frontiers | Frontiers in Energy Research

TYPE Original Research
PUBLISHED 03 July 2024
DOI 10.3389/fenrg.2024.1395954

OPEN ACCESS

EDITED BY
Fateh Krim,
University Ferhat Abbas of Setif, Algeria

REVIEWED BY
Narottam Das,
Central Queensland University, Australia
Sahaj Saxena,
Thapar Institute of Engineering and Technology, India

*CORRESPONDENCE
Doney Abraham,
doney.abraham@ntnu.no

RECEIVED 04 March 2024
ACCEPTED 06 June 2024
PUBLISHED 03 July 2024

CITATION
Abraham D, Toftegaard Ø, D. R. BBJ, Gebremedhin A and Yildirim Yayilgan S (2024), Consequence simulation of cyber attacks on key smart grid business cases.
Front. Energy Res. 12:1395954.
doi: 10.3389/fenrg.2024.1395954

Consequence simulation of cyber attacks on key smart grid business cases

Doney Abraham[1]*, Øyvind Toftegaard[1,2], Binu Ben Jose D. R.[3], Alemayehu Gebremedhin[4] and Sule Yildirim Yayilgan[1]

[1]Department of Information Security and Communication Technology, Norwegian University of Science and Technology, Gjøvik, Norway, [2]Norwegian Water Resources and Energy Directorate, Oslo, Norway, [3]School of Electrical Engineering, Vellore Institue of Technology, Chennai, India, [4]Department of Manufacturing and Civil Engineering, Norwegian University of Science and Technology, Gjøvik, Norway

The increasing threat of cyber-attacks on modern power systems highlights the need for a comprehensive examination through simulations. This study conducts an in-depth simulation of cyber-attacks on critical smart grid components, including smart meters, substation automation, and battery management systems, to expose and analyze potential disruptions to power system operations. We identify vulnerabilities that can lead to severe grid instabilities, such as voltage variations, system collapses, and inverter failures. Our analysis underscores the complex interactions between cyber threats and grid components, revealing how disruptions extend beyond mere load interruptions to affect the core infrastructure. We advocate for integrating established cybersecurity frameworks like NIST, ISO/IEC 27001, and IEC 62443, essential in fortifying grid stability against these dynamic threats. Our findings highlight the urgent need for continuous adaptation and enforcement of these frameworks to enhance resilience and ensure the reliability of modern power grids against cyber-attacks.

KEYWORDS

smart grids, cybersecurity, cyber attacks, solar panels, battery parks, circuit breakers, virtual power plants, consequences

1 Introduction

Integrating smart grid technologies in the energy sector has revolutionized power systems, offering enhanced efficiency, reliability, and sustainability (Kirmani et al., 2023). However, this integration also introduces new vulnerabilities, particularly cybersecurity (Zheng et al., 2022). Cyber attacks on smart grids can have severe consequences, impacting the stability and functionality of the grid (Amin et al., 2020). As the smart grid evolves to incorporate advanced technologies and communication networks, the risk of cyber threats increases, posing challenges to

Abbreviations: AMI, Advanced Metering Infrastructure; AC, Alternating Current; AI, Artificial Intelligence; CB, Circuit Breaker; DoS, Denial-of-Service; DDoS, Distributed Denial-of-Service; DC, Direct Current; HAN, Home Area Network; IoT, Internet of Things; MITM, Man In The Middle; DER, Distributed Energy Resource; VPP, Virtual Power Plants; kV, Kilovolt; MVA, Mega V A; MW, Megawatt; V, Volt; PV, PhotoVoltaic systems; kW, Kilowatt; ms, Millisecond; S, Second; PCC, Point of Common Coupling.

the integrity and security of the system (Wang and Lu, 2013; Rice and AlMajali, 2014).

For instance, the Ukraine power grid attack in 2015 is a stark reminder of the vulnerabilities present in modern energy systems. Hackers were able to disrupt the power supply to thousands of customers, highlighting the tangible impacts of cyber intrusions (Case, 2016). Saudi Aramco, the national oil company of Saudi Arabia, was hit by a destructive malware attack that erased data on 30,000 computers and disrupted the company's operations, marking it as one of the most dangerous cyberattacks against a single business (Bronk and Tikk-Ringas, 2013). Similarly, the Stuxnet worm demonstrated the potential for cyberattacks to damage infrastructure physically, as it did with Iranian nuclear facilities, by manipulating industrial control systems (Langner, 2011). These incidents underscore the need for robust cybersecurity measures to protect smart grid components.

