mitigation catalogues. Figure 16 shows the application of ISO 31000 for cybersecurity in energy systems.

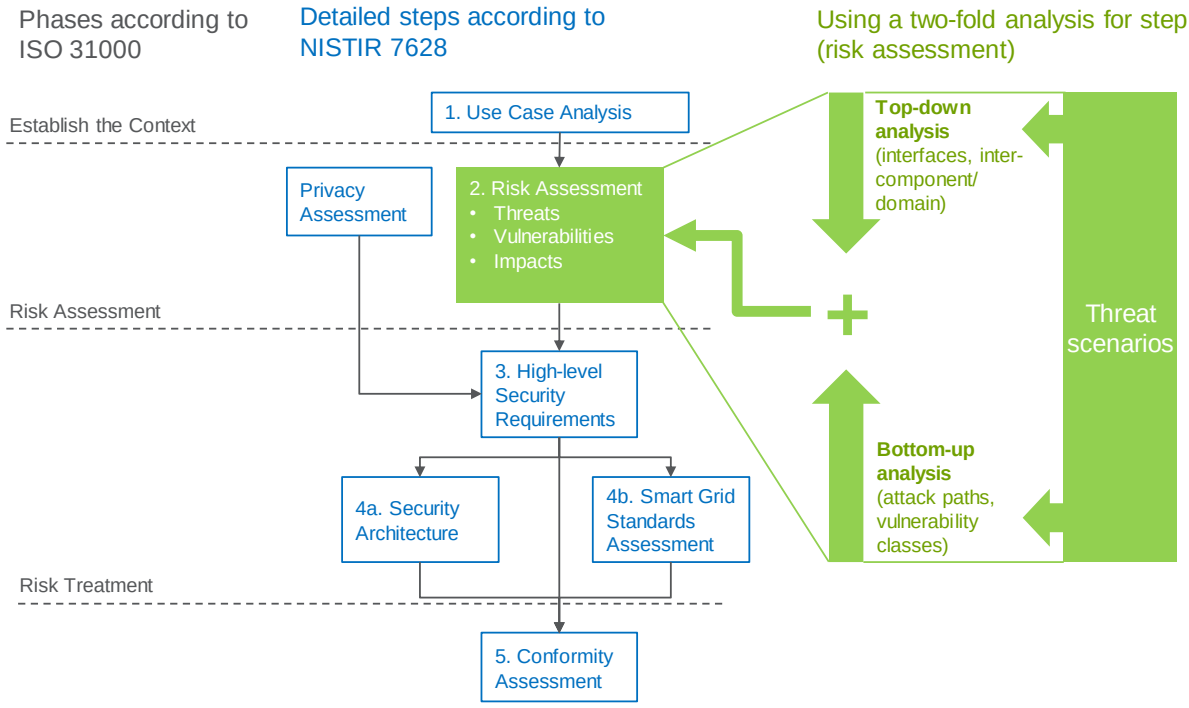

Figure 16: Mapping of NISTIR 7628 Smart Grid Cyber Security Strategy to ISO 31000

Figure 17 provides a more detailed view of both analyses in the risk assessment methodology, which are the focus of this study, and which are further elaborated in the next sections.

For further context on energy cybersecurity risk assessments the reader is referred to [48], [49], [50], [51], [52], [53], [54].

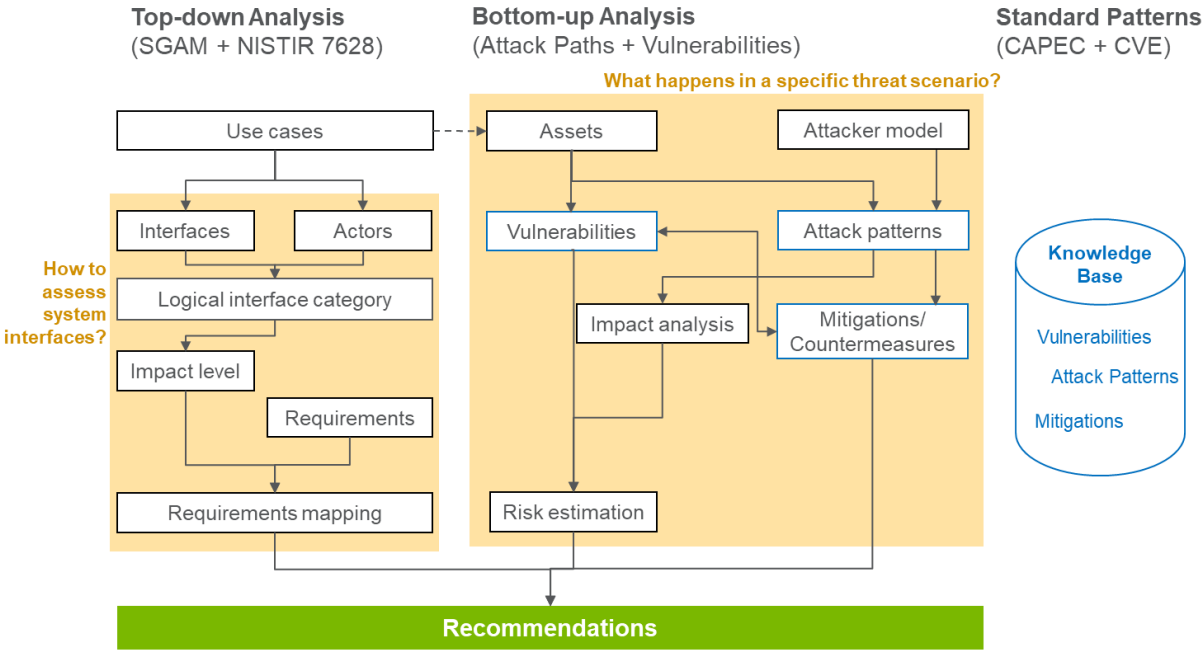

Figure 17: Steps applied in the top-down and bottom-up analysis, based on energy system interfaces, threat scenarios, and specific knowledge bases[13].

4.2 Top-down risk analysis of system interfaces

4.2.1 Methodology based on system model and Use Cases

Step 1 – Set up system model

A model is needed to scope the system in a representative way, which is technology-agnostic and able to take into account ongoing smart grid developments.

It is assumed that the smart grid consists of generic systems and interfaces which can be combined to individual technical bundles of solutions and services, also referred to as Use Cases. Two approaches can be applied. Either one assumes there is a meaningful set of Use Cases which represent the (future) energy system, its components, interfaces and data objects exchanged; an example is the Mandate 490 Use Case list. Alternatively, one can refer to a so-called reference architecture already acknowledged by industry experts; this could be the Mandate 490 Smart

[13] For our knowledge base we use currently most sophisticated databases, like CAPEC or CVE, which are also referenced by ENISA. However, we see a clear need for action to enhance the existing databases regarding OT domain related patterns and vulnerabilities. This would require an extended reporting of OT vulnerabilities to databases, like CVE.

Grid Architecture Model (SGAM)[14], the NIST Conceptual Model for Smart Grid Systems and the NISTIR 7628 data interface architecture. Mapping of the M/490 Use Cases with the NIST model while acknowledging different responsibilities of actors and topologies in Europe and US shows that one can be fully mapped to the other.

Focus is therefore put on the logical interface class concept from NISTIR 7628 which takes the basic assumption that 22 interface types in energy systems exist which are vulnerable to generic attacks and exploits. Note that those can also be combined to a data exchange process in a scenario approach where more sophisticated attack graphs can be assessed to a technology package (see bottom-up analysis).

Such reference architecture includes industrial control systems in the scope of critical infrastructure automation. As such also the gas infrastructure (considered to be an ICS system in the OT domain) can be modelled in a similar and possibly even simpler manner compared to electricity infrastructure which has more critical interfaces in the OT domain.

Step 2 – Map mitigation measures in place

Mitigation measures from various sources can be mapped to the interfaces. It is not always straightforward to state against which attacks specific mitigations are effective. This gap is fine when risk mitigation against a wide range of threats is considered. Still, one should also reflect on the state-of-the-art by taking into account threats which could break individual mitigations. Therefore, Common Attack Pattern Enumeration and Classification (CAPEC)[15] and NESCOR[16] methods are combined with the NISTIR 7628 methods.

Step 3 – Assign risks per interface depending on considered Use Cases

The M/490 Smart Grid Coordination Group published a Smart Grid Information Security (SGIS) report in Dec. 2014 [55]. This provides a high-level guidance on how standards can be used to develop Smart Grid Information Security. It presents concepts and tools to guide stakeholders to integrate information security into daily business. The report recommends Security Levels (SL) for each SGAM Domain/Zone based on type of equipment used and the maximum potential power loss for a given system. These SL-recommendations are depicted in Table 4 and range from 1 to 5, respectively low and high risk.

Initially, those expert estimates were only considered a first hint on where important data and interfaces are located and which vulnerability might manifest itself when data is compromised. It guides organisations in identifying more critical areas in the smart grid domain [55]. Evidently caution should be taken that these numbers may deserve refinement while taking into account specific situations. Nevertheless, it is a simple and at the same time meaningful 5-level taxonomy which can be used for a risk assessment. Simply stated, security level 5 breaches at the transmission/operation domain/zone combination will have the highest system impact. As it is used in various national roadmaps across Europe as a basic input, it shows to be a meaningful and documented way of systems and their data exchanges. The SL thresholds are not revised in this study, nor do any updates exist at European level

[14] See Use Cases and the Smart Grid Architecture Model (SGAM)

[15] Common Attack Pattern Enumeration and Classification public catalogue

[16] National Electric Sector Cybersecurity Organisation Resource

since the conclusion of the M/490 work. It is worth highlighting that for specific national/regional applications other thresholds may be considered more appropriate from a power system stability perspective. The Continental European power system's reserves are designed to cope with a contingency of either a sudden loss of load of 2GW or a loss of generation of 3 GW. Both would relate to Critical security level impact. Smaller synchronous areas (GB, Ireland, Scandinavia) may also consider lower thresholds; note that that the initial SGIS SL levels were considered applicable for all of Europe. However, in some parts of the system (e.g. sparse networks) cascading risks may be higher and lower thresholds could be appropriate. Also, decision makers may argue that type of loads which risk loss of power may need to be differentiated in importance (assigning critical loads).

Table 4: Security level definitions as provided by the M/490 Smart Grid Information Security report

Security Level	Security Level Name	Europeans Grid Stability Scenario Security Level Examples
5	Highly Critical	Assets whose disruption could lead to a power loss above 10 GW Pan European Incident
4	Critical	Assets whose disruption could lead to a power loss from above 1 GW to 10 GW European / Country Incident
3	High	Assets whose disruption could lead to a power loss from above 100 MW to 1 GW Country / Regional Incident
2	Medium	Assets whose disruption could lead to a power loss from 1 MW to 100 MW Regional / Town Incident
1	Low	Assets whose disruption could lead to a power loss under 1 MW Town / Neighborhood Incident

Table 5: Risk levels in the SGAM plane (domain/zone), as provided by the M/490 Smart Grid Information Security report (the levels depicted are explained in the table 4 of this report)

SGIS-SL High-Level Guidance					
Generation	Transmission	Distribution	DER	Customer	
3 - 4	3 - 4	3 - 4	2 - 3	2 - 3	Market
3 - 4	3 - 4	3 - 4	2 - 3	2 - 3	Enterprise
3 - 4	5	3 - 4	3	2 - 3	Operations
2 - 3	4	2	1 - 2	2	Station
2 - 3	3	2	1 - 2	1	Field
2 - 3	2	2	1 - 2	1	Process

The authors of this study make a suggestion to extend this security level notion developed by M/490 with certain aspects of direct effects and attack probabilities. This would follow the principle that risk equals probability * impact. An appraisal of risk for a specific interface could then be provided by the following formula:

$$risk = SL \cdot 2^{DOE} \cdot \sum_{i=1}^{n} API_i$$

This includes the SGIS Security Level (SL) for an interface to include the impact of an attack. The variable DOE is an indicator for whether there are direct operational effects and can have the value 1 or 0. The probability of an event is included via Attack Probability Indicators (API)[17], which are based on quantifications of the hacker's motivation, asset reachability and propagation of secret. Note that this risk assessment is still driven by one or a set of Use Cases considered and does not apply to a system interface generically.

Step 4 – Perform gap analysis to highlight new measures

This results in an assessment of risks per interface class, when looking at specific Use Cases. When using a mapping catalogue of measures vs. mitigation classes, this allows to prioritise which measures to implement in addition. The analysis can be performed for a system with mitigations in place, a system without any mitigations, or a system with all possible mitigations in place. Comparing the results also allows to understand better in a structural manner which mitigations need further attention.

Specific consideration for gas systems

With regards to the SGIS Security Level of the M/490 mandate, the levels can, up to some points be used in the context of the gas sector. However, some special characteristics of the gas sector lower the threats for security of supply here. With electricity risk assessments focusing on simultaneous or cascading effects of generation and consumption, the aspect of the availability of generation as well as loads is much more emphasised than in the gas sector. In contrast, the physical threats imposed by gas leaks are substantial, so small system incidents may still deserve a high-risk rating compared to the electricity sector.

While the effect of reputation loss and loss of customer service can be easily mapped onto the gas sector, there should be a similar analysis on the importance of the gas distribution infrastructure and its systems. The effect of having inherent storage 'smoothens' the effect of assets missing or possibly misbehaving and leads to a different protection goal prioritisation. However, the security needed for RTU, IEDs and various other systems form the control overlay point of view can be transferred from the electricity domain.

While the sense of urgency may be lower in the gas sector, and many security measures similar, there is still value in further research to set appropriate security levels for gas, which would allow for an application of the methodology provided in this study to individual organisations. Such process could again be led by the industry and integrated in common frameworks like M/490.

[17] The API reflects an indicator for the plausibility of attacks, not an assured value.

4.2.2 Assumptions

Some assumptions are taken in this top-down approach, and deserve to be highlighted:

- The Reference Architecture and considered Use Cases are valid representations of the system
- A mitigation measure catalogue is available and considered state-of-the-art
- Black swan detection[18] and prevention is not a realistic aim. Risk management still implies attacks can successfully happen.
- SGIS SL attribution to individual utilities is feasible
- Threats are considered to be sufficiently generic to address most striking issues
- Standards sufficiently represent the domain in terms of threat understanding and risk management
    - ISO 31000 in terms of risk management practice
    - ISO / IEC 27019 in terms of the ISMS governance to be taken
    - IEC 62559 to gather information from involved stakeholders in the risk management process
    - NESCOR based on EPRI work
    - NISTIR 7628 in terms of smart grid cybersecurity mitigations
    - CAPEC as well as OWASP classification are meaningful databases for attacks[19]
- The method does not cover future resilience requirements of a system (and does not cover zero-day exploits)
- Disruptive technologies or events (such as breaking a certain degree of encryption or zero-day exploits in firmware ROMs) cannot be considered, however the top-down analysis provides recommendations on cybersecurity requirements to enable a certain level of security to address not just known threats as the bottom-up analysis is aiming for
- The analysis is static and focuses on hardening the critical systems. Stealth attacks and lurking attackers cannot be taken into account when planning and recommending mitigations. One assumption must be that the measures work best with a clearly unpenetrated system landscape.
- Data protection and security is both subject to EU as well as national law; this approach only considers the vulnerability of disclosures based on the M/490 SGIS DPC method.
- Including ICS assessments and measures is sufficient for risk management of gas infrastructure

The benefit of the top-down approach is it incorporates best practices and relevant international standards in a consistent and transparent approach which can be applied to various energy actors and specific Use Cases. It is based on the following:

[18] Nassim Nicholas Taleb's 2007 book with the same title,calls a 'Black Swan' event something which is highly unlikely to happen, though still possible (with an analogy to a black swan able to survive as a bird in nature). Typically, those events also tend to have a high impact because no one prepares for this low-probability event to ever manifest itself.

[19] A comprehensive database specifically for ICS does not exist at the moment. As the relevant interfaces of intelligent control devices (IED) or remote terminal units (RTU) in the energy system are mostly based on web-based technologies for remote services, it is meaningful to apply and transfer CAPEC and OWASP classification which are comprehensive databases for attacks on web-based systems.

- Anticipated future smart grid market/system operation as reflected in the Use Cases of M/490 (using the approach of IEC 62559)
- Reference architecture from the perspective of IEC 62357, IEC 63097 and NIST
- Standardised vocabulary for the actors based on IEC 60050: Electropedia and M/490, and which in this study is mapped to NISTIR 7628
- Standardised risk management process according to ISO 31000, compliant with ISO 27019 method as recommended by ENISA
- Relevant mitigations for interfaces classes generic in the smart grid based on NISTIR 7628 Vol.1 – 3
- Data protection and privacy by using M/490 SGIS DPC classification as established method
- NESCOR threats database can be applied
- CAPEC Attack classification can be applied
- Selection of "real-life" attack scenarios to check for mitigation effectiveness

As stated at the beginning of this chapter, the top-down approach has its limitations as it does not directly give insights in the possible propagation of an incident after an interface is breached. For understanding specific attack paths, an additional bottom-up analysis is performed, which also enriches the risk appraisal mentioned in Step 3 of the top-down analysis.

4.2.3 Example study

The top-down risk analysis is illustrated by taking the Use Case of "*Optimization of revenue in a local distribution system"*. For further information on how to set up Use Cases (in line with IEC 62559), and how these were applied in the EC initiated work of Mandate 490, please refer to Annex 8.3 which includes also a mapping of use cases on the SGAM model. Figure 18 shows both the Use Case as well as the misuse case of this example. A Use Case depicts an intended behaviour of a system operation or market process. The misuse case documents the non-intended system behaviour such as a cyberattack.

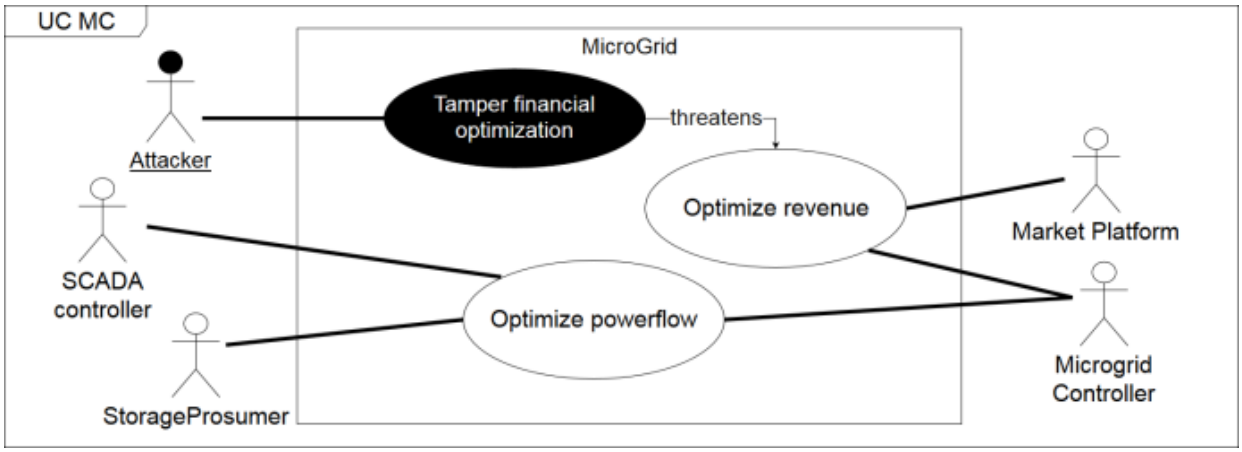

Figure 18: Use and Misuse Case Diagram of "Optimization of revenue in a local distribution system"

The objective of this Use Case is a financial optimization of the energy flow in the system. Four main actors are identified and described. The sequence diagram in Figure 19 represents the interaction of these actors:

- A **microgrid controller (MC)** optimizes the power flow and the revenue of the network region.
- A **market platform (MP)** analyses the market clearing prices for supporting the MC in optimizing the revenue.
- A **SCADA controller (SC)** reacts to the signals of the MC and controls the energy production and consumption.
- A fourth actor combines the producing, consuming and storing actors (incl. wind or a gas turbines, households or cold warehouses and e-mobility batteries) in one actor, called **Storage Prosumer (SP)**.

Figure 18 also shows the **Attacker** who wants to tamper the financial optimization, and which represents a misuse case. All cases are described in clear template structures.

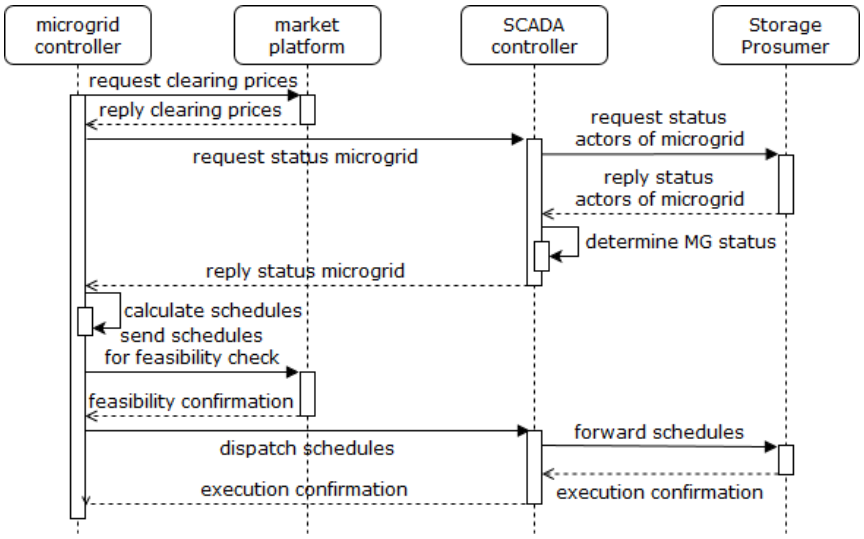

Figure 19: Sequence diagram of the local distribution system Use Case example

Next, the SGAM is used for a structured and standardised representation of the Use Case across domains, zones and layers (Figure 20).

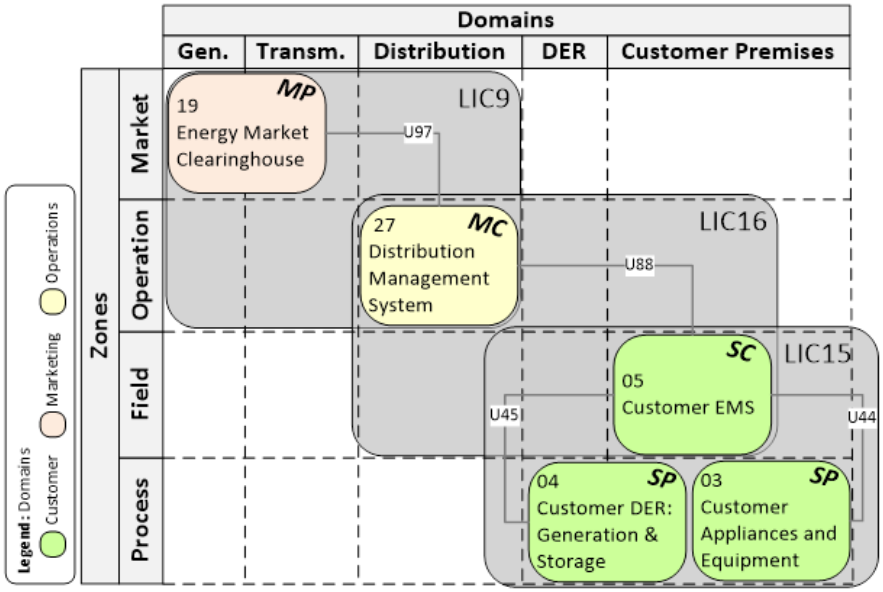

Figure 20: SGAM representation of the Use Case example

The SGAM representation is used in the security analysis. The numbering and main terminology is taken from NISTIR 7628 which can relatively easily be mapped to common definitions and roles in the EU power system. The MC is represented by the *Distribution Management System* (No. 27); the MP by the *Energy Market Clearinghouse* (No. 19); the SC by the *Customer Energy Management System* (No. 05) and the SP by the *Customer DER* (No. 04) and the *Customer Appliances* (No. 03). This is also used to derive the interfaces between the actors and their appropriate Logical Interface Category (LIC), which is also illustrated in the SGAM representation of Figure 20. In a real case study, this process of mapping information on systems to come to a model by which security risks can be assessed, is a process which should be supported by a security and domain expert.

With this allocation, a Confidentiality-Integrity-Availability (CIA) assessment can be done for every interface of the Use Case (Table 6).

Table 6: Interface categories of the Use Case example ((H is high, M is medium, L is low importance requirement))

LIC	Description	C	I	A
9	Interface with B2B connections between systems usually involving financial or market transactions.	H	H	M
15	Interface between systems that use customer (residential, commercial, and industrial) site networks such as HANs and BANs.	L	M	M
16	Interface between external systems and the customer site.	H	M	L

This already provides for a review of the importance of the interfaces between the individual systems relevant for this Use Case. As stated in section 4.2.2, this only leads to the definition of needed mitigation for the interfaces, in other words providing basic protection and prioritisation.

To assess the risk or come to prioritisation of efforts, again the mapping onto the SGAM plane can be used. As described in the methodology the SGIS SL can be used for basic risk indications of domain /zone combinations. For a risk appraisal also, the process dimension of data being exchanged has to be taken into account. Applying the risk formula presented in Section 4.2.1, the following results (Table 7) can be obtained to identify the most vulnerable interfaces.

Table 7: Risk quantification of interface categories in the Use Case example

Interface	CIA	API				Damage		Risk
		Motivation	*Exposure*	*Access numbers*	*API level*	*SGIS SL*	*DOE*	
9	HHM	3	1	2	6	2	1	12
15	LMM	2	2	3	7	1	1	7
16	HML	3	3	3	9	2	1	18

Table 7 represents a CIA (confidentiality, integrity and availability) analysis. The levels for those goals are based on high, medium and low (H, M and L). In addition, attack probability is calculated for the factors of attacker motivation, exposure of the interface and number of parties being able to access this interface. The possible values range form 0-3 whereas 3 means highest value. The sum of those factors is the attack probability indicator (API). The interface is allocated to a domain/zone combination in SGAM, leading to a Security level (SGIS SL) from the M/490 guidance. In addition, the failure of an interface can either have a direct operational effect/impact (DOE) in the system or not. The multiplied numbers provide a risk estimation.

Finally, all related security requirements for a logical interface class can be derived for each communication interface of the Use Case. ENISA or NIST catalogues provide specific lookup mitigation documents to identify the mitigation measure for each logical interface class depending on the impact level (CIA), e. g. NIST category access control *SG.AC-7: Least Privilege* or *SG.AC-21: Passwords* for LIC 9. This uses the LIC definition, the impact level and the possible security enhancements from the respective domains. See also Annex 8.6 for a shortlist of international standards applicable to every LIC.

This example illustrates that the interfaces have different risk profiles which can be exploited, all based on different context factors (system specific, and Use Case specific) and expert judgment assumptions. This allows to come to a prioritisation of critical interfaces and guidance on possible prioritisation for implementation or monitoring of security measures. For this specific Use Case, the analysis shows the most critical interfaces are those directly related to the MC actor, which guides further security effort needs.

4.2.4 Static interface analysis

As explained, the top-down approach is based on a review of interface risks exposures, considering specific Use Cases. The method is not applied to the fullest extent in scope of this study which would involve a strong simplification to cover the presumed entire energy (or even just the electricity) system.

In this section a simple static analysis of logical interface classes is provided, as simple guidance to identify the more critical interfaces in a described electricity system. As such it is an additional step compared to the SGIS SL

guidance on the SGAM domain/zone plane as provided by M/490 (see earlier Section 4.2.1). To develop such guidance for the electricity system, first a mapping is made of the NIST based smart grid system interfaces onto the SGAM plane (Figure 21)

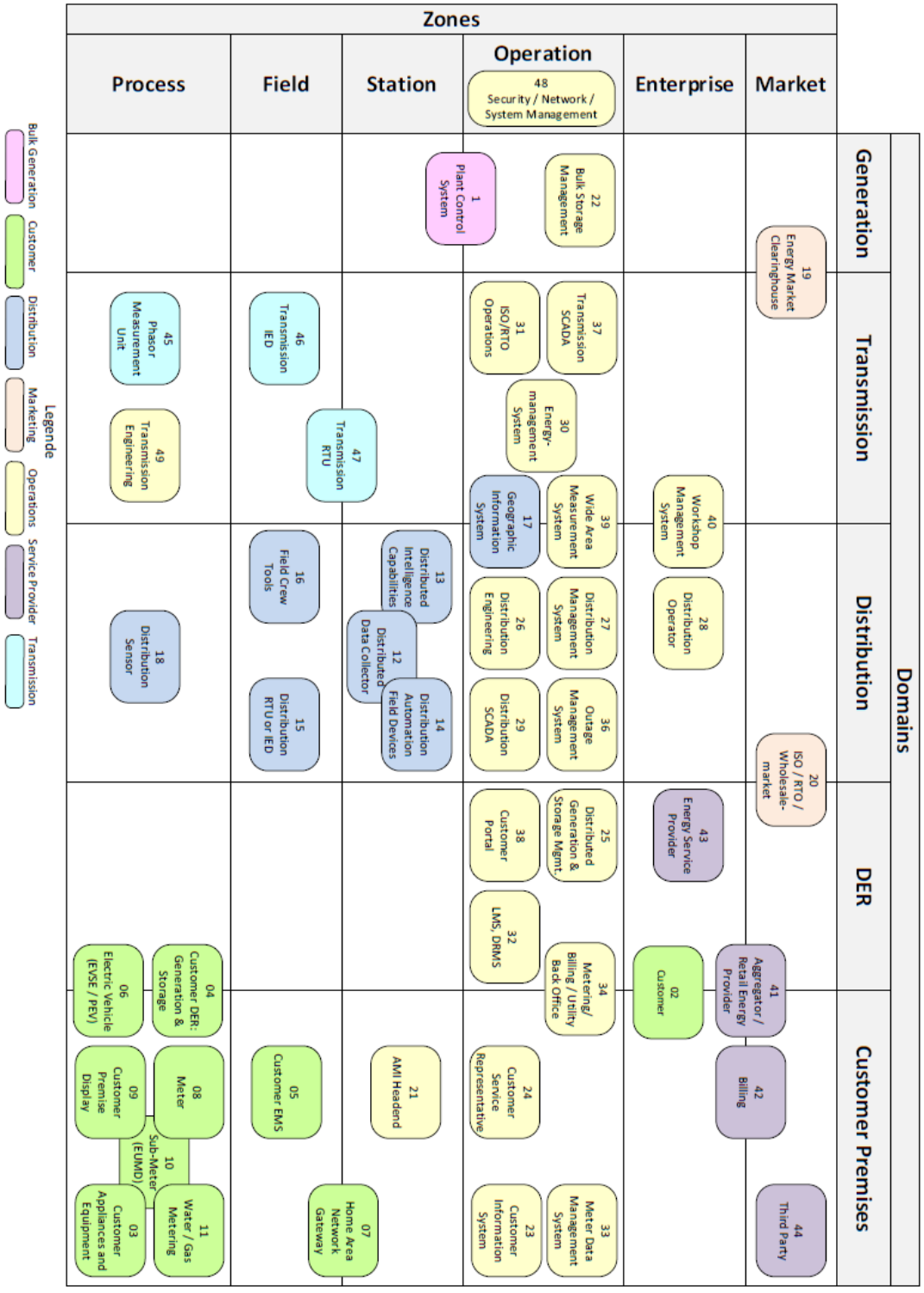

Figure 21: Mapping of NIST conceptual model interfaces on the Smart Grids Architecture Model (part 2)

Using this mapping and the interfaces from the NISTIR 7628, it is possible to allocate data exchanges between the domain/zone combinations. This leads to an overview of the interfaces of individual systems belonging to a specific domain/zones combination. Applying the security levels provided in the SGIS mapping, all the generic interfaces can be assigned a security level between 1 to 5. Typically, the most important interfaces are those from the transmission/operation combination, mostly SCADA related interfaces with a direct operational impact.

The NISTIR 7628 describes about 175 data exchange interfaces between 48 documented systems. These are the main drivers for actual processes taking place. The interfaces between systems are further combined to so-called Logical Interfaces Categories (LICs) in the NIST conceptual model. This sums up to 22 generic types of interfaces which exist in electric utilities. From the NIST perspective, there is no prioritisation of those interfaces. Each class of data exchange has specific context attributes which can be analysed. Some systems are internal to a utility, some are real-time interfaces, some are external to a utility or relate to systems shared between actors.

Table 8: Logical Interface Categories (LICs)

LIC	Description
1	Interface between control systems and equipment with high availability, and with compute and/or bandwidth constraints
2	Interface between control systems and equipment without high availability, but with compute and/or bandwidth constraints
3	Interface between control systems and equipment with high availability, without compute or bandwidth constraints
4	Interface between control systems and equipment without high availability, without compute or bandwidth constraints
5	Interface between control systems within the same organisation
6	Interface between control systems in different organisations
7	Interface between back office systems under common management authority
8	Interface between back office systems not under common management authority
9	Interface with business to business (B2B) connections between systems usually involving financial or market transactions
10	Interface between control systems and non-control/ corporate systems
11	Interface between sensors and sensor networks for measuring environmental parameters, usually simple sensor devices with possibly analogue measurements
12	Interface between sensor networks and control systems
13	Interface between systems that use the Automated Metering Infrastructure (AMI) network
14	Interface between systems that use the AMI network for functions that require high availability

LIC	Description
15	Interface between systems that use customer (residential, commercial, and industrial) site networks such as home or building area networks (HAN/BAN)
16	Interface between external systems and the customer site
17	Interface between systems and mobile field crew laptops/equipment
18	Interface between metering equipment
19	Interface between operations decision support systems
20	Interface between engineering/ maintenance systems and control equipment
21	Interface between control systems and their vendors for standard maintenance and service
22	Interface between security/network/system management consoles and all networks and systems

Table 8 lists the Logical Interfaces Categories and provides a brief description of each. In a static analysis concept as proposed here, the interfaces can be grouped for their importance. This can either be done based on their assigned Confidentiality-Integrity-Availability attributes (preferably with most weight for the Availability attribute, see 3.1) or by a more quantitative approach. This considers both the data exchanged and the interface type itself.

