Smart-Grid-Enabled Business Cases and the Consequences of Cyber Attacks

Øyvind Toftegaard[1,2(✉)], Doney Abraham[2], Sujeet Shenoi[3], and Bernhard Hämmerli[2,4]

[1] Norwegian Energy Regulatory Authority, Oslo, Norway
oyat@nve.no
[2] Norwegian University of Science and Technology, Gjøvik, Norway
[3] University of Tulsa, Tulsa, OK, USA
[4] Lucerne University of Applied Sciences and Arts, Lucerne, Switzerland

Abstract. The introduction of smart metering systems is a paradigm shift for the power grid. New business cases such as virtual power plants and local flexibility markets are evolving. Security risks and the potential consequences of smart-grid-enabled business cases have been assessed by researchers. However, the research efforts have not ranked the business cases according to their potential disruptive consequences, which makes it difficult to prioritize risk reduction measures.

This chapter describes the results of a survey of market players that sought to rank smart-grid-enabled business cases based on their perceptions of cyber attack consequences. As expected, the consequence perceptions of the market players vary considerably between the business cases. Consequence scenarios suggested by the market players are employed to explain the highest-ranked business cases, which include digital twins, remote access to smart meter circuit breakers, and grid flexibility and balance management. The survey results can support governments and market players in assessing power grid risk and prioritizing risk reduction measures.

Keywords: Smart Grids · Business Cases · Cyber Attacks · Consequences

1 Introduction

Power grids are large and complex systems of systems. Regional grids are connected by transmission lines and national grids are synchronized across borders. Market players such as authorities, grid operators, end-users, vendors and generators must work coherently to ensure safe and reliable grid operation. Digitalization and smart functions are increasingly employed to support and enhance market player interactions.

The U.S. National Institute of Standards and Technology defines a smart grid as "a power network that uses information technology to deliver electricity

Published by Springer Nature Switzerland AG 2024
J. Staggs and S. Shenoi (Eds.): ICCIP 2023, IFIP AICT 686, pp. 17–39, 2024.
https://doi.org/10.1007/978-3-031-49585-4_2

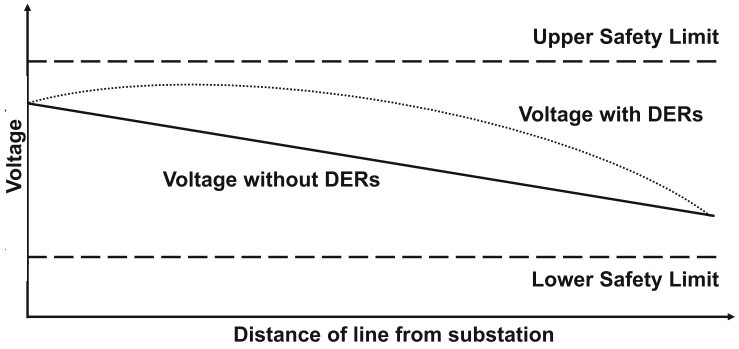

Fig. 1. Voltage properties on a power distribution line [11].

efficiently, reliably and securely" [16]. Future smart grids will need much digitalization to accommodate the shift to green energy in Europe and elsewhere in the world. Because green energy resources are highly decentralized and volatile, digital systems are necessary to balance power production and consumption. The expected increases in digital management and grid complexity will render it more challenging than ever to combat cyber attacks and mitigate their consequences.

This study applies the U.S. Cybersecurity and Infrastructure Security Agency definition of consequences – "[t]he effect of a loss of confidentiality, integrity or availability of information or an information system on an organization's operations, its assets, on individuals, other organizations, or on national interests" [15]. Table 1 summarizes the consequences of key cyber attacks on European power market players as reported by the news media between 2015 and 2022.

The key function of a smart grid is power supply. The grid requires supervision, control and protection equipment to remain operational. Grid protection is provided by protective relays, automatic devices that sense abnormal grid conditions and operate circuit breakers to disconnect faulty portions of the grid.

The most common protective relays are overcurrent, differential, directional and distance (impedance) relays. They differ in their functions, input measurements and triggering abnormalities. While protective relays are adequate in classical power grids, significant complexities to their use are imposed by the smart grid concept. The complexities arise from the large volume of distributed energy resources (DERs) and the need for self-healing [10]. As a result, protective relays that change their settings in real-time are required [13,17–19].

Figure 1 shows a simplified illustration of voltages on a power distribution line with and without the presence of distributed energy resources [11]. Manipulations of distributed energy resources may cause the power line voltage to peak or drop, crossing beyond the safety limits. As a result, protective relays will disconnect certain distributed energy resources or, in the worst case, disconnect the power line itself.

The introduction of smart metering systems is the first step in the realization of smart grids [28]. The next steps will involve artificial intelligence, digital

Table 1. Consequences of cyber attacks on European power market players.

Target	Method	Objective	Consequence
Ukraine Grid Operator (2015)	Black Energy, KillDisk wiper	Power disruption	225,000+ customers lost power for more than two hours
Ukraine Grid Operator (2016)	Crash override, wiper tool	Power disruption	Customers connected to a substation lost power for about one hour
Hydro (Norwegian End-User) (2019)	LockerGoga ransomware	Financial gain	Business systems lost functionality
Elexon (UK Market Platform) (2020)	Revil/Sodinokibi ransomware	Financial gain	Office systems lost functionality and internal data posted on dark web
Volue (Norwegian Tech Supplier) (2021)	Ryuk ransomware	Financial gain	Office systems lost functionality
Nordex Designs (German Wind Turbine Manufacturer) (2022)	Unknown	Unknown	Turbines lost remote monitoring functionality temporarily
Enercon (German Wind Turbine Manufacturer) (2022)	AcidRain wiper	Satellite communications disruption	5,800 turbines lost remote monitoring and control functionality
Rosseti (Russian Power Corporation) (2022)	Ukraine supplier backdoor	E-mobility disruption	Electric vehicle chargers on Moscow/Saint Petersburg motorway disabled
Deutsche Windtechnik (German Wind Farm Operator) (2022)	Unknown	Unknown	Turbines lost remote monitoring functionality for one to two days
Encevo Group (Luxemburg Power Corporation) (2022)	BlackCat/AlphV ransomware	Financial gain	Office systems lost functionality and customer data posted on the dark web