The widespread adoption of Smart Grid technology has introduced both new opportunities and challenges in the energy sector, making it a subject of increasing interest in various business case scenarios (Rodríguez-Molina et al., 2014). Understanding the potential impact of cyber-attacks on smart grid-enabled business cases is crucial for developing effective defence strategies and ensuring the resilience of the grid infrastructure (Olowu et al., 2021). This understanding guides deploying advanced security solutions that can detect, mitigate, and prevent significant disruptions caused by cyber threats.

The primary objective of this paper is to validate the perceived consequences of key smart grid-enabled business cases by comparing them to the outcomes observed in simulated scenarios. Additionally, this study aims to assess the ranking of perceived consequences against those determined through simulation results. By doing so, the research seeks to understand the potential repercussions of cyber threats on smart grid business cases and prioritize them accordingly to inform future mitigation strategies. This study presents a comprehensive study on the consequence simulation of key Smart Grid-enabled business cases. To address this, we apply simulation methods to model and evaluate the direct consequences of adopting Smart Grid technology in different business case scenarios. The objective is to assess the feasibility and effectiveness of implementing Smart Grid technology in real-world business case scenarios. Our simulation results will provide valuable information for researchers, industry stakeholders, and policymakers interested in the development and implementation of Smart Grid technology. Additionally, the use of simulation methods enables us to explore the complex interactions among different components of the Smart Grid system and their impact on business outcomes.

2 Grid operations and built-in protective systems

The power grid operates with intricate precision, and unexpected events, such as a sudden reduction in consumption, prompt protective measures to ensure stability (Amani and Jalili, 2021). When consumption abruptly drops, protection systems leap into action, their vigilant sensors detecting anomalies and swiftly signalling the circuit breakers (CB relays) to open. This prompt response prevents potential overloading and safeguards the grid's intricate balance (Waseem and Manshadi, 2020).

In the broader context of grid function, two critical concepts, spinning reserves and black start procedures, play pivotal roles in anticipating and addressing potential outages (Vazquez, 2006). Spinning reserves are like silent sentinels, their pre-allocated power capacities synchronized with the grid, poised to inject instant support in times of need (Rebours and Kirschen, 2005). In the event of a sudden consumption loss, spinning reserves spring into action, bridging the gap left by the sudden drop and ensuring the grid's frequency remains steady. This dynamic balance prevents uncomfortable voltage fluctuations and maintains an uninterrupted power flow (Kirby, 2003).

However, in the event of a total power grid outage, the focus turns to the black start capability of the system (O'Brien et al., 2022). This remarkable capability empowers power plants to initiate the complex choreography of grid restoration. Gradually, power is rekindled in various grid segments, with a precise sequence that does not depend on external sources. This intrinsic self-reliance ensures that the grid reawakens, without needing external support (Jiang et al., 2017).

Amidst the intricate and comprehensive measures implemented, the safeguard systems remain vigilant, fulfilling their crucial role as protectors. In business case scenarios where spinning reserves might not react instantaneously to voltage dips resulting from sudden consumption losses, these unyielding protection systems come to the rescue. If detected voltage dips surpass predefined thresholds and the spinning reserves' response time is inadequate, the protection systems signal the circuit breakers to open. These rapid action confines disruptions, isolating the affected part of the grid and preventing any domino effects (Eto et al., 2007).

The grid's stability and recovery strategy involves coordinating spinning reserves, black start procedures, and protection systems. Simulating these business cases is crucial to refining the grid's response and fortifying its resilience in uncertainty.

3 Related work

The findings from Sgouras et al. (2014) reveal that cyber attacks on smart meters exhibit varying consequences. When individual meters are targeted, they may experience temporary isolation or malfunction, but without significant implications for the overall power grid. However, these attacks can lead to minor disruptions. The study highlights the impact of Denial-of-Service (DoS) attacks on the utility server, which can diminish packet transfer capacity and disrupt server-client communication. Particularly concerning is the Distributed Denial-of-Service (DDoS) attack during critical peak hours, compromising communication with approximately 89.7% of smart meters. This compromise hampers the availability of remote load commands for demand response, thereby limiting the ability to shed load during peak hours. Consequently, the interruption probability increases, which affects reliability indices and customer interruptions. The research underscores the need for mitigation strategies to ensure the protection and resilience of smart grid systems.