Given the combination of the SGIS SL and the LIC assessments, the interfaces categories can be prioritised. In addition, a weighted approach can be done considering the average number of times the Logical Interface Category is actually used in the conceptual model.

This provides a ranked list of the most important interfaces classes for the reference architecture with an average/relative security level (see Table 9).

Table 9: Logical Interface Categories ranked for importance (high to low) from a security perspective

LIC	Description	A	I	C	# occurences[20]	Rank
9	Interface with business to business (B2B) connections between systems usually involving financial or market transactions	M	H	H	14	**1**
6	Interface between control systems in different organisations	M	H	L	13	**2**

[20] The number of occurrences of an interface in the NISTIR 7628 is based on the smart grid reference architecture landscape comprising of more than 200 interfaces between the 50+ systems. Those 200 instances of interfaces are classified by the 20+ logical interface. Based on the number of occurrences of this class in the conceptual model, an interface is more likely to be a good attacking point since more possibilities exist for the attacker to come up with access to such an interface.

LIC	Description	A	I	C	# occurences[20]	Rank
18	Interface between metering equipment	L	H	M	13	**3**
10	Interface between control systems and non-control/ corporate systems	M	H	L	12	**4**
5	Interface between control systems within the same organisation	H	H	L	11	**5**
7	Interface between back office systems under common management authority	L	H	H	11	**6**
13	Interface between systems that use the AMI network	L	H	H	11	**7**
14	Interface between systems that use the AMI network for functions that require high availability	H	H	H	11	**8**
15	Interface between systems that use customer (residential, commercial, and industrial) site networks such as HANs and BANs	M	M	L	10	**9**
16	Interface between external systems and the customer site	L	M	H	9	**10**
1	Interface between control systems and equipment with high availability, and with compute and/or bandwidth constraints	H	H	L	8	**11**
2	Interface between control systems and equipment without high availability, but with compute and/or bandwidth constraints	M	H	L	8	**12**
3	Interface between control systems and equipment with high availability, without compute or bandwidth constraints	H	H	L	8	**13**
4	Interface between control systems and equipment without high availability, without compute or bandwidth constraints	M	H	L	8	**14**
8	Interface between back office systems not under common management authority	L	H	H	8	**15**
17	Interface between systems and mobile field crew laptops/equipment	M	H	L	8	**16**
20	Interface between engineering/ maintenance systems and control equipment	M	H	L	5	**17**
12	Interface between sensor networks and control systems	M	M	L	2	**18**

LIC	Description	A	I	C	# occurences[20]	Rank
19	Interface between operations decision support systems	M	H	L	2	**19**
11	Interface between sensors and sensor networks for measuring environmental parameters, usually simple sensor devices with possibly analogue measurements	M	M	L	1	**20**
21	Interface between control systems and their vendors for standard maintenance and service	M	H	L	1	**21**
22	Interface between security/network/system management consoles and all networks and systems	L	H	H	1	**22**

As the Logical Interface Categories each have specified mitigation recommendations, a ranked list of mitigations can thus be deduced as guidance. While all mitigations recommended by various organisations have their value evidently, this ranking can be useful in case of budget, resource or monitoring prioritisation. The ENISA and NIST mitigation catalogues (which can be mapped to each other) assigns mitigations to (logical) interfaces. Thus, the relevance of a certain mitigation is specified by whether it contributes to safeguarding important interfaces of important systems. Based on the ranking of the LICs one can thus prioritise mitigations focusing on e.g. a top 5 or top 10 of the Logical Interface Categories. This should not be taken as guidance on how to restrict measure implementations though. Without the context of an incident, the mitigations are generic to some degree. From the nearly 200 mitigations in the full ENISA/NIST mapping roughly 30 percent can be seen as unique ones. It is either recommended to take the remaining 70 percent as basic protection which must be done in any case and prioritise the rest, or alternatively focus on the interface classes and individual mitigations for those classes to be prioritised.

Limitations of the static approach

The method focuses also on providing a basic protection which assumes not to be broken. The mitigations are intended to protect, and the basic assumption is that of a clean and safe system infrastructure which has not been penetrated nor has any hidden infections. If an attack is successful, there is not a simple way to get a capture point and "clean" the infected methods using this method aside from a clean restart from an untainted backup[21]. To deal with sophisticated APT attacks, a different analysis is necessary. The method presented here fits in the basic layer of

[21] Which would require a correctly parametrized version of the original control soft- and firmware and, at least in the case of recovery of firmware, that the mechanism for firmware deployment on the devices is still uncompromised.

an ‘onion principle’ of security which demands pervasive security measures or “security-in-depth” at every layer of a system.

The more professional the attacker is, or the more elaborate specific threat scenarios are, the more detailed a risk management approach needs to be. Furthermore, mitigations recommended by authorities and sector organisations are presented as packages. It is recommended to implement them all. Time, resource and budget may dictate some prioritisation for organisations with lower cybersecurity maturity, hopefully as a transition phase.

To assess risks quantitatively guidance can be taken from the SGIS SL. However, it has to be kept in mind that the levels are not equidistant to each other; in other words, they do not scale. The organisation applying a formula with those input factors must be aware of this. Also, the likeliness of an event is difficult to link to the vulnerability of an interface or system and may impact the risk appraisal. High-profile attackers might focus on more than a low hanging fruit, and one could question whether an attack of a nation state or other resourceful attacker on a small organisation utility is likely.

The number of occurrences of an interface category across business processes, and a prioritisation of the factors AIC can contribute to a basic risk assignment for an interface class. This factor can also be put in context with the SGIS security level of a system. Those basic input factors can make for a very easy to comprehend starting point of a risk management for any specific organisation or public authority.

The described static interface analysis applies to the electricity sector. A similar method could be developed for automation technology in the gas sector. As stated before, the steps need further quantitative information on the importance of specific interfaces, as well as the potential damage from exploiting information and data of those interfaces. In this study no specific hack of gas control data is taken into account. However, threats such as spoofing meters to get rid of billing, attacking IEDs for disruption of usual operations and taking over control room systems, all have the same technical background and might result in similar criticalities.

This method focuses on system characteristic of organisations with little to no specific attacks and threats by certain attack agents. No assumptions are made regarding the attackers in general, nor their skill set regarding certain attack vectors. The analysis focuses on providing basic protection to interfaces and the corresponding systems, taking into account why a certain mitigation was recommended by ENISA and NIST for those interfaces.

4.3 Bottom-up risk analysis of threats

4.3.1 Methodology

The bottom-up threat analysis is based on common procedures for cybersecurity vulnerability analysis. It serves a two-fold objective by identifying specific vulnerabilities of a given system configuration:

- It can support the risk estimation from the top-down analysis (Attacker Probability Indicators) by better understanding hacker motivations and system vulnerabilities

- Also, on its own it allows to explore a particular system architecture and classify threat scenarios and attack impacts in a consistent manner.

Figure 22 describes the steps. The process is supported by a Threat Scenario Template (see Annex 8.8).

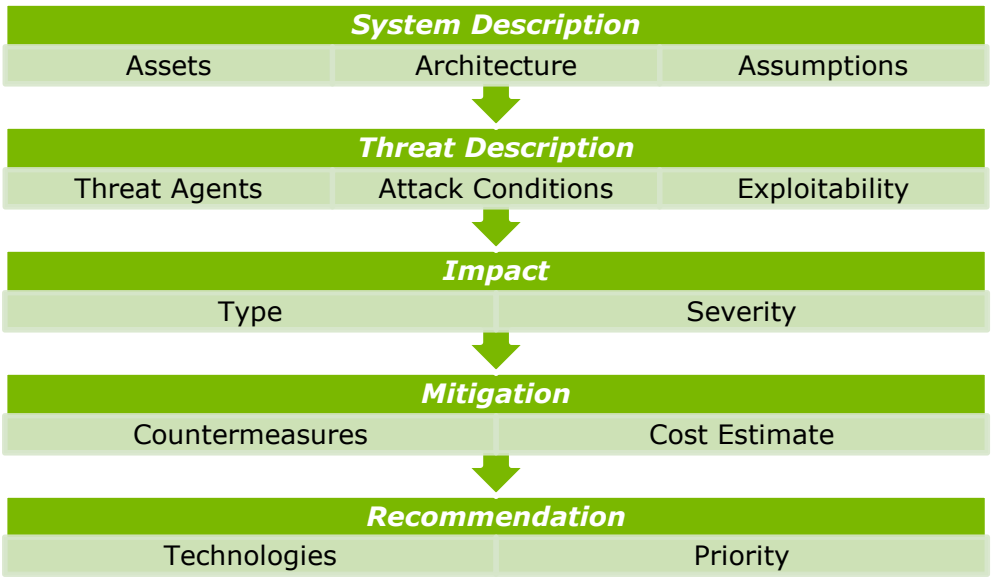

Figure 22: Bottom-up Threat Analysis methodology

The bottom-up threat analysis relies on a description of the analysed system. This is a necessary starting point in all vulnerability-focused security analyses [50]. The process starts with a description of the threat narrative and a definition of considered threat agent classes. Experts then explore the potential misuse cases and attack vectors to derive a set of conditions under which the threat can be implemented. Attack conditions are mapped onto mitigation technologies and measures that are suitable to stop a given pattern. A security gap is identified by recognizing attack conditions for which there is no effective mitigation currently implemented in the system. The analysis could provide an estimate of the cost for implementation and maintenance of recommended mitigations to thwart a sufficient set of attack conditions aggregated from cost estimates for single mitigations.

The analysis is performed for a select number of threat scenarios that are meaningful for the analysed system. The type of threat scenario is chosen depending on the intended technical depth of the analysis, the available detail in the system description or other user criteria. A selection is made based on existing literature including NESCOR, with the objective to cover the full set of system interfaces and Use Cases referred to in the top-down analysis.

Creation of novel threat scenarios is generally a creative process that requires knowledge on the application domain, ICT and ICS infrastructure, processes and business culture as well as working knowledge of exploitation of vulnerabilities and implementation of threats. To support this process the methodology uses the high-level attack graph. Each path leads from the entry-point to the threat objectives of a category of scenarios. Each of these categories can be analysed with respect to possible intended outcomes together with assets related to this outcome.

For example in Figure 23, there is an attack path using entry to the Enterprise Zone as an initial attack vector and propagating from there to the Operation and the Field Zone that defines a scenario of a remote attack to disable power distribution in a given area by triggering breakers on field level.

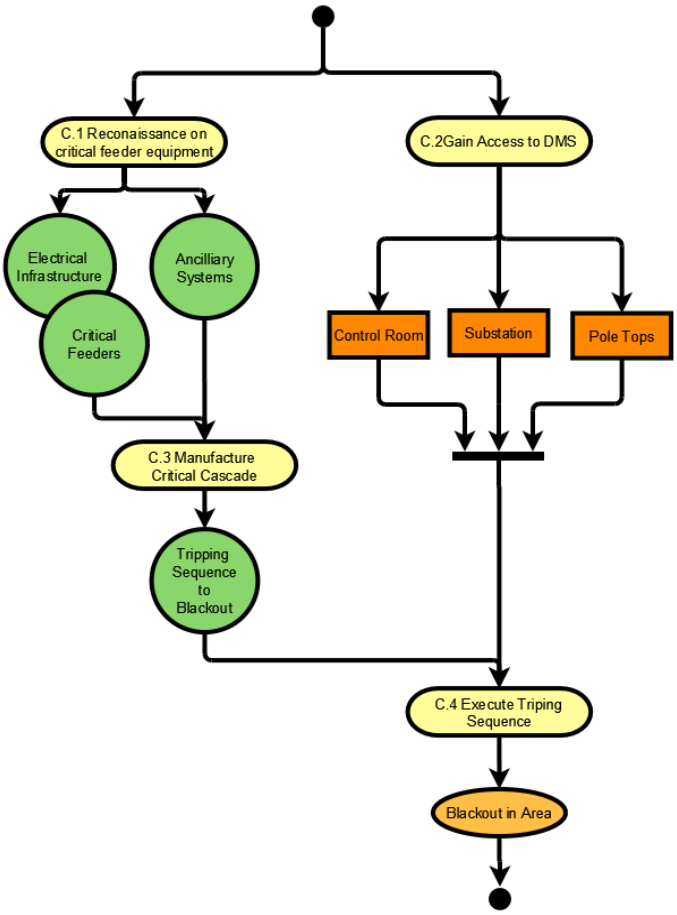

Figure 23: Example of an Attack Execution Graph for a scenario in which a Distribution Management System is targeted

The bottom-up analysis is used to highlight specific impacts per scenario, as well as high-priority measures to address these scenarios.

4.3.2 Prioritisation of Recommended Mitigations by Scenario Impact Quantifications

This section describes the prioritisation of mitigations to derive a focused set of (minimum) requirements based on specific threats and objectives of stakeholders. The method uses expert knowledge to define fundamental impact and mitigation levels and provides stakeholders with the opportunity to focus results on prevention of most critical impacts, and to prioritise mitigations with respect to limited resources.

Expert knowledge should be founded on in-depth analysis of individual threat scenarios. The detailed process for assessing a single scenario is described in annex 8.7. This section focuses on the key (non-technical) parameters that shape the analysis. Stakeholders should prioritise impact categories based on individual security objectives and general risk-based decisions. For example, it can be assumed that most utilities prioritise “security of supply” over “damage to goodwill” or “macro-economic damages”. Stakeholders or regulators may further focus effort onto mitigations important to high-impact scenarios by weighting threat scenarios relative to their impact-rating.

In the following paragraphs a suggested algorithm for prioritisation of mitigations is described.

4.3.2.1 Impact-based priorities for threat scenarios

The analysis is based on a set of threat scenarios S and a set of impact categories I. An impact-severity for each impact category in each threat scenario is sought. It is assumed that this estimate is given as a value in the range of 1 to 5. The impact quantification requires expert knowledge of the threat scenario. The weight of impact categories is more subjective and in essence a non-technical choice; it is worth addressing such weighting via a stakeholder consultation.

Stakeholders choose weights $w_I: I \to [0,1]$ for all impact categories, signifying the priority of preventing certain categories of impact over others.

Experts set impact levels $l_I: S \times I \to \{1, \dots, 5\}$ which ideally are based on a thorough analysis of severity of impact of any given threat scenario.

From these values an estimate of the **criticality of individual scenarios** σ **is calculated** as weighted average sum:

$$\sigma: S \to [0,5]$$
$$\sigma(s) \mapsto \frac{1}{|I|} \sum_{i \in I} w_I(i)\, l_I(s,i)\,.$$

The function σ provides for a (partial) ranking of threat scenarios from the lowest overall impact scenario to the highest. This ordering is used in the following section to allow focusing mitigation efforts on the most critical scenarios. Table 10 provides a suggested weighting of impact categories. Values of zero imply that these categories are not considered for this specific analysis presented here. The weights have to be adapted to individual concerns of actors from impacted organisations if the method is applied to different utilities or subsystems. It is unlikely that stakeholders assign uniform weights to all impact categories. The weights in this table are exemplary.

Table 10: Weights to prioritise impact categories

Impact Categories (NESCOR based)	Weight (suggested)
Public Safety Concern	1
Workforce Safety Concern	1

Impact Categories (NESCOR based)	Weight (suggested)
Ecological Concern	0
Financial Impact of Compromise on Utility (excluding #5)	0
Cost to return to normal operations	0,5
Negative impact on generation capacity	0
Negative impact on the energy market	1
Negative impact on the bulk transmission system	0
Negative impact on customer service	1
Negative impact on billing functions	1
Damage to goodwill toward utility	1
Immediate macro-economic damage	0
Long-term economic damage	0
Loss of privacy	1
Loss of sensitive business information	1

Weights and impact factors are combined to derive a ranking of scenarios as defined by σ, shown in Table 11. The rows list the threat scenarios provided in Section 2.2. The columns provide the impact categories as given in Table 10 which contributes to the score of scenarios according to their weight. This results in a ranking of scenarios.

For example, Scenario 7, covering a black-out in the distribution system, there is evidently a large impact estimated at level 5 on public safety, the utility's customer service and macro-economics, but not directly on the workforce or the wider transmission system (if not propagated of course). When applying Table 10, the impact category 'macro-economic damage' is deemed not of relevance of the analysis (score 0), which means this impact category is not influencing the final ranking of scenarios by impact level. This results in a ranking of the weighted impact for Scenario 7 to be 3rd rank, as opposed to the 2nd rank when uniformly distributed weights would have been considered. In this way the priorities given by stakeholders on the criticality of wider impacts (which in itself does not necessitate cybersecurity expertise) can be considered in an overall analysis.

The impact categories of Table 10 result in the weighted impact and are based on an expert judgement which require regular revision while applying the method to specific organisations. The final ranking is based on the weighted impact, starting with the highest number.

The result provides an estimated impact for each scenario, as given in Table 11. The first four scenarios are retained to identify the highest priority mitigations in the next section:

1. Scenario 3: 'Phishing' Employees on Enterprise Level propagates to Field Zone for process disruption

2. Scenario 9: Supply Chain Vulnerabilities Used to Compromise DGM Equipment
3. Scenario 7: Threat Agent Triggers Blackout via Remote Access to Distribution System
4. Scenario 11: Rogue Firmware Enables Unauthorized Mass Remote Disconnect

Table 11: Scenario ranking based on expert impact estimates and stakeholder priorities

	Threat Scenario	Public Safety Concern	Workforce Safety Concern	Ecological Concern	Financial Impact of Compromise on Utility	Cost to return to normal operations	Negative impact on generation capacity	Negative impact on the energy market	Negative impact on the bulk transmission system	Negative impact on customer service	Damage to goodwill toward utility	Immediate macro economic damage	Long term economic damage	Loss of privacy	Loss of sensitive business information	Average Impact	Weighted Impact	Rank	Rank-based scenario weight
1	Infection through intrusion detection system	1	1	1	3	3	1	1	1	2	2	2	1	1	2	2		1.60	0.97	10	0
2	Virus/Trojan infiltrates industrial control system	1	1	1	1	2	1	2	1	3	2	2	1	1	2	2		1.53	1.07	7	0
3	Social engineering: phishing employees on enterprise level	4	4	3	3	4	3	3	1	2	2	4	2	2	2	2		2.73	1.67	1	1
4	Malicious update to firmware in the field to influence single substation	4	2	2	1	2	1	1	1	1	1	2	1	1	2	1		1.53	1.00	9	0
5	Cross-sector, cross-border message flooding	3	2	1	1	1	2	2	1	1	1	2	1	1	1	1		1.40	0.90	11	0
6	Compromise equipment through SCADA apps	3	2	2	2	2	2	1	2	1	2	2	1	1	2	3		1.87	1.13	5	0
7	Advanced persistent threat (APT) to DSO flexibility management system	5	1	2	2	4	1	3	1	5	1	3	5	3	1	2		2.60	1.53	3	1
8	Plant tripped off-line through compromised vendor (software update by manufacturer)	3	3	2	2	2	5	2	2	1	1	3	3	2	1	2		2.27	1.13	5	0
9	Compromised distribution grid management through supply chain vulnerabilities	5	4	3	2	4	1	1	1	2	2	3	1	2	2	3		2.40	1.60	2	1
10	Weakened Security during Disaster	2	1	3	1	3	1	1	1	1	1	2	1	1	3	3		1.67	1.03	8	0
11	Unauthorized Mass Remote Disconnect Through Firmware update	3	1	1	2	4	1	3	1	1	5	3	2	2	1	1		2.07	1.33	4	1

This ranking can provide new insights. The only scenario (Scenario 7) that directly addresses a blackout is ranked less critical than two scenarios that only have the potential of resulting in a blackout (Scenario 3 and 9). This shows the relevance of setting weights for impact prioritisation in Table 10. Given that the four highest ranked scenarios all are very likely attack vectors to facilitate a disruption of service, and Scenario 7 only concerns a single distribution grid whereas the other scenarios potentially affect a larger area, the ranking can be justified. Scenario 3 'Phishing' is reasonably prioritised very high, as it is based on an often exploited attack vector, which already was used for large-area blackouts. A similar case can be made for Scenario 9. Compromised supply-chains threaten the core trust in

the adequate functionality of widely used components, microcontrollers, sensors and firmware, which cannot effectively be analysed once implemented in a complex product.

The approach is particularly useful in future applications which aim to enumerate many scenarios and try to narrow the list down for further analysis. Note, alternative criteriacriteria for risk analysis of the energy sector or a specific energy company could be to focus on those scenarios which have a stronger OT focus. The focus view as given in Figure 8 (see section 2.2) could then be applied as metrics for scenario selection.

The suggested methodology can also be used to evaluate expert stakeholder opinions on regular basis.

4.3.2.2 Scenario-ordering based prioritisation of mitigations

In a next step, priorities for mitigations are derived based on expert knowledge on the effectiveness and necessity of mitigations per scenario, as well as the scenario prioritisation as explained in the previous section.

Experts choose mitigation levels $l_M: S \times M \rightarrow \{1, \dots, 5\}$ for each mitigation (class) to defend against a specific threat scenario.

The impact-based prioritisation of scenarios gives a weighting function $w_S: S \rightarrow [0,1]$ of scenarios. An example weighting function is to apply a weight of 1 to the first n scenarios and a weight of 0 to all remaining scenarios. (see Table 12 for $n = 4$)

Table 12: Prioritisation (selection) of considered threat scenarios

Priority	Threat Scenario
0	Infection through intrusion detection system
0	Virus/Trojan infiltrates industrial control system
1	Social engineering: phishing employees on enterprise level
0	Malicious update to firmware in the field to influence single substation
0	Cross-sector, cross-border message flooding
0	Compromise equipment through SCADA apps
1	Advanced persistent threat (APT) to DSO flexibility management system
0	Plant tripped off-line through compromised vendor (software update by manufacturer)

Priority	Threat Scenario
1	Compromised distribution grid management through supply chain vulnerabilities
0	Weakened Security during Disaster
1	Unauthorized Mass Remote Disconnect Through Firmware update

The weights w_S are applied to each mitigation level l_M. These weighted mitigation levels are then aggregated to provide a single priority over all considered/selected scenarios for each mitigation category. The maximum function is recommended to reflect that a security measure can only protect sufficiently if it is implemented at least at the given maturity. The expression of the weighted maximum mitigation level thus is as follows:

$$\rho: M \rightarrow [0,5]$$
$$\rho(m) = \max_{s \in S} w_S(s) l_M(s,m).$$

The priority of mitigations provides an estimate of the importance of a mitigation category to prevent manifestation of any threat scenario under consideration.

Table 13: Resulting required levels for ENISA mitigations

Threat scenario	SM 1 Security Governance and Risk Management	SM 2 Third Parties Management	SM 3 Secure Lifecycle Process for Smart Grid Components and Operating Procedures	SM 4 Personnel Security, Awareness and Training	SM 5 Incident Response and Information Knowledge Sharing	SM 6 Audit and Accountability Capability	SM 7 Continuity of Operations Capability	SM 8 Physical Security	SM 9 Information Systems Security	SM 10 Network Security	Scenario selection
Infection through intrusion detection system	2	1	2	1	1	1	3	1	5	4	0
Virus/Trojan infiltrates industrial control system	3	2	1	2	1	2	1	1	5	5	0
Social engineering: phishing employees on enterprise level	**3**	**1**	**3**	**5**	**3**	**2**	**1**	**2**	**3**	**3**	1
Malicious update to firmware in the field to influence single substation	3	1	4	1	2	2	4	4	3	4	0
Cross-sector, cross-border message flooding	2	3	2	2	4	2	4	1	5	5	0
Compromise equipment through SCADA apps	4	2	4	4	2	2	2	2	3	3	0
Advanced persistent threat (APT) to DSO flexibility management system	**4**	**2**	**2**	**3**	**4**	**3**	**2**	**2**	**5**	**5**	1
Plant tripped off-line through compromised vendor (software update by manufacturer)	3	4	5	4	1	2	4	1	2	5	0
Compromised distribution grid management through supply chain vulnerabilities	4	5	4	2	1	3	3	1	1	1	1
Weakened Security during Disaster	4	2	1	5	3	2	5	4	4	2	0
Unauthorized Mass Remote Disconnect Through Firmware update	**4**	**5**	**5**	**1**	**2**	**3**	**4**	**3**	**1**	**1**	1
Maximum	**4**	**5**	**5**	**5**	**4**	**3**	**4**	**3**	**5**	**5**	

Table 13 provides result of this analysis and highlights the recommended ENISA mitigation categories to prevent given threat scenarios. For example, the scenario on rogue firmware updates enabling mass remote disconnections (last scenario), clearly calls for strict implementation of ENISA mitigation categories on third-party management and secured life cycle processes of grid components and operating procedures.

With the four scenarios prioritised based on impact and weighting in previous section, and the mitigation level mapping against the 10 ENISA categories, the analysis highlights five measure categories as very important, three as important, and two as relatively important. The reader can deduct from the full table how the recommendation setting would have been different in case of another scenario prioritisation. Selecting for example the first scenario instead of the third, would reduce the priority for SM 4.

Note that where this illustration gives a somewhat generalised view by applying the broad ENISA categories and an average (conceptual) European power system, the approach can be fine-tuned for specific architectures and/or more detailed mitigation catalogues.

4.4 Risk analysis for systems at different level of cybersecurity maturity

In the top-down approach the generic interfaces and their classes, e.g. SCADA to market, SCADA to metering, metering to aggregator etc., can be tested for maturity related to the mitigations recommended for those interfaces. The risk analysis can show which interfaces need most protection for an initial attack (though has limitations to understand how an attack or threat ripples through an infrastructure after an initial penetration). When providing a summary of mitigations for a level, it is also possible to assess costs needed for a certain level of protection, ranging from basic to sophisticated. The use of the maturity model thus provides a static view on which mitigations are advised to reach a given maturity at a given cost range (due to system legacy, vendor choices and other preconditions) with focus on specific interfaces. Weighted mitigation levels can provide a prioritisation on which mitigation classes should be implemented first, taking into account stakeholder view on impact category prioritisation and threat scenario selection, as well as constraints in costs, resources, operations and timing.

Maturity is also of relevance to the bottom-up approach. Incidents, threats and attacks provide an overview of what has happened or could potentially happen. They should not be hypothetical nor singular events. Therefore, after forensics took place, breaches are closed and mitigations are reflected. A CAPEC [56] based analysis then shows the common attacks patterns used and possible mitigations. Also, here the level of mitigations can be assessed against maturity levels to understand options for mitigation in terms of costs and risk containment.

In real applications of utilities, assessing the maturity of measures taken in both top-down and bottom-up analyses, documenting them and consolidating these in a governance model with re-evaluations is vital for its cybersecurity risk management.

In scope of this study where pan-EU recommendations are sought, the concept of a simple maturity model can be applied too. The key is to assess reasonable (and simple/simplified) levels and map mitigations onto them. Thus, the aggregated mitigations make for a level of technical or organisational maturity.

There is a differentiation of security approaches in the IT as well as OT domain across European utilities. These differences are assumed to be driven by differences in size, customer structure, legacy, legislation, financial strength and even company culture. There is no robust data to verify such correlations exactly, though industry expertise as well as the survey/interviews conducted in this study again confirm the varying maturity levels across system operators.

An exhaustive classification of all electricity/gas utilities considering IT/OT cybersecurity practices is not feasible in the scope of this study. Therefore, this study puts forward a set of so-called generic utilities which can be defined based on maturity of their cybersecurity operations.

As the risk assessment applied in earlier sections is based on the measure classes as set by ENISA, also the maturity levels refer to these classes. Three maturity levels are suggested ranging from Low to Medium to High. Table 14 shows the effectiveness of implementation of each ENISA class for each level of maturity, ranging from basic (1) to advanced (3). It is emphasised this model is a simplification of reality and used as a tool to handle the diversity of actors and maturity across Europe and across types of actors. Note that even at the lowest level, the IT/OT security level is deemed to be reasonable for present operations of the system. This mapping should not be

interpreted as drawing conclusions on which parts of the system are inherently unsafe. Still, those low-level utilities lack mostly governance aspects and dedicated organisational units, as well as budgets or responsible dedicated personnel, which differentiates them from higher maturity levels.

Table 14: Effectiveness of each ENISA measure class in organisations with overall Low, Medium or High maturity. Level 1 implies basic effectiveness, while 3 is advanced effectiveness.

Measure class (ENISA)	Low	Medium	High
Security governance	1	2	3
Risk management	1	2	3
Management of third parties	1	2	2
Secure lifecycle process for smart grid components/systems and operating procedures	1	1	2
Personnel security, awareness and training	1	2	2
Incident response & information knowledge sharing	1	2	2
Audit and accountability	1	1	2
Continuity of operations	1	2	3
Physical security	2	3	3
Information systems security (incl. SG IA category)	1	2	3
Network security	2	3	3

Annex 8.10 provides a further interpretation of the maturity levels in relation to more specific mitigation types. The interpretation and context of all three levels is the following:

The low-profile utility: Basic risks from operational perspective are covered, and measures in place. Capabilities can be improved to a higher-level. The measures can be stricter, more meaningful and more complex over time – but still, basic protection is always granted. Low-profile utilities deal with more third parties as they tend to have less IT/OT skilled personnel. This is manageable but deserves attention. Contracts cover most issues, but less formal checks may take place due to budget and time constraints. A complete asset management process with dedicated life cycle data coverage is not fully implemented at low-profile utilities. In addition, personnel are less trained to everyday business constraints. Knowledge sharing is done by informed newsletters or vulnerabilities form CERT; no dedicated (e.g. STIX /TAXII) infrastructure is used and in place. Audits are limited. Continuity of operations after an incident is mostly focused on brownout and blackout recovery capabilities caused by incidents like natural disasters. Physical security like access control, asset protection as well as network security are already at a very good level. This is basic technology which can be bought form OEMs and third parties and is usually invested in. Information systems security is low. More capabilities and strict processes could be applied and enforced in daily operations. Third-party security for the control networks etc. has been implemented as even with limited budget, investments here are enforced by OEMs. In general, this utility type is characterised by doing the minimum amount of needed

security. Due to limitations in size, budget and personnel, also cybersecurity capabilities are limited and improvable if the conditions and priorities change.

The medium-profile utility: The medium-profile utility has more sophisticated measures in place already, and more budget can be spent on individual measures and mitigations against threats. The organisation as an entity takes security more as an overall priority and shows awareness of risks across the organisation. Specific processes such as audits and lifecycle reviews may remain still lower priorities. It should be noted that progress to a higher maturity level is not a simple step, as improving (asset) data processes, integrating internal audit/monitoring processes, and adapting legacy assets in the field all require considerable time, investment and organisational mindset shift.

The high-profile utility: As with the medium level utility in comparison to the low-profile utility, stronger governance is enforced and controlled. Risk management is based on more sophisticated scenarios, more progressive methodologies, and more elaborate sets of attackers and threats are envisioned and dealt with. In addition, continuity of operations considers sophisticated cyberattacks. Physical security as well as network security are state-of-the-art. Investment means and dedicated units exist. Nevertheless, due to size and complexity, processes and organisational capabilities may not be maxed out yet.

4.5 Applicability of the risk analysis methodology

This Chapter presented a blueprint risk management approach for the European energy sector. The methodology builds on the ISO31000 process, the NISTIR 7628 methodology, as well as the Smart Grid Architecture Model and security levels developed in M/490. The objective is to provide a framework which applies maturity levels and prioritises mitigation measures for specific organisations.

The approach combines a top-down approach which analyses interfaces and specific use cases, with a bottom-up approach which provides detailed analyses of specific threat scenarios. A further abstraction can be made of the top-down approach by a so-called static interface analysis. Figure 24 gives a decision-tree view on when which approach is advised to be applied. Still, it is emphasized the methods are complementary and could be used combined in an integrated assessment.

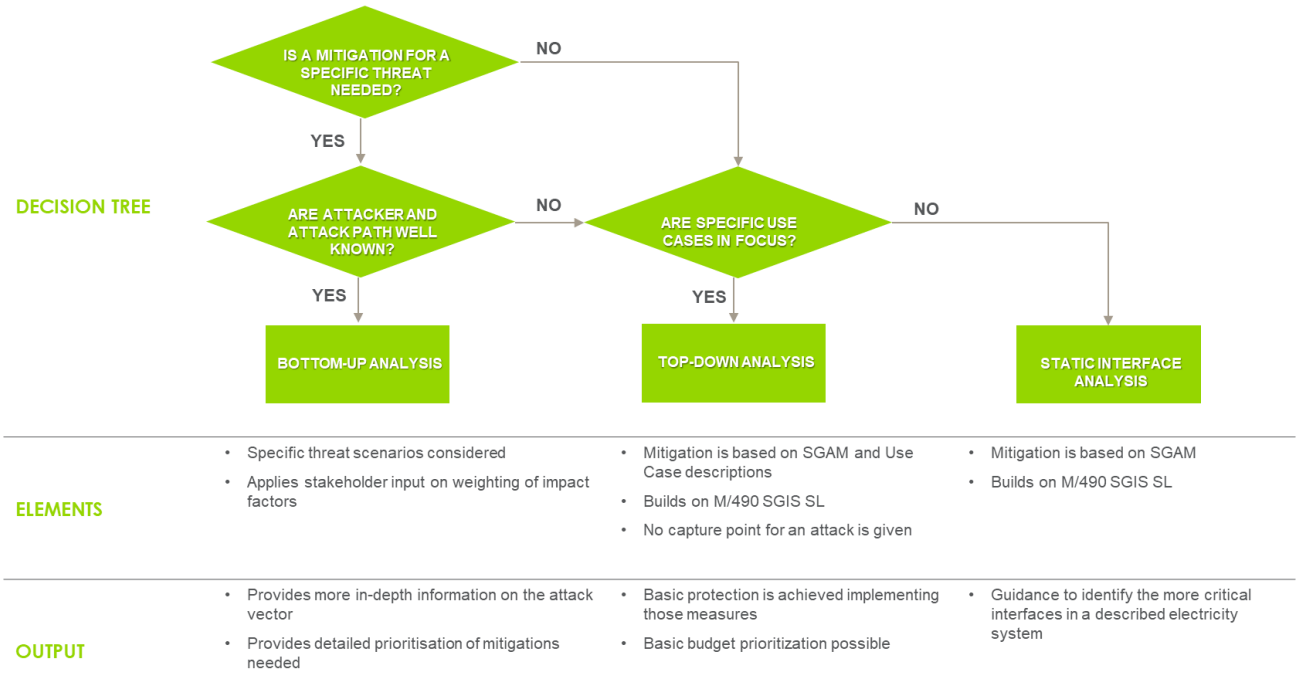

Figure 24: Overview of risk management approaches presented in this Chapter

These assessments allow to identify critical issues and priority mitigation measures. An assessment example is provided for the bottom-up analysis based on the 11 high priority scenarios developed in Chapter 2. The results of this assessment and a set of developed maturity levels are integrated in an EU wide cost projection when considering bringing a set of organizations to a higher maturity in the next chapter.