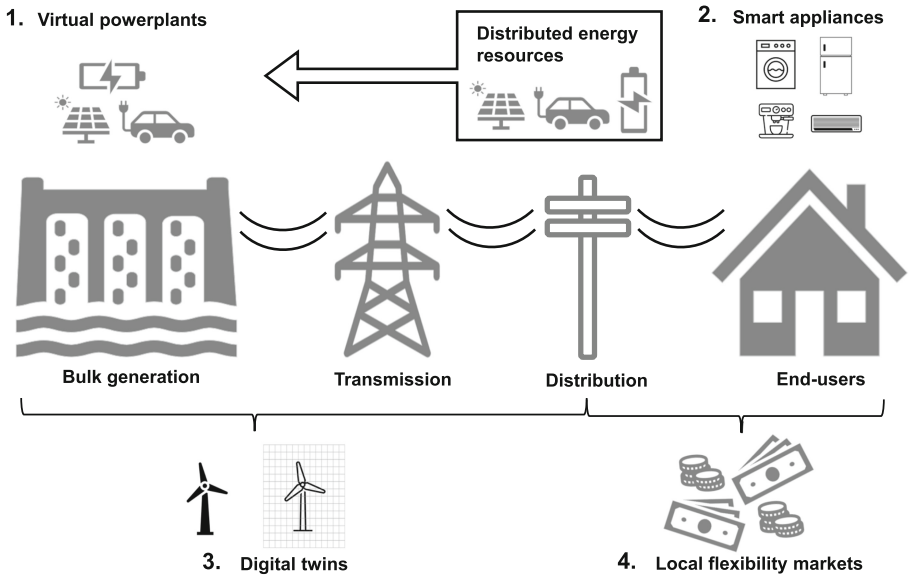

Fig. 2. Smart-grid-enabled business case examples.

twins and other evolving and potentially disruptive technologies. The massive amounts of data collected, communicated and processed by smart grids will propel innovation and many new business cases.

A business case describes perceived business needs that provide services or products. In this study, smart-grid-enabled (SGE) business cases are defined as services or products that utilize the information technology layer of the power network to support smart grid functions.

Figure 2 shows examples of smart-grid-enabled business cases. The business cases include virtual power plants that aggregate distributed energy resources to sell energy in the wholesale market, smart appliances that react automatically to pricing and other management signals to manage power consumption, digital twins that simulate turbine and grid component wear and tear for maintenance planning, and local flexibility markets that leverage end-users to balance distribution grids.

This research has focused on developing a ranking of the perceived consequences of cyber attacks on smart-grid-enabled business cases. Researchers have attempted to evaluate the risks to smart-grid-enabled business cases [1,12,21]. However, their efforts cover the potential consequences of cyber attacks on single business cases or limited sets of business cases. Additionally, since the business cases are not ranked by their consequence levels, it is difficult to determine which business cases should be prioritized for risk reduction investments. This is problematic because security investments may be directed at business cases with low cyber attack consequences instead of business cases that are critical.

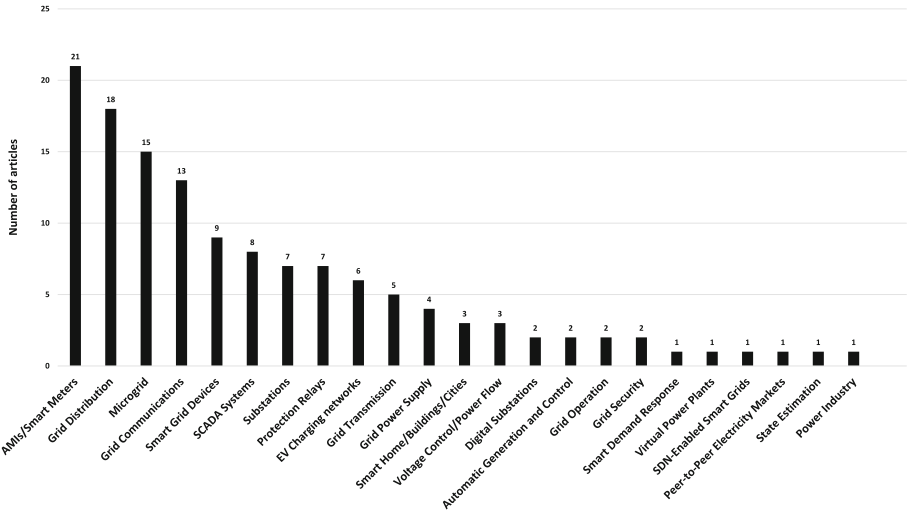

Fig. 3. Research articles in smart-grid-enabled business areas [1].

The focus of this research was to determine the smart-grid-enabled business cases perceived as having the most severe cyber attack consequences. The goal was to rank smart-grid-enabled business cases based on their potential consequence levels. The ranking is vital to entities that own or operate grid infrastructure assets, entities that provide services and authorities that regulate grid security. The ranking would also be a good starting point for researchers pursuing other inquiries such as validating consequence levels through simulation.

2 Previous Work

Several researchers have discussed the consequences of cyber attacks on smart-grid-enabled business cases. However, most of them consider single business cases such as smart meters [2], electrical vehicle (EV) charging [9] or distributed energy resources [11]. Other researchers have analyzed the consequences of cyber attacks on multiple business cases. For example, Li et al. [12] reviewed cyber attack methods on cyber-physical power systems, identifying outages as consequences of cyber attacks on smart substations and financial loss and billing difficulties as consequences of cyber attacks on smart meter systems. Procopiou and Komninos [21] analyzed current and future smart grid threats and their consequences. Their analysis used smart homes as the starting point and included evaluations of load control, demand response and outage management systems.

Abraham et al. [1] have conducted a study of research articles that discuss consequence verification during smart-grid-related risk assessments. Figure 3 shows the distribution of articles by business area. If the most-covered business areas are those with the greatest consequences, the distribution suggests that

business cases involving advanced metering infrastructures/smart metering systems, grid distribution and microgrids have the highest consequence levels.