Authors in Sun et al. (2021) explore the vulnerabilities in smart grid systems' hardware and communication aspects. The authors

highlight that hardware vulnerabilities provide cyber attackers with the capability to execute diverse cyber attacks, resulting in severe operational impacts within distribution systems. In extreme cases, these attacks can reduce utility companies' revenues, infringe on customers' privacy, and even power outages. On the other hand, communication vulnerabilities arise due to the limitations of packet encryption in protecting sender and receiver identities, allowing attackers to target specific operations. The integrity of smart grid communication can be compromised through the recovery of local Home Area Network (HAN) passphrases and the utilization of spoofed MAC addresses, enabling the creation of false network messages. Additionally, availability can be affected by signal jamming and Denial-of-Service (DoS) attacks, resulting in disruptions in message transmission and potential operational issues for both the control centre and devices. This paper highlights the criticality of addressing these vulnerabilities to ensure the security and reliability of distribution systems.

Tweneboah-Koduah et al. (2018) demonstrated that the smart metering system could be compromised due to SQL injection and DoS attacks, resulting in data confidentiality and integrity loss. Mudgal et al. (2022) demonstrates DoS attack and Man In The Middle (MITM) attack on smart meters. The consequences of these attacks are load fluctuations on the consumer side, and the location of these fluctuations is not limited to the area under attack. There is also an economic loss for the service provider. The two attacks are then extended to an IEEE-30 bus system, and their impact is studied using MATPOWER simulations which showed a similar loss in load power reading of smart meters.

Chen et al. (2016) highlights the potential consequences of successful attacks on substation circuit breakers. Such attacks can result in the tripping of multiple circuit breakers, leading to cascading events that may impact substations. The worst-case scenario involves a power system blackout, which can have severe economic consequences. A real-world example is the cyber attack on the Ukrainian power grid (Alert, 2016) that demonstrated the necessity for cyber security measures at substations.

Fakhar et al. (2023) provides a comprehensive review of smart grid mechanisms for green energy management, offering in-depth analysis and insights into advanced strategies that enhance the efficiency and security of smart grid systems. Their research is crucial for understanding how to effectively integrate and manage renewable energy sources within smart grids, ensuring sustainability and resilience against cyber threats. Kumar et al. (2022) explore the comparison between wired and wireless modes of digital protection schemes leveraging on Parallel Redundancy Protocol (PRP) topology. Their findings highlight the advantages and challenges of each mode, particularly in maintaining communication security and data integrity within smart grid systems, making it valuable for enhancing cybersecurity measures in grid infrastructures.

The study by Nur-E-Alam et al. (2022) on rooftop PV or hybrid systems and retrofitted low-E coated windows for energy-efficient buildings in Bangladesh not only offers practical applications of renewable energy in smart grids but also provides tangible examples of how integrating solar PV systems can significantly improve energy efficiency and sustainability in smart grid-enabled environments. This research is valuable for those seeking real-world examples of renewable energy adoption. Kayamboo et al. (2022) research on IoT-based cyber-physical distribution system planning delves into integrating IoT technologies and cybersecurity measures in smart grids. Their study emphasizes the importance of robust planning and management strategies to secure smart grid infrastructures against cyber threats.

Paidimukkala et al. (2022) focuses on improving power quality in solar-powered bidirectional smart grid systems and integrating electric vehicles. Their work addresses the challenges of maintaining grid stability and power quality with the increasing penetration of renewable energy sources and electric vehicles. It provides crucial insights into managing and optimizing smart grid operations. Espe et al. (2018) systematically examine how prosumers play a critical role in the sustainability and efficiency of smart grids. By evaluating prosumer-based smart grids' evolution and future directions, the authors present several propositions and research directions crucial for understanding the dynamic interactions within smart grid systems. This work is particularly relevant to discussions on the participatory role of prosumers in enhancing smart grid operations and resilience against cyber-attacks. The insights from this study can significantly inform the development of robust, self-healing smart grids that leverage the active participation of prosumers to maintain grid stability and security.

Kumar et al. (2020) discuss the application of Artificial Intelligence (AI), Internet of Things (IoT), and blockchain in distributed energy resources (DER)-based smart grids. Their study highlights how these technologies enhance smart grids' reliability, resilience, and security through automated services and real-time monitoring. This research explores advanced technological integrations that fortify grid operations against cyber threats. Rasheed and Ahmed (2022) investigates the use of deep neural networks for load forecasting in smart grids, addressing the challenges of demand prediction in dynamic environments. Their study emphasizes the importance of accurate forecasting for grid stability and efficiency, which is crucial for managing energy distribution and mitigating cyber-attack impacts. Elomari et al. (2022) focus on optimizing energy systems within smart grids, including solar PV integration. Their research provides insights into the design and implementation of efficient energy management strategies, enhancing the operational stability of smart grids.