5 Cost projections

KEY MESSAGES

European electricity TSOs and DSOs are estimated to spend presently about 700 million Euro annually on cybersecurity related measures. As highlighted in Chapters 1 to 3, the energy system is changing rapidly. The pace and effectiveness of applying cybersecurity strategies differs across European energy companies. A number of EU policy options can be developed to advance the maturity of energy system actors, building on the NIS directive and its implementation. This Chapter lists several options at conceptual level to clarify which distinctive objectives can be pursued, and how these would impact aggregated costs for the impacted operators.

Normative instruments can address the electricity and/or gas sector. They can also address either large system operators, small DSOs and/or market actors (suppliers, aggregators, etc). Regulatory requirements can take the form of obligations and monitoring schemes, but can also include strong compliance enforcement rules which would push organisations to higher maturity.

Cost projections are developed for each option. This uses a logical modelling approach by taking into account the bottom-up risk analysis on 11 high-priority scenarios and a simple maturity model based on ENISA's mitigation classes as presented in Chapter 4. To make projections for the entire European energy system, clear assumptions need to be made regarding present maturity state of energy system actors and various cost keys (across all ENISA mitigation classes to advance in maturity). These assumptions are explained in this Chapter and can serve as input in future discussion, research and stakeholder consultation sessions on this topic.

Present cybersecurity expenditures by system operators in electricity account for about 0.02 ct€/kWh, or an average 0.11% of average retail tariffs and bills. New legislative instruments aiming to advance all grid operators to at least medium or alternatively high maturity level could increase present expenditures by 3 to 6%. Attention is needed regarding the uncertainty related to these figures. Main causes for this uncertainty are confidentiality of expenditure information by organisations on cybersecurity, limited view on present maturity across the large number of energy organisations in Europe all with different legacy, ambiguity within organisation budgets on which part would be attributed to cybersecurity in the OT domain (beyond normal ICT measures), and the difficulty in generalising the additional cost of new measures.

5.1 Objective

This study aims to give reasonable and underpinned cost impact projections for EU cybersecurity related policy options. These options are not interpreted as a list of technical or company specific organisational measures, but rather as a level of ambition and harmonisation the EU would put forward in future legislative proposals such as the initiation of network code on cybersecurity, to bring organisations to a certain maturity level. This study develops the

following range of policy options (Table 15), which could result in specific (higher) maturity levels of organisations and are further analysed via cost projections.

Table 15: Policy options for cost impact analysis

Option		Application							
		Electricity				Gas			
		TSO	DSO large	DSO all	Market	TSO	DSO large	DSO all	Market
0	Do nothing beyond full NIS directive implementation								
1	Informative and economic instruments								
2	Normative instruments: *obligation to all System Operators*								
3	Normative instruments: *obligation to all energy actors*								
4	Normative instruments: *compliance enforcement to large System Operators*								
5	Normative instruments: *compliance enforcement to large System Operators, obligation to all others*								
6	Normative instruments to electricity sector: *compliance enforcement to large System Operators, obligation to all others*								

No new normative measure applied, thus no clear view on maturity change

Normative measures to bring organisation to maturity level Medium

Normative measures to bring organisation to maturity level High

In this approach, policy options can focus on either electricity or gas sector (or both) and apply to specific types of actors. The distinction small/large DSO could be based on the number of connected customers, e.g. the 100.000 threshold also applicable in other energy legislation. Market actors include mainly for the electricity sector generators (small and large), traders, aggregators, and for the gas sector storage operators and traders. It could be possible to make further subcategories in these market actors based on size and system impact.

The **interpretation of the policy options** is as follows:

0. Represents the as-is situation, based on present maturity assumptions and cybersecurity efforts from energy sector organisations. Essentially this can be interpreted as the early-stage of NIS directive application.
1. Reflects additional informative and economic options (see a list of examples in chapter 6.2). No specific cost assumption is developed for such option. It is assumed that both the cost and the impact will be less than that for normative instruments aimed at the energy sector.
2. Relates to a set of legal obligations imposed on TSOs and DSOs in the electricity and gas sector. TSOs and larger DSOs are already covered by the NIS directive. Smaller DSOs would in this option also be covered by legislation. Also new requirements (e.g. a network code) could be envisaged here for all operators, providing a stronger common framework by regulation.
3. Relates to a set of legal obligations imposed on all system operators and market actors in the electricity and gas sector.
4. Is a result obligation (set of compliance rules) on TSOs and larger DSOs, which would drive these to a high maturity level (if application is effective).
5. Is a result obligation (set of compliance rules) on TSOs and larger DSOs, complemented with requirement obligations for smaller DSOs and market actors.
6. Is a variant of option 5 which applies only to the electricity sector. This could be motivated to balance urgency and resources, with the gas sector (which is already covered by the NIS directive) seeing new normative measures potentially at a later stage.

The EC is already considering a number of very specific measures such as vendor certification and made a proposal for a coordinated response scheme (See 2017 cybersecurity package). Additional options are explored in the SG TF EG2. Cost appraisals of these specific options are not in scope of the analysis.

Evidently putting forward any cost projection needs to be done while acknowledging a vast set of uncertainties. Experience has shown that at individual company level cybersecurity related budgets even in a clear program plan can be uncertain. When projecting costs at EU-wide level for a high-level described cybersecurity policy the uncertainty rises. It is therefore important in this study to give sufficient insight in the many different cost drivers at individual company level, and the assumptions made in the modelling exercise to come to sensible and defensible EU-wide figures, and at least have a conceptual framework for expressing such costs.

It is noted that the Impact Assessment of the NIS directive gave general cost estimates already. That analysis considered the energy sector to already have most advanced measures in place and thus to be a benchmark for other sectors. The analysis assumed about 6.6 % of the ICT budget of energy companies is spent on ICT security measures (not including energy OT domain).

The projections put forward in this chapter are based on benchmarking with present expenditures including the OT domain, and a link with specific types of cybersecurity measures coming from the risk analysis presented in chapter 4.

5.2 Present situation of costs for cybersecurity

The **main cost drivers** for implementing cybersecurity measures and demonstrating compliance can be listed as follows:

Table 16: Main cost drivers for implementing cybersecurity measures

Category of cost driver	Description
Size	Smaller companies commonly face resource constraints necessitating costly outsourcing.
Asset types	Distribution architectures are more complex and require larger budgets to achieve compliance.
Asset management system	Organisations with poor management practices face steeper program adoption costs.
Cyber asset age	Older cyber assets may not be supported and are challenging to monitor.
Governance	Lack of clear ownership guidelines complicates the standards adoption process.
Staffing options	Developing in-house cybersecurity capability requires long-term planning. Outsourcing these functions is expensive and may not provide the best outcomes.
Support options	External expertise that can work on specific assets sets is in scarce supply.
Time	Standards adoption takes careful planning over several years

In 2017, European electricity TSOs and DSOs spent about 700 million € (see Figure 25) on cybersecurity measures, based on data sourced directly from vendors by Navigant Research [16][22]. A large part of the market focuses on Western-European countries with a stronger drive for distribution and substation automation, as well as countries with more progress in smart meter deployment. Vendors projected an annual market growth of about 4% over the coming decade, mainly based on NIS directive implementation, rising maturity, and further smart meter deployment. This does not yet take into account other legislative measures considered by European policy makers. Also, it is important to note that these figures focus mostly on the OT domain of system operators, not on the (usual) IT spectrum of cybersecurity measures nor on organisational impact (processes and staffing). The shown transmission upgrades cover aspects such as PMUs, dynamic line rating and other field sensors, and EMS/SCADA. Smart Grid IT & Analytics covers items such as workforce management, outage management and customer information systems. Definitions on IT/OT delineations may differ depending on source and expert. The Navigant Research study takes into account vendor estimates that typically identify about 3 to 5% of infrastructure investments with electricity TSOs and large DSOs as attributed to cybersecurity measures. In Eastern Europe this is estimated as slightly lower at about 2-3%.

[22] See also Annex 8.13

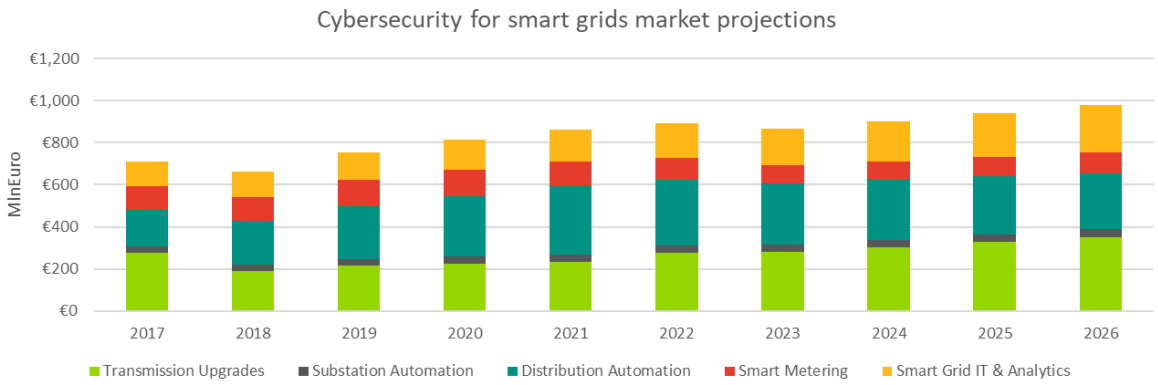

Figure 25: Market size for OT related cybersecurity with European electricity TSOs and DSOs as projected by vendors under business-as-usual conditions [Source: Navigant Research]

It is difficult for individual organisations and regulators to monitor costs specifically related to cybersecurity measures, let alone the specific split of IT versus OT related costs or even rough ratios between both. Also, from vendor data, the split into cybersecurity specific costs is not always evident as capabilities may be embedded in standard system operator products (e.g. a DSO AMI and DMS, or a TSO EMS). The figures for OT costs provided here, though coming directly from vendors, are estimate derivatives from broader smart grid related solutions[23]. A guiding estimate from interviews with vendors gave following split (Table 17). This shows the view that substation and grid element cybersecurity measures cover predominantly field assets and their communication interfaces, while smart metering efforts are most on data hubs and AMI which can be considered part of the normal business IT domain.

Table 17: Split of IT vs OT expenditures in various transmission and distribution segments [Source: Navigant Research]

Segment	IT	OT
Transmission Upgrades	20%	80%
Substation Automation	40%	60%
Distribution Automation	30%	70%
Smart Metering	90%	10%

Assumptions for cost projection: The cost projection assessment of this study uses the European 2017 expenditures as reference point for impact of specific policy options on OT related costs. On a European aggregate

[23] This includes Advanced distribution management systems (ADMSs), Asset management systems (AMSs), Customer information systems (CISs), Demand response management systems (DRMSs), Distributed energy resources management systems (DERMSs), Energy management systems (EMSs), Geographic information systems (GISs), Meter data management systems (MDMSs), Mobile workforce management systems (MWMSs), Outage management systems (OMSs), SCADA, asset analytics, grid operations analytics, demand-side analytics, and customer analytics.

level, these figures show that TSOs spend 0.92% of their annual revenues on cybersecurity measures, while DSOs spend about 0.48% on such measures. Revenues are derived from national energy consumption figures and average grid tariffs as reported by EUROSTAT[24]. To put all this in a different perspective, this accounts for about 0.02 ct€/kWh, or an average 0.11% of average retail tariffs and bills, which already is due to cybersecurity measures taken by electricity system operators today.

These indicators are slightly higher than the cost information retrieved from system operators directly. Input from a limited number of system operators in this study (See survey Section 3.3) indicated about 0.1 to 0.5% of total annual revenues. This range of figures is considered due to different populations (bulk market figures, versus select operators), but also highlights the difference in interpretation as to which costs are attributable directly to cybersecurity. Experience from US utilities in implementing NERC CIP v3/5 indicated a cybersecurity cost of about 0.1% of annual revenues. Also, cybersecurity maturity has a direct relation to the overall IT budget of utilities, with smaller companies often having even proportionally smaller cybersecurity budgets.

To better understand present expenditures and enhance cost projections for benchmarking and regulatory reviews, a closer national monitoring of specific cost figures on cybersecurity could be done in future by the national authorities. A European agency, like ACER or ENISA, could analyse aggregate and check samples. Another option is for a EU framework with compulsory metrics how to evaluate and report categories of cybersecurity expenditures.

No robust data was obtained on expenditures for gas system operators. Input from the survey conducted in this study did not allow to set reference costs as data was too limited. Furthermore, no public reports are identified which can provide such costs for the gas sector. A working assumption in absence of better data is that gas TSOs allocate the same share of their revenues on cyber security measures as electricity TSOs, while for DSOs this is substantially less (assumed half) compared to their electricity colleagues due to lower shares of decentralisation and digitization in the gas distribution system. As stated earlier, the criticality of cybersecurity risks in the gas sector is considered lower than in the electricity system. This is based on different trends of digitization and decentralization, and also acknowledged in stakeholder interviews. When pursuing future cybersecurity best practices, legislation or regulatory cost analyses for the gas sector, these cost assumptions need to be reviewed in closer detail.

5.3 Methodology for projections of policy options

The following steps are taken to guide the cybersecurity implementation cost projections

1. Formulate a number of alternative EU level policy options

[24] For example, EU28 countries had a total electricity consumption of close over 3000TWh in 2017 [Source: ENTSO-E statistical factsheet 2018], while the average Unit Transmission Tariff due to direct TSO costs was 8.37 €/MWh [Source: ENTSO-E overview of transmission tariffs 2017]. This adds up to 25 Billion Euro TSO expenditures. As shown in Figure 25 TSOs invest about 230 million Euro annually on OT related cybersecurity measures, which comes to 0.92% of their annual revenues. Taking into account the average retail tariff across EU28 of 0.205 €/kWh [Source: Eurostat using a weighting of households and non-households, and including taxes and levies], this leads to an average cybersecurity component in the bill of 0.11% or a cost per consumer of 0.02 ct€/kWh.

2. Propose a number of maturity levels
3. Map EU system operators and other actors to these maturity levels
4. Assess cost impacts of classes of energy cybersecurity measures
5. Perform the risk analysis of Chapter 4 to identify recommended classes of measures.
6. Use the mapping of organisations by maturity level and the recommended measures at EU level, to assess EU-wide cost impacts of advancing in cybersecurity maturity

Step 1 – Formulate a number of alternative EU level policy options

One characteristic of the selected policy options is the extent of application, which can on one hand be electricity and/or gas sector oriented, and on the other hand focus on TSOs, DSOs, and/or other market actors. Another characteristic of a policy option is whether the instrument pushes for self-regulation by the sector by imposing the specific sets of measures, or whether a clear compliance enforcement framework is in place. This second characteristic is interpreted in this analysis as a differentiation of maturity level aimed for.

Step 2 – Propose a number of maturity levels

Several cybersecurity maturity frameworks exist (e.g. ES-C2M2) or are under development (e.g. the preparatory work of the EU SGTF EG2). In the context of this study a pragmatic approach towards maturity levels is taken. Three type organisations are proposed which relate to low, medium and high mature organisations in the field of cybersecurity. Each type organisation is characterised by the extent to which energy cybersecurity measures are effectively implemented. This classification is based on input from the project team's survey, stakeholder interviews and own estimates. Section 4.4 elaborated a simple three level maturity model (Table 18).

Table 18: Effectiveness of each ENISA measure class in organisations with overall Low, Medium or High maturity. Level 1 implies basic effectiveness, while 3 is advanced effectiveness.

Measure class	Low	Medium	High
Security governance	1	2	3
Risk management	1	2	3
Management of third parties	1	2	2
Secure lifecycle process for smart grid components/systems and operating procedures	1	1	2
Personnel security, awareness and training	1	2	2
Incident response & information knowledge sharing	1	2	2
Audit and accountability	1	1	2
Continuity of operations	1	2	3
Physical security	2	3	3
Information systems security (incl. SG IA category)	1	2	3
Network security	2	3	3

Policy options can be structured as follows (see also Table 15):

- **Imposing obligations** on actors, which implies these need to progress to maturity level Medium.
- **Imposing compliance enforcement** requirements on actors, which implies these need to progress to maturity level High.

This relates only to the ENISA measure classes which are highlighted as key recommendation based on the risk assessment explained in Section 4. It needs to be clearly understood this as such links back to the developed high-priority threat scenarios as well as the impact weights and assessments in the various threat scenario analyses.

Step 3 – Map EU system operators to the type organisations

An own expert assessment is made on which proportion of EU energy companies fits with each defined maturity level as shown in Table 19. It is emphasised that the %-figures are estimates and should be interpreted with reasonable levels of uncertainty; by no means do these numbers pretend to represent actual monitoring information.

Table 19: Mapping of energy companies to maturity levels in today's situation. The last column informs on the approximate number of organisations in Europe

Sector	Actor	Low	Medium	High	Number of organisations
Electricity	TSO	0%	20%	80%	42
	DSO (large)[25]	0%	20%	80%	27
	DSO (small)	30%	40%	30%	~2400
	Market actors	20%	40%	40%	~102
Gas	TSO	0%	40%	60%	43
	DSO (large)	0%	40%	60%	183
	DSO (small)	30%	50%	20%	~1256
	Market actors	0%	50%	50%	~98

The assumptions are based on present size and operational responsibilities of system operators, as well as the assumption of an effective NIS directive implementation (which in reality will differ from country to country). As such no low-level TSO nor large DSO is considered, based on enforced regulatory measures. The differentiation

[25] The threshold for large DSOs is those entities with more than 100.000 connections. A similar threshold is applied in other EU legislation and studies. Apart from having evidently more limited resources, the operators with less than 100.000 connections also can have local generation plants in their portfolio.

medium/high is based on distribution of size and related capabilities. As electric utilities face more ICS equipment and are more confronted with real-time impact at wider regional level (see Section 1) compared to the gas sector, the shares are assumed different between gas and electricity TSO/DSOs. In the analysis 80% of electricity TSOs and large DSOs are assumed to be at high maturity, versus 60% of gas operators. Smaller DSOs are assumed to have lower maturity on average based on size and individual impact. Many DSOs outsource even basic IT and OT services to third parties and have limited budget and personnel available for supporting dedicated security processes. Basic processes are in place but can be improved. In both electricity and gas, 30% of the small DSOs are considered to be of low maturity presently. Across the larger DSOs, both in electricity and gas no low-maturity operators are assumed (as with TSOs). The category of other market participants covers a broad mix of large generator companies to smaller (new) aggregators and pure market traders/retailers. They cannot all be considered part of the critical infrastructure, and some may have less general budget and revenue. A deeper analysis on impact of these other market parties and subcategories on the overall system cybersecurity level may be recommended for future work. It needs to be recognized that also the total number of actors and their total market size (million €/yr turnover) differs strongly between the types. Policy options may seek proportional burden/effort sharing.

Step 4 – Establish company/sector reference costs and cost allocation keys

There exists no public robust dataset of costs for individual cybersecurity measures in the energy sector, nor on applied costs per type of system actor or country. The cost projection assessment in this study therefore applies a top-down approach to come to cost estimates per class of measures. The pan-EU metrics of Section 5.2 are used to come the following cost allocation keys (Table 20). The OT costs for electricity TSOs and DSOs are based on the reference costs as explained in section 5.2. For gas operators no robust data was found, hence the TSO and DSO OT costs are assumptions based on similar efforts for TSOs compared to the electricity sector, and substantially lower needs at distribution level due to lower levels of distributed resources and automation. For IT cybersecurity costs the lower cost levels as reported by utilities are applied, assuming these did not invest strongly yet in dedicated OT security. No reliable information exists for market actors, and therefore a strong assumption of 0.10% is taken in line with IT based cybersecurity costs for system operators

Table 20: Reference cost for IT and OT cybersecurity expenditures (estimate). Bracketed figures indicate higher levels of uncertainty.

	Actor	IT costs (% of revenues)	OT costs (% of revenues)
Electricity	TSO	0.10%	0.92%
	DSO	0.10%	0.48%
	Other	((0.10%))	((0.10%))
Gas	TSO	0.10%	(0.92%)
	DSO	0.10%	(0.24%)
	Other	((0.10%))	((0.10%))

Also the ENISA mitigation classes applied in the risk analysis are attributed with a cost allocation key depending on how much resources are assumed to be invested in IT or OT aspects (Table 21).

Table 21: Cost allocation across IT and OT domain for ENISA mitigation classes (estimate)

Measure class	IT focus	OT focus
Security governance	100%	0%
Risk management	100%	0%
Management of third parties	100%	0%
Secure lifecycle process for smart grid components/systems and operating procedures	20%	80%
Personnel security, awareness and training	50%	50%
Incident response & information knowledge sharing	100%	0%
Audit and accountability	100%	0%
Continuity of operations	50%	50%
Physical security	20%	80%
Information systems security (incl. SG IA category)	100%	0%
Network security	80%	20%

The parameters of Tables 19-20-21 allow to map which actor is incurring which annual expenditure for which type of cybersecurity measure category in today's situation. This is the reference for the cost projections of several EU policy options.

Step 5 – Extrapolate results to EU-wide costs per policy ambition

Based on the risk assessment developed in Section 4, and the methodology outlined in steps 1 to 4, a high-level projection can be made for costs of the various policy options identified in Section 5.1. Depending on priorities, impact weightings and identified threat scenarios an urgency-based ranking of mitigation classes is deduced in the analysis of Section 4.3.

In this cost projection a working assumption can be taken that e.g. all mitigation classes that scored 3, 4 or 5 should be considered in the various policy options. Based on the analysis of Section 4.3 (where the minimum priority score was 3) this implies all ENISA mitigation classes are considered. This is considered an appropriate starting point. In case further prioritisation is deemed relevant, one can follow the full work flow with other parameters and re-asses the cost projections (resulting in equal or lower figures).

Another key assumption taken is that for an industry actor segment to advance in maturity for a specific ENISA cybersecurity measure category from level 1 to 2 implies a doubling of annual expenditures on that specific category; an advancement of level 2 to 3 implies an additional 50% of annual expenditures. This is a strong assumption.

Interviews with industry stakeholders highlighted the uncertainty in the sector on the (monetary) effort needed to advance to a higher cybersecurity level.

5.4 Cost impact of advancing cybersecurity maturity

In Figure 26, a direction of annual cost projections in the various policy options is provided. The cost projections are broken down per system actor. These numbers represent overall EU28 annual expenditures.

As stated before, presently Europe's electricity system operators are estimated to spend a total of 700 million Euro annually on cybersecurity measures in the OT domain. Many are assumed to have a reasonable maturity level already with experiences gained over the past decades and recent national applications of the NIS directive. The described policy options 2 and 4, aiming for respectively obligation requirements to all operators or clearer compliance enforcement rules for the largest ones, are projected to add 10 to 20 million Euro annually in the electricity sector. Projected costs in the gas sector are assumed to be more limited due to lower degrees of decentralisation and digitization at distribution level as explained earlier. Projected costs for other market actors carry high uncertainty due to an even wider variety in size, legacy and operational models as system operators, and deserve more detailed analysis if legislative instruments are considered. Section 5.3 gave a structured view of how to build up a cost projection estimate. It is emphasized many of the parameters are uncertain in nature. The most impacting parameters are the shares of organizations across the three defined maturity levels.

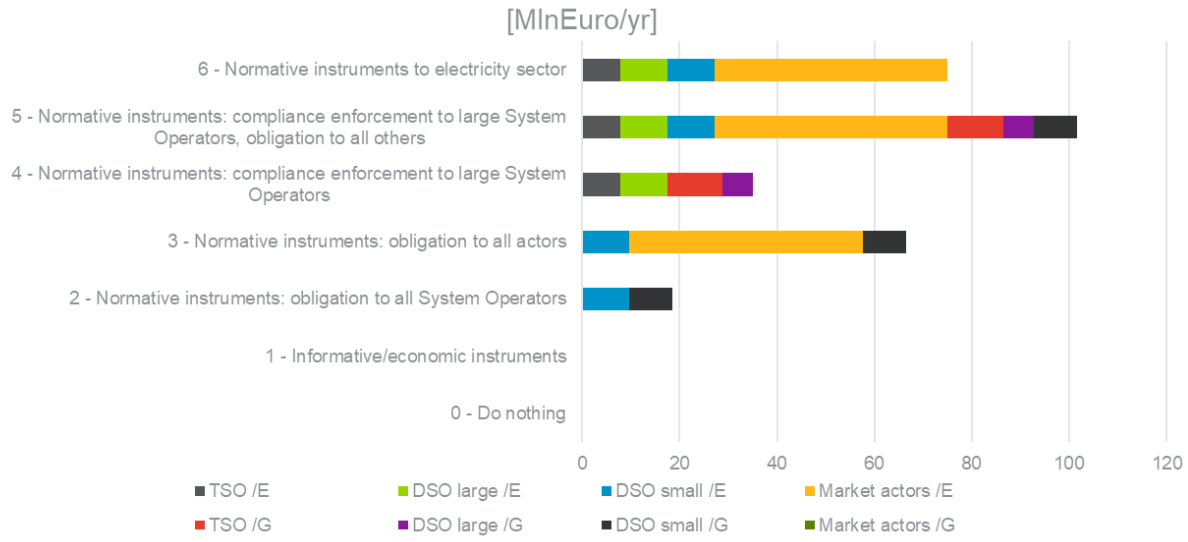

Figure 26: Cost projections for the identified policy options (additional annual costs in addition to today's ~700MlnEuro/year market)

It is crucial to interpret these figures with following understanding:

- These cost projections cover the capital and operational expenditures made by system operators and market actors on annual basis, taking into account reference data and assumptions as described earlier. These do not take into account additional costs or savings from initiatives related to knowledge sharing, standardisation, external certification/auditing etcetera.
- The underlying reference data is transparently described in this chapter, including the limited robust data sources and the need to rely on expert estimates and assumptions. The projections should therefore be interpreted in terms of order of magnitude and terms of comparison across actors and with other energy system costs. Another assumption on today's reference costs, e.g. by attributing more of a system operator's capital or operational expenditures to cybersecurity, will evidently substantially impact the projections.
- This study reviewed the present status of measures applied with TSOs and DSOs via stakeholder input/survey. Experts confirm the direction that higher maturities are seen with larger system operators, or those more advanced in digitizing their system operations. A more detailed monitoring across the EU28 and all energy actors will provide a more accurate view on present maturity levels, and harmonisation benefits.
- For most experts there is no simple rule as to what the cost may be to advance in maturity level by implementing new cybersecurity programs which reach deeper into the OT domain. The barriers rather than being pure financial are more related to complexity, long duration and lack of skilled workforce. System operators with extensive experience in dedicated cybersecurity programs report cycles of several years on clearly prioritised items.
- Analysing the cost for market actors (other than system operators) deserves a more profound study on its own due the large number of organisations and the wide variety in size, infrastructure and system impact.

For clarity and to trigger discussion the overall projections of Figure 26 are split in those for the electricity sector (Figure 27) and the gas sector (Figure 28).

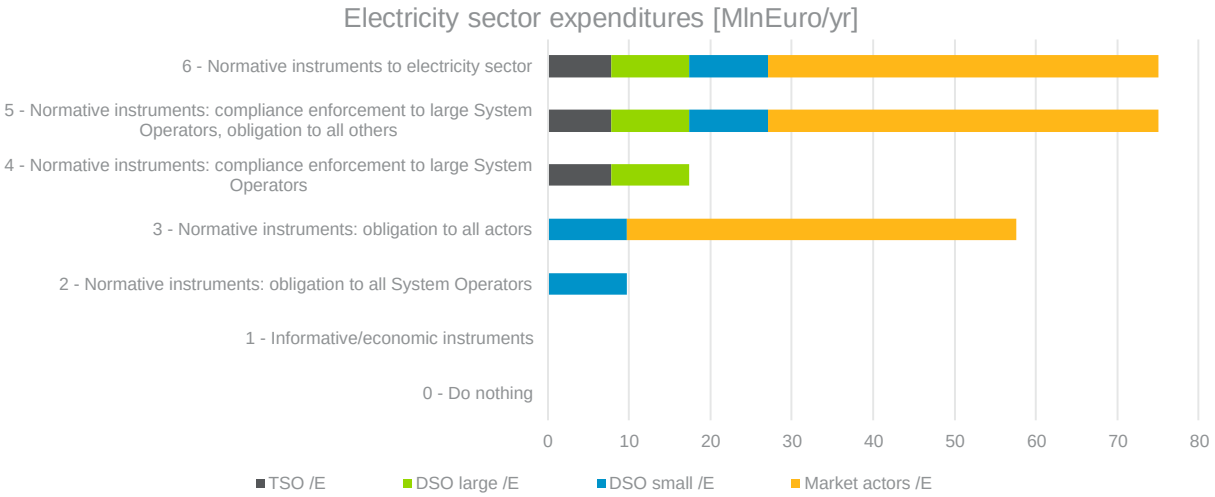

Figure 27: Cost projection for each policy option when applied only to the electricity sector in EU28. This is in addition to present annual expenditures among others based on the NIS directive implementation.

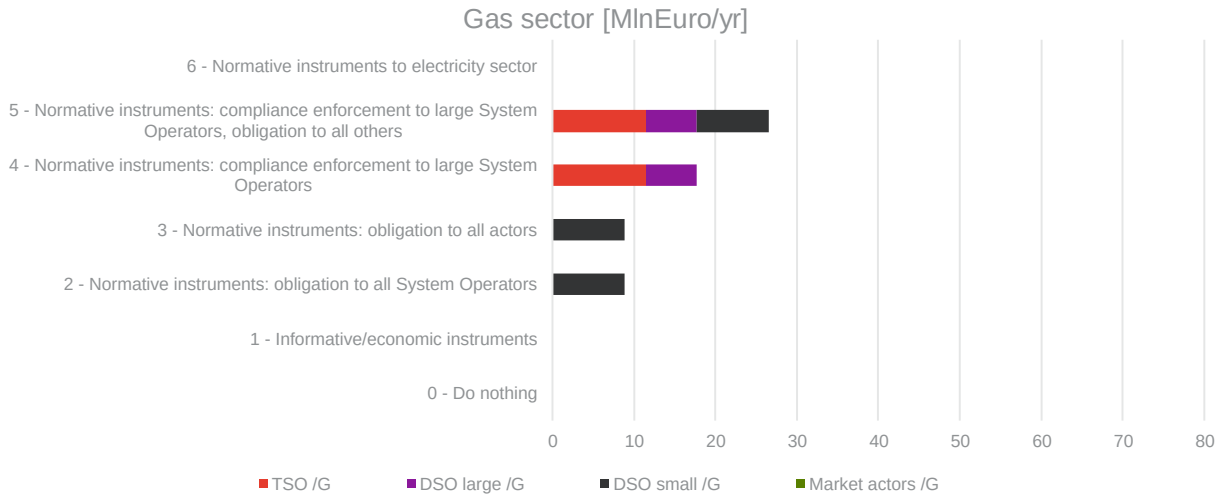

Figure 28: Cost projection for each policy option when applied only to the gas sector in EU28. This is in addition to present annual expenditures among others based on the NIS directive implementation.

The policy options where normative instruments would be imposed (e.g. a new legislation by means of a NIS directive update or network code specifically focused on the energy sector) are considered to have a projected cost impact of an additional various tens to 100 million€/year across the EU28 on top of a ~700 million€/year market. While on individual operator level these may be substantial costs, especially for smaller ones which have less progressed, this needs to be placed in the appropriate context. The impact on the energy consumer bill will be less than 0.2%. The benefits of appropriate cybersecurity levels (though not explicitly quantified in this study), are directly in line with some of the key objectives of the energy system to ensure reliable and secure energy to Europe's end consumers and economy. Most importantly such progress will require time, more industry guidance, and buy-in from regulators and other authorities.

6 EU industry and regulatory recommendations

6.1 Context

Cybersecurity has rapidly become a clear priority for organisations and for the European internal market. Across various industries the energy sector is acknowledged as being the more critical one due to importance of ensuring availability and integrity as well as the complexity of adopting new effective and future-proof measures. This calls for specific attention to what is needed in the European electricity and gas sector. The energy system is undergoing a massive transformation with more decentralised actors (renewable supply, demand flexibility, storage) which interact in a pan-European interconnected system and markets, and which benefit from digitized solutions. This wave of digitization and decentralisation settles on a system which has legacy assets designed to remain operational in closed networks for decades, and for which operational security and control measures exist to ensure continuity of operations but which may not be able to cope with the instantaneous impact of cyberattacks. Earlier industry-wide, policy driven and organisation-specific initiatives have tried to keep pace in implementing cybersecurity strategies for both the IT and OT domain and the interconnection of both. Given the diverse speed of implementation, organisational resources, and legacy systems, the level of maturity is considered highly diverse across Europe. Furthermore, a complete overview of actual, applied measures and spent efforts on cybersecurity for each member state or organisation is missing at the moment. In addition, organisations face substantial challenges in adopting well-tuned new strategies.