In summary, previous work has focused on the consequences of cyber attacks on smart-grid-enabled business cases. However, the efforts do not rank business cases based on their consequence levels. Additionally, the efforts are relatively narrow in that they focus on single or small sets of business cases.

3 Survey Methodology

The research methodology described in this chapter engaged an interview-based exploratory survey. The research objective was to establish a ranked list of smart-grid-enabled business cases based on their perceived cyber attack consequence levels. The ranking would indicate the business cases that require further consequence assessments to identify high-risk products and services in future smart grids.

Specifically, the research study sought to determine the smart-grid-enabled business cases in Norway with the most severe perceived cyber attack consequences. Norway is one of the most digitalized countries in the world [14]. In 2022, the Norwegian energy mix was 89% hydroelectric and 10% wind [4]. The country achieved 97% smart meter coverage in January 2019 [30]. In 2022, 21% of all operational automobiles and 79% of automobiles sold were electric vehicles [27]. The rapid digitalization and increasing complexity of the Norwegian power grid make it vital to understand the consequences of cyber attacks on smart-grid-enabled business cases.

3.1 Interviews

A total of 22 interviewees from 17 Norwegian power market players were solicited for their perceptions of the potential consequences of cyber attacks on smart-grid-enabled business cases. Nineteen interviews were conducted in Norway between December 2022 and April 2023, each interview lasting between 45 and 60 min. The interviewees comprised 16 males and six females. Two interviewees were in the 20–30 age group, six in the 30–40 age group, five in the 40–50 age group, three in the 50–60 age group and six in the 60–70 age group. All the interviewees, except for the four end-users and three of the five authority employees, had extensive technical backgrounds in cyber security and/or information technology.

Table 2 provides details about the 22 interviewees. The interviewees were drawn from five types of entities, authorities, grid operators, end-users, vendors and generators. The sizes of the entities were determined based on their Norwegian krone revenues converted to their euro equivalents. The Proff Forvalt business information tool [22] was used to obtain annual revenue turnover data. The European Commission definitions of entity sizes [5] were employed based on their annual turnover: micro (up to two million euros), small (above two million

Table 2. Interviewee characteristics.

Market Player	Entity/Role	Size	I	N_I	BC
Authorities	Norwegian Energy Regulatory Authority	Medium	3	3	24
	Norwegian Water Resources and Energy Directorate	Large	1	1	
	Norwegian Data Protection Authority	Medium	1	1	
Grid Operators	Transmission system operator	Large	1	1	21
	Distribution system operator	Large	1	1	
	Distribution system operator	Small	1	1	
	Grid operator association	Small	1	1	
End-Users	Private consumer	N/A	1	1	16
	Private prosumer	N/A	1	1	
	Real estate company	Large	1	2	
	Private end-user association	Medium	1	1	
Vendors	Smart meter vendor	Small	1	2	15
	Grid component/technology vendor	Large	1	1	
	Technology vendor	Large	1	1	
Generators	Hydroelectric and wind power	Large	1	1	13
	Renewables and energy community	Micro	1	2	
	Hydroelectric power	Large	1	1	
			19	22	59

I: Number of interviews, N_I: Number of interviewees, BC: Number of business cases

up to ten million euros), medium (above ten million up to 50 million euros) and large (above 50 million euros).

The interview process relied on the Australian Council for Educational Research (ACER) creative thinking framework [23]. ACER defines creative thinking as "the capacity to generate many different kinds of ideas, manipulate ideas in unusual ways and make unconventional connections in order to outline novel possibilities that have the potential to elegantly meet a given purpose."

In the context of this research, the novelty of the business cases called for creativity in identifying potential consequences. The ACER creative thinking framework provides three overarching strands comprising various aspects that support creative thinking. The three strands and six aspects shown in Table 3 were used in the interview process.

Table 4 shows an example of a completed survey form.

Consequence ranks and consequence ratings were assigned to assess smart-grid-enabled business cases based on the perceived consequences:

- **Consequence Ranks:** 1 (highest rank), 2, ..., N (lowest rank).
- **Consequence Ratings:** Very High, High, Moderate, Low, Very Low.

Consequence ranking was employed to compare smart-grid-enabled business cases against each other by assigning ranks from 1 to N, where N is the number of business cases. Consequence rating was used to compare smart-grid-enabled business cases using a scale from Very High to Very Low. The advantage gained from using consequence ranks and ratings is that the two methods mutually validate each other.

Table 3. Interview process based on the ACER creative thinking framework [23].

Strand	Aspect	Description
Strand 1		Generation of business cases
	Aspect 1.1	Number of business cases
	Aspect 1.2	Detail levels of business cases
Strand 2		Scenario experimentation
	Aspect 2.1	Perspective shifting
	Aspect 2.2	Scenario manipulation
Strand 3		Ranking and quality control
	Aspect 3.1	Fitting after ranking
	Aspect 3.2	Rank validation through rating

Table 4. Example of a completed survey form.

Business Case	Scenario Description	Consequence Rank (Rating)
Remote access to smart meter circuit breakers	Remote access to large numbers of circuit breakers leading to a massive outage	1 (Very High)
E-mobility and charging services	Remote access to manage charging loads leading to a small outage	2 (High)
...	...	... (...)
...	...	... (...)
...	...	... (...)
Direct metering of individual appliances	Disclosure of private consumption data	N (Low)

Cyber attacks compromise the confidentiality, integrity or availability of information and information systems [15]. In turn, the compromises negatively impact an organization's assets, operations and individuals, other organizations or national interests. The interview guide used in the study specified the evaluation of consequences according to the European Union Network and Information Security (NIS) Directive (Article 6, No. 1) [6]. The directive lists six factors that should be considered when determining the significance of a disruptive impact:

- Number of users relying on the business case.
- Dependencies of other sectors on the business case.

- Potential impacts of incidents, in terms of degrees and durations, on economic and societal activities or public safety.
- Market share of the business case.
- Geographic spread with regard to the areas affected by the incidents.
- Importance of the business case for maintaining a sufficient level of service, taking into account the availability of alternative means for providing the service.

The study did not employ a consequence matrix with threshold values, such as for financial loss or blackout duration, for the consequence levels. Instead, interviewees provided ranks and ratings for smart-grid-enabled business cases subjectively based on their perceptions.

3.2 Data Analysis

To enable the data analysis, perceived consequence ratings were given consequence scores S as follows: Very High ($S = 5$), High ($S = 4$), Moderate ($S = 3$), Low ($S = 2$) and Very Low ($S = 1$). The individual consequence scores provided by the interviewees were combined to determine the total consequence score for each smart-grid-enabled business case. The computation employed a methodology used to evaluate the evidence strength of identity documents [29]. Specifically, the total consequence score B_j for the j^{th} smart-grid-enabled business case is given by:

$$B_j = S_{1,j} + 2\sum_{i=2}^{N} \frac{S_{i,j}}{2^i} \tag{1}$$

where $S_{i,j}$ is the score provided by interviewee i for business case j. The convergent series used to compute the total score requires the first score $S_{1,j}$ to have the greatest value and the remaining scores have exponential reductions in their values. For this reason, the individual scores for a business case are ordered from the highest to the lowest values. The first score $S_{1,j}$ is always the highest individual score and the last score $S_{N,j}$ is always the lowest individual score.

The advantage of the methodology is that a single individual outlier score of say, Very High, for a business case would not be valued too highly. Specifically, the business case would not be valued higher than a business case whose individual scores have more consensus. Another advantage is that a large number of low individual scores would prevent the total consequence score from having a high value. Figure 4 demonstrates the convergent function properties for two computations, one (A) with individual ordered scores $1, 1, 1, 1$ and the other (B) with individual ordered scores $3, 2, 2, 2$.

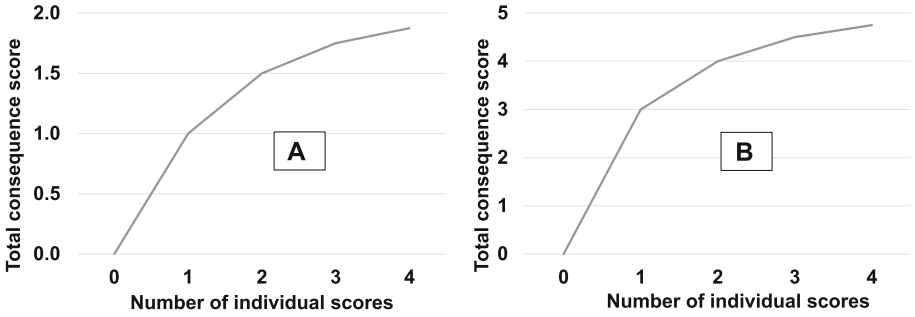

Fig. 4. Convergent function examples.

4 Results

Tables 5, 6, 7 and 8 present the 59 smart-grid-enabled business cases provided by the interviewees ranked by their perceived consequence scores adjusted for consensus. The business cases are ranked based on the combination of the interviewees' perceived consequence ratings and interviewee consensus according to Eq. 1. The smart-grid-enabled business cases with the greatest perceived consequences adjusted for consensus are digital twins, remote access to smart meter circuit breakers, and grid flexibility and balance management.

To understand the consequence rating data in the tables, consider the top-ranked digital twins business case. For this business case, the entry 1 (O1) for the High rating means that one interviewee (1) gave it a High rating and this one interviewee was from a grid operator (O1). Also, the entry 3 (O1, E2) for the Very High rating means that three interviewees (3) gave it Very High ratings, and one of the three interviewees was from a grid operator (O1) and the other two interviewees were end-users (E2).

Table 9 shows the consequence scenarios for the smart-grid-enabled business cases with the top ten ranks in Tables 5, 6, 7 and 8. The top four business cases all have power outage as their main consequence. Privacy and financial consequences are relevant to the fifth-ranked business case. Business cases ranked six through nine have grid instability in their consequence scenarios. National security and financial consequences are relevant to the tenth-ranked business case.

Table 10 shows the smart-grid-enabled business cases with the greatest perceived consequence ranks per interviewee for each market player group. Some of the market players in the same group ranked the same business cases on top. However, none of the top-ranked business cases were identified by two or more market player groups. Thus, there are considerable differences in the perceptions of different market players regarding the business cases with the greatest cyber attack consequences.

Figure 5 shows the smart-grid-enabled business cases with the highest consensus on the consequence ratings. Despite having 22 interviewees, the maximal consensus is four interviewees for one smart-grid-enabled business case. Also,

Table 5. Business cases ranked by perceived consequence ratings while considering consensus.

Rank	Business Case	Consequence Ratings				
		Very Low	Low	Moderate	High	Very High
1	Digital twins				1 (O1)	3 (O1, E2)
2	Remote access to smart meter circuit breakers		1 (A1)	1 (O1)		3 (A1, V2)
3	Grid flexibility and balance management			1 (A1)	1 (G1)	2 (E2)
4	Substation automation (circuit breakers)					3 (A3)
5	Centralized storage of personal data				2 (G2)	1 (A1)
6	SCADA system and sensor communications integration			1 (A1)	1 (E1)	1 (O1)
7	Virtual power plants			1 (G1)	1 (V1)	1 (O1)
8	Battery park management systems		1 (A1)	3 (O1, G2)		1 (A1)
9	System integration and operational technology digitalization					2 (A1, V1)
10	Smart meter consumption data				4 (V2, E2)	
11	Advanced process automation for grid management				1 (O1)	1 (O1)
12	Artificial intelligence and machine learning for optimizing production and maintenance				3 (A1, O2)	
13	E-mobility and charging services				3 (E1, G2)	
14	Substation integration of advanced metering infrastructures and SCADA systems				3 (O1, V2)	
15	Microgrids and energy communities		1 (A1)	1 (V1)	2 (G2)	

A: Authority, O: Grid operator, E: End-user, V: Vendor, G: Generator

Table 6. Business cases ranked by perceived consequence ratings while considering consensus (continued).