This study outlines the complexity of the European energy sector in this regard, typical threat scenarios, a proposal for an organisation-wide risk management approach, and a first projection of the cost impact in advancing cybersecurity maturity levels via EU policy instruments.

The main recommendations from the analysis and stakeholder engagement all confirm that the NIS directive and EC cybersecurity package provide the appropriate basis, and that its objectives and tools can be further developed for the specific challenges of the energy sector.

6.2 Overview on European policy options

The risk assessment performed in this study points out which cybersecurity measures should have higher priority depending on the maturity of organisations and highlighted scenario(s) or are more common across all situations. These technical measures can be promoted via a **set of policy options**. The cost projection in chapter 5 is based on a classification of potential policy options. These options can be achieved by normative, informative and economic instruments. This section provides further description on such potential instruments. Finally, section 6.3 concludes final recommendations for instruments based on the findings of the past chapters.

Some are implementable on the national level, others may require a European or an international approach. A further important aspect is the degree to which instruments tie in with pre-existing regulations via a specific transitional scheme. Conversely, it is important when introducing new courses of action to identify any possibly conflicting regulations, and to assess their significance.

Research contains numerous different classifications of policy instruments. It is conventional to distinguish between three classes: informative, economic and normative instruments. The classification is exemplified with potential instruments:

- **Normative instruments** require extensive involvement of European and national authorities and can have a strong effect on the market actors. These effects can be positive or negative and may not be in line with the intended objected. However, they ensure high planning security for market actors. Examples are
    - rules and bans;
    - mandatory cybersecurity certification schemes for products and services;
    - obligation on regular internal cybersecurity audits;
    - regular random compliance tests for installed equipment and units or processes in organisations by a defined authority (like for cars);
    - obligation of national monitoring reports on incidents, security gaps or cybersecurity expenditures;
    - stronger obligation for national authorities / Member States to coordinate national cybersecurity strategies / regulation with neighbouring countries;
    - definition of state-of-the art measures by regulation either in respect of responsible organisation (e.g. ENISA, ACER, CERT) or applied standards (presumption of conformity);
    - voluntary commitment, these can also be referred to simply as ‘standards’ and can be seen as normative measures or informative.
- **Informative instruments** are in general simple to be implemented, but require further actors like agencies or national bodies to be executed. They can increase transparency, enable cost synergies and reduce transaction costs for market actors to implement technical mitigation measures. Examples are
    - information campaigns or competence centres;
    - extended guidelines from relevant authorities to inform relevant stakeholders in the energy sector about cybersecurity frameworks / measures and best practices to increase security level specifically in the energy sector;
    - product labelling for pre-defined cybersecurity levels of generation units, industrial control systems or services, to address supply chain risks;
    - assessment and ranking regarding the security level of equipment of manufactures by independent authority;
    - definition of national contact person / authority for affected stakeholders regarding incidents and cybersecurity related processes;
    - regional cybersecurity forums for the energy sector.
- **Economic instruments** can result in strong incentives for market actors to change their behaviour or invest in certain technologies. However, economic instruments are usually strongly linked to questions regarding the right allocation of costs and market distortion. Examples are
    - clear financial incentives (subsidies or sanctions) for reaching goals or implementing standards;
    - coordination and support of research and pilot projects;
    - subvention of (certified) cybersecurity trainings for TSOs/DSOs or other actors.

Additionally, it is important in this context to categorise the instruments according to the target groups to which they apply as illustrated in Chapter 5. These particularly include:

- Transmission system operators
- Distribution system operators
- Market actors, like system users, manufacturers or retailers, aggregators or electricity power exchange

To address diverse actors, also including manufacturers of telecommunication equipment, on European level may requires coordination beyond just the energy domain.

6.3 Recommendations to advance cybersecurity maturity in the energy sector

Chapter IV in the NIS directive on “Security of the network and information systems of operators of essential services” puts forward broadly three types of objectives and requirements:

- Risk management;
- Security measures; and
- Incident response/handling.

Main recommendations for further progress can be structured along these same objectives as sketched in Figure 29. A full list of formulated recommendations is described in Table 22.

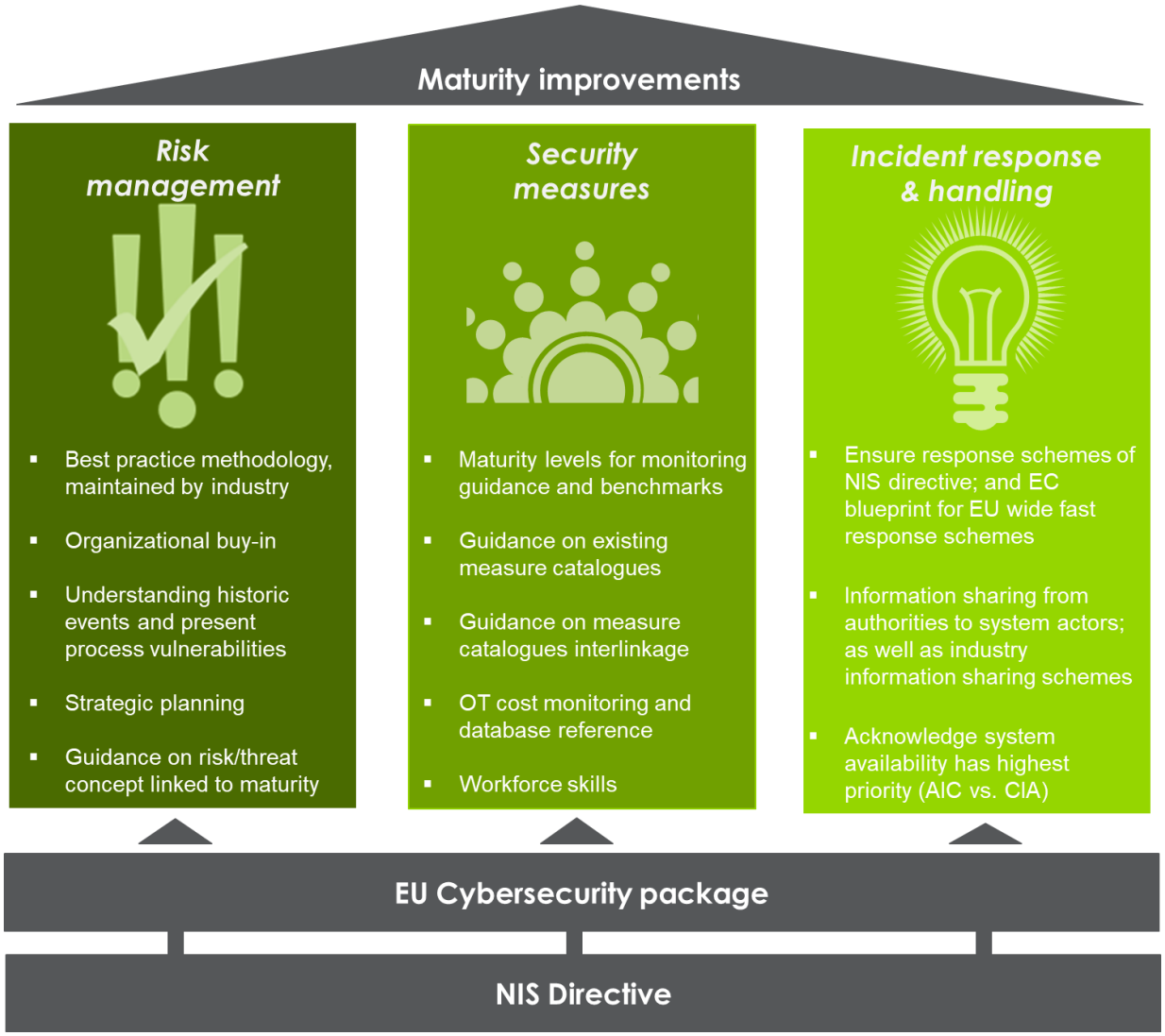

Figure 29: Main recommendations for advancing the objectives of the NIS directive and the Cybersecurity strategy in the energy sector

Table 22: Industry and regulatory recommendations for cybersecurity in the European energy sector

Objective	Recommendation
Risk management	Push best practice methods for risk management at country and organisation level, as well as standardisation at sector level. Apply a broad scope of processes and threat types. The risk analysis/management methodology of this study (Chapter 4) can serve as blueprint, or alternatively ISO27001 can be taken more specifically for information security. Analyse risks and mitigation options, but mostly show clear awareness for critical interfaces and processes where industry action is needed. An option is to establish a NIS directive and future European cybersecurity regulation implementation committee for the energy sector to facilitate the national implementation and feed into legislative processes. Experience can be taken from existing working groups on this specific domain as well as the European Stakeholder Committees on the European Network Codes.
	Aim for buy-in across the organization on the importance for cybersecurity in the company culture. Ensure there is senior management sponsorship for related programs. Actively discuss between system operators and NRA/government. Participate in open discussion in the sector and push for knowledge sharing to enhance NIS directive implementation and preparation of further legislative or voluntary industry guidance.
	Use understanding of historic events, enhanced OT vulnerability databases, and view on critical interfaces/processes to elaborate threat scenario lists and perform detailed scenario analyses to understand priority mitigations.
	Strategic planning/roadmap is needed across the organisation. Avoid disperse processes or reporting (cost/assets).
	Guidance is needed internally in the organisation or within the sector on risk definition, risk management objective, aimed maturity level and cost effectiveness. A 100% secure system is never possible, and any cybersecurity planning will face constraints in time, budget and resources, requiring a smart prioritisation of measure implementations.
	Clearer guidance on implementation is needed on risk level exposure going beyond Art 14(4) of the NIS directive, to avoid risk definitions and risk management frameworks become too abstract. Risk level differentiation already exists in the SGIS SL guidance or with more details in the approach suggested in Chapter 4. Clearer impact related risk levels could be made, e.g. comparable to electricity Security of Supply metrics sometimes enshrined in grid codes, national law or regulatory incentives (e.g. related to N-1 resiliency, max. LOLE, SAIDI, SAIFI parameters). This evidently requires the possibility of applying detailed risk analysis methodologies to assess risk exposures and impact of cybersecurity mitigation measures.
Security measures	Clear maturity levels are needed to have a comparative tool across EU in the energy sector, to identify areas for improvement and facilitate sharing of best practices. The maturity levels themselves can already provide for simple guidance on cybersecurity roadmaps to create buy-in from senior management or public authorities. Progress is to be monitored by regular inquiries and benchmarks performed by a national authority, integrated in the process of preparing national monitoring reports for the energy sector.
	Most available guidelines focus on the question which measures and frameworks exist. Still the industry needs more clarity on how to implement existing measures. Take lessons learned from advanced but complex guidance documents. Take lessons learned from other industries, e.g. telecom legislation or GDPR which show less ambiguity.
	Clarity is needed on relationship between various national and international mitigation catalogues already in place.

Objective	Recommendation
	Avoid financing becomes a bottleneck when overall benefits are considered to outweigh the costs. For regulated operators clear NRA guidance on cost recovery and allocation is crucial. This can possibly split overall IT cybersecurity measures, and OT related expenditures which suffer more from inherent time delays and are more entwined with normal infrastructure CAPEX/OPEX. Also, a reference database of unit costs for energy specific OT cybersecurity expenditures may help, such as already exists for electricity and gas transmission assets developed by ACER. Special treatment of OT related cybersecurity costs in tariff reviews may speed up progress and a least give guidance and clarity. The suggested monitoring exercise on cybersecurity progress would clearly link to this.
	In addition to tools and finance issues, a main barrier for raising in cybersecurity maturity is for most stakeholders still the lack in skilled workforce. This domain needs also a long-term investment in education. On the shorter-term, sector guidance on how to apply security-as-as-service by external support can help.
Incident response and handling	The NIS directive prescribes reporting to the relevant authority or CSIRT; as well as from the CSIRT to relevant other Member States. The EC's Blueprint for rapid emergency response needs to be activated further.
	Additional fast response schemes or information sharing tools should be promoted, also directly between industry actors.
	Information sharing from authorities to operators of essential services is key.

Article 15 of the NIS directive gives prescriptions for implementation and enforcement already. With further policy instruments it is recommended to bear in mind following key principles for any upcoming cybersecurity regulation:

- Avoid lock-in to very specific practices, which may complicate future legislative updates or national legislation. Cybersecurity threat developments and solutions are highly dynamic.
- For any instrument, consider sufficient implementation guidance. An option could be to have stakeholder implementation committees (in analogy with gas/electricity network codes under auspices of ACER/ENTSOs)
- Open industry standards (globally) need to be driven further with sufficient attention for European energy system context. Policy tools can be used to ensure timely progress in industry standardisation, e.g. via mandate-driven preparatory work and harmonised standards as reference for compliance efforts.

As explained earlier, one needs to consider which specific actors to apply legislative proposals to, based on risks posed on the system, and costs of implementation (Chapter 5). Differentiations can be made by sector (gas/electricity), according to size (including smaller DSOs or not), and by restricting it to system operators or extending to all market actors (including generators, traders, aggregators).

Regardless of which instrument is applied there is a need for clear monitoring tools in cybersecurity risk management. This would ensure threat scenarios are regularly reviewed, effectiveness of measures is reviewed, and cost monitoring is transparent to facilitate best practice sharing and regulatory processes.

7 References

[1] Council of the European Union, *COUNCIL DIRECTIVE 2008/114/EC,* 2008.

[2] The European Parliament and the Council of the European Union, *DIRECTIVE (EU) 2016/1148,* 2016.

[3] European Commission, *Clean Energy For All Europeans,* 2016.

[4] European Commission, *Communication from the Commission on a European Programme for Critical Infrastructure Protection,* 2006.

[5] European Parliament, European Council, European Economic and Social Committee and Committee of the Regions, *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace,* 2013.

[6] European Commission, *The European Agenda on Security,* 2015.

[7] European Commission, *A Digital Single Market Strategy for Europe,* 2015.

[8] European Commission, *Proposal for a regulation of the European Parliament and the European Council on ENISA, the "EU Cybersecurity Agendy, and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act"),* 2017.

[9] Energy Expert Cyber Security Platform, *Cyber Security in the Energy Sector: Recommendations for the European Commission on a European Strategic Framework and Potential Future Legislative Acts for the Energy Sector,* 2017.

[10] Rapid7 Labs, *National Exposure Index,* 2018.

[11] Symantec, *Internet Security Threat Report,* 2018.

[12] Telecommunication Union of the United Nations, *Global Cybersecurity Index,* 2015.

[13] International Energy Agency, *Digitalization & Energy,* 2017.

[14] German Energy Agency (dena), *Schnittstellen und Standards für die Digitalisierung der Energiewende,* 2018.

[15] Electric Power Research Institute, *Electric Power System Resiliency, Challanges and Opportunities,* 2016.

[16] Navigant Research, *IoT and Analytics for Utilities Market Overview,* 2018.

[17] Navigant Research, *5G and the Internet of Energy,* 2017.

[18] European Commission, *Workshop on digitising the energy value chain,* 2018.

[19] Magazin für die Energiewirtschaft, *Kennzahlenvergleich für Netzleitstellen - Netzleitstellen im Vergleich,* 2018.

[20] D. C. ,. M. K. D. S. N. B. a. C. G. B. Johnson, „Attackers Deploy New ICS Attack Framework 'TRITON' and Cause Operational Disruption to Critical Infrastructure," 14 December 2017. [Online]. Available: https://www.fireeye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html.

[21] C. Bing, „Trisis has the security world spooked, stumped and searching for answers," 16 January 2018. [Online]. Available: https://www.cyberscoop.com/trisis-ics-malware-saudi-arabia/.

[22] *TRISIS Malware Analysis of Safety System Targeted Malware,* 2017.

[23] S. M. a. E. Reese, „A Totally Tubular Treatise on TRITON and TriStation," 7 June 2018. [Online]. Available: https://www.fireeye.com/blog/threat-research/2018/06/totally-tubular-treatise-on-triton-and-tristation.html.

[24] „RiSI Database," [Online]. Available: http://risidata.com.

[25] NCSC, „Guidance," [Online]. Available: https://www.ncsc.gov.uk/index/guidance.

[26] *ENISA Threat Landscape Report 2017,* 2018, pp. 1-86.

[27] Smart Grids Task Force Expert Group 2, *Interim Report, Recommendations for the European Commission on Implementation of a Network Code on Cybersecurity,* 2017.

[28] Computer Emergency Response Team, *https://cert.europa.eu,* 2018.

[29] 1. National Electric Sector Cybersecurity Organization Resource (NESCOR) Technical Working Group, „Electric Sector Failure Scenarios and Impact Analyses – Version 3.0," 2015.

[30] *ENISA Threat Taxonomy,* 2016.

[31] P. Eder-Neuhauser, T. Zseby, J. Fabini und G. Vormayr, „Cyber attack models for smart grid environments," *Sustainable Energy, Grids and Networks,* Bd. 12, pp. 10-29, 2017.

[32] M. Atighetchi, B. Simidchieva, F. Yaman, T. Eskridge, M. Carvalho und N. Paltzer, „Using ontologies to quantify attack surfaces," *CEUR Workshop Proc.,* Bd. 1788, pp. 10-18, 2016.

[33] 1. National Electric Sector Cybersecurity Organization Resource (NESCOR) Technical Working Group, „Analysis of Selected Electric Sector High Risk Failure Scenarios First Version," 2013.

[34] N. Beach-Westmoreland, J. Styczynski und S. Stables, „When The Lights Went Out," 2016.

[35] A. (. B. A. R. Dabrowski, J. (. B. A. R. Ullrich und E. R. (. B. A. R. Weippl, „Grid Shock : Coordinated Load-Changing Attacks on Power Grids — The Non-Smart Power Grid is Vulnerable to Cyber Attacks as Well," in *ACSAC 2017*, 2017.

[36] Smart-Grid Task Force Stakeholder, *Best available techniques reference document for cyber-security and privacy of the 10 minimum functional requierements of the smart metering system,* 2016.

[37] A. Berger et al, *Reference Architecture for Secure Smart Grids in Austria – RASSA,* 2016.

[38] Offis Institut, University of applied sciences Salzburg, Ecofys, *Protection and security analysis as part of the development of smart grids in Switzerland,* 2016.

[39] Secunet, *Secure information and communication technologies for an intelligent energy network,* 2013.

[40] National Renewable Laboratory (NREL), *States of Cybersecurity: Electricity Distribution System Discussions,* 2017.

[41] A. Selhofer, K. Tidten und S. Beirer, *Whitepaper Anforderungen an Österreich sichere Steuerungs- und Telekommunikationssysteme,* 2018.

[42] Raad voor de leefomgeving en infrastructuur (Rli), *Power Supply under Digital Voltage,* 2018.

[43] Cyber Security Raad, *Towards a secure digital connected Society - Advice on the Cybersecurity of the Internet of Things,* 2017.

[44] T. S. G. I. P. C. S. W. Group und T. S. G. I. Panel, „Introduction to NISTIR 7628 Guidelines for Smart Grid Cyber Security," 2010.

[45] B. Guttman und E. A. Roback, An introduction to computer security: the NIST handbook, DIANE Publishing, 1995.

[46] *Framework for Improving Critical Infrastructure Cybersecurity,* 2010.

[47] C. Dan, C. B. d. Q. Pedro und G. G. Fernando, *Appropriate security measures for smart grids,* 2012, p. 84.

[48] Å. J. Holmgren, „A Framework for Vulnerability Assessment of Electric Power Systems," in *Crit. Infrastruct. Reliab. Vulnerability*, A. T. Murray und T. H. Grubesic, Hrsg., Berlin, Heidelberg: Springer Berlin Heidelberg, 2007, pp. 31-55.

[49] G. H. Kjølle, I. B. Utne und O. Gjerde, „Risk analysis of critical infrastructures emphasizing electricity supply and interdependencies," *Reliab. Eng. Syst. Saf.,* Bd. 105, pp. 80-89, 2012.

[50] S. Kriaa, M. Bouissou und Y. Laarouchi, „A new safety and security risk analysis framework for industrial control systems," *Risk and Reliability,* 2018.

[51] S. Kriaa, M. Bouissou, L. Piètre-Cambacedes und Y. Halgand, „A Survey of Approaches Combining Safety and Security for Industrial Control Systems," *Reliab. Eng. Syst. Saf.,* Bd. 139, pp. 156-178, 2 2015.

[52] M. A. McQueen, W. F. Boyer, M. A. Flynn und G. A. Beitel, „Quantitative cyber risk reduction estimation methodology for a small SCADA control system," *Proc. Annu. Hawaii Int. Conf. Syst. Sci.,* Bd. 9, p. 226, 2006.

[53] M. A. McQueen, W. F. Boyer, M. A. Flynn und G. A. Beitel, „Time-to-Compromise Model for Cyber Risk Reduction Estimation," *Qual. Prot. Secur. Meas. Metrics,* Bd. 23, pp. 49-64, 2006.

[54] NSA, „A Framework for Assessing and Improving the Security Posture of Industrial Control Systems (ICS)," pp. 1-18, 2010.

[55] „SG-CG / M490 / F Overview of SG-CG Methodologies Version 3.0," 2017.

[56] CAPEC, „A Community Knowledge Resource for Building Secure Software," 2015.

[57] W. Paper, P. Gustafson, D. Lillis, B. A. Becker, T. O. Sullivan, M. Scanlon, Y. Devices, L. Control, U. Ultrasound, E. U. D. G. Connect, E. Keshet, K. Findings, C. Lévy-Bencheton, E. Darra, G. Tétu, G. Dufay, M. Alattar, R. Roshan, A. K. Ray, K. International, J. K. Choi, R. G. Dinda, H. Chaouchi, T. Internet, D. F. O. R. Science, C. On, D. Economy, A. S. Devices, S. C. Alliance, A. T. D. L. E-guide, M. Togan, B.-c. Chifor, I. Florea, G. Gugulea, UL, P. Fremantle, P. Scott, A. Oxford, T. Green, D. Howell, E. Wilson, V. Chellappan, K.

M. Sivalingam, BSI, K. C. Montgomery, J. Chester, K. Kopp und T. Internet, *Security Call to Action — Good practices and Recommendations,* Bd. 153, 2015, pp. 16-19.

[58] R. a. M. K. Mattioli, *Communication Network Interdependencies in Smart Grid,* 2015.

[59] *National Cyber Security Strategies,* 2012.

[60] C. Trick, „When The Lights Are Out“.

[61] ". (. E. C. S. Platform), „Cyber Security in the Energy Sector — Recommendations for the European Commission on a European Strategic Framework and Potential Future Legislative Acts for the Energy Sector,“ 2017.

[62] NIST, „Security and Privacy Controls for Federal Information Systems and Organizations Security and Privacy Controls for Federal Information Systems and Organizations,“ *Sp-800-53Ar4,* p. 400+, 2014.

[63] S. Grid und C. Committee, „SMART GRID INTEROPERABILITY PANEL NISTIR 7628 User´s Guide A White Paper developed by the Smart Grid Interoperability Panel Smart Grid Cybersecurity Committee,“ 2014.

[64] ENISA, *Analysis of ICS-SCADA Cyber Security Maturity Levels in Critical Sectors,* 2015.

[65] „Smart Grid Information Security,“ 2012.

[66] „Guidelines for Smart Grid Cybersecurity,“ 2014.

[67] Q. Zhu und T. Basar, „A hierarchical security architecture for smart grid,“ in *Smart Grid Communications and Networking*, E. Hossain, Z. Han und H. V. Poor, Hrsg., 2012.

[68] B. Zhu, A. Joseph und S. Sastry, „A taxonomy of cyber attacks on SCADA systems,“ *Proc. - 2011 IEEE Int. Conf. Internet Things Cyber, Phys. Soc. Comput. iThings/CPSCom 2011,* pp. 380-388, 2011.

[69] K. Zetter, „Inside the Cunning, Unprecedented Hack of Ukraineś Power Grid,“ *WIRED,* 2016.

[70] J. Wynn, J. Whitmore, G. Upton, L. Spriggs, D. McKinnon, R. McInnes, R. Graubart und L. Clausen, „Threat Assessment & Remediation Analysis (TARA),“ *MITRE Tech. Rep.,* p. 60, 2011.

[71] C. Wueest, „Targeted Attacks Against the Energy Sector,“ *Symantec Corp.,* pp. 1-29, 2014.

[72] W. Wang und Z. Lu, „Cyber security in the Smart Grid: Survey and challenges," *Comput. Networks,* Bd. 57, pp. 1344-1371, 2013.

[73] K. Wälder und O. Wälder, Methoden zur Risikomodellierung und des Risikomanagements, 2017.

[74] S. Vidalis und A. Jones, „Analyzing Threat Agents and Their Attributes.," *Eciw,* pp. 1-15, 2005.

[75] V. Veen, Y. Fratantonio, M. Lindorfer, D. Gruss, C. Maurice, G. Vigna, H. Bos, K. Razavi und C. Giuffrida, „Drammer: Deterministic Rowhammer Attacks on Mobile Platforms," *Proc. 2016 ACM SIGSAC Conf. Comput. Commun. Secur. - CCS'16,* pp. 1675-1689, 2016.

[76] V. V. Vadlamudi, O. Gjerde und G. Kj??lle, „Dependability and security-based failure considerations in protection system reliability studies," *2013 4th IEEE/PES Innov. Smart Grid Technol. Eur. ISGT Eur. 2013,* pp. 9-13, 2013.

[77] M. Uslar, M. A. Ammelsvoort, D. Christina, J. Engel, C. Neureiter und C. Nabe, „Schutz- und Sicherheitsanalyse im Rahmen der Entwicklung von Smart Grids in der Schweiz," 2016.

[78] M. Uslar, C. Rosinger und S. Schlegel, „Anwendung des NISTIR 7628 für Informationssicherheit im Smart Grid Architecture Model (SGAM)," *Tagungsband VDE-Kongress 2014 Smart Cities,* p. 6, 2014.

[79] M. Uma und G. Padmavathi, „A survey on various cyber attacks and their classification," *Int. J. Netw. Secur.,* Bd. 15, pp. 390-396, 2013.

[80] R. J. Turk, *Cyber Incidents Involving Control Systems,* 2005, pp. 1-58.

[81] J. Trefke, S. Rohjans, M. Uslar, S. Lehnhoff, L. Nordstrom und a. Saleem, „Smart Grid Architecture Model use case management in a large European Smart Grid project," *IEEE PES ISGT Eur. 2013,* pp. 1-5, 2013.

[82] I. A. Tøndel, J. Jensen und L. Røstad, „Combining misuse cases with attack trees and security activity models," *ARES 2010 - 5th Int. Conf. Availability, Reliab. Secur.,* pp. 438-445, 2 2010.

[83] D. Tofan und T. Nikolakopoulos, *The cost of incidents affecting CIIs,* 2016.

[84] A. Teixeira, G. Dán, H. Sandberg und K. H. Johansson, „A cyber security study of a SCADA energy management system: Stealthy deception attacks on the state estimator," *IFAC Proc. Vol.,* Bd. 18, pp. 11271-11277, 2011.

[85] A. Teixeira, S. Amin, H. Sandberg, K. H. Johansson und S. S. Sastry, „Cyber security analysis of state estimators in electric power systems," in *49th IEEE Conf. Decis. Control*, 2010.

[86] Symantec, „Dragonfly: Cyberespionage Attacks Against Energy Suppliers," 2014.

[87] E.-c. C. Study und J. Stevens, „Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2) (Case Study) James Stevens Senior Member, Technical Staff - CERT® Division," 2014.

[88] K. Stouffer, J. Falco und K. Scarfone, „Guide to Industrial Control Systems (ICS) Security," *Recomm. Natl. Inst. Stand. Technol.,* pp. 1-157, 2007.

[89] W. Stölzle, „Supply Chain Event Management," *Gabler Lex. Logistik,* Bd. 44, pp. S. 503--504, 2004.

[90] A. Stock, B. Glas, N. Smithline und T. Gigler, „OWASP Top 10 2017," *Web Appl. Secur. Proj.,* 2017.

[91] W. Stallings und L. Brown, Computer Security: Principles and Practice, Third Hrsg., Pearson Educated Limited, 2015, p. 840.

[92] C. Spataru und J. W. Bialek, „Energy networks: A modelling framework for European optimal cross-border trades," *IEEE Power Energy Soc. Gen. Meet.,* Bde. %1 von %22014-Octob, pp. 1-5, 2014.

[93] H. M. Sneed, „Integrating Legacy Software into a Service Oriented Architecture," *Softw. Maint. Reengineering, 2006. CSMR 2006. Proc. 10th Eur. Conf.,* pp. 1-11, 2006.

[94] U. C. T. E. Secretariat, „Introduction to the UCTE Operation Handbook".

[95] J. Searle und G. Rasche, „NESCOR Guide to Penetration Testing for Electric Utilities," pp. 1-58, 2013.

[96] B. Schneier, „Attack Trees," *Dr. Dobbś J. Softw. Tools Prof.,* 1999.

[97] H. G. Schaathun, „Session objectives Threats , Threat Agents , and Vulnerabilities Threat Paths Responsive Controls Preventive Controls," *Power,* 2010.

[98] C. Salter, O. S. Saydjari, B. Schneier und J. Wallner, „Toward A Secure System Engineering Methodology," *Proc. 1998 Work. New Secur. Paradig. (NSPW ́98),* pp. 2-10, 1998.

[99] M. Sabir Idrees, Y. Roudier und L. Apvrille, „Model the System from Adversary Viewpoint: Threats Identification and Modeling," *Electron. Proc. Theor. Comput. Sci.,* Bd. 165, pp. 45-58, 2014.

[100] K. C. Ruland, J. Sassmannshausen, K. Waedt und N. Zivic, „Smart grid security -- an overview of standards and guidelines," *e & i Elektrotechnik und Informationstechnik,* Bd. 134, pp. 19-25, 01 2 2017.

[101] C. Piaszczyk, „Model Based Systems Engineering with Department of Defense Architectural Framework," *Syst. Eng.,* Bd. 14, pp. 305-326, 2011.

[102] A. Opel, „Design and implementation of a support tool for attack trees," *Internsh. Thesis, Otto-von-Guericke Univ. Magdebg. (March 2005),* 2005.

[103] NIST, „Security and Privacy Controls for Federal Information Systems and Organizations Security and Privacy Controls for Federal Information Systems and Organizations," National Institute of Standards and Technology, 2014.

[104] Nist, N. S. Publication, N. I. Standards und Technology, „NIST Special Publication 1108 NIST Framework and Roadmap for Smart Grid Interoperability Standards," *Nist Spec. Publ.,* Bd. 0, pp. 1-90, 2010.

[105] C. Neureiter, D. Engel und M. Uslar, „Domain Specific and Model Based Systems Engineering in the Smart Grid as Prerequesite for Security by Design," *Electronics,* Bd. 5, p. 24, 5 2016.

[106] P. Neray, *Anatomy of the TRITON ICS Cyberattack,* 2018.

[107] A. P. A. P. Moore, R. J. R. J. Ellison und R. C. R. C. Linger, „Attack modeling for information security and survivability," 2001.

[108] L. Mili, „Taxonomy of the Characteristics of Power System Operating States," *2nd NSF-RESIN Work.,* pp. 1-13, 2011.

[109] S. E. McLaughlin, D. Podkuiko, A. Delozier, S. Miadzvezhanka und P. D. McDaniel, „Embedded Firmware Diversity for Smart Electric Meters.," in *HotSec*, 2010.

[110] R. Mattioli und K. Moulinos, *Analysis of ICS-SCADA Cyber Security Maturity Levels in Critical Sectors,* 2015.

[111] R. Mattioli und K. Moulinos, *Communication Network Interdependencies in Smart Grid,* 2015.

[112] M. Masera, I. N. Fovino und B. Vamanu, *ICT aspects of power systems and their security,* Citeseer, 2011.

[113] L. Marinos, *Smart Grid Threat Landscape and Good Practice Guide,* 2013, pp. 1-83.

[114] L. Marinos, *ENISA Threat Taxonomy,* 2016.

[115] D. Liveri und A. Sarri, *An Evaluation Framework for National Cyber Security Strategies,* 2014, p. 15.

[116] Z. Li, P. Avgeriou und P. Liang, „A systematic mapping study on technical debt and its management," *Journal of Systems and Software,* Bd. 101, pp. 193-220, 2015.

[117] E. LeMay, M. D. Ford, K. Keefe, W. H. Sanders und C. Muehrcke, „Model-based security metrics using adversary view security evaluation (advise)," in *Quant. Eval. Syst. (QEST), 2011 eighth Int. Conf.*, 2011.

[118] R. Lee, M. Assante und T. Connway, „ICS CP/PE (Cyber-to-Physical or Process Effects) case study paper--German steel mill cyber attack," *Sans ICS,* 2014.

[119] R. M. Lee, M. J. Assante und T. Conway, „German Steel Mill Cyber Attack," *Ind. Control Syst.,* pp. 1-15, 2014.

[120] R. M. Lee, M. J. Assante und T. Conway, „Analysis of the Cyber Attack on the Ukrainian Power Grid," *Sans,* p. 23, 2016.

[121] L. Labaka, J. Hernantes und J. M. Sarriegi, „Resilience framework for critical infrastructures: An empirical study in a nuclear plant," *Reliab. Eng. Syst. Saf.,* Bd. 141, pp. 92-105, 2015.

[122] D. Kushner, „The real story of stuxnet," *ieee Spectr.,* Bd. 3, pp. 48-53, 2013.

[123] S. Kriaa, M. Bouissou und L. Piètre-Cambacédès, „Modeling the Stuxnet attack with BDMP: Towards more formal risk assessments," *7th Int. Conf. Risks Secur. Internet Syst. Cris. 2012,* 2012.

[124] S. Kriaa, M. Bouissou und Y. Laarouchi, „A Model Based Approach For SCADA Safety and Security Joint Modelling: S-cube," 10 2015.

[125] T. Krause und H. Tanriverdi, „Gegen den Strom," *Süddeutsche Zeitung Magazin.*

[126] B. Kordy, L. Piètre-Cambacédès und P. Schweitzer, „DAG-Based Attack and Defense Modeling: Don't Miss the Forest for the Attack Trees," *Comput. Sci. Rev.,* Bd. 318003, pp. 1-57, 11 2013.

[127] J. König, P. Närman, U. Franke und L. Nordström, „An extended framework for reliability analysis of ICT for power systems," *2011 IEEE PES Trondheim PowerTech Power Technol. a Sustain. Soc. POWERTECH 2011,* pp. 1-6, 2011.

[128] P. Kocher, D. Genkin, D. Gruss, W. Haas, M. Hamburg, M. Lipp, S. Mangard, T. Prescher, M. Schwarz und Y. Yarom, „Spectre Attacks: Exploiting Speculative Execution," 2018.

[129] M. Karresand, „A Proposed Taxonomy of Software Weapons," 2002.

[130] P. Karpati, A. L. Opdahl und G. Sindre, „Investigating security threats in architectural context: Experimental evaluations of misuse case maps," *J. Syst. Softw.,* Bd. 104, pp. 90-111, 2015.

[131] C. Internet Security, „The CIS Security Metrics," *Cent. Internet Secur.,* Bd. 1.1.0, p. 175, 2010.

[132] D. Inc, „CRASHOVERRIDE Analysis of the Threat to Electric Grid Operations," pp. 1-35, 2017.

[133] J. D. Howard und T. A. Longstaff, „A common language for computer security incidents," 1998.

[134] K. Harrison und G. White, „A taxonomy of cyber events affecting communities," *Proc. Annu. Hawaii Int. Conf. Syst. Sci.,* pp. 1-9, 2011.

[135] S. Hansman und R. Hunt, „A taxonomy of network and computer attacks," *Comput. Secur.,* Bd. 24, pp. 31-43, 2 2005.

[136] A. Gyrard, C. Bonnet und K. Boudaoud, „The STAC (Security Toolbox : Attacks & Countermeasures) ontology," *22nd Int. World Wide Web Conf. Brazil, May 13-17, 2013,* pp. 165-166, 2013.

[137] O. M. Guillen, D. Schmidt und G. Sigl, „Practical Evaluation of Code Injection in Encrypted Firmware Updates," in *2016 Design, Automation & Test in Europe Conference & Exhibition (DATE)*, 2016.

[138] C.-H. Genzel, O. Hoffmann und R. Sethmann, „Zusammenfassung relevanter Informationssicherheitsstandards für deutsche Verteilungsnetzbetreiber," 2017.

[139] I. Friedberg, K. McLaughlin und P. Smith, „Towards a Cyber-Physical Resilience Framework for Smart Grids," in *Intell. Mech. Netw. Config. Secur.*, Springer LNCS, 2015.

[140] B. Filkins, „IT Security Spending Trends," *SANS Institute InfoSec Read. Room,* 2016.

[141] EPRI, „Guidelines for Leveraging NESCOR Failure Scenarios in Cyber Security Tabletop Exercises," 2014.

[142] ENISA, „Cyber security : Cyber security : future challenges and opportunities Authors :".

[143] ENISA, *Cyber Insurance: Recent Advances, Good Practices and Challenges,* 2016.

[144] Enisa, *Introduction to Return on Security Investment,* 2012, p. 18.

[145] Z. Drias, A. Serhrouchni und O. Vogel, „Taxonomy of attacks on industrial control protocols," *Int. Conf. Protoc. Eng. ICPE 2015 Int. Conf. New Technol. Distrib. Syst. NTDS 2015 - Proc.,* 2015.

[146] G. L. Doorman, K. Uhlen, G. H. Kjolle und E. S. Huse, „Vulnerability analysis of the Nordic power system," *IEEE Trans. Power Syst.,* Bd. 21, pp. 402-410, 2 2006.

[147] A. Dobrovoljc, D. Trcek und B. Likar, „Predicting Exploitations of Information Systems Vulnerabilities Through Attackers´Characteristics," *IEEE Access,* Bd. XX, pp. 1-1, 2017.

[148] M. a. C. Dekker, *Annual Incident Reports 2013,* 2013.

[149] S. G. C. Committee, „NISTIR 7628 User's Guide," SMART GRID INTEROPERABILITY PANEL, 2014.

[150] J. Clarke, M. G. Hidalgo, A. Lioy, M. Petkovic, C. Vishik und J. Ward, *Consumerization of IT: Risk Mitigation Strategies,* 2012.

[151] A. Cherepanov, „WIN32/INDUSTROYER A new threat for industrial control systems," 2017.

[152] C. Cheh, K. Keefe, B. Feddersen, B. Chen, W. G. Temple und W. H. Sanders, „Developing Models for Physical Attacks in Cyber-Physical Systems," *Proc. 2017 Work. Cyber-Physical Syst. Secur. Priv. - CPS 1́7,* pp. 49-55, 2017.

[153] T. (. I. T. Casey, „Threat Agent Library Helps Identify Information Security Risks," *Intel White Pap.,* p. 12, 2007.

[154] E. J. Byres, M. Franz und D. Miller, „The use of attack trees in assessing vulnerabilities in SCADA systems," *Int. Infrastruct. Surviv. Work.,* pp. 1----9, 2004.

[155] M. Brecht und T. Nowey, „A closer look at information security costs," *Econ. Inf. Secur. Priv.,* pp. 3-24, 2013.

[156] C. Brasca, E. Ciapessoni, D. Cirio, A. Pitto, M. Sforna und A. Morini, „Extended risk analysis of power and ICT systems," *2013 4th IEEE/PES Innov. Smart Grid Technol. Eur. ISGT Eur. 2013,* pp. 1-5, 2013.

[157] E. Bompard, T. Huang, Y. Wu und M. Cremenescu, „Classification and trend analysis of threats origins to the security of power systems," *Int. J. Electr. Power & Energy Syst.,* Bd. 50, pp. 50-64, 9 2013.

[158] D. Bodeau, R. Graubart, J. Picciotto und R. McQuaid, Cyber Resiliency Engineering Framework, 2012, p. 78.

[159] M. Bishop, Introduction to computer security, Bd. 11, 1992, pp. 121-127.

[160] M. H. Beek, H. Muccini und P. Pelliccione, „Software Engineering for Resilient Systems," *9th Int. Work. SERENE 2017 Geneva, Switzerland, Sept. 4-5, 2017,* Bd. LNCS 10479, pp. 91-105, 2017.

[161] S. Bavarian und L. Lampe, Communications and access technologies for smart grid, 2010, pp. 111-146.

[162] E. Baezner, E. T. H. Robin und), Cyber and Information warfare in the Ukrainian conflict, 1 Hrsg., 2017, pp. 1-28.

[163] M. Assante und R. Lee, „The Industrial Control System Cyber Kill Chain," *SANS Inst. InfoSec Read. Room,* 2015.

[164] A. Ashok, M. Govindarasu und J. Wang, „Cyber-Physical Attack-Resilient Wide-Area Monitoring, Protection, and Control for the Power Grid," *Proc. IEEE,* Bd. 105, pp. 1389-1407, 2017.

[165] C. Anderson und K. Sadjapour, Iranś Cyber Threat, 2018.

[166] A. AlMajali, E. Rice, A. Viswanathan, K. Tan und C. Neuman, „A systems approach to analysing cyber-physical threats in the Smart Grid," in *2013 IEEE Int. Conf. Smart Grid Commun.*, 2013.

[167] H. Acker, S. Loitz und W. H. Wellssow, „Improving the accuracy of system security assessment in highly stressed transmission grids," *2013 4th IEEE/PES Innov. Smart Grid Technol. Eur. ISGT Eur. 2013,* pp. 1-5, 2013.

[168] N. Abrek, „Attack Taxonomies and Ontologies," *Netw. Archit. Serv.,* pp. 1-10, 2015.

[169] *System Operation Guideline (draft).*

[170] *Smart Grid Reference Architecture,* 2012.

[171] „Smart Grid Reference Architecture," 2012.

[172] *Six Monthly Report on the Implementation of the Cyber Defence Policy Framework,* 2016, p. 54.

[173] *SG-CG / / H Smart Grid Information Security,* 2014, pp. 1-95.

[174] *Security for industrial control systems — Framework overview — A good practice guide.*

[175] „Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors," 2018.

[176] „Leitfaden Informationssicherheit IT-Grundschutz kompakt," 2012.

[177] *Information technology — Security techniques — Information security controls for the energy utility industry,* 2017.

[178] „Industrial Control System Security — Top 10 Bedrohungen und Gegenmaßnahmen 2016," 2016.

[179] *IEC 62351-2 Ed.1: Data and Communication Security - Part 2: Glossary of terms,* 2007, pp. 0-31.

[180] *IEC 62351-1 TS Ed.1: Data and communication security - Part 1: Introduction and overview,* 2007, pp. 0-31.

[181] *Framework for Improving Critical Infrastructure Cybersecurity,* 2017, pp. 1-41.

[182] „Die Lage der IT-Sicherheit in Deutschland 2016," 2016.

[183] „Destructive Malware," 2017.

[184] „Defending Critical Infrastructure," *Interfaces (Providence).,* Bd. 36, pp. 530-544, 2006.

[185] *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace,* 2013.

[186] „Cyber-attack against ukrainian critical infrastructure," 2016.

[187] „Cyber Security and in the Energy and Sector," 2017.

[188] *Common Vulnerability Scoring System v3.0: Specification Document,* 2016, pp. 1-38.

[189] *Common cyber attacks: reducing the impact,* 2016.

[190] *CIP-009-4 Cyber Security — Recovery Plans for Critical Cyber Assets,* 2011, pp. 1-6.

[191] *CIP-008-4 Cyber Security — Incident Reporting and Response Planning,* 2011, pp. 1-6.

[192] *CIP-007-4 Cyber Security — Systems Security Management,* 2011, pp. 1-6.

[193] *CIP-006-4 Cyber Security — Physical Security of Critical Cyber Assets,* 2011, pp. 1-6.

[194] *CIP-005-4 Cyber Security — Electronic Security Perimeter(s),* 2011, pp. 1-6.

[195] *CIP-003-4 Cyber Security — Security Management Controls,* 2011, pp. 1-6.

[196] *CIP –004–4 — Cyber Security — Personnel and Training,* 2011, pp. 2-5.

[197] *CIP 002-4 Cyber Security — Critical Cyber Asset Identification,* 2011, pp. 1-6.

[198] „CCMC SEGCG / M490 / G Smart Grid Set of Standards," 2017.

[199] „Attack Trees for Selected Electric Sector High Risk Failure Scenarios," 2013.

[200] The European Parliament and the European Council, *REGULATION (EU) 2016/679,* 2016.

8 Annex

8.1 Overview of relevant cyber incidents

Table 23 Overview of relevant cyber incidents in the energy sector based on ENISA, RISI Online Incident Database, Symantec and US-CERT

ID	Year	Title	Location	Description	Attack Vectors	(Intended) Outcome
1	1982	CIA Trojan Causes Siberian Gas Pipeline Explosion	Siberia, USSR	Thomas Reed, senior US national security official, claims in his book “At The Abyss” that the United States allowed the USSR to steal pipeline control software from a Canadian company. This software included a Trojan Horse that caused a major explosion of the Trans-Siberian gas pipeline in June 1982. The Trojan ran during a pressure test on the pipeline but doubled the usual pressure, causing the explosion. (#1, #2) “In order to disrupt the Soviet gas supply, its hard currency earnings from the West, and the internal Russian economy, the pipeline software that was to run the pumps, turbines, and valves was programmed to go haywire, after a decent interval, to reset pump speeds and valve settings to produce pressures far beyond those acceptable to pipeline joints and welds,” Reed writes. (#3) The scheme to plant bugs in Soviet software was masterminded by Gus Weiss, who at the time was on the National Security Council and who died last year. Soviet agents had been so keen to acquire US technology, they didn’t question its provenance. (#4) Russian newspaper sources deny the report, saying an explosion did take place, but it was caused by poor construction, not by planted software. “What the Americans have written is rubbish,” said Vasily Pchelintsev, who in 1982 headed the KGB office in the Tyumen region, the likely site of the explosion described in the book.” (#5) Impact: The software sabotage had two effects, explains Reed. The first was economic. By creating an explosion with the power of a three-kiloton nuclear weapon, the US disrupted supplies of gas and consequential foreign currency earnings. But the project also had important psychological advantages in the battle between the two superpowers. “By implication, every cell of the Soviet leviathan might be infected,” Reed writes. “They had no way of knowing which equipment was sound, which was bogus. All was suspect, which was the intended endgame for the entire operation.”	malicious update	physical damage
2	1994	The Salt River Project Hack	Arizona, U.S	Between July 8th and August 31st, 1994, the perpetrator, Lane Jarret Davis, accessed a computer or computers belonging to the Salt River Project via a dial-up modem on a backup computer. He was able to access data and delete files on systems responsible for the monitoring and delivery of water and power to Salt River Project customers, as well as customer, financial and personnel records. The impacts reported on this incident are very contradictory. According to probation records Davis was able to access the canal control SCADA system for at least 5 hours, and he would have accessed customer, financial and personnel records. SRP estimated that they suffered a $40,000 loss, not including the loss of productivity. The press reports and statement by Assistant Attorney General Michael Chertoff that Davis had control of the SCADA system controlling the Roosevelt Dam spill gates are believed to be	disgruntled employee	financial damage

ID	Year	Title	Location	Description	Attack Vectors	(Intended) Outcome
				incorrect. According to emails from SRP representatives to the Washington Post, the canal SCADA system and dam SCADA systems were not connected.		
3	2000	Russian gas pipeline attack	Russia	According to Russian officials, the largest natural gas extraction company in the country was successfully attacked in 2000. The attackers used a Trojan to gain access to the control of the gas pipelines. Through this switchboard, the flow for individual gas pipelines could have been modified, which would have easily caused a widespread disruption.	Trojan	physical damage disruption of service
4	2001	Californian's power distribution attack	California, U.S	In 2001 an attack took place against California's power distribution centre, which controls the flow of electricity across California. Due to apparently poor security configuration, the attacker was able to compromise two Web servers that were part of a developer network and penetrate further from there. Fortunately, the attackers were stopped before they could attack any of the systems which were tied into the transmission grid for the Western United States.	server compromise	disruption of service
5	2003	Power Industry Slammer	United States	A server on the utilities' control centre LAN running SQL was not patched. The worm apparently migrated through the corporate networks until it finally reached the critical SCADA network via a remote computer through a VPN connection. The SCADA control network used frame relay. The telecommunications frames relay provider utilised Asynchronous Transfer Mode (ATM) through the telecommunications network backbone for a variety of services. The ATM bandwidth became overwhelmed by the worm, blocking SCADA traffic on the Frame Relay service.	server compromise	collateral
6	2003	(slammer) DoS to Monitoring System Ohio Nuclear Plant	Ohio, U.S	In 2003 the safety monitoring system of the Ohio nuclear power plant apparently went offline for several hours due to a Slammer worm infection. Fortunately, the power plant was already offline due to maintenance and the installed secondary backup monitoring system was unaffected by the worm. Nevertheless the incident raised safety concerns.	server compromise (worm)	collateral
7	2003	Sabotage attack against marine terminal in Venezuela	Venezuela	At the beginning of 2003 a marine terminal in Venezuela was targeted by a sabotage attack. Details of this attack are scarce and vague, but it seems that during a strike an attacking group managed to get access to the SCADA network of the oil tanker loading machinery and overwrote programmable logic controllers (PLCs) with an empty program module. This halted machinery, preventing oil tankers from loading for eight hours till the unaffected backup code was reinstalled on the PLCs. The attack was not too sophisticated as it was easily spotted. A small modification of the PLC code instead would have probably gone unnoticed for a long time.	code inclusion CAPEC-175	damage disruption of service
8	2003	London August 2003 Power Blackout	United Kingdom	The blackout was caused by a sequence of events. During this time period a scheduled maintenance shutdown was underway on one circuit of the line. Next, an alarm was received at the Electricity nation control centre, indicating that a transformer or its associated shunt reactor was in distress and could fail, causing significant safety and environmental impacts. National Control contacted EDF Energy and asked them to disconnect the distribution system from the transformer and switch off. After the switching process took place, the automatic protection equipment on a circuit interpreted the switching as a fault. The automatic protection relay disconnected this circuit from the rest of the transmission system causing a loss of supply.	accident	

ID	Year	Title	Location	Description	Attack Vectors	(Intended) Outcome
9	2003	SCADA/EMS Alarm System Failure Contributes to Blackout	United States	According to the U.S.-Canada Power System Outage Task Force Report, a significant contributing factor to the August 14th blackout was the failure of the First Energy (FE) Energy Management System (EMS) Alarm system and the operators' unawareness of this critical failure.	accident	
10	2004	SCADA workstation infected by Korgo worm	U.S	The SCADA operator workstations got hit with the W32/Korgo worm virus. They were out of service starting at 14:33 and all terminals were back by 18:23. These three terminals were on the corporate Intranet outside the SCADA firewall.	server compromise (worm)	collateral
11	2006	Kama sutra virus	India	A 'Kama Sutra' virus attack was observed in the Indian power network.	server compromise (virus)	collateral
12	2007	Computer Glitch Causes Major Power Outage	United States	A computer glitch is being blamed for a massive power outage in the Phoenix area. Between 80,000-100,000 Salt River Project customers were affected. The outage lasted 20-30 minutes. The Salt River Project has a system in place to balance loads if it is unable to supply power. That didn't happen on the day of the outage. There was a computer problem that thought it did and it triggered the widespread outage.	accident (software error)	
13	2008	Cyberattacks to power equipment from cities	Worldwide	In 2008, Tom Donahue, a senior Central Intelligence Agency (CIA) official told a meeting of utility company representatives that cyberattacks had taken out power equipment in multiple cities outside the United States. In some cases, the attacker tried to extort money from the energy companies, threatening them with further blackouts.	unspecified cyber attack	financial gain
14	2008	Failed Sensor on Wind Turbine Caused Shower of Ice Shards	United Kingdom	A sensor that was supposed to turn off the wind turbine under icy conditions did not operate as expected. Ice formed on the blades and showered nearby homes with large chunks of ice.	accident	
15	2008	Blackout in Florida	United States	A field engineer was diagnosing a malfunctioning 138 kV switch at Florida Power and Light Flagami substation in West Miami, Florida. Without authorisation, the engineer disabled two levels of relay protection. The local primary protection and the local backup breaker failure protection were disabled. Standard procedures were violated. Removing two levels of protection is not allowed. When the switch was opened an electrical arc was generated that migrated to other energised equipment and ground causing a major short circuit.	accident (malpractice)	
16	2008	Georgia Nuclear Power Plant Shutdown	United States	Hatch Nuclear Power Plant was forced to shut down for 48 hours after a contractor updated software on a computer that was on the plant's business network. The computer was used to monitor chemical and diagnostic data from one of the facility's primary control systems. The software was designed to synchronise data on both systems. When the updated computer rebooted, it reset the data on the control system to interpret the lack of data as a drop in water reservoirs that cooled the plant's radioactive nuclear rods. The safety system triggered a shutdown. The engineer was not aware that the control system would be synchronised as well and that a reboot would reset the control system.	accident (faulty/malicious update)	

ID	Year	Title	Location	Description	Attack Vectors	(Intended) Outcome
17	2009	Energy Company virus attack	Australia	A virus attack on Integral Energy's computer network forced the company to restructure all of its 1,000 desktops. External security experts were called in to rebuild all of the desktop computers to contain and remove the virus. The malware had not affected the power grid. Chris Gatford, a security consultant from Hacklabs, had conducted penetration testing on critical infrastructure said there was often 'ineffective segregation' or more typically none at all between the IT network and the network that monitors and controls the infrastructure. However a spokesperson from Integral Energy stressed that the virus attacks Microsoft products and the network doesn't run on Microsoft and there was no way that the virus could make its way onto the grid. The virus was the W32 Virut.CF strain which has been described as 'a particularly sinister file infector' that spreads quickly and is considered difficult to remove. Integral Energy's computer networks were protected by a Symantec security solution, a source said. The Symantec website states that the virus installs a back door enabling hackers to issue commands to the infected machines via an internet relay chat (IRC) channel. According to Gatford, the antivirus software was not updated in a timely manner on some machines or the Symantec product could not detect it. Integral Energy supplies electricity to Western Sydney and the Illawarra region of New South Wales distributing electricity to 2.1 million people in NSW.	server compromise (virus)	collateral
18	2009	Spies breach electricity grid in U.S.	United States	The U.S. electrical grid is under attack from Russian and Chinese cyber spies who have inserted software that could disrupt the system, current and former national security officials tell the Wall Street Journal. The report follows a Pentagon announcement Tuesday which showed more than $100 million was spent in the last six months responding to and repairing damage from cyberattacks and other computer network problems, military leaders said.	APT	disruption of service
19	2009	Texas power company hack	United States	A former employee of a Texas power utility was arrested on May 28, 2009 for crippling the company's energy forecast system. The ex-employee, Don Chul Shin was fired from Energy Future Holdings on March 3, 2009 for performance reasons and was escorted off of the property. However, the company failed to immediately shut off his VPN access. Later that day, Shin's account was used to log onto the corporate network, e-mailing out proprietary data to a personal Yahoo account linked to Shin and modifying and deleting files. Company logs indicated that the VPN connection originated from Shin's IP address. While logged onto the corporate VPN, an e-mail was sent asking the engineering group operating the Comanche Peak nuclear reactor asking what would happen if the load were to be "increased to 99.7 % of capacity". Shin was responsible for programming the models which controlled the management of EFH power generation facilities, including the Comanche Peak reactor. The company reported the sabotage on March 6, 2009. Energy Future Holdings is the corporate parent of three large Texas electric companies, including Luminent, which operates the Comanche Peak nuclear power plant.	disgruntled employee	information damage (information)

ID	Year	Title	Location	Description	Attack Vectors	(Intended) Outcome
20	2009-2010	Operation Night Dragon	Worldwide	Operation Night Dragon, which was uncovered in 2010, is a typical example of global oil companies being targeted, but this time not with the aim of disruption in mind. The attacks started in late 2009 and were directed at finding project details and financial information about oil and gas field exploration and bids. The attackers started by compromising public facing Web servers through SQL injection and installing Web shells on them. Once they had control over the server they used common hacking tools to harvest local passwords, dump password hashes, sniff authentication messages and exploit internal active directory configuration. This allowed them to move on to other internal computers using the gathered passwords. In addition, spear phishing messages were used to compromise additional computers. The attackers did not use any zero-day vulnerabilities during their attacks. Rather they used publicly available tools for each individual job. On compromised computers a common Backdoor Trojan was installed that communicated back to the C&C server, allowing remote access to the computer. This allowed the attacker to find and extract valuable information.	server compromise	disruption of service
21	2010	Dragonfly	Worldwide	The current targets of the Dragonfly group, based on compromised websites and hijacked software updates, are the energy sector and industrial control systems, particularly those based in Europe.	APT	damage disruption of service
22	2010	Iran nuclear plant attack, Stuxnet	Narantz, Iran	This threat started in July 2010. Stuxnet is the first known autonomous threat to target and sabotage industrial control systems to such an extent. Stuxnet is a sophisticated piece of malware, which uses seven vulnerabilities to spread and infect its targets. The most notable vulnerability is the Microsoft Windows Shortcut 'LNK/PIF' Files Automatic File Execution Vulnerability (CVE-2010-2568), which allows it to auto-execute on USB drives. Spreading through infected portable media drives allowed it to also infect networks isolated by air gaps that are unreachable from the internet. This was most likely the first infection vector used by Stuxnet. In addition, it is able to infect project files, which are used to control Programmable Logic Controllers (PLCs). This allowed the worm to infect computers whenever the engineer exchanged the project files. Besides this, it also spread through network shares, a printer spooler vulnerability, an old Windows RPC (remote procedure calls) vulnerability and a known password in the WinCC database.	malicious update code inclusion server compromise	damage (physical)
23	2011	Duqu, the next Stuxnet	Worldwide	On October 14, 2011, we were alerted to a sample by the Laboratory of Cryptography and System Security (CrySyS) at Budapest University of Technology and Economics. The threat appeared very similar to the Stuxnet worm from June of 2010. CrySyS named the threat Duqu [dyü-kyü] because it creates files with the file name prefix '~DQ'. The research lab provided their detailed initial report to us, which we have added as an appendix. The threat was recovered by CrySyS from an organisation based in Europe and has since been found in numerous countries. We have confirmed W32.Duqu is a threat nearly identical to Stuxnet, but with a completely different purpose. Duqu infections have been confirmed in six possible organisations in eight countries.	virus infection	damage

ID	Year	Title	Location	Description	Attack Vectors	(Intended) Outcome
24	2012	Flame attack, Iran's oil industry and Iran's Natanz nuclear	Iran	Iran's key oil industry was briefly affected last month by the powerful computer virus known as Flame, which has unprecedented data-snatching capabilities and can eavesdrop on computer users, a senior Iranian military official said Wednesday. The comment is the first direct link between the emergence of the new malware and an attack inside a highly sensitive computer system in Iran, which counts on oil revenue for 80% of its income. The full extent of last month's disruptions has not been disclosed, but Iran was forced to cut internet links to the country's main oil export terminal, presumably to try to contain the virus.	virus infection	
25	2012	Shamoon/Disttrack attack to oil producers	Saudi Arabia	On 15 August 2012, the computer network of Saudi Aramco was struck by a self-replicating virus that infected as many as 30,000 of its Windows-based machines. Despite its vast resources as Saudi Arabia's national oil and gas firm, Aramco, according to reports, took almost two weeks to recover from the damage. Viruses frequently appear on the networks of multinational firms but it is alarming that an attack of this scale was carried out against a company so critical to global energy markets. Later dubbed Shamoon, the virus caused significant disruption to the world's largest oil producer. Shamoon's main function appears to have been the indiscriminate deletion of data from computer hard drives. Although this did not result in an oil spill, explosion or other major fault in Aramco operations, the attack affected the business processes of the company, and it is likely that some drilling and production data were lost. Shamoon also spread to the networks of other oil and gas firms, including that of RasGas. The incident comes after years of warning about the risk of cyberattacks against critical infrastructure.	virus infection	damage (data)
26	2012	U. S. Electric Utility Virus Infection	United States	A virus infection was discovered in a turbine control system at a U. S. power plant. The infection ultimately impacted approximately 10 computers on the control system network. A third-party technician used a USB drive that was infected with a variant of the Mariposa virus. The infection was responsible for the downtime of the impacted systems and it delayed the plant restart for approximately 3 weeks.	virus infection	disruption of service
27	2013	Austrian and German power grid DoS attack	Austria and Germany	In 2013 part of the Austrian and German power grid nearly broke down after a control command was accidentally misdirected. It is believed that a status request command packet, which was broadcast from a German gas company as a test for their newly installed network branch, found its way into the systems of the Austrian energy power control and monitoring network. Once there, the message generated thousands of reply messages, which generated even more data packages, which in turn flooded the control network. To stop this self-inflicted DDoS attack, part of the monitoring and control network had to be isolated and disconnected. Fortunately the situation was resolved without any power outages.	accident	
28	2014	Russian-Based Dragonfly Group Attacks Energy Industry	United States	Dragonfly a group that has been operating since at least 2011, first started by targeting defence and aviation companies in the U.S. and Canada. In 2013, the group moved their focus into the U.S. and European energy firms. Dragonfly gains entry through these methods: 1. Spear phishing emails delivering malware. 2. Watering hole attacks that redirected visitors to energy industry-related websites hosting an exploit kit. 3. Infecting legitimate software from three different ICS (industrial control systems) equipment manufacturers. As of now Dragonfly's main motive seems to be cyber espionage, with a likelihood of sabotage in the future.	APT spear phishing watering hole malicious update	information damage

ID	Year	Title	Location	Description	Attack Vectors	(Intended) Outcome
29	2015	Ukraine Distribution Grid Operators	Ukraine	On Dec. 23rd in 2015 nearly 225,000 customers in three areas of the Ukraine had to endure 3 hours of blackout due to (likely) the first cyber attack on the control system of a power grid. The perpetrators had entered the enterprise IT through targeted emails carrying weaponised VBA Word or Excel attachments. Opening the files installed the RAT "Black Energy 3" on the workstations. From there the attackers extended their foothold and access privileges for at least 6 months until they deployed specially crafted malware to the SCADA and field system enabling them to affect multiple substations.	APT spear phishing watering hole credential harvesting code inclusion	disruption of service
30	2016	Israeli Power Grid Massive cyber attack	Israel	Israel underwent record-breaking electricity consumption for two days with a demand of 12,610 Megawatts due to the freezing temperatures, confirmed Israel Electric Corporation. In Mid-July 2015, the Israel's National Cyber Bureau had already warned about the computer-based hacking attacks, which shut down portions of the country's electricity grid. The identity of the suspects behind this attack has not been disclosed, and the energy ministry provided no details about how the attack was carried out. However, a spokesperson for Israel's Electricity Authority confirmed some of its computer systems had been shut down for two days due to the cyber attack.	APT	cyber warfare
31	2016	Michigan electricity utility downed	Michigan, U.S	April 25, the BWL became aware of a malware incident that affected the BWL's corporate network. As a precaution, they immediately initiated a self-imposed lockdown of all corporate systems. This incident had no impact on the delivery of water and electricity. All of BWL's utility operations are and remain fully functional. The water and electricity authority needed a week to recover from the ransomware attack that fortunately only hit its enterprise systems.		financial gain
32	2016	Virus in NPP	Gundremmingen, Germany	Virus Confiker and Ramnit had been found on computers for a cargo crane that had no internet connection nor a connection to the control room.	Worm (USB-Stick)	collateral
33	2017	Attack on UK TSO	UK	EirGrid Vodafone router attacked via Vodafone's Direct Internet Access (DIA) service, leading to direct TSO network access.		
34	2017	North Korean Actors Spear Phish U.S. Electric Companies	North Korea, USA	"We can confirm that FireEye devices detected and stopped spear phishing emails sent on Sept. 22, 2017, to U.S. electric companies by known cyber threat actors likely affiliated with the North Korean government. This activity was early-stage reconnaissance, and not necessarily indicative of an imminent, disruptive cyber attack that might take months to prepare if it went undetected."	spear phishing	cyber warfare
35	2017	APT activity alert	USA	"Since at least May 2017, threat actors have targeted government entities and the energy, water, aviation, nuclear, and critical manufacturing sectors, and, in some cases, have leveraged their capabilities to compromise victims' networks. Historically, cyber threat actors have targeted the energy sector with various results, ranging from cyber espionage to the ability to disrupt energy systems in the event of a hostile conflict. [1] Historically, threat actors have also targeted other critical infrastructure sectors with similar campaigns." Propagation of threat could be detected through all phases of Stage 1 of the ICS CKC.	APT	cyber warfare
36	2017	Gaza Cybergang attacks Oil and Gas facilities	MENA Region	"In mid-2017, the attackers were discovered inside an oil and gas organisation in the MENA region, infiltrating systems and pilfering data, apparently for more than a year. While traces of Android mobile malware have been spotted, attackers have continuously used the Downeks downloader and the Quasar or Cobaltstrike RATs to target Windows devices, enabling them to obtain remote		cyber warfare

ID	Year	Title	Location	Description	Attack Vectors	(Intended) Outcome
				access spying and data exfiltration abilities. This is now achieved more efficiently using the CVE 2017-0199 vulnerability which enables direct code execution abilities from a Microsoft office document on non-patched victim Windows systems. The use of Microsoft Access database files has also enabled the attackers to maintain low levels of detection, as it's not an uncommon method to deliver malware. These developments have helped the attackers continue their operations, targeting a variety of victims and organisations, sometimes even bypassing defences and persisting for prolonged periods."		
37	2017	TRITON	UK	"Mandiant recently responded to an incident at a critical infrastructure organisation where an attacker deployed malware designed to manipulate industrial safety systems. The targeted systems provided emergency shutdown capability for industrial processes. We assess with moderate confidence that the attacker was developing the capability to cause physical damage and inadvertently shutdown operations. This malware, which we call TRITON, is an attack framework built to interact with Triconex Safety Instrumented System (SIS) controllers. We have not attributed the incident to a threat actor, though we believe the activity is consistent with a nation state preparing for an attack. TRITON is one of a limited number of publicly identified malicious software families targeted at industrial control systems (ICS). It follows Stuxnet which was used against Iran in 2010 and Industroyer which we believe was deployed by Sandworm Team against Ukraine in 2016. TRITON is consistent with these attacks, in that it could prevent safety mechanisms from executing their intended function, resulting in a physical consequence."	malware (trilog.exe)	disruption of service

8.2 Overview of selected high-priority scenarios in the European energy sector

Table 24 Overview of selected high-priority scenarios in the European energy sector

Threat ID	System	Description	Attack Vector	Threat Agent	Outcome	Example	Source
1	ICT-System	Infection through intrusion detection system / firewall (IDS)	Security System	All external	Access		Offis
2	IT/OT-System	Virus/Trojan infiltrates ICS (industrial control system) systems as an unintended collateral	Operation Zone	all intentional	Disruption, Environmental, Damage	Gundremmingen 2016, Integral Energy 2009	Offis
3	Office ICT-System	Phishing Employees on Enterprise Level propagates to field level manipulation	Enterprise Zone	Nation State, Organised Crime	Disruption	Ukraine 2015/16	Offis
4	Substation	Malicious Update to Firmware in the Field to Influence Function of Single Substation	Field Zone	Nation State	Disruption, Environmental, Damage	Siberian Gas Pipeline 1982	Offis
5	Control centre (TSO, DSO)	Cross-sector, cross-	Field Zone	Careless Employee	Disruption, Damage	Germany-Austria 2013	Offis

Threat ID	System	Description	Attack Vector	Threat Agent	Outcome	Example	Source
		border message flooding					
6	IT/OT-System	Compromise through SCADA App	Personal mobile device	Nation State, Hacker	Access		Offis
7	DSO	Advanced persistent threat (APT) to power disruption in DSO flexibility management system	Operations Zone	Hackers, Nation State	Disruption	Ukraine 15, DGM.11	Offis / NESCOR
8	Generation	Plant tripped off-line through access gained through a compromised vendor remote connection	Field Zone	All external	Disruption	Generic: software update by manufacture GEN.15	NESCOR
9	Supply Chain	Supply Chain Vulnerabilities Used to Compromise Distribution Grid Management (DGM) Equipment	Operations Zone	Nation State	Access	DGM.8	NESCOR
10	IT/OT-System	Weakened Security during Disaster enables DGM Compromise	Operations Zone	all	Access	Manhattan Terror Attack 2017, DGM.9	NESCOR
11	Smart Meter	Rogue Firmware Enables Unauthorized Mass Remote Disconnect	Supply Chain	Nation State	Disruption	AMI.31	NESCOR

8.3 Use Cases and the Smart Grid Architecture Model (SGAM)

The work of Mandate 490 provided a Smart Grid Architecture Model (SGAM) as reference for Use Cases and further analyses. SGAM gives clear interoperability layers in the smart grid domain which is defined by zones and domains (Figure 30).