Rank	Business Case	Consequence Ratings				
		Very Low	Low	Moderate	High	Very High
16	Central control systems for building management		2 (E2)		2 (G2)	
17	Power grid sensors			1 (O1)		1 (O1)
18	Market platforms		1 (A1)		2 (E2)	
19	Digital components from untrusted parties				2 (E2)	
20	Multiple smart home appliance suppliers				2 (E2)	
21	Integration of production plans in SCADA systems				2 (G2)	
22	Digital management of hydroelectric power plants				2 (A1, G1)	
23	Concurrent consumption tariffs				2 (E2)	
24	Operators of smart home products and home energy management systems		1 (O1)	4 (A1, O3)		
25	Processing of personal customer information			1 (V1)	1 (E1)	
26	Managed service provider operation of renewables			3 (A1, O2)		
27	Applications integrated by aggregators			3 (A1, E2)		
28	Remote management of smart appliances			3 (G3)		
29	Smart meters and smart appliances		2 (E1, G1)	2 (E2)		
30	Digital supply chains for SCADA systems					1 (V1)
31	Aggregator management of power consumption		1 (A1)		1 (V1)	

A: Authority, O: Grid operator, E: End-user, V: Vendor, G: Generator

Table 7. Business cases ranked by perceived consequence ratings while considering consensus (continued).

Rank	Business Case	Consequence Ratings				
		Very Low	Low	Moderate	High	Very High
32	Smart meter/home area network data streams			2 (A2)		
33	Additional data collected by smart meters		2 (V2)	1 (O1)		
34	Information-driven emergency response				1 (O1)	
35	Grid self healing				1 (O1)	
36	Heating appliances that pose fire hazards				1 (E1)	
37	Near real-time algorithm-based grid balancing				1 (O1)	
38	Physical robots on the ground				1 (O1)	
39	Smart appliance performance monitoring				1 (A1)	
40	Additional information-driven processes				1 (A1)	
41	Home area network or price based consumption management		1 (A1)	1 (A1)		
42	Peer-to-peer electricity trading	1 (A1)	2 (V2)			
43	In-home battery or electric vehicle to grid			1 (E1)		
44	Grid frequency stabilization			1 (G1)		
45	Sharing and transportation of grid data and information			1 (O1)		

A: Authority, O: Grid operator, E: End-user, V: Vendor, G: Generator

Table 8. Business cases ranked by perceived consequence ratings while considering consensus (continued).

Rank	Business Case	Consequence Ratings				
		Very Low	Low	Moderate	High	Very High
46	Automated data processing for grid operations			1 (O1)		
47	Transmission line routing optimization			1 (O1)		
48	Wind farms and solar parks			1 (O1)		
49	Prosumers with smart home systems			1 (O1)		
50	Market platforms for local end-user flexibility			1 (A1)		
51	Drones			1 (O1)		
52	Autonomous grid management for businesses			1 (V1)		
53	Direct metering of individual appliances		2 (V2)			
54	Sensors for building energy management systems		2 (G2)			
55	Dynamic electricity supplier transfer based on price		1 (A1)			
56	Solar panels		1 (A1)			
57	Smart energy products and services		1 (E1)			
58	Artificial intelligence driven protective relays		1 (V1)			
59	Information about maintenance and end of use		1 (A1)			

A: Authority, O: Grid operator, E: End-user, V: Vendor, G: Generator

Table 9. Ten business cases with the greatest perceived consequences.

Rank	Business Case	Consequence Scenario
1	Digital twins	Adversaries with access to grid-related digital twins may use them to identify vulnerabilities, optimize damage or disturb operations, leading to large outages. Access to digital twins of building energy management systems can help enable manipulations leading to financial consequences or physical damage
2	Remote access to smart meter circuit breakers	Adversaries may gain remote access to circuit breakers, leading to small to large outages
3	Grid flexibility and balance management	Manipulation or loss of access to management systems controlling large aggregated loads may lead to outages
4	Substation automation (circuit breakers)	Adversaries may gain remote access to circuit breakers leading to injuries or death, grid imbalance or small to large outages
5	Centralized storage of personal data	Assuming future data storage with very high resolution, potential consequences of cyber attacks include privacy breaches, financial consequences or data being used for various nefarious purposes
6	SCADA system and sensor communications integration	Adversaries with access to sensors may inject false data, leading to power disturbances or outages due to bad decision making.
7	Virtual power plants	Cyber attacks on management systems of virtual power plants may lead to grid instabilities or outages
8	Battery park management systems	Adversaries with access to battery park management systems may manipulate or dis-connect loads, leading to grid imbalances or potential battery fires. The worst case is outages, especially if other loads are disconnected simultaneously
9	System integration and operational technology digitalization	Adversaries with access to operational technology environments may manipulate power production or modify or delete data, leading to grid disturbances or outages
10	Smart meter consumption data	End-user consumption data may reveal military preparations or movements, posing threats to national security. Adversaries may also modify consumption data, leading to financial impacts on victims

three interviewees agreed on the same consequence ratings for seven of the business cases.

Figure 6 shows the smart-grid-enabled business cases with the largest spreads in the consensus on consequence ratings. While the remote access to smart meter

Table 10. Business cases ranked with the greatest consequences.

Market Player	Business Case	N_I
Authorities	Substation automation (circuit breakers)	3
	Artificial intelligence and machine learning for optimizing production and maintenance	1
	System integration and operational technology digitalization	1
Grid Operators	SCADA system and sensor communications integration	1
	Virtual power plants	1
	Digital twins	1
	Information-driven emergency response	1
End-Users	Digital components from untrusted parties	2
	Heating appliances that pose fire hazards	1
	Grid flexibility and balance management	2
Vendors	Advanced process automation for grid management	1
	Remote access to smart meter circuit breakers	2
	Digital supply chains for SCADA systems	1
Generators	Integration of production plans in SCADA systems	1
	Digital management of hydroelectric power plants	1
	Microgrids and energy communities	2

N_I: Number of interviewees

circuit breakers business case has the second highest consequence rank in Table 5, it is also one of four business cases with the least consensus.