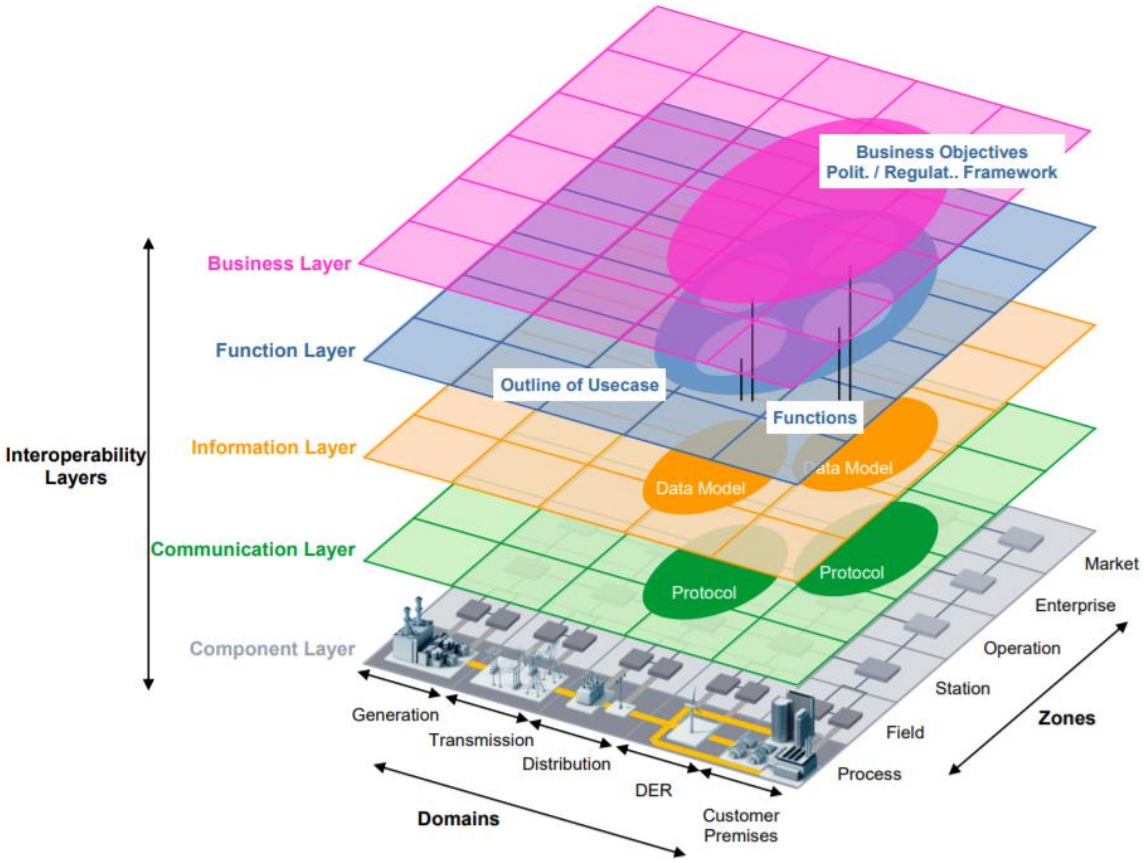

Figure 30: Smart Grid Architecture Model (Mandate 490)

Example Use Case "Control of Distributed Energy Resources" in NISTIR 7628 – modelled based on IEC 62559 information gathered form stakeholders

A simple scenario or business process is used to introduce the Use Case method. Within a virtual power plant various mostly small distributed energy resources (DER) are combined to achieve substantial block of flexible capacity and, thus, to act as if they were a bigger single unit. Trading of energy at markets or providing various ancillary services is one focus of this virtual power plant (e.g. energy arbitrage, portfolio imbalance minimization, frequency control, voltage control, grid recovery or contingency planning). Based on their individual generation forecasts, virtual power plant (VPP) operators contract with market participants and create schedules to operate their individual units for a so-called combined product. To realize such a plan at operational level, generation and load has

to be adapted to the needs of the market bid. Typically, this is done by direct control of the individual plants (control unit for DER) or by providing incentives to the owners to behave appropriately. In Figure 31, the communication and data exchange of the actors in this Use Case is displayed in a so-called UML sequence diagram that is explained in the following paragraphs.

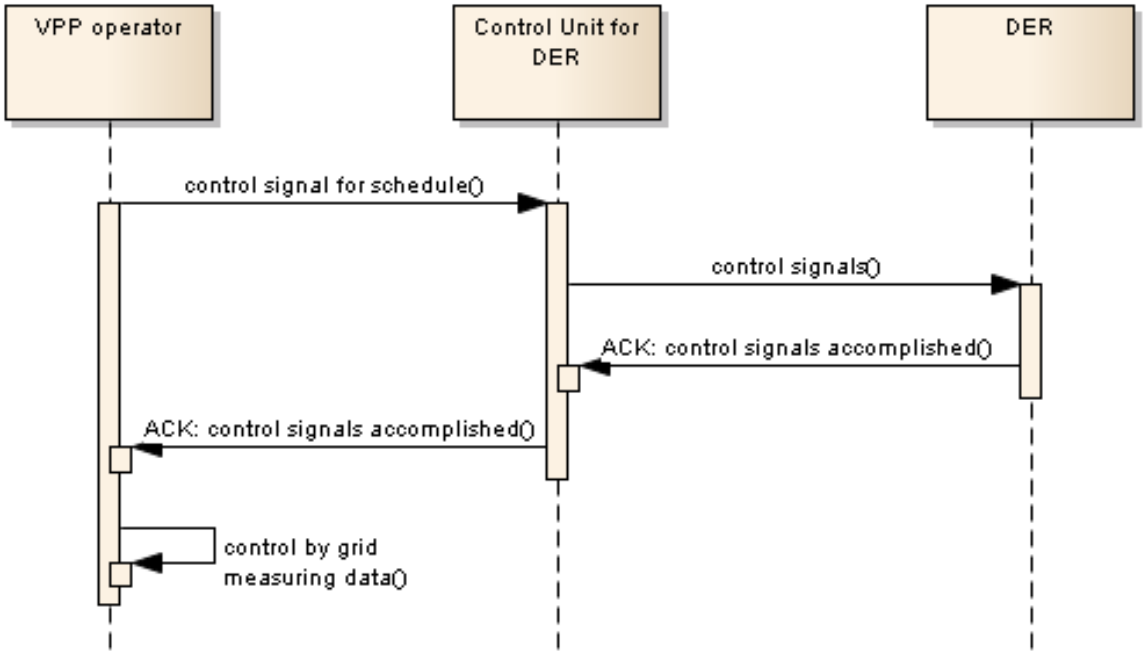

Figure 31: Example Use Case sequence diagram

Applying the aforementioned methodology, the following five steps have to be taken to assess security requirements from NISTIR 7628 to this Use Case.

Identifying and (formally) specifying the Use Case in PAS 62559 templates

The IEC PAS 62559 template is taken to specify the Use Case of the former paragraph. The definition of the Use Case is here reduced to the identified actors and sequence diagram. Additional effort as well as information can be found in the IEC 62559 template. The identified actors are:

- DER;
- VPP operator; and
- Control Unit for DER.

The sequence diagram of Figure 31 is useful to get an overview about the communication between the actors and to identify interfaces.

Identification and mapping of LI, communication links and interface categories

The identified actors and communication links have to be mapped on the NISTIR 7628 descriptions. Figure 32 shows the scenario as a so-called high-level diagram from NISTIR 7628. The DER is controlled via the Customer EMS and the VPP Operator gets involved in the control process via the LMS/DRMS system. The communication links, U106 and U45 from the NISTIR 7628 annex, and their corresponding interface categories, 10 and 15, are identified using the generic blueprint from the authors.

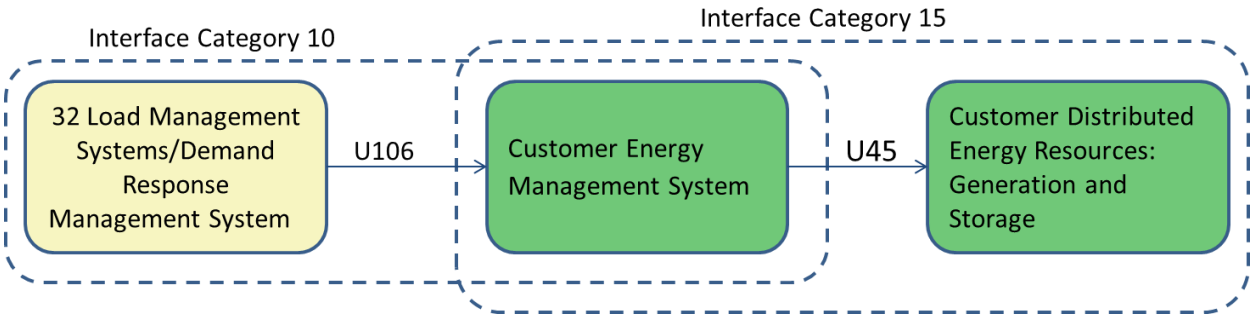

Figure 32: Logical Interface Categories and systems of the Use Case

The colours used in Figure 32 reflect the domains of the Logical Interface diagrams. The system with number 32 LMS/DRMS (= yellow, domain operations) sends two different signals to the system number 5 Customer EMS (CEMS) (green = domain customer). After an appropriate ramp-up time the two signals, of tariffs and schedules, are submitted. If the time of the schedule is reached, real-time measurements are used to check the fulfilment. If the schedule is not satisfied, direct control, using a control signal for the Customer DER, is initialized. Once the signals are sent to the CEMS, the CEMS decides how to react, based on pre-defined and engineered rule sets, and sends control signals to the CDER. After accomplishing the tasks, first, the CDER acknowledges to the CEMS and the CEMS acknowledges to the LMS/DRMS, as can be seen in Figure 31.

Integration of the LI onto the SGAM Functional Layer

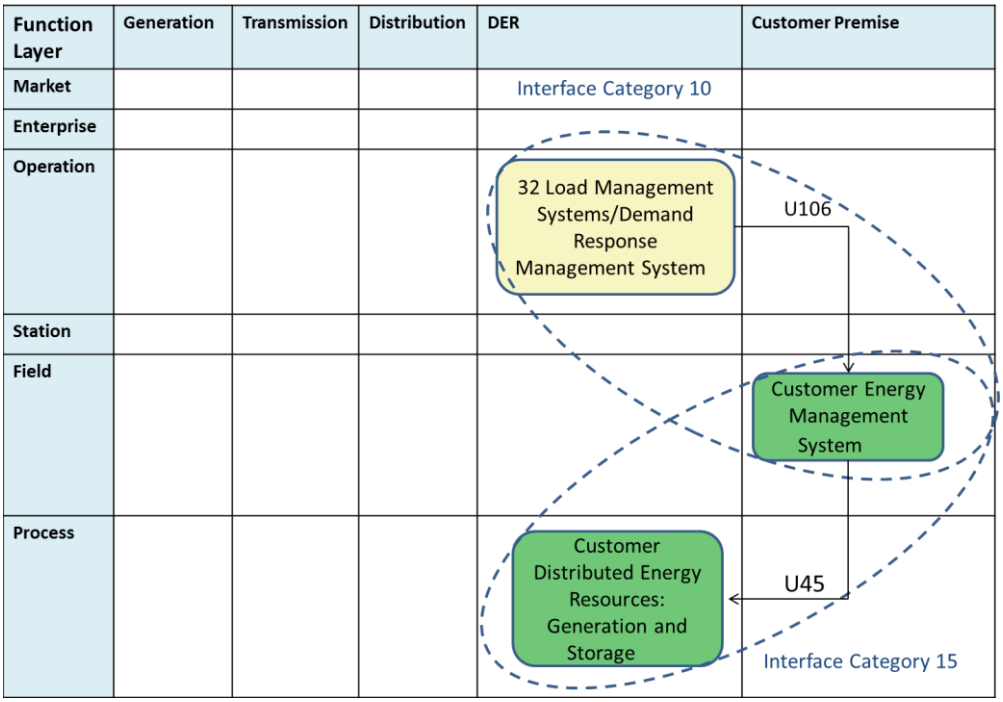

Figure 33: Mapped actors and interfaces

Within this step of the methodology, the mapping onto the SGAM layers is conducted. For this example, it is done in the Function Layer of the architecture. Figure 33 provides an overview of the mapped actors as well as the corresponding communication links. Utilising this kind of graphical representation makes it easier to check which domains are covered by which actors as well as to recognize the hierarchical zone they reside in.

Using the SG-CySecReq annex from NISTIR 7628

In the NISTIR 7628 the interfaces are categorised and for the different categories protection goals, like CIA analyses and high-level security requirements, are determined. Based on the previous identified interfaces and categories,

Table 25 shows the corresponding SG-CySecReq and the resulting sum of these to obtain requirements for the communication from the LMS/DRMS to the DER.

In addition, security requirements from other standards can be used from the annex lookup tables of the NISTIR 7628 report, volume 1 and 3. For this very example, the two LIC will provide various mitigations from the NISTIR 7628 series.

Table 25 CIA and SG-CySecReq analysis for the example

Category	Value	Value	Result
Logical Interface Class:	10	15	
Confidentiality:	Low	Low	**Low**
Integrity:	High	Medium	**High**
Availability:	Medium	Medium	**Medium**
Smart Grid Cybersecurity Requirements	AC-14 (Permitted Actions without Identification or Authentication)	AC-14	**AC-14**
	IA-04 (User Identification and Authentication)	IA-04	**IA-04**
	SC-05 (Denial-of-Service Protection)	SC-05	**SC-05**
	SC-06 (Resource Priority)	SC-06	**SC-06**
	SC-07 (Boundary Protection)	SC-07	**SC-07**
	SC-08 (Communication Integrity)	SC-08	**SC-08**
	SC-26 (Confidentiality of Information at Rest)	SC-26	**SC-26**
	SI-07 (Software and Information Integrity)	SI-07	**SI-07**
		SC-03 (Security Function Isolation)	**SC-03**
		SC-09 (Communication Confidentiality)	**SC-09**

Mapping additional SGAM layers

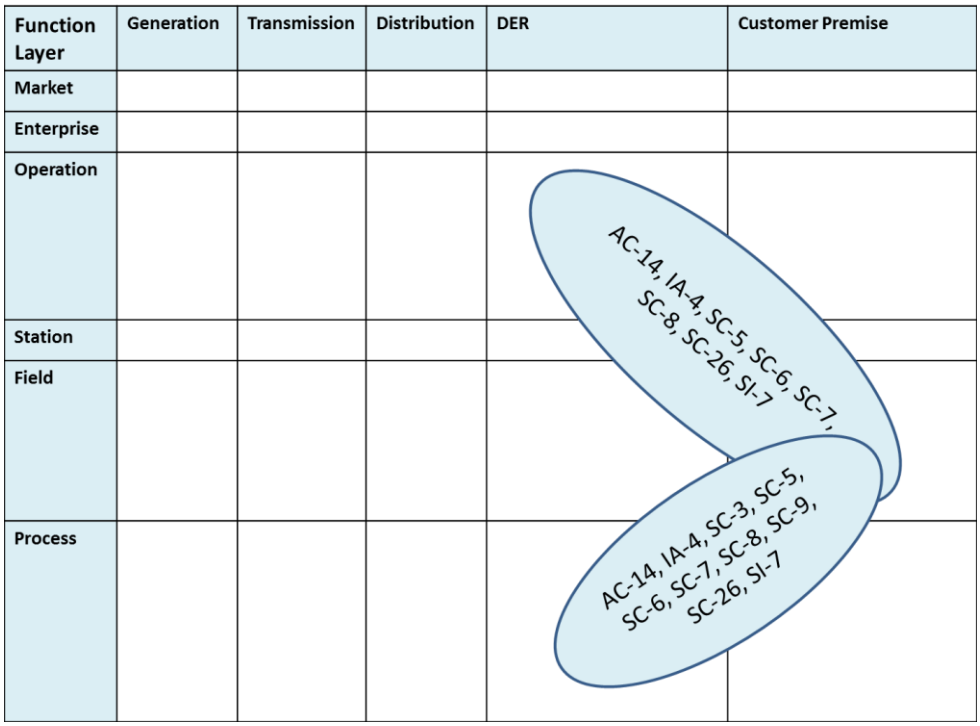

Figure 34: NISTIR 7628 requirements

In this step, the identified SG-CySecReq and their actors and communication links are mapped onto the individual further SGAM planes. Figure 34 shows where the high-level requirements are placed on the Business Layer. Figure 35 shows the corresponding SG-CySecReq, from the SG-CySecReq classes. Additional aspects can be identified and assessed to the responsible architects for the individual layer.

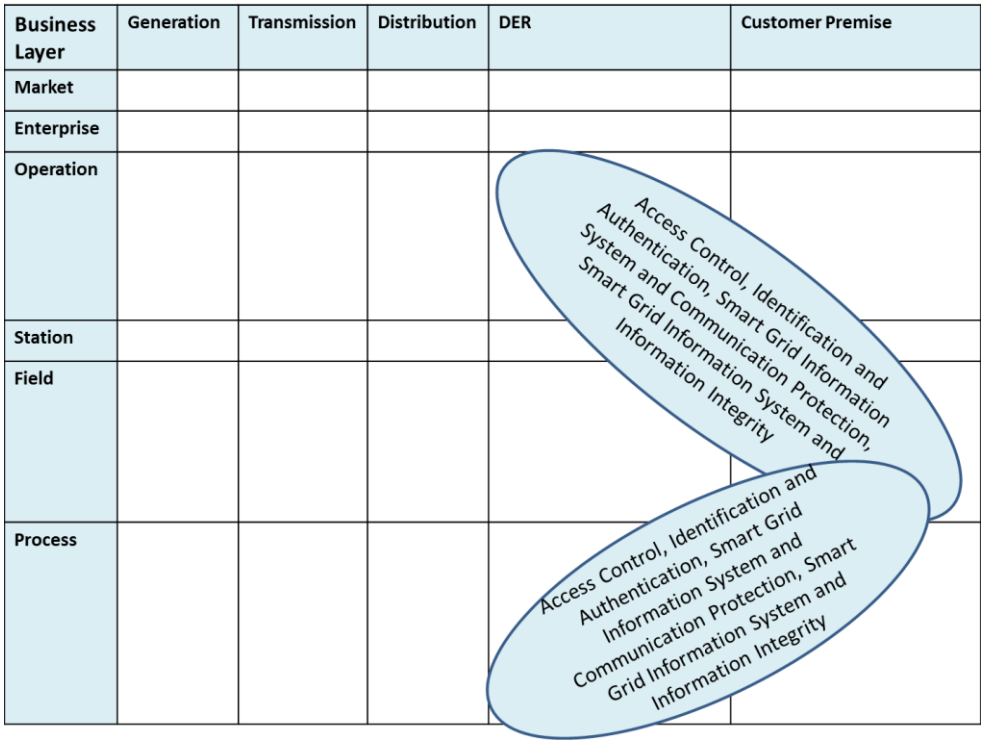

Figure 35: high-level security requirements

The Use Case Risk Analysis investigates the failure modes caused by cyber attacks to the ICT infrastructure supporting DER control functions and how they impact on grid operation. Considering the information assets and scenarios related to the DER Control Use Case, the Impact and Likelihood Levels have been evaluated to obtain the corresponding (phase 1) SGIS Levels.

What is more relevant is that the Risk Levels assigned to the Use Case assets will drive the identification of the Security Requirements and the deployment of the Security Solution in the next steps.

8.4 Mapping of NISTIR and ENISA recommendations

Table 26: Mapping of mitigation measures / recommendations of NISTIR 7628 and ENISA

NISTIR 7628 Recommendations	ENISA Recommendations
SG.ID	SM 1.1.Information Security Policy
SG.AU-1	SM 1.2 Organisation of Information Security
SG.SA-1	SM 1.3 Information Security procedures
SG.RA-2	SM 1.4 Risk management Framework
SG.RA-4	SM 1.5 Risk Assessment
SG.RA-2	SM 1.6 Risk treatment plan
SG.SC-7	SM 10.1 Secure Network Segregation
SG.SC-18	SM 10.2 Secure Network Communications
SG.PS-7	SM 2.1 Third party agreements
SG.SA-2	SM 2.2 Monitoring third party services and validating solutions against predefined acceptance criteria
SG.CA-2	SM 3.1 Security Requirements analysis and specification
SG.ID	SM 3.2 Inventory of smart grid components/Systems
SG.CM	SM 3.3 Secure Configuration Management
SG.MA	SM 3.4 Maintenance of Smart Grid Components
SG.CM	SM 3.5 Software/firmware upgarde of smart grid components
SG.MP-6	SM 3.6 Disposal of Smart grid Components
SG.SI-6	SM 3.7 Security testing of smart grid components
SG.PS	SM 4-1 Personnel Screening
SG.PS	SM 4.2 Personnel changes
SG.PM	SM 4.2 Security and Awareness Programm
SG.PM	SM 4.4 Security Training and certification of personnel
SG.IR	SM 5.1 Incident response capabilities
SG.RA-6	SM 5.2 Vulnerability assessment
SG.RA-2	SM 5.3 Vulnerability management
SG.IR	SM 5.4 Contact with authorities and security interest groups
SG.AU	SM 6.1 Auditing capabilities
SG.CA-6	SM 6.2 Monitoring of Smart Grid Information Systems
SG.AU-1	SM 6.3 Protection of audit information
SG.CP	SM 7.1 Continuity of operations capabilities
SG.SC-1	SM 7.2 Essential communication Services
SG.PE-3	SM 8.1 Physical security
SG.PE-7	SM 8.2 Logging and monitoring physical access
SG.PE-1	SM 8.3 Physical security on third party premises
SG.SA	SM 9.1 Data Security
SG.AC	SM 9.2 Account management
SG.AC-1	SM 9.3 Logical Access Control
SG.MA-6	SM 9.4 Secure Remote Access
SG.SC	SM 9.5 Information Security on Information Systems
SG.MP-1	SM 9.6 Media Handling

8.5 Overview of categories of NISTIR 7628 security requirements

- **SG.AC Access Control**: The focus of access control is ensuring that resources are accessed only by the appropriate personnel, and that personnel are correctly identified. Mechanisms need to be in place to monitor access activities for inappropriate activity.
- **SG.AT Awareness and Training:** Smart Grid information system security awareness is a critical part of Smart Grid information system incident prevention. Implementing a Smart Grid information system security program may change the way personnel access computer programs and applications, so organisations need to design effective training programs based on individuals' roles and responsibilities.
- **SG.AU Audit and Accountability:** Periodic audits and logging of the Smart Grid information system need to be implemented to validate that the security mechanisms present during Smart Grid information system validation testing are still installed and operating correctly. These security audits review and examine a Smart Grid information system's records and activities to determine the adequacy of Smart Grid information system security requirements and to ensure compliance with established security policy and procedures. Audits also are used to detect breaches in security services through examination of Smart Grid information system logs. Logging is necessary for anomaly detection as well as forensic analysis.
- **SG.CA Security Assessment and Authorisation:** Security assessments include monitoring and reviewing the performance of Smart Grid information system. Internal checking methods, such as compliance audits and incident investigations, allow the organisation to determine the effectiveness of the security program. Finally, through continuous monitoring, the organisation regularly reviews compliance of the Smart Grid information systems. If deviations or nonconformance exist, it may be necessary to revisit the original assumptions and implement appropriate corrective actions.
- **SG.CM Configuration Management:** The organisation's security program needs to implement policies and procedures that create a process by which the organisation manages and documents all configuration changes to the Smart Grid information system. A comprehensive change management process needs to be implemented and used to ensure that only approved and tested changes are made to the Smart Grid information system configuration. Smart Grid information systems need to be configured properly to maintain optimal operation. Therefore, only tested and approved changes should be allowed on a Smart Grid information system. Vendor updates and patches need to be thoroughly tested on a non-production Smart Grid information system setup before being introduced into the production environment to ensure that no adverse effects occur.
- **SG.CP Continuity of Operations:** Continuity of operations addresses the capability to continue or resume operations of a Smart Grid information system in the event of disruption of normal system operation. The ability for the Smart Grid information system to function after an event is dependent on implementing continuity of operations policies, procedures, training, and resources. The security requirements recommended under the continuity of operations family provide policies and procedures for roles and responsibilities, training, testing, plan updates, alternate storage sites, alternate command and control methods, alternate control centres, recovery and reconstitution and fail-safe response.
- **SG.IA Identification and Authentication:** Identification and authentication is the process of verifying the identity of a user, process, or device, as a prerequisite for granting access to resources in a Smart Grid information system.
- **SG.ID Information and Document Management**: Information and document management is generally a part of the organisation records retention and document management system. Digital and hardcopy

information associated with the development and execution of a Smart Grid information system is important, sensitive, and needs to be managed. Smart Grid information system design, operations data and procedures, risk analyses, business impact studies, risk tolerance profiles, etc., contain sensitive organisation information and need to be protected. This information must be protected and verified that the appropriate versions are retained. The following are the requirements for Information and Document Management that need to be supported and implemented by the organisation to protect the Smart Grid information system.

- **SG.IR Incident Response:** Incident response addresses the capability to continue or resume operations of a Smart Grid information system in the event of disruption of normal Smart Grid information system operation. Incident response entails the preparation, testing, and maintenance of specific policies and procedures to enable the organisation to recover the Smart Grid information system's operational status after the occurrence of a disruption. Disruptions can come from natural disasters, such as earthquakes, tornados, floods, or from manmade events like riots, terrorism, or vandalism. The ability for the Smart Grid information system to function after such an event is directly dependent on implementing policies, procedures, training, and resources in place ahead of time using the organisation's planning process. The security requirements recommended under the incident response family provide policies and procedures for incident response monitoring, handling, reporting, testing, training, recovery, and reconstitution of the Smart Grid information systems for an organisation.
- **SG.MA Smart Grid Information System Development and Maintenance:** Security is most effective when it is designed into the Smart Grid information system and sustained, through effective maintenance, throughout the life cycle of the Smart Grid information system. Maintenance activities encompass appropriate policies and procedures for performing routine and preventive maintenance on the components of a Smart Grid information system. This includes the use of both local and remote maintenance tools and management of maintenance personnel.
- **SG.MP Media Protection:** The security requirements under the media protection family provide policy and procedures for limiting access to media to authorised users. Security measures also exist for distribution and handling requirements as well as storage, transport, sanitization (removal of information from digital media), destruction, and disposal of the media. Media assets include compact discs; digital video discs; erasable, programmable read-only memory; tapes; printed reports; and documents.
- **SG.PE Physical and Environmental Security**: Physical and environmental security encompasses protection of physical assets from damage, misuse, or theft. Physical access control, physical boundaries, and surveillance are examples of security practices used to ensure that only authorised personnel are allowed to access Smart Grid information systems and components. Environmental security addresses the safety of assets from damage from environmental concerns. Physical and environmental security addresses protection from environmental threats.
- **SG.PL Planning:** The purpose of strategic planning is to maintain optimal operations and to prevent or recover from undesirable interruptions to Smart Grid information system operation. Interruptions may take the form of a natural disaster (hurricane, tornado, earthquake, flood, etc.), an unintentional manmade event (accidental equipment damage, fire or explosion, operator error, etc.), an intentional manmade event (attack by bomb, firearm or vandalism, hacker or malware, etc.), or an equipment failure. The types of planning considered are security planning to prevent undesirable interruptions, continuity of operations planning to maintain Smart Grid information system operation during and after an interruption, and planning to identify mitigation strategies.

- **SG.PM Security Program Management:** The security program lays the groundwork for securing the organisation's enterprise and Smart Grid information system assets. Security procedures define how an organisation implements the security program.
- **SG.PS Personnel Security**: Personnel security addresses security program roles and responsibilities implemented during all phases of staff employment, including staff recruitment and termination. The organisation screens applicants for critical positions in the operation and maintenance of the Smart Grid information system. The organisation may consider implementing a confidentiality or nondisclosure agreement that employees and third-party users of facilities must sign before being granted access to the Smart Grid information system. The organisation also documents and implements a process to secure resources and revoke access privileges when personnel terminate.
- **SG.RA Risk Management and Assessment:** Risk management planning is a key aspect of ensuring that the processes and technical means of securing Smart Grid information systems have fully addressed the risks and vulnerabilities in the Smart Grid information system.

  An organisation identifies and classifies risks to develop appropriate security measures. Risk identification and classification involves security assessments of Smart Grid information systems and interconnections to identify critical components and any areas weak in security. The risk identification and classification process is continually performed to monitor the Smart Grid information system's compliance status.

8.6 International standards applicable to Logical Interface Categories

Cyber threats address digital interfaces between actors of our energy system. Various international standards exist classifying these interfaces. Based on these generic interface classes our energy system can be described in a logical syntax to assess its cybersecurity risks. The advantage of using standardised interfaces is to incorporate implicitly a variety of threats as the individual risks of each interface class are pre-defined by the standard.

The following table shows the identified logical interface classes to describe the European energy system based on the Smart Grid Architecture Model (SGAM) and NISTIR 7628. It maps each interface class to further corresponding international standards. When analysing Use Cases (Annex 8.3) and performing risk assessments, such lookup tools allow to check and (if relevant) prioritise security measures.

Table 27: overview of generic interface classes of the energy system based on NISTIR 7628

interface class ID	interface class description	Mapping to international standards
1	Interface between control systems and equipment with high availability, and with compute and/or bandwidth constraints	IEC 61850, IEC 60870-5-101 and 104
2	Interface between control systems and equipment without high availability, but with compute and/or bandwidth constraints	IEC 61850, IEC 60870-5-101 and 104
3	Interface between control systems and equipment with high availability, without compute or bandwidth constraints	IEC 61850, IEC 60870-5-104, IEC 60870-6-TASE2
4	Interface between control systems and equipment without high availability, without compute or bandwidth constraints	IEC 61850, IEC 60870-5-104, IEC 60870-6-TASE2
5	Interface between control systems within the same organisation	IEC 61850, IEC 60870-6-TASE2, IEC 61968, IEC 61970
6	Interface between control systems in different organisations	IEC 61850, IEC 60870-6-TASE2, IEC 61968, IEC 61970
7	Interface between back office systems under common management authority	IEC 61968, IEC 61970
8	Interface between back office systems not under common management authority	IEC 61968, IEC 61970
9	Interface with business to business (B2B) connections between systems usually involving financial or market transactions	IEC 61968, IEC 61970, IEC 62325
10	Interface between control systems and non-control/ corporate systems	IEC 61968, IEC 61970
11	Interface between sensors and sensor networks for measuring environmental parameters, usually simple sensor devices with possibly analogue measurements	IEC 61850, IEC 60870-5-101
12	Interface between sensor networks and control systems	IEC 61850
13	Interface between systems that use the advanced metering infrastructure (AMI) network	IEC 61968, IEC 61970

interface class ID	interface class description	Mapping to international standards
14	Interface between systems that use the AMI network for functions that require high availability	IEC 61968, IEC 61970
15	Interface between systems that use customer (residential, commercial, and industrial) site networks such as HANs and BANs	IEC 61850, IEC 61400-25, IEC 61968, 61970
16	Interface between external systems and the customer site	IEC 61850, IEC 61968, IEC 61970
17	Interface between systems and mobile field crew laptops/equipment	IEC 61850
18	Interface between metering equipment	IEC 61850, IEC 61334 (PLC for metering), IEC 62056 (DLMS/COSEM, IEC TC13 WG14)
19	Interface between operations decision support systems	IEC 60870-6-TASE2, IEC 61968, IEC 61970
20	Interface between engineering/ maintenance systems and control equipment	IEC 61850, IEC 60870-5-101 and 104
21	Interface between control systems and their vendors for standard maintenance and service	IEC 61850, IEC 60870-5-104
22	Interface between security/network/system management consoles and all networks and systems	IEC 62351-7

8.7 Bottom-up threat analysis methodology

This annex describes in more detail how specific threat scenarios in energy systems can be analysed. The next annex 8.8 provides for the specific template to describe threat scenarios.