5 Discussion

The greatest cyber attack consequences were perceived for the digital twins, remote access to smart meter circuit breakers, and grid flexibility and balance management business cases (Table 5). These three business cases are connected to load control scenarios and power outages in the event of compromises (Table 9). In the case of smart metering, the high rank fits well with the survey paper of Abraham et al. [1] (Fig. 3), where smart meters is the business area whose consequences are the most assessed. Furthermore, the sixth rank for the SCADA system and sensor communications integration business case in this study fits well with grid communications ranked fourth by Abraham and colleagues. Similarities are seen when comparing the business case ranks in this study with the numbers of assessments per business area reported by Abraham et al. However, the large number of business cases reported in this study (59) indicates the complexity of smart grids and how challenging it is to identify the business cases with the greatest cyber attack consequences.

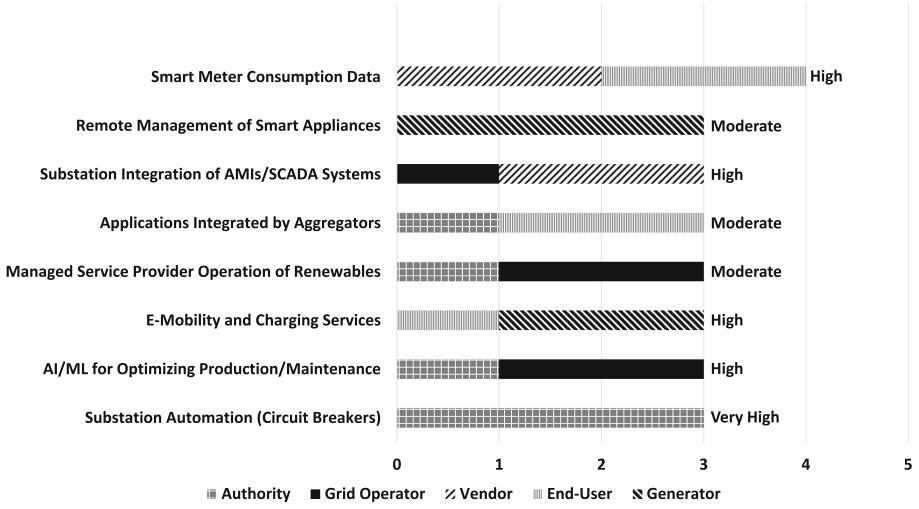

Fig. 5. Perceived consequence/consensus histogram.

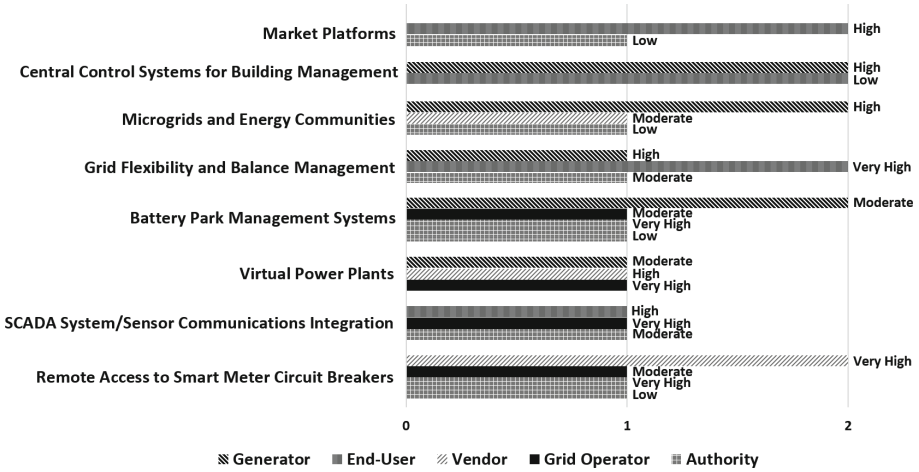

Fig. 6. Perceived consequence/non-consensus histogram.

The differences in the business cases reported with the greatest perceived consequences in Table 10 reveal how differently market players as well as individuals perceive smart grid consequences. The fact that none of the interviewees from all the market player groups gave the top rank to the same smart-grid-enabled business case suggests that the complexity of smart grids makes it challenging to anticipate potential consequences.

Figures 5 and 6 demonstrate little general consensus on the consequence levels of smart-grid-enabled business cases. The most consensus was observed in the

smart meter consumption data business case, but the consensus is small, just four of the 22 interviewees. The least consensus was seen in the battery park management system and remote access to smart meter circuit breakers business cases, whose perceived cyber attack consequences ranged from Very High to Low. The reason may be that the potential consequences depend on how business cases are implemented. An example is if smart meters were to have a capacity limit beyond which on-board circuit breakers should not be installed. In this case, large industrial, healthcare and public service facilities would not be impacted as much by cyber attacks on smart meters as small residential buildings. It is not known whether or not the interviewees were aware of and applied such details when they evaluated the cyber attack consequences. Additionally, limited knowledge about a new grid technology such as battery parks likely made it difficult for the interviewees to evaluate their disruptive potential.

Clearly, the differences in perceived consequences point to additional research to verify the findings of this study. Such verification could require going beyond interview-based surveys and performing real-world analyses.

6 Study Validity

This section discusses the threats to the validity of this study, which include critical realism, risk perception, and internal and external validity.

6.1 Critical Realism and Risk Perception

Human perception is known to be influenced by knowledge and experience. Critical realism theory distinguishes between the perceived empirical domain and hidden mechanisms [3]. According to critical realism, unobservable mechanisms cause observable events. These hidden mechanisms exist independent of human perceptions. Figure 7 shows how the perceived empirical domain and hidden mechanisms together constitute the real domain.

According to critical realism theory, interviewees' perceptions are colored by their personal theories, knowledge and understanding. Therefore, the interviewees' responses would not reflect the "real" domain, but their perceptions. When applying critical realism, the real consequences of cyber attacks can be understood only if the underlaying structures that generate each consequence are understood. This is problematic because smart-grid-enabled business cases can be described as complex socio-technical systems, implying that the structures that generate the consequences would be highly complex.

Perceptions of consequence scenarios and their severity levels are based on subjective observations and experiences. Therefore, the perceived consequences do not necessarily reflect the real consequence levels, but are rather the result of best efforts. However, subjective perceptions provide useful indications in risk assessments and are good starting points for further research.