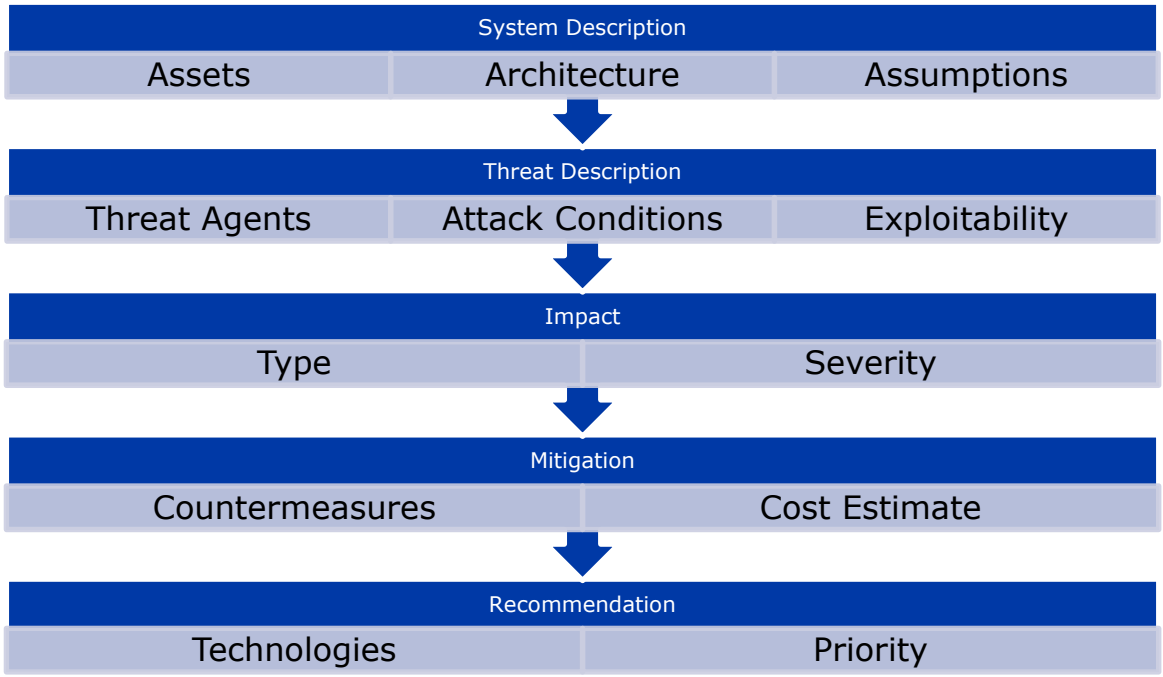

Figure 36: Bottom-up Threat Analysis methodology

Based on RFC 4949, the internet Security Glossary, a threat is "circumstance, capability, action or event, that could breach security and cause harm" [Stallings 2015]. That is, a threat scenario describes risks manifested through threat agents, assets and vulnerabilities. A scenario should provide an answer to the three parts of the question: Who threatens what in which way? A scenario is made up of descriptions of assets/functions, attack vectors and attacker types.

This study considers only threats based on malicious intent comparable to the classification of threat origins in (Bompard et al. 2013), namely physical threats (terrorist attack, act of war, sabotage), human threat (insider threat) and cyber threats (malware, hacking). These categories are extended in this study by using existing threat agent libraries.

The next part of a scenario should be a description of attack vectors towards the identified objectives of the specified attackers. Attack graphs are a common language that is used in safety and security context; specific examples are Fault Tree Analysis and Attack Execution Graphs respectively. A formal representation improves the re-usability of results. First concepts for connecting attack graph ontologies with CIM and IEC 61850 exist and can be extended for

the purpose of cybersecurity risk assessments in power systems. Depending on the level of abstraction in the scenario description specific details down to the technical level can be included.

Attack graphs can be attributed with restrictions on attacker types, vulnerability and architectural context and be mapped onto mitigation recommendations. An attack path within the derived graphs lead to attacker objectives that can be used to analyse potential effects which is fundamental input to risk analysis

The following public references guide the approach applied in this study:

Table 28 Public references used for the approach applied in the study

Category	Description
NISTIR 7628	Interface Categories, Actor Classes, Mitigation Enumeration
CAPEC	Attack Pattern Classification, Recommendations, and Attack Conditions
Electric Sector Cybersecurity Threat Model (NESCOR)	Threat Scenarios
NIST SP 800-30	Attacker Model
M/490 SGIS	Impact Levels

Threat Agent Classification

One crucial component for the plausibility of a threat scenario is a description of threat agents and their ability and motivation to implement a threat scenario. It is useful to establish a classification system of threat agents that reduces the complexity by identifying realistic and distinguishable agent categories. These categories can then are used in threat scenario descriptions to discuss the likelihood of a successful attack.

Classification of threat agents is based on their motivation and objectives, their capabilities and resources. Table 29 provides a selection of different classification systems for threat agent categories defined using threat agent attribute classifications from the Intel Threat Agent Library. (Casey 2007)

Table 29 NISTIR 7628 Threat Agent Classification

Category	Description
Nation States	State-run, well organised and financed. Use foreign service agents to gather classified or critical information from countries viewed as hostile or as having an economic, military or a political advantage.
Hackers	A group of individuals (e.g., hackers, phreakers, crackers, trashers, and pirates) who attack networks and systems

Category	Description
	seeking to exploit the vulnerabilities in operating systems or other flaws.
Terrorists/ Cyberterrorists	Individuals or groups operating domestically or internationally who represent various terrorist or extremist groups that use violence or the threat of violence to incite fear with the intention of coercing or intimidating governments or societies into succumbing to their demands.
Organised Crime	Coordinated criminal activities including gambling, racketeering, narcotics trafficking, and many others. An organised and well-financed criminal organisation.
Other Criminal Elements	Another facet of the criminal community, which is normally not well organised or financed. Normally consists of few individuals, or of one individual acting alone.
Industrial Competitors	Foreign and domestic corporations operating in a competitive market and often engaged in the illegal gathering of information from competitors or foreign governments in the form of corporate espionage.
Disgruntled Employees	Angry, dissatisfied individuals with the potential to inflict harm on the Smart Grid network or related systems. This can represent an insider threat depending on the current state of the individual's employment and access to the systems.
Careless or Poorly Trained Employees	Those users who, either through lack of training, lack of concern, or lack of attentiveness pose a threat to Smart Grid systems. This is another example of an insider threat or adversary.

Step 1 – Narrative and system description

The narrative provides an informal description of the scenario, focusing on providing an answer to the question of "Who?", "How?" and "What?" to be formalised in the template.

A description is provided of the considered assets, focusing on the system components, zones and conduits. The result is a list of actors and interfaces as well as a (graphical) description of the interrelations. Explicitly mention all assumptions on security measures deployed in the system or lack thereof.

Security related assumption need to be specified. Assumptions informally describe the state of security with respect to actors and interfaces, e.g. the security level of deployed security measures. Assumptions are enumerated using the scheme “A.<number>”. The description of assumptions should mention applicability to zone or domain (in the SGAM Reference Architecture).

Step 2 – Threat Description

Develop a ‘Misuse Case’

Optional: Attack Tree

Attack Trees are used to derive a tree of conditions and refining sub-conditions for the execution of threat scenarios. The conditions allow to identify effective and efficient mitigations to prevent threat agents from fulfilling individual conditions. Conditions in the attack tree have to be enumerated. Use the graphical notation of Attack Trees from (National Electric Sector Cybersecurity Organization Resource (NESCOR) 2013) to improve re-usability of attack trees.

Optional: Attack Execution Graph

An Attack Execution Graph (AEG) shows the propagation of a threat, for example through SGAM Zones and Domains, which allows better estimation of impacts to the power grid and effective perimeter security.

- Each Access node in the AEG should reference the actor in the NISTIR 7628 Logical Reference Model that it is related to. This automatically positions the access type in the SGAM Reference Architecture Model.
- A Knowledge node may reference the source of the knowledge using the actor representation from the NISTIR 7628 Logical Reference Model.
- A Skill node may reference the limitations of the related skill or capability of a threat actor with relation to actors of the NISTIR 7628 model.
- Each Attack Step in the AEG has to be annotated with the Logical Interface from NISTIR 7628 it is exploiting or an actor if the step handles lateral movement or other actor internal exploitation.
- A Goal node has to assign the area of effect in the SGAM Reference Architecture Model which directly relates it to the Smart Grid Domains of NISTIR 7628.

Reference to Interfaces and Actors of NISTIR 7628 allows to discuss the severity of the threat scenario with respect to existing and with respect to recommended mitigations.

As an example, Figure 37 shows three abstract entry vectors into the system and different pathways to spread vertically between zones Enterprise, Operation and Field. Two general objectives are the exfiltration of data and the modification of processes. The graph is not showing obvious physical attack steps or lateral movement of the attacker. The compromise of a single device in a zone is considered as a compromise of the whole zone.

Figure 37: Common shared cyber attack pathways (white: attack steps, orange: access, red:objectives)

Steps in the common shared cyber attack pathways are enumerated as Generic Condition (GC.<number>). The specific attack patterns that can be used to execute individual steps depend on the specific architecture of the attacked system. For example, GC.3 Gain Access to Field Device may be executed by exploiting vulnerabilities in the vendor supply chain, i.e. delivering a device with modified firm- or software, by using open vendor update interfaces to inject modified updates, or by getting hold of access credentials.

Attack Patterns

Attack Steps in an Attack Execution Graph and nodes of an Attack Tree might refer to known attack patterns. To ensure coverage, the Common Attack Pattern Enumeration and Classification (CAPEC) Database should be searched in four ways:

- Browsing by Category,
- Browsing by Mechanism of Attack,
- Browsing by Domain of Attack,
- Searching for keywords in CAPEC List.

Attack patterns often are linked to standard mitigations which should be considered here to complete the mitigations derived from top-down analysis.

Threat Conditions

Threat conditions are nodes in attack trees and are enumerated “C.<number>”, for clarification conditions should be associated with attack steps in attack execution graphs. Attack steps should be linked to existing attack patterns using the CAPEC database.

Attack execution can be derived by following the logical interface interconnections in the NISTIR 7628 Logical Reference Model or by assuming the possibility of lateral or vertical movement as given by the generic high-level Attack Execution Graph in Figure 37.

Refine assumptions, narrative, variants and threat agent descriptions if necessary.

Vulnerabilities and Weaknesses

Link threat conditions onto related weaknesses from the Common Weakness Enumeration (CWE). Research and list examples of relevant vulnerabilities that exploited these weaknesses for related components from the Common Vulnerability Enumeration (CVE). Insert CVE recommendations to the list of recommended mitigations.

Step 3 – Assess impact of threats

Qualify the category of impact of the scenario by comprising a list of potential effects with a focus on likely objectives of an attacker. Similar to NESCOR, the derived impacts are mapped onto impact categories. Each impact category should be qualified by a severity index (or none if the impact does not apply). The index is based on the SGIS Security Level (SGIS SL).

Step 4 - Identify mitigations

Threat Scenario Mitigation Generation

The threat analysis provides a set of threat mitigations from the conditions under which a threat could be executed by analysing each condition (Attack Tree) or each attack step (Attack Graph). Refer to available standard databases, e.g. CAPEC, for recommended mitigations if available. Mitigations are enumerated within a scenario using the scheme “M.<number>” and externally “<Scenario ID> M.<number>”.

Mapping onto Reference Architecture

A threat scenario provides a list of related interface reference from NISTIR 7628 and maps each threat condition and attack step onto affected interfaces. The parallel analysis of Use Case scenarios provides a mapping of interfaces onto Logical Interface Categories and recommended protection measures from NISTIR 7628.

Mitigation Gap Analysis

Identify gaps between recommended mitigations from the Logical Interface Classes and refine both recommendations into a single recommendation list. To identify mitigation gaps, derive relevant measures based on expert input and categorise them by mapping onto fitting NISTIR 7628 Smart Grid Cyber Security Requirements. This list is compared to the list of recommended mitigation and the level of implementation is determined for each existing measure. Use the Levels of Implementation (Fully, Largely, Partially, Not) from the NESTOR Failure Scenario Toolkit. To identify gaps between recommendations and existing mitigations identify the risk level

Table 30 Mitigations table and priorities

Recommended Mitigations	Existing Implementation Status	Risk/Severity	Recommendation
SG.AC 1	Partial	Highly Critical	
SG.AU 5	Fully	Medium	
…	…	…	

Step 5 – Set clear recommendations

Next step is to select mitigations that are both effective and efficient, as well as to prioritise these.

Prioritisation of Mitigation Gaps

Any mitigation whose mitigation status is not “Fully Implemented” is to be considered a gap. In order to prioritise mitigation gaps, each gap is localized on a risk matrix and mapped onto a priority between 1 (low) and 5 (high).

Table 31 risk matrix, illustration of security levels and implementation status

Implementation Status / Security Level	Fully Implemented	Largely Implemented	Partially Implemented	Not Implemented
Highly Critical	3	5	5	5
Critical	2	4	5	5
High	1	3	4	5
Medium	1	2	3	4
Low	1	1	2	3

Priorities define the urgency of taking action, i.e. implementing or reviewing existing mitigations. The type of action depends on the existing level of implementations as given in Table 32.

Table 32 Recommended actions depend on Implementation Level

Category	Description
Fully Implemented	Review quality and implementation of implementation level
Largely Implemented	Review existing implementation and fix remaining gaps
Partially Implemented	Review existing implementation and roll out to full system coverage
Not Implemented	Design and implementation of protection measures required

8.8 Threat Scenario Template

8.8.1 Scenario Description

Threat scenario identification		
ID	***Area Domain(s)/ Zone(s)***	***Name of Threat Scenario***

8.8.2 Narrative

Narrative	
Short Description	
Long Description	
Parent Scenario	
Related Scenarios	
Variants of Scenario	
Related Incidents	

8.8.3 System Description

Assets	
ID	***Asset Description***
System Archtecture Diagrams	

Relation of Assets to Logical Interface Model		
Related Actors		
ID	**Name**	**Related Assets**
Related Logical Interfaces		
ID	**Name/Data Objects**	**Related Assets**

8.8.4 Security Attributes

Security Attributes			
Threat Agent Classes			
ID	**NISTIR 7628 Class**	**Scenario Objective**	**Restrictions/Engagement Rules**
TA.1	Nation States		
TA.2	Hackers		
TA.3	Terrorists/ Cyberterrorists		
TA.4	Organised Crime		
TA.5	Other Criminal Elements		
TA.6	Industrial Competitors		
TA.7	Disgruntled Employees		
TA.8	Careless or Poorly Trained Employees		

Security Assumptions	
ID	Assumption Description
A.	

8.8.5 Misuse Case Diagram

Misuse Case Diagrams

8.8.6 Attack Description

Attack Vectors through General Attack Execution Graph
Attack Trees (Attack Conditions)
Attack Execution Graphs (Detailed Attack Steps)

Attack Steps/Conditions		
ID	*Description*	*References (e.g. CAPEC)*
	Related Weaknesses (e.g. CWE)	*Related Vulnerabilities (e.g. CVE)*
	Affected Actors	*Affected Logical Interfaces*
	Impact/Effect (typical)	*Exploitability (typical)*
C.		

8.8.7 Evaluation of Risk

Security Impact Description	
Access gained	
Data objects modified	
Physical impact	
Information exfiltrated	
Recovery	

NESCOR Impact Categories		
ID	*Name*	*Severity (1..5)*
1	Public safety concern	
2	Workforce safety concern	
3	Ecological concern	
4	Financial Impact of Compromise on Utility (excluding #5)	
5	Cost to return to normal operations	
6	Negative impact on generation capacity	
7	Negative impact on the energy market	
8	Negative impact on the bulk transmission system	
9	Negative impact on customer service	
10	Negative impact on billing functions	
11	Damage to goodwill toward utility	
12	Immediate macro economic damage	
13	Long-term economic damage	
14	Loss of privacy	
15	Loss of sensitive business information	

Probability of Occurrence	
TA Motivation	
Threat Exploitability	

8.8.8 Mitigation/Countermeasures

Threat Mitigations			
Vuln/AP Id	***Recommended Countermeasure***	***Complexity/Cost***	***Gap?***

8.9 Status of cybersecurity of non-EU system operators

The status of cybersecurity practices in other parts of the world needs to be seen in context of its energy system characteristics and applicable legislation. In literature and wider industry reference is sometimes made to US practices where the system has different reliability performance and other regulatory frameworks compared to EU. This section addresses some practical challenges and experiences from US utilities regarding cybersecurity measure implementation, without linking it to high or low maturity and without assigning best practices which would partly be specific for its system and regulatory context. Further background on US NERC CIP implementation experiences are given in Annex 8.9.

In 2017, the National Renewable Energy Laboratory (NREL) performed a survey [40] on the status of cybersecurity at utilities in the US. NREL prepared a questionnaire of 33 questions segmented in the categories: Demographics, Standards and Governance, Oversight, Planning, Execution and Performance, Support. In total, 250 utilities in the US were contacted. The results are based on a complete set of answers from 22 utilities. Key findings and conclusions for the participants are the following:

- The **biggest challenges** for utilities are the installed equipment basis, budget, skilled workforce, technology availability and maturity. In terms of budget, utilities reported challenges to clearly identify how to account for the costs and the benefits of cybersecurity expenses. Clear regulation or guidelines on accountable costs or types of costs for cybersecurity could address this issue.
- Various number of cybersecurity frameworks and guidelines (e. g. NISTIR 7628, NIST Cybersecurity Framework, ES-C2M2) are used, but NREL sees a **lack of cohesive use of cybersecurity guidelines** and unclear reasons for selecting one instead of another. The authors propose to enhance capacity building via workshops or trainings to identify and clarify publicly available standards and guidance.
- They conclude that **utilities have the tendency to rely on national or local associations**. These authorities and agencies play a key role as first contact for utilities and to provide effective guidance and spread best practices regarding risk assessments and technical implementation from more advanced utilities to less advanced utilities.
- All the participating utilities reported having a cybersecurity team. But **most do have small to very small cybersecurity teams** of 1 to 5 persons (see Figure 37). In terms of budget, the majority reported to spend less than 100k USD/year on cybersecurity. In general, this amount represents not more than 10% of the overall IT budget, as a higher IT budget does not necessarily imply a higher cybersecurity budget (see Figure 38). Furthermore, costs for IT and OT cybersecurity are often managed differently and result in a **lack of clarity on overall costs for cybersecurity**.

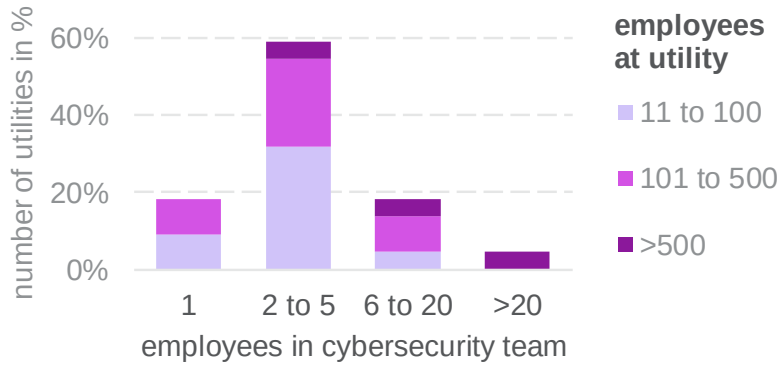

Figure 38: US distribution of employee numbers in cybersecurity team depending on utility size, source: Ecofys based on [40]

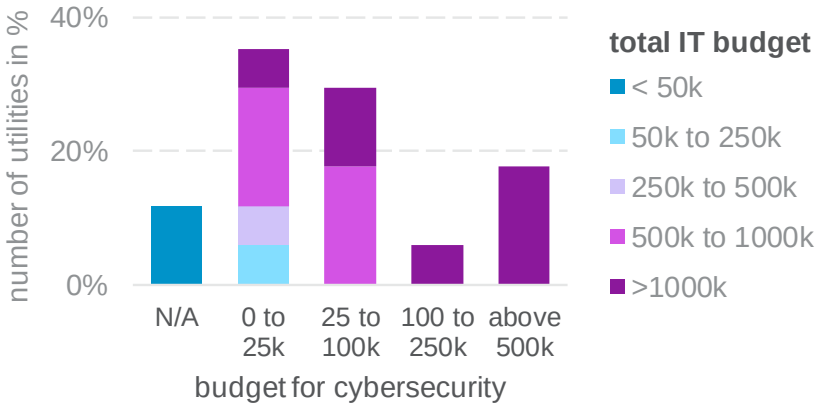

Figure 39: US view on annual IT and annual cybersecurity budgets in participating utilities, source: Ecofys based on [40]

8.10 Cybersecurity program cost drivers – NERC CIP experience

Implementing a standards based cybersecurity program is a complex challenge for electric generation, transmission and distribution operators. The cost of implementation is a function of many factors that are unique to every company. In this section we look to explore the cost drivers that come into play during the various phases of implementation. The objective of this work is to offer guidance and advice on specific issues that are common during the process so that common obstacles may be negotiated and attendant costs minimized. The context of this appendix is mainly based on US experience.

8.10.1 Importance of Mandatory Enforceable Framework (Why the effort?)

Like aviation, banking and transportation, bulk electric in North America has adopted various frameworks to aid in the safe operations, reliability and/or security of the system being regulated. Organisations pursued more specifically with the Bulk Electric System (BES), a set of cybersecurity standards that have been evolving more into a set of risk-based practices.

The new Critical Infrastructure Protection Version 5 (CIP v5) Standards began going into effect in July 2016, with some requirements subject to an implementation plan terminating September 1st, 2018. This phased approach was agreed on between the North American Electric Reliability Corporation (NERC) and Industry leaders so that additional time was allowed to meet more difficult requirements. This shift required expending tremendous amounts of resources (people and funding) to accomplish this significant task. The majority of transition efforts occurred between July 2014 and July 2016, however industry continues to implement low impact requirements and those requirements subject to the NERC implementation plan.

NERC and the industry recognized that significant work would be required, and agreed that a pilot study to understand what would be involved was necessary, a year before the entire 1500 plus registered entities would begin undertaking this implementation effort. Lessons observed wanted to be captured and then shared with all of government and industry of how to implement enhanced cybersecurity standards, and what resources were necessary.

In this thought piece, we will provide a background of mandatory and enforceable CIP standards, the different phases of implementation, common challenges , and estimated macro cost drivers associated with building and sustaining these standards.

8.10.2 Progress in the North American Reliability Corporation (NERC)

The North American Reliability Corporation or NERC's origins go back to 1968. It was formed to develop a set of standards for the security and reliability of North American bulk electric systems (BES). The purpose of the standards was the effective and efficient reduction of risks to the reliability and security of the bulk power system. After the 2003 Northeast Blackout, the Federal Energy Regulatory Commission (FERC) made NERC standards mandatory and gave the organisation the power to enforce them. Although the second largest blackout of the

electric grid in history which affected some 55 million people was the triggering event, the need for enforceable and uniform standards and practices had been growing for years.

NERC Reliability Standards are developed using an industry-driven, ANSI-accredited process that ensures the process is open to all persons who are directly and materially affected by the reliability of the North American bulk power system; transparent to the public; demonstrates the consensus for each standard; fairly balances the interests of all stakeholders; provides for reasonable notice and opportunity for comment; and enables the development of standards in a timely manner.

NERC Reliability Standards define the reliability requirements for planning and operating the North American bulk power system and are developed using a results-based approach that focuses on performance, risk management, and entity capabilities. The Reliability Functional Model defines the functions that need to be performed to ensure the Bulk Electric System operates reliably and is the foundation upon which the Reliability Standards are based.

The Standards Committee (SC) oversees and prioritises NERC's standards development activities. The Standards Committee also coordinates NERC's development of Reliability Standards with the North American Energy Standards Board's (NAESB) wholesale electric business practices. Standards drafting teams, which are made up of industry volunteers and supported by NERC staff, work collaboratively to develop requirements using results-based principles that focus on three areas: measurable performance, risk mitigation strategies, and entity capabilities.

Compliance Monitoring by NERC is used to assess, investigate, evaluate, and audit to measure compliance with its Standards. Sanctioning of confirmed violations is based on the Violation Risk Factors and Violation Severity Levels. Violators must submit and execute a mitigation plan approved by NERC and are subject to large fines. CIP Programs are implemented for the BES through policy driven plans. Most often, senior level executive management is directly accountable for the development of CIP compliance policies and programs as well as their efficacy.

The CIP standards are one of several bodies of Standards set forth by NERC and are in place to provide uniform Physical and Cybersecurity standards and practices.

8.10.3 The CIP Standards Framework

NERC Reliability Standards continually evolve over time, becoming more comprehensive and adjusting to new threats and a changing technical and security environment. The current Mandatory Standards subject to enforcement cover a wide area of operations.[26] The standards collectively address 14 major Reliability categories including the Critical Infrastructure Protection (CIP), which covers the following:

- CIP-002 BES Cyber System Categorisation
- CIP-003 Security Management Controls
- CIP-004 Personnel & Training

---

26 http://www.nerc.net/standardsreports/standardssummary.aspx

- CIP-005 Electronic Security Perimeter(s)
- CIP-006 Physical Security of BES Cyber Systems
- CIP-007 System Security Management
- CIP-008 Incident Reporting and Response Planning
- CIP-009 Recovery Plans for BES Cyber Systems
- CIP-010 Configuration Change Management and Vulnerability Assessments
- CIP-011 Information Protection

To summarize what is involved in each of the 10 CIP standards, we now briefly describe what each of the cyber standards entails. Recognize that each of these standards involves significant challenges, and hence depending on the maturity of the organisations' cyber efforts, and the specific electrical services the entity provides (generation, transmission) to the Bulk Electric System, various amounts of resources are necessary to build, implement and sustain each of these cyber standards.

CIP-002 BES Cyber System Categorisation

Determining what devices are subject to specific regulations requires the company to investigate each microprocessor and programmable device that support BES operations. This process requires each device be evaluated against twenty-three (23) threshold-driven criteria, covering factors that range from an entities registration, to the number and type of generation or transmission interconnections, and the type of control area protections implemented. The process also requires an evaluation of the criticality of each device. If the failure, comprise, or inability to operate as designed could impact BES within 15 minutes, they are subject to regulation (15 minute impactful). Under this standard, the CIP Senior Manager (or delegate) approves the identifications at least once every 15 calendar months and must then comply with the controls included in CIP-003-6 through CIP-011-2 corresponding to each impact category and cyber system type.

Challenges This is difficult for all organisations. It is a challenge to apply the guidelines to their unique infrastructure. In the one analysis, 10 of the 23 major findings, or "lessons learned" involved the interpretation and application of the rules required to segregate CIP assets.[27] Other challenges include: conducting field work to have a complete inventory of thousands of devices; implementing the categorisation process on the devices; and conducting engineering analysis to determine if the device is 15-minute impactful or not.

Improving Maturity The development of use case scenarios and flowchart tools can help facilitate this process. Employee training that promotes asset management practices across multiple departments is critical.

27 Lesson Learned CIP Version 5 Transition Program CIP-002-5.1 Requirement R1: Impact Rating of Generation Resource Shared BES Cyber Systems Version: January 29, 2015

CIP-003 Security Management Controls

This provision requires that documented cybersecurity policies and plans be in place for high and medium impact BES Cyber Systems including the following areas:

- personnel & training;
- Electronic Security Perimeters, including Interactive Remote Access;
- physical security of BES Cyber Systems;
- system security management;
- incident reporting and response planning;
- recovery plans for BES Cyber Systems;
- configuration change management and vulnerability assessments;
- information protection; and declaring and responding to CIP Exceptional Circumstances.

Low impact organisation are required to have documentation for:

- cybersecurity awareness,
- physical security controls,
- electronic access controls for external routable protocol connections and Dial-up Connectivity, and
- Cybersecurity Incident response

Challenges As with CIP-002-5, difficulties were found in the interpretation of the requirements. Getting internal stakeholders to agree to a governance structure, and everything that comes with it (budgets for resources, technologies and consultants) can be a complicated and time consuming exercise.

Improving Maturity Improvements in this area can require a fundamental systemic shift in the culture. A framework of clear policies and procedures, not only for the CIP program, but for all other areas of operations should be in place. Example documentation and guidance as provided under NIST, ISO and other frameworks can aid in the development of concise terminology and structure that can help improve outcomes and minimize cost.

CIP-004 Personnel and Training

This standard requires documented processes or programs for security awareness, cybersecurity training, personal risk assessment (PRA), and access management.

Challenges Organisations of all sizes and maturity levels often times face their most difficult challenges when managing employees. The CIP-004 standards requires documentation and evidence that employees subject to the rules receive regular training and have a current background check. The standards also require that systems be in place to limit physical and electronic access to assets and resources. Integration of Human Resource Systems, Physical Access Control Systems, and Network Administration operations that function in real-time can be technically complex undertaking.

Improving Maturity As with most CIP requirements, interdepartmental coordination is primary to the establishment of mature practices. Human resources plays a key role in vetting, onboarding, and the management of ongoing training.

CIP-005 Electronic Security Perimeter (ESP)

This standard requires the implementation of one or more documented processes that meet the specified requirements. For medium and large BES this includes an internal isolated network enclave to house networked devices. The only way to communicate with these systems are through defined gateways or Electronic Access Points. Inbound and outbound network traffic as well as user permissions are strictly controlled. These enclaves must also have network intrusion detection systems in place that alert the operations centre to malicious activity. Any remote access to these systems must be encrypted and use multi-factor authentication.

Challenges Establishing and managing these systems requires specialized staffing that can be difficult to find. Outsourcing these functions is technically challenging given the requirement that these systems be isolated and heavily protected. OT technicians often have the long-standing expertise to operate assets from a reliability perspective but lack the infrastructure and experience to manage the firewalls.

Improving Maturity Fostering the long-term development of staff is fundamental to the creation of the highly specialized skillsets necessary.

CIP-006 Physical Security of BES Cyber Systems

This requirement calls for operational and procedural controls to restrict physical access to qualified personnel. Restricted areas must be alarmed for unauthorized access and strict control and record keeping is required for all visitors. The systems must be maintained and regularly tested.

Challenges Tailgating and other prohibited employee activity can be the most challenging aspect to control. Training and clear policies that provide for enforced penalties can help address these issues.

Improving Maturity Constant training exercises, well placed signage on doors of protected areas, as well as clear and consistent policy enforcement can help foster a culture of security.

CIP-007 Systems Security Management

These requirements expand CIP-005-5 requirements to provide for monitoring using Security Event and Information Management Systems (SEIM) software platforms. Other requirements include patch management practices, ports and services management, as well as tightening data access control practices through password management and event logging.

Challenges SEIM software platform must be integrated with a number of network systems and controls. Every organisation has a unique combination of IT and OT hardware and software systems that manage critical infrastructure. Each SEIM deployment must be individually configured using techniques that can be extremely time

intensive to set up and tune. These standards also require that configuration management and security controls be in place on every single programmable device. This is a technically challenging task given the range of system types and large number of devices.

Improving Maturity A security management roadmap based on a gap analysis study can prioritise the requirements for mature risk-informed planning. Security automation tools such as Crossbow and SMSS for patch management, as well as Tripwire and Industrial Defender for change monitoring and management are often required to limit the amount of labor required and to reduce human error.

CIP-008 Incident Reporting and Response Planning

Security incident response provisions require that the organisation create an Incident Response Plan (IRP) addressing: a process to identify, classify, and respond to cybersecurity incidents; a process to determine if the Cybersecurity Incident is a reportable to the Electrical Systems – Information Sharing and Analytics Centre (ES-ISAC) within an hour; and identification of roles and responsibilities of response personnel. The plan must also be tested on a regular basis.

Challenges While consulting expertise may be involved in the development phase, it is up to the organisation to test, validate and improve the plan on a regular basis. These requirement may involve coordinated activities across many departments. Proper IRP programs have executive sponsorship that provides staff with the interdepartmental authority to work with and manage process stakeholders.

Improving Maturity CIP IRP efforts are part the larger Business Continuity picture. CIP-007 requirements often result in the IT SOC monitoring OT environments. The traditional divide between back office IT systems and OT SCADA systems needs to evolve into a more mature information systems network that can provide a secure and integrated disaster recovery and business continuity architecture.

CIP-009 Recovery Plans for BES Cyber Systems

The backup and recovery provisions require that the organisation develop backup and recovery plans for each applicable device, addressing: identification of roles and responsibilities of recovery personnel, documented processes to backup data, documented processes to recover failed or compromised devices, and processes to preserve data that is needed in incident investigations. It also requires a mechanism to document and incorporate lessons learned in incident recovery plans. The plan also requires operational testing of the recovery of BES Cyber Systems on a regular basis.

Challenges Budgeting constraints may prevent the deployment of more advanced technologies. Test environments must be engineered in a way that can be documented to substantively replicate the production environment. The specialized knowledge required to architect and operate virtual server systems and seamless failover capability may require dependence on third-party providers.

Improving Maturity The recovery plan should also be integrated with corporate business continuity planning and exercised on a regular basis. The presence of current generation cybersecurity controls such as Unified Threat

Management (UTM) and Intrusion Prevention Systems can help limit exposure. An architecture that builds in security enclaves and has overlapping security control systems will provide deep defensive capability that limits potential data loss or destruction.

CIP-010 Configuration Change Management and Vulnerability Assessments

Installed software must have a documented baseline configuration that includes operating systems or firmware.

This includes any custom software installed, any logical network accessible ports, and any security patches applied. When changes are made to the configuration, there must be a process to authorise and document the changes within 30 days. If these changes impact Electronic Security Perimeter(s) or System Security Management, the change must be tested and validated and new baselines and procedures implemented. Cyber Vulnerability Assessments (CVA) must also be performed on regulated systems. Transient Cyber Assets such as laptops and other devices as well as Removable Media such as USB and Smart phone drives must also have systems in place to protect against misuse.

Challenges It can particularly difficult to test software and systems present in the OT environment without introducing additional risk. Active penetration testing introduces more network traffic and looks to interact with production systems. The collecting and interpreting of packet information can be skillset that is difficult to find.

Improving Maturity Change management processes in the IT and OT environment of the organisation should be unified so that any improvements leverage capabilities that are mutually beneficial. This includes the use of integrated ITSM and other change management platforms.

CIP-011 Information Protection

This standard requires that sensitive information is identified and protected in storage, transit, and use. Disposal and/or data destruction practices must also be documented to prevent the unauthorized retrieval of data.