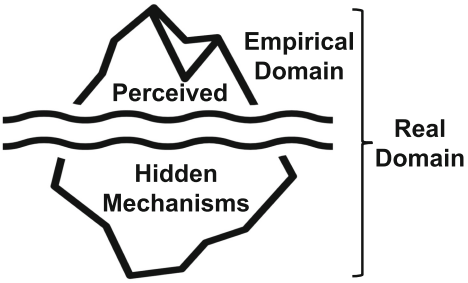

Fig. 7. Critical realism iceberg (based on [3]).

6.2 Internal and External Validity

Internal validity considers the extent to which observed results represent the truth in a study population and are, therefore, not due to methodological errors [20]. To ensure that the interviewees fully understood the task of ranking their proposed business cases from highest to lowest, a numerical rank (1, 2, ..., N) and a categorical rating (Very High to Very Low) were applied. This approach enabled the interviewer and interviewees to identify when logical failures occurred. Examples included a business case ranked 1 and rated High and another business case ranked 2 and rated Very High. During such situations, which occurred multiple times, the interviewees were asked to reconsider their responses. This method of securing interviewee understanding of the task strengthened the internal validity. A threat to the internal validity of this study is that only one to three individuals were interviewed per market player entity. Therefore, uncertainty exists whether or not the opinion of an interviewee's entity as a whole would be the same as that of the interviewee.

External validity considers the extent to which results from a study may be generalized [24]. A threat to the validity of this study is that it only sought perceived consequence rankings in the empirical domain. Thus, the results are influenced by the backgrounds of the interviewees and do not necessarily reflect the perceptions of others. Furthermore, because the only results are perceptions, it is unknown how well the results capture the real world. Therefore, the consequence rates obtained in this study need to be verified, perhaps through simulation.

Figure 8 illustrates how internal validity belongs to the empirical domain whereas external validity belongs to the real domain. Similar to the critical realism iceberg, the truth of the interviewees in this study is limited to their perceptions. The truth in the real domain is constructed by mechanisms, some of which would be invisible to the interviewees.

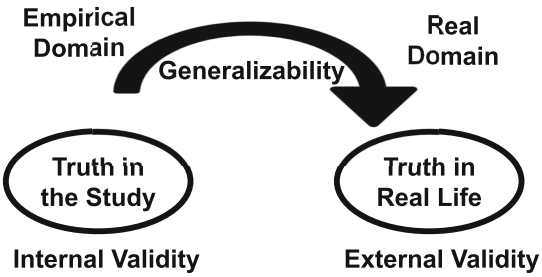

Fig. 8. Internal and external validity (based on [20]).

7 Empirical to Real Consequences

The results derived in the empirical domain are based on the perceived consequences of the interviewees and are, therefore, their personal opinions. However, because some real consequences are not visible as part of the perceived consequences, insights into the real consequences may be gained by conducting an investigation in a near-real (laboratory) domain.

An electric vehicle may be employed as a use case to explore the real consequences. Electric vehicle charging should be performed at intervals so as not to affect other grid operations and reduce the peak load time. Shafiq et al. [26] have shown that a load loss of 6.89% occurs when charging is done at irregular intervals. Fernandez et al. [7] have provided an assessment of the impacts of electric vehicles on the power distribution network. Their suggested strategy is based on a large-scale distribution planning model used to investigate two real power distribution areas. The first was a residential area with 6,000 end-users and 3,676 vehicles and the second was a commercial area with 61,000 end-users and 28,626 vehicles. Simulations of the effects of electric vehicle loads on system losses demonstrated that the loss could increase up to 40%, considering that electric vehicles accounted for 62% of the total number of vehicles.

Sayed et al. [25] studied an electric vehicle charging attack and its impacts on power grid operation. Their case study, which accounted for electric vehicle locations and loads, involved a simulated attack under various scenarios involving the ESCC9-bus system and 7-bus test case [8]. Attack simulations involving residential facility loads and electric vehicle loads demonstrated that electric vehicle loads had greater consequences on grid operations. Sayed and colleagues also showed how adversaries could estimate the grid topology and create targeted attacks that maximized negative impacts on the grid.

Weiss [31] has warned that frequency manipulations in the power grid could lead to catastrophic disruptive events as in the case of the celebrated Aurora generator test conducted in 2007 at Idaho National Laboratory. During the test, researchers caused a generator to catch fire by manipulating the power frequency. Power frequency is a measure of the amount of energy injected into the grid; the greater the energy injected, the higher the frequency. When the frequency

deviates from the accepted standards, clocks may show the wrong time and electric equipment can be destroyed. Therefore, it is essential to use near-real-domain experiments to investigate and evaluate the consequences in order to mitigate future attacks.

8 Conclusions

The research study of market players has sought to rank smart-grid-enabled business cases based on their qualitative perceptions of cyber attack consequences. The results reveal that the business cases with the greatest perceived cyber consequences are digital twins, remote access to smart meter circuit breakers, and grid flexibility and balance management. Although it was possible to identify the business cases with the greatest perceived consequences, little consistency was observed in the rankings by individuals and groups of market players. The principal reason for the inconsistent rankings appears to be the complexity of smart grids and smart-grid-enabled business cases.

The study results can support governments and market players in assessing power grid risk and prioritizing risk reduction measures. The results would also be useful to policymakers in defining the scope of smart grid cyber security legislation and regulations, and to researchers who wish to move the study results from the empirical domain to real-world applications and verification through simulation.

Acknowledgments. This research was supported by the Norwegian Energy Regulatory Authority and the Norwegian Water Resources and Energy Directorate. The authors also wish to thank Jon-Martin Storm, Janne Hagen and Silje Aakre for their assistance in this research.