Challenges Encrypting older software applications that are not designed to protect the data in use can be difficult. Encryption of the database and data in transit can often be retrofitted onto legacy systems.

Improving Maturity Development of a risk-informed roadmap for data protection is critical to the allocation of limited cybersecurity budgets.

Understanding the cost framework for CIP Implementation

The overall cost of CIP compliance varies a great deal depending on applicable guidelines and the maturity level of the organisation. Large Utility companies that operate under High-Impact BES (Bulk Electric System) regulations spend over $1 MM annually in consulting fees to maintain compliance. Low impact BES operators may be able to spend under $50 K on consulting, providing they have existing cybersecurity controls in place and that the organisation has developed a clear framework of policies and procedures that can be adopted. The cost of salaries, benefits and technology requires can cost ten to fifteen times what a company spends on consulting. The case

studies in this whitepaper are based on actual consulting engagement cost where there is a clearer understanding of the tasks and challenges involved.

Every organisation has unique challenges and the NERC CIP framework is continually evolving. Important insights can be gained however by evaluating the scope and depth of the existing standards, challenges involved, and then looking at each section of the regulations to better understand the cost drivers for compliance.

Organisational Maturity and Challenges of CIP Compliance

BES organisations transitioning to new mandatory compliance guidelines will have existing sets of operational and technical cybersecurity control systems in place. Mature organisations may already have a cybersecurity policy framework and well-defined procedures that are uniformly repeated and monitored. These organisations may be able to transition existing practices with less difficulty than less mature organisations that are more reactive in their management of cybersecurity. Challenges which impact less mature entities more heavily include:

- inventorying existing facilities and assets;
- classifying assets;
- implementing solutions for new inventory and change management requirements;
- anticipating future changes to standards; and
- the need to adapt and fund an Implementation Study to address new challenges.

Other challenges include developing a consistent and common understanding of the language used for compliance; maintaining current cybersecurity functions while building new ones; and most importantly, ensuring there are sufficient resources and time to comply with the standards. It is uncommon to have staff solely dedicated to compliance transition, however the process consumes a considerable amount of time and can require from 20 individuals to 50 or more. This can seriously impact staff that are already fully utilised.

Planning Compliance Systems in Practice

The following elements are driven at the executive level and effected by senior management.

- Understanding the scope of all required activities and gaining broad stakeholder / SME support
- Creating governance structure that may cut across departments / silos (policies and procedures)
- Securing resources (SMEs, budgets, etc) to implement and maintain a program
- Implementing awareness/training early and often so people doing the work know why, what, and how.
- Integrating internal controls, or checks and balances throughout the process to make sure the work is done correctly, on-time, and is fully/consistently documented

The program manager is responsible for driving the communication throughout the organisation and overseeing the implementation effort. Project managers are assigned to coordinate interdepartmental efforts. Weekly meetings are held to discuss the status of action items, address emerging issues, and make strategic and technical decisions. Meetings are also required to provide updates to the executive level committee or board.

Defining an escalation process or program to resolve any disagreement on pivotal issues is an important topic best addressed at the planning stage.

Designing Compliance Systems in Practice

Developing a gap analysis or Implementation Study to document and address the new requirements provides a roadmap to guide transition. A complete list of compliance practices that need to be created or updated must be documented. Proposed CIP compliance procedures should be peer reviewed and version controlled for clarity. Organisations need to have a single understanding of the meaning and intent of applicable standards and how it impacts their organisation. Without a collective knowledge of CIP requirements and the development of a "culture of compliance", any designs that are produced will not function as a whole.

A single person needs to be in charge to make final decisions and set direction for the planning, design and implementation. Typically this person is the CIP Program Manager. He/She is responsible for implementing a process for continuous improvement during all phases. What lessons are to be learned, what worked and what didn't, and how can design efforts be improved. The company will need to find a balance that can succeed given fiscal and organisational constraints. Examples include: automation vs. manual process; new technology or software vs. existing technology or software; internal resources vs external resources; compliant vs. best in class; etc. The design will also need to include acceptance testing during the implementation phase to ensure proper functionality.

All sections of the CIP compliance programs should contain a clear explanation of how the following elements are to be addressed:

- Reporting- Any reports that need to be generated from information collected to database. Examples include Training and CVA reports, Physical and data access by employees, configuration and change management, asset inventory and associated reports required during CIP audit or program management.
- Work History- Design and development of methods used for collecting evidence that specific tasks have been performed is central to the compliance program. Examples include actions taken during an incident and the exercise of an IRP, performance of patch management and many, many others. In other words, a record of who, what, where, etc for every task.
- Document Requirements- A standard format and design for all CIP policy and procedure and other documentation which includes versioning.
- Process Management – Development of Flowcharts and other tools for documenting Process Management and the design and configuration of CIP software and databases.
- Recurring Tasks- A clear understanding and methods for assuring that recurring tasks are completed and reviewed in a timely manner.
- Event Driven Tasks- A clear understanding and methods for assuring that all tasks required as a result of an incident involving or change to BES assets are documented and reviewed in a timely manner.
  Database Development- Specifications for database resources necessary to collect, store and manage Program data in a manner that allows the information to be organised, analysed and reported on.
  Custom software or COTS software – Specifications for or configuration of software systems to collect and manage CIP program information. Examples include asset inventory, Log Management, Employee Training, Access and others.

Implementing Compliance Systems in Practice

There were several major implementation issues that impacted participants converting to the new Standards. Organisational challenges occurred when engaging new business units and personnel that did not have any standards and requirements experience. Training staff in the new concepts and practices took significant time and effort as did working through the process of integrating the new requirements into core job functions. Additionally, the effort to organise compliance information and metrics was much more labor intensive than expected.

The most significant technical challenge was the introduction of BES Cyber Systems. This object represents the grouping of BES Cyber Assets possessing one or more common characteristics which can serve one or more Applicable Systems to which a requirement pertains. This process took typically several months to complete and required a fundamental re-thinking of how controls were to be documented.

In addition, another technical challenge is staff needed to implement and learn new technologies and applications to support compliance business processes. A representative sample of technologies that were introduced as part of the transition process included the following:

- Patch management software products for both Substations and Control Centres
- Change Management Database (ITSM)
- Log Management Systems
- Multi-Factor Authentication Enterprise Access Control
- Evidence Repository

Common Implementation Roadblocks

- Categorisation processes, high-level Physical Security Perimeter and Electronic Security Perimeter requirements can take significant time and resources and can be a steep learning curve for employees.
- Communicating with vendors and managing expectations can be problematic unless SLA driven contracts with bonuses and claw-backs are written into contracts.
- Significant challenges to projects include the education of staff and fostering working relationships between departments. Achieving these goals will decrease time and resources across all tasks.
- As noted elsewhere in this whitepaper, the identification and classification of assets as required under CIP-002 can be difficult.

8.10.4 CIP Compliance Cost Drivers

The following components are representative of the factors that come into play during implementation and influence the total cost of the compliance program.

- Size of the individual utilities (large / medium / small) *Smaller companies commonly face resource constraints necessitating costly outsourcing.*

- Composition of the utility's assets (transmission and generation) *Distribution architectures are more complex and require larger budgets to achieve compliance.*
- Current state of the utility's asset management system and the inclusion of cyber assets associated with the BES assets. *Organisations with poor management practices face steeper program adoption costs.*
- The age of the utility's cyber asset inventory. *Older equipment may not be supported and is challenging to monitor.*
- Current state of the utility's cyber – security organisational governance structure and ownership of the cyber assets. *Lack of clear ownership guidelines complicates the standards adoption process.*
- Current utility staffing and cyber – security skill set. *Developing in-house cybersecurity capability requires long-term planning. Outsourcing these functions is expensive and may not provide the best outcomes.*
- Availability of qualified consulting firms to provide assistance and necessary technical support as needed. *Expertise that can work on specific assets sets is in scarce supply.*
- Implementation time lines *Standards adoption takes careful planning over a number of years*

8.10.5 Cost benchmarks

NERC Implementation Study: CIP Version 5 Transition Program

The Implementation Study by NERC on the Version 5 Transition Program was conducted in 2014. It collected a representative sample of six responsible entities that volunteered to transition to compliance with the new standards during an accelerated time frame. During the Implementation Study, the study participants focused on technical solutions and processes needed to implement the CIP Version 5 standards the identification of issues that called for additional guidance and clarity. The following material is a summary of the information contained in the report.

The process of adopting new Cybersecurity standards starts with the planning phase, then transitions to the design phase which sets the stage for the final implementation phase.

Information was gathered from the participants as they transitioned from the Version 3 to the more stringent and risk-based Version 5 standards. High-level observations indicate the following practices during CIPv5 adoption:

- Executive level policies are typically driven by cross-sectional committee of stakeholders.
- The CIP steering committee, or board is responsible for defining the processes, identifying and assigning people, developing the systems necessary and establishing necessary documentation and evidence collection.

To be successful the program depends on several key elements:

- The development and promotion of a consistent culture of compliance across the entire organisation requires more understanding and communications between all of the parties involved.
- This includes Executive management who provides organisation-wide leadership;
- Managers and Supervisors for direction and oversight;

- Engineering subject matter experts to design appropriate protections;
- Field technical subject matter experts to implement, operate, and maintain;
- Enterprise-level security personnel to manage security controls; and
- Compliance and regulatory personnel determine compliance requirements.
- Processes need to be documented in a clear and concise manner so they can be readily understood by all.
- There are three logical groups for structuring governance teams: Executive Sponsors and Advisory Committee; Policy Development teams for Control Centres, Substations, Generation, Information Technology, Security, Compliance and others; and Department level teams to ensure the procedures are implemented.

A clear path and approach to transition to compliance includes setting expectations for compliance and enforcement. Responsible entities should clearly know what evidence they need to retain to demonstrate compliance with the CIP standards. Compliance Monitoring entities need to have a consistent view of how to monitor compliance of responsible entities. It is important to provide an understanding of the technical- and compliance-related resources and efforts needed to transition and manage compliance with the standards.

The entirety of CIP standards runs hundreds of pages and covers a wide area of topics. In order to gain some perspective on the magnitude of different tasks, we can model how they impact an organisation. To do so we categorise the activity type for each specific requirement across all CIP domains.

This can help shed light on the workload of each activity type and how they impact the Utility.

Reporting, Work History and Document Requirements

The amount of information that must be developed for compliance is considerable. Many organisations attempt to use Commercial of The Shelf (COTS) solutions such as SharePoint or other information management solutions. Even mature organisations can struggle with the adoption or adaptation of systems that can organise, update and retrieve specific data sets accurately. Organisations which have existing procedural frameworks that are updated and maintained in a repeatable manner will not be as challenged with the information management aspects of CIP adoption.

Information Management impacts all compliance activity

Database

Maintaining many of the CIP requirements often requires the database solutions to capture and store the requisite information. A fundamental component of CIP requirements is to ensure that only qualified personnel have access to sensitive areas of the facility. These qualifications include up-to-date training, background checks, a record of when

information is accessed by the individual, and configuring the correct physical and information permissions. These integrated systems may already be in place in many larger Utilities and are generally observed best practices.

Tracking the details of software and hardware configuration is an incredibly complex task. Specialized configuration monitoring and management systems designed to meet CIP requirements can be expensive to implement and maintain.

Compliance requires dedicated database systems

Process Management

NERC CIP compliance is centred on the creation and maintenance of compliance activities that are designed to ensure the proper management and protection of critical infrastructure. Accountability and responsibility is clearly delineated in the policies and procedures that are developed by the organisation. Developing a common and transparent understanding of who needs to do what during daily operations as well as during an incident are critical. Organisations that tend to have informal lines of responsibility and are reactive to changes in the environment will be especially challenged when meeting these responsibilities.

Flowcharts are important tools for documenting Process Management

Specialty Tools

This category covers specific cybersecurity capabilities that may require significant upgrades. Mature information systems depend on an array of overlapping detection and prevention capabilities. Individual enclaves are developed to further protect and provide defensive depth to the architecture of the network. Hardware and software systems that provide adequate protection against the current threat environment require a highly skilled workforce and a significant budget.

Outdated Cybersecurity Controls need to be updated and new ones introduced

Recurring

Many compliance aspects revolve around continual verification and process improvement activities. Adherence to a schedule of required activities need to be factored into daily operations schedules and may impact utilisation.

CIP compliance needs to be integrated into daily operations

Event Driven

Knowing what to do in case of emergency is always easier to practice than to figure it out in the middle of a crisis. There are also many processes throughout the standards framework that serve to integrate activities to ensure desirable outcomes.

Understanding trigger events and required actions is critical

Summary

Estimating costs involves much more than purchasing new hardware and software (special tools and database). The greatest impact to the organisation will be caused by the large increase in the amount of compliance information and data. 41 % of detailed Standards involve tracking of, reporting on, or documentation of specific activities that fall under the requirements. This would suggest that information management practices costs are a central and fundamental driver of CIP implementation. Without the ability to retrieve and demonstrate evidence during an audit, the organisation may well fail.

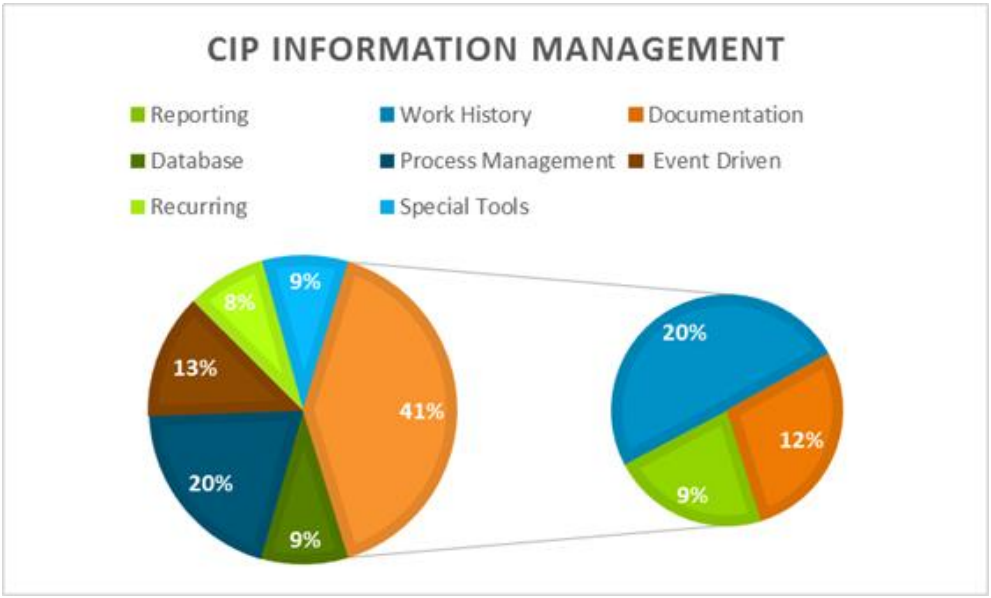

Figure 40: Allocation of effort, source: Navigant Research

8.10.6 Case study 1 - Low Impact Implementation

A Low impact BES located in Florida with $60 MM in revenues was required to meet CIP-003 requirements after completing an evaluation of CIP-002 categorisation. The Utility had not made any specific efforts to develop the required materials and engaged a consulting company that specialized in CIP compliance. The cost of the engagement was significantly influenced by the Maturity of the Utility. By examining the cost breakdown of the engagement consulting costs we can identify where specific activities were help was necessary and then reverse map the areas work to specific Maturity Areas as expressed in the ES-C2M2 model. Higher engagement costs is any one specific area suggests that the Maturity Indicator Level (MIL) is relatively low. These costs do not include labor and resources incurred by the organisation.

IDENTIFY	**$17,004.25**
Asset Management	$3,628.00
Business Environment	$241.00
Governance	$6,611.00
Risk Assessment	$5,194.25
Risk Management Strategy	$1,330.00

The Utility first had to have an accurate and up-to-date inventory of its assets in order to determine the applicability of CIP-003 standards. Sufficient documentation was developed to demonstrate that the Utility had an accurate understanding of its assets and how they interact. It was also necessary to develop a risk-informed strategy for governing and managing those assets.

PROTECT	**$20,859.00**
Access Control	$387.00
Awareness and Training	$3,573.50
Data Security	$917.00
Information Protection Processes	$6,079.50
Protective Technology	$9,661.00

Once there was a current and accurate topology available, the next task was to document the Cyber security controls that were in place to protect electronic access controls for external routable protocol connections and Dial-up Connectivity. A significant amount of discovery was necessary to understand and document the physical and electronic controls that are in place to protect critical infrastructure. The basic Cybersecurity awareness programs were in place were also updated and documented per CIP-003 requirements.

An additional set of tasks were performed to create a Cybersecurity Incident Response Plan (IRP) that detailed the steps necessary to respond and recover from an incident.

RECOVER	**$**	**434.50**
Recovery Planning	**$**	**434.50**
RESPOND	**$**	**1,231.50**
Mitigation	**$**	**387.00**
Response Planning	**$**	**362.50**
Analysis	**$**	**482.00**

The overall cost of implementing the CIP-003 standards amounted to just under .1 % of annual revenues, a significant expenditure for the community owned Utility.

8.10.7 Case study 2 - Medium/High-Impact Implementation

There is a significant difference between low impact BES standards (CIP-003) and medium and High-Impact BES facilities that must comply with CIP-003 through CIP-011 Standards. To gain insight, we can examine a large US Utility company with more than 2 Billion in annual revenues and more than 1,500 employees began the process to become compliant in 2014. This Utility was subject to the CIPv3 standards and has mature cybersecurity practices

as defined under C2M2. Policies, procedures and practices are well documented and the level of cyber protection capabilities is very high. The Utility hired a consulting organisation specializing in compliance to support planning, design and implementation efforts. The total consulting cost of the project amounted to $2 MM over the two year effort or.05% of revenues on an annualized basis. The work was completed and a mock audit was successful two months before the deadline.

Developing and categorising its asset inventory to determine CIP applicability took months to implement, and required support from 50+ field personnel and corporate experts. The main issue is the entity lacked a comprehensive inventory of its field implemented devices, aside from those applicable to CIPv3 standards. The entity was required to visit each of its transmission and generation facilities over a large geographical area, develop an inventory of potentially applicable devices, research potentially applicable devices to understand device capability, and populate its asset management application. All of this took place before the entity formally evaluated the list of devices under its categorisation process; an effort that required 20+ SMEs and nearly a month of dedicated time to complete.

Following its categorisation efforts, the entity determined that nearly all newly applicable devices were not subject to existing governance documents (policies and procedures) that identify responsibilities and business processes. The entity commenced efforts to modify its existing CIPv3 policies and procedures, and in some instances created new governance documents to integrate the new business units, departments and personnel into its CIP program. This effort spanned nearly twelve months, requiring frequent meetings with SMEs and legal representatives to agree upon responsibilities and document the business processes to be implemented that would adhere to the CIP requirements and produce evidence to demonstrate compliance. From an anecdotal perspective, the greatest challenge was getting new personnel to accept and embrace the CIP culture of compliance.

Maybe unique to this entity is it efforts to enhance its asset management application to also support the implementation of CIP business processes, such as the tracking of baseline configurations (device attributes) and the creation / retention of work orders that require business processes be implemented against devices. While this effort took considerable time, required third-party expertise, and required months of tuning, testing and report enhancements, the final product automated many processes and provided the entity with a consistent method for initiating, tracking, and documenting its compliance activities, thus reducing the burden of managing paperwork.

The last and probably the greatest challenge and cost driver for the entity was implementing its CIPv5 business processes on the 1,200 newly identified devices now subject to CIPv5. As one could imagine, this took nearly one year to complete, requiring continuous support from field personnel, managers, and executive management. However, the primary cost driver was not the sheer scope of the devices requiring security control, but rather the compliance training and development of personnel who would undertake the activity. Before the business processes were even implemented, considerable time had to be spent integrating new personnel into the program to confirm they understood the procedures, understood the actions taken against each device, and understand how to document compliance activities to develop evidence. And following security control implementation, even more time was spent organising and validating the compliance evidence, and directing corrective actions to remediate errors and gaps.

8.10.8 Conclusion

The North American Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) Standards Framework plays a unique role in protecting the grid. The set cybersecurity standards that describe what must happen, but not how to do it. The majority of CIP standards complement the NIST standards which focus more on the "how". The C2M2 framework gives a logical methodology to measure the proficiency or "maturity" currently in place.

The overview of CIP standards described what was required of each along with the introduction of challenges and how maturity can influence the adoption process. Having understood more about what was required we then looked to develop a cost framework for CIP implementation. Qualitative overviews were provided to better understand common challenges of CIP compliance Management Systems as well as discussions regarding planning, designing and implementing compliance systems in practice. From this discussion we can then identify overall CIP compliance cost drivers and an approach.

Next we developed new methodologies to provide some form of quantitative insight in the CIP standards. The first approach was to break down the entire body of standards into task types and then establish a magnitude for each. By doing so it was demonstrated that information management systems are central and fundamental to the compliance effort.

A Low Impact Implementation Case Study was conducted to gauge how project expenditures matched up to the cyber security competency. The utility had a low level of competency in several areas that drove up the time and expense required to meet the standards. This was a significant cost proportional to the revenues of the organisation.

The Medium/High-Impact Implementation Case that was performed on a large regional Utility with overall high competency. The Utility was required to meet modifications to existing standards as well as adopt new ones. Although this effort took two years and cost over a million dollars, it represented a very small cost proportional to the revenues of the organisation.

As a general observation we note that organisations which have reactive and unorganised approaches to cybersecurity face the steepest learning curves and the highest costs. Those entities which have documented policies and repeatable processes which are reviewed on a regular basis face a much smaller challenge and are able to build on and adapt structures that are already in place. It is important for every organisation to perform a detailed analysis and understanding of the current state of cyber-capabilities before implementing any uniform Critical Infrastructure Protection Standards.

We also note that organisations would be wise to examine the amount of data required and the pivotal role that information management systems play. Significant reduction in implementation costs can be achieved through proper understanding and planning for a standard based program before it begins.

8.11 Simple maturity levels

The analysis of Chapter 5 on cost impacts applies a simple maturity level model based on ENISA's mitigation categories. The following table extends this view by making the explicit link to subcategories of these 10 classes.

Table 33 Allocation of applied mitigation per maturity level, 0: no mitigation applied, 1: low maturity level, 2: medium maturity level, 3: high maturity level, source: Offis, Ecofys

Category of mitigation	Applied mitigation per maturity level				
		0	1	2	3
Risk management	SM 1.1 Information Security Policy		X	X	X
	SM 1.2 Organisation of information security		X	X	X
	SM 1.3 information security procedures		X	X	X
	SM 1.4 Risk management framework			X	X
	SM 1.5 Risk assessment			X	X
	SM 1.6 Risk treatment plan				X
Management of third parties	SM 2.1 Third-party agreements			X	X
	SM 2.2 Monitoring third parties services and validating solutions against pre-defined acceptance criteria				X
Secure lifecycle process for smart grids	SM 3.1 Security requirements analysis and specification		X	X	X
	SM 3.2 Inventory of smart grid components/systems		X	X	X
	SM 3.3 Secure configuration management of smart grid components/systems				X
	SM 3.4 Maintenance of smart grid components/systems				X
	SM 3.5 Software/firmware upgrade of smart grid components/systems		X	X	X
	SM 3.6 Disposal of smart grid components/systems		X	X	X
	SM 3.7 Security testing of smart grid components/systems		X	X	X
Personnel security awareness and training	SM 4.1 Personnel screening				X
	SM 4.2 Personnel changes			X	X
	SM 4.3 Security and awareness program		X	X	X
	SM 4.4 Security training and certification of personnel		X	X	X
Incident Response	SM 5.1 Incident response capabilities		X	X	X
	SM 5.2 Vulnerability assessment		X	X	X
	SM 5.3 Vulnerability management			X	X
	SM 5.4 Contact with authorities and security interest groups			X	X
Audit and accountability	SM 6.1 Auditing capabilities		X	X	X

Category of mitigation	Applied mitigation per maturity level			
	SM 6.2 Monitoring of smart grid information systems			X
	SM 6.3 Protection of audit information			X
Continuity of operations	SM 7.1 Continuity of operations capabilities		X	X
	SM 7.2 Essential communication services	X	X	X
Physical security	SM 8.1 Physical security	X	X	X
	SM 8.2 Logging and monitoring physical access	X	X	X
	SM 8.3 Physical security on third-party premises		X	X
Information System Security	SM 9.1 Data security	X	X	X
	SM 9.2 Account management	X	X	X
	SM 9.3 Logical access control		X	X
	SM 9.4 Secure remote access		X	X
	SM 9.5 Information security on information systems			X
	SM 9.6 Media handling			X
Network security	SM 10.1 Secure network segregation	X	X	X
	SM 10.2 Secure network communications	X	X	X

8.12 Stakeholder engagement

Throughout the project an engagement process with industry experts was set up:

- Bilateral contacts with ENISA, ACER, ENTSO-E, ENCS, GIE.
    - These were intended to explore ongoing related initiatives in these organisations and capture initial viewpoints and suggestions
- Workshop with the EU Smart Grid Task Force Expert Group 2
    - To understand the link between this study and the EG2 work plan
    - To get feedback on the methodology proposed in this study
- Survey addressed to gas and electricity system operators via ENTSO-E, GIE, ENCS; giving 15 responses providing facts and views on
    - General risk assessment methodology in their organisation
    - Specific measures presently in their organisation
    - Staffing and governance
    - Threat scenarios
    - National and European actions
- About 12 bilateral contacts with system operators as follow-up to the survey (some not included before) for further understanding on
    - Status of national NIS directive implementation for the energy sector
    - Company progress, strategy and barriers to advance in cybersecurity maturity
    - Views on key parameters used in this study's bottom-up analysis

The information provided in the survey and all bilateral contacts is treated with confidentiality. This report only refers to aggregate views and analysis of the authors.

8.13 Industry survey template

1. General risk assessment methodology applied in your organisation

Q1-1. Have you established a cybersecurity risk management process throughout the organisation based on standards? If so, can you name the most relevant standards applied?

Click or tap here to enter text.

Q1-2. Do you incorporate cybersecurity in your enterprise architecture management (EAM) process?

Click or tap here to enter text.

Q1-3.: Can you name the most relevant legal restrictions that drive your cybersecurity risk assessment process? Please clarify whether these are EU legislations, national legislations, or other provisions (e.g. regulatory).

Click or tap here to enter text.

Q1-4. Does your organisation have an established internal computer emergency response team (CERT)?

Click or tap here to enter text.

Q1-5. In which knowledge exchange platforms are you active? To which extent do you see the confidential nature of many specific cybersecurity measures and experiences as a barrier to knowledge sharing?

Click or tap here to enter text.

2. Specific measures presently applied in your organisation

Q2-1. Does your organisation's cybersecurity approach make use of public attack databases for setting policies? Can you specify whether you use NESCOR[28] , CAPEC[29]or other intelligence sources?

Click or tap here to enter text.

Q2-2. Do you use any of the following specific mitigation standards? You can provide further clarification.

[28] http://smartgrid.epri.com/NESCOR.aspx

[29] https://capec.mitre.org/

ENISA guidance	☐Click or tap here to enter text.
NISTIR 7628	☐Click or tap here to enter text.
NIST SP 800-53	☐Click or tap here to enter text.
DHS Catalog	☐Click or tap here to enter text.
NERC CIPs	☐Click or tap here to enter text.
NRC Regulatory Guidance	☐Click or tap here to enter text.
Other related ones	Click or tap here to enter text.

Q2-3. Do you apply methods or standards developed in the Mandate 490 Smart Grid Information Security group (SGIS)[30], e.g. the SGAM framework?

Click or tap here to enter text.

Q2-4. Do you apply measures and mitigations generic to industrial control systems in your company?

Click or tap here to enter text.

Q2-5. Which of the following aspects are addressed in your organisation's mitigation approach?

Access Control	☐
Audit and accountability	☐
Awareness and training	☐
Configuration management	☐
Continuity of operations	☐
Identification and authentication	☐
Incident response	☐
Information and Document management	☐
Information Systems and communication protection	☐
Information systems and information integrity	☐
Information Systems and Service Acquisition	☐
Media Protection	☐
Personnel Security	☐
Physical and environmental security	☐
Planning	☐
Risk management and assessment	☐
Security assessment and authorisation	☐
Security Program Management	☐

[30] ftp://ftp.cencenelec.eu/EN/EuropeanStandardization/HotTopics/SmartGrids/SGCG_SGIS_Report.pdf

Smart grid Information System Development and maintenance	☐

Q2-6. Which are the most important (top 5) mitigation measures for your organisation?

- …
- …
- …
- …
- …

Q2-8. Which are the most cost intensive (top 5) mitigation measures for your organisation? Please provide a ranking, express the relative costs of various measures if possible.

1. … , (comprising approx. X % of total annual ICT budget)
2. …
3. …
4. …
5. …

3. Staffing of your organisation and governance with respect to cybersecurity

Q3-1. How many compliance staff members for cyber security in energy systems do you have at your organisation approximately?

Click or tap here to enter text.

Q3-2. How often does your organisation perform an enterprise level risk assessment?

Click or tap here to enter text.

Q3-3. Has the organisation's budget for governance and oversight activities stayed at the same level, increased or declined over the past 12 months?

Click or tap here to enter text.

Q3-4. What is your organisation's approximate total expenditure spend-to-date on your efforts to update critical infrastructure protections? (incl. IT, legal support, consulting, internal resource time, etc.)?

Click or tap here to enter text.

Q3-5. What is your company's approximate annual anticipated-total-spend on management and oversight of critical infrastructure cybersecurity programs?

Click or tap here to enter text.

Q3-6. Rate the following challenges in terms of their impact on your cybersecurity implementation plans. (High, Medium, Low)

	High	Medium	Low
Qualified and available Subject Matter Experts with specific skill sets	☐	☐	☐
Increases in number of assets/devices that need to be monitored/protected	☐	☐	☐
Employee training, background investigations, etc.	☐	☐	☐
Cultural shift towards secure business practices	☐	☐	☐
Implementation of new technologies and systems	☐	☐	☐

4. Threat scenarios

Q4-1. Which are the most common cybersecurity attack types (top 3) your organisation's infrastructure has been subject too?

- …
- …
- …

Q4-2. Do you consider it likely that there are attacks on your systems which are unnoticed? Does your organisation establish a forensics process to avoid such attacks in future and are mitigations put into your cybersecurity governance?

Click or tap here to enter text.

National and European actions addressing cybersecurity measures in the energy sector

The European NIS Directive provides various legal measures to increase the level of cybersecurity in various domains. The recent Commission communication of September 2017 also provides further guidance for national implementation as well as additional European initiatives.

Q5-1. Which further regulatory and policy actions do you believe are relevant at national level to boost cybersecurity levels in the energy sector?

Click or tap here to enter text.

Q5-2. Which further regulatory and policy actions do you believe are relevant at European level to boost cybersecurity levels in the energy sector?

Click or tap here to enter text.

Q5-3. In the case of a large-scale (regional / pan-European) attack scenario where a substantial part of the energy system may be affected by a serious security breach, what is in your opinion needed to isolate and mitigate the incident? E.g. who could/should monitor, who could/should trigger an alarm, who could/should escalate an alarm, who should act upon an alarm and be responsible for specific decisions?

Click or tap here to enter text.

Q5-4. Should in your opinion European or national certifications authorities play a role in cybersecurity aspects to set up common criteria evaluations schemes? If so, which components of the energy system should be included in this process?

Click or tap here to enter text.

8.14 Navigant Research market data

Chapter 5 builds on a Navigant Research analysis of Q3/2017 regarding 'Cybersecurity for the Digital Utility'. This report examines cybersecurity issues for smart grids to determine which security issues present the most viable opportunities for smart grid cybersecurity vendors. Navigant Research interviewed a wide variety of stakeholders, including utilities, security vendors, systems integrators, component manufacturers, and well-known subject matter experts. The forecast in this report segments the smart grid into five application areas: transmission upgrades, SA, DA, smart metering, and smart grid IT & analytics. This report draws heavily on other Navigant Research reports and forecasts concerning smart grid technology markets. Smart grid cybersecurity exists only because those other markets generate products and services that must be secured.

Navigant Research's industry analysts utilise a variety of research sources in preparing Research Reports. The key component of Navigant Research's analysis is primary research gained from phone and in-person interviews with industry leaders including executives, engineers, and marketing professionals. Analysts are diligent in ensuring that they speak with representatives from every part of the value chain, including, but not limited to, technology companies, utilities, and other service providers, industry associations, government agencies, and the investment community.

Additional analysis includes secondary research conducted by Navigant Research's analysts and its staff of research assistants. Where applicable, all secondary research sources are appropriately cited within this report.

These primary and secondary research sources, combined with the analyst's industry expertise, are synthesized into the qualitative and quantitative analysis presented in Navigant Research's reports. Great care is taken in making sure that all analysis is well-supported by facts, but where the facts are unknown and assumptions must be made, analysts document their assumptions and are prepared to explain their methodology, both within the body of a report and in direct conversations with clients.

Navigant Research is a market research group whose goal is to present an objective, unbiased view of market opportunities within its coverage areas. Navigant Research is not beholden to any special interests and is thus able to offer clear, actionable advice to help clients succeed in the industry, unfettered by technology hype, political agendas, or emotional factors that are inherent in cleantech markets.

Ecofys - A Navigant Company

Ecofys Germany GmbH | Albrechtstraße 10 c | 10117 Berlin | **T** +49 (0)30 29773579-0 | **F** +49 (0)30 29773579-99 | **E** info@ecofys.com | **I** ecofys.com

ECOFYS

A Navigant Company

Ecofys - A Navigant Company

Ecofys Germany GmbH
Albrechtstraße 10 c
10117 Berlin

T: +49 (0) 30 29773579-0
F: +49 (0) 30 29773579-99

E: info@ecofys.com
I: ecofys.com