References

1. Abraham, D., Toftegaard, Ø., Gebremedhin, A., Yayilgan, S.: Consequence verification during risk assessments of smart grids. In: Staggs, J., Shenoi, S. (eds.) Critical Infrastructure Protection XVII, pp. 39–61. Springer, Cham (2024)
2. Anderson, R., Fuloria, S.: Who controls the off switch? In: Proceedings of the First IEEE International Conference on Smart Grid Communications, pp. 96–101 (2010)
3. Bhaskar, R.: A Realist Theory of Science. Routledge, New York (2008)
4. Energy Facts Norway, Electricity Production, Oslo, Norway (2023). www.energifaktanorge.no/en/norsk-energiforsyning/kraftproduksjon
5. European Commission, SME Definition, Brussels, Belgium (2023). single-market-economy.ec.europa.eu/smes/sme-definition_en
6. European Parliament and the Council of the European Union, Directive (EU) 2016/1148 of the European Parliament and of the Council of 6: Concerning Measures for a High Common Level of Security of Network and Information Systems Across the Union, Document 32016L1148, Belgium, Brussels (2016)
7. Fernandez, L., Román, T.S., Cossent, R., Domingo, C., Frias, P.: Assessment of the impact of plug-in electric vehicles on distribution networks. IEEE Trans. Power Syst. **26**(1), 206–213 (2011)

8. Glover, J., Overbye, T., Sarma, M.: Power System Analysis and Design, SI Cengage Learning, Boston (2017)
9. Gumrukcu, E., et al.: Impact of cyber-attacks on EV charging coordination: the case of a single point of failure. In: Proceedings of the Fourth Global Power, Energy and Communications Conference, pp. 506–511 (2022)
10. Khalid, H., Shobole, A.: Existing developments in adaptive smart grid protection: a review. Electr. Power Syst. Res. **191**, Article no. 106901 (2021)
11. Langer, L., Smith, P., Hutle, M.: Smart grid cybersecurity risk assessment. In: Proceedings of the International Symposium on Smart Electric Distribution Systems and Technologies, pp. 475–482 (2015)
12. Li, F., Yan, X., Xie, Y., Sang, Z., Yuan, X.: A review of cyber-attack methods in cyber-physical power systems. In: Proceedings of the Eighth IEEE International Conference on Advanced Power System Automation and Protection, pp. 1335–1339 (2019)
13. Liu, Z., Hoidalen, H.: A simple multiagent system based adaptive relay setting strategy for a distribution system with wind generation integration. In: Proceedings of the Thirteenth International Conference on Developments in Power System Protection (2016)
14. Mattila, J., et al.: Digibarometer 2022: A Digital Green Transition (in Finnish). Taloustieto Oy, Helsinki, Finland (2022)
15. National Initiative for Cybersecurity Careers and Studies, Vocabulary, Cybersecurity and Infrastructure Security Agency, Washington, DC (2023). niccs.cisa.gov/cybersecurity-career-resources/glossary#C
16. National Institute of Standards and Technology, Smart Grid: A Beginner's Guide, Gaithersburg, Maryland (2019). www.nist.gov/el/smart-grid/about-smart-grid/smart-grid-beginners-guide
17. Pandakov, K., Hoidalen, H.: Distance protection with fault impedance compensation for distribution network with DG. In: Proceedings of the IEEE Power and Energy Society Innovative Smart Grid Technologies Conference Europe (2017)
18. Pandakov, K., Hoidalen, H., Marvik, J.: Implementation of distance relaying in distribution networks with distributed generation. In: Proceedings of the Thirteenth International Conference on Developments in Power System Protection (2016)
19. Pandakov, K., Hoidalen, H., Marvik, J.: Fast protection against islanding and unwanted tripping of distributed generation caused by ground faults. In: Proceedings of the Twenty-Fourth International Conference on Electricity Distribution, Paper No. 0716 (2017)
20. Patino, C., Ferreira, J.: Internal and external validity: can you apply research study results to your patients? J. Bras. Pneumol. **44**(3), 183 (2018)
21. Procopiou, A., Komninos, N.: Current and future threats framework in the smart grid domain. In: Proceedings of the IEEE International Conference on Cyber Technology in Automation, Control and Intelligent Systems, pp. 1852–1857 (2015)
22. Proff, Proff Forvalt Credit and Market Tools (in Norwegian), Oslo, Norway (Forvalt.no) (2023)
23. Ramalingam, D., Anderson, P., Duckworth, D., Scoular, C., Heard, J.: Creative Thinking: Definition and Structure. Australian Council for Educational Research, Camberwell, Australia (2020)
24. Runeson, P., Host, M.: Guidelines for conducting and reporting case study research in software engineering. Empir. Softw. Eng. **14**(2), 131–164 (2009)
25. Sayed, M., Atallah, R., Assi, C., Debbabi, M.: Electric vehicle attack impact on power grid operation. Int. J. Electr. Power Energy Syst. **137**, Article no. 107784 (2022)

26. Shafiq, S., Irshad, U., Al-Muhaini, M., Djokic, S., Akram, U.: Reliability evaluation of composite power systems: evaluating the impact of full and plug-in hybrid electric vehicles. IEEE Access **8**, 114305–114314 (2020)
27. Statistics Norway, Four of five new cars in 2022 were EVs (in Norwegian), Oslo, Norway, 24 March 2023. www.ssb.no/transport-og-reiseliv/landtransport/statistikk/bilparken/artikler/fire-av-fem-nye-biler-i-2022-var-elbiler
28. Toftegaard, Ø., Hagen, J., Hämmerli, B.: Are European security policies ready for advanced metering systems with cloud backends? In: Staggs, J., Shenoi, S. (eds.) Critical Infrastructure Protection XVI, pp. 47–69. Springer, Cham (2022). https://doi.org/10.1007/978-3-031-20137-0_2
29. Toftegaard, Ø., Yang, B.: Towards an operable evaluation system for evidence of identity. In: Proceedings of the Forty-Second IEEE International Computer Software and Applications, vol. 2, pp. 565–570 (2018)
30. Venjum, A.: Smart Meters (AMS) (in Norwegian), Report No. 24/2019, Norwegian Water Resources and Energy Directorate, Oslo, Norway (2019). publikasjoner.nve.no/rapport/2019/rapport2019_24.pdf
31. Weiss, J.: Aurora generator test. In: Radvanovsky, R., Brodsky, J. (eds.) Handbook of SCADA/Control Systems Security, pp. 107–114. Routledge, New York (2016)