El Mrabet et al. (2018) surveys the security challenges in smart grids, reviewing various attack schemes and defence strategies. They argue that most existing research has focused on confidentiality, integrity, and availability but often needs to look more into account accountability. They recommend comprehensive detection and countermeasure techniques, including network security, data security, device security, attack detection and mitigation, and forensic methods. Similarly, Ding et al. (2022) provides an overview of cyber threats impacting smart grid security, examining intrinsic vulnerabilities and external cyber-attacks across all smart grid components. They present a structured smart grid architecture, review global cyber-attack incidents and propose potential cybersecurity solutions such as blockchain and artificial intelligence techniques. In addition, Gunduz and Das (2020) reviews cybersecurity issues in IoT-based smart grid applications, analyzing types of cyber-attacks, network vulnerabilities, attack countermeasures, and security requirements. Their comprehensive survey highlights recent advances and countermeasures in smart grid cybersecurity.

Abraham et al. (2023) surveyed the research landscape between 2009 and 2023 pertaining to smart grid cyber risk assessment and real consequence verification. The study yielded significant findings, including the recognition of 23 business domains within smart grid-enabled environments that are susceptible to cyber risks, alongside six distinct approaches to validate the real consequence verification of cyber attacks on smart grids. A study by Toftegaard et al. (2023) established a list of smart-grid-enabled business cases ranked by perceived consequence level. The entire list consisted of 59 business cases identified and ranked by 22 interviewees. The 10 consequences ranked highest are provided in Table 1. Eight of the ten business cases have consequence scenarios connected to electricity supply. Either large or small outages, loss of power, or grid imbalance. The fifth business case is connected to privacy and the 10th is to national security and financial loss. The study highlights that there is a great variation in the perceptions of the interviewees and therefore a lot of inconsistency between the individual ranking of smart-grid-enabled business cases. As any individual's perceptions are colored by the person's previous experiences, it does not necessarily reflect the real-world situation. Therefore, the authors call for further research, such as consequence simulations to rank suitable business cases based on assessments in near real-world environments.

4 Methodology

The methodology for this study involves the simulation of selected business case scenarios built upon previous studies' findings and insights (Abraham et al., 2023; Toftegaard et al., 2023). The simulation aims to emulate potential cybersecurity threats and their impact on the power grid's components, particularly smart meters, flexibility resources, substation automation circuit breakers, virtual power plants and battery park management systems. These scenarios will be analyzed to understand the severity of the threats and their implications on grid stability, energy distribution, and consumer safety.

Advanced software tools such as MATLAB and Simulink are employed for the simulation. These tools are pivotal for creating accurate and dynamic models of smart grid components and their interactions under cyber-attack scenarios. The power system considered in the simulation setup has two substations (Substation one and Substation 2) with capacities of 10 MVA and 4 MVA, respectively. Substation one operates at 110/6.6 kV, which feeds industrial and domestic loads. Substation 2 operates at 6.6 kV/400 V, feeding only the domestic loads. PV systems are installed at the houses in the domestic load, with an aggregate capacity of 2,800 kW. Water heaters, heat pumps, electric vehicles, and air conditioners for domestic loads with a total load of 160 kW are used as flexibility resources in the domestic load. Battery parks (Lithium-Ion) with a capacity of 10 MW and 24 h of autonomy have also been included on the secondary side of the primary substation. The nominal voltage of the battery park is 12 kV, and the rated ampere-hour capacity is 30 kAh. The battery park can charge up to a State of Charge (SoC) of 90% and discharge up to 24%, providing a depth of discharge (DoD) of 66%.

The findings of the simulations inform recommendations for strengthening the cybersecurity framework of the power grid, enhancing its resilience against potential cyber threats.

4.1 Business cases

To create a test bed setup for simulating the load and energy requirements, a village equivalent to 7,000 individual households and specific prerequisites are considered. Firstly, to ensure that the load is accurately simulated, data on the energy consumption patterns of the residents, as well as the different types of appliances and equipment used in the village, must be gathered. Secondly, it should be ensured that the energy supply is adequate to meet the demand, so we need to assess how much energy is required in order to power a village of this size. This could involve using a hydro generator, but we must determine how much energy is needed to meet the demand. Additionally, distributed energy resources (DERs), such as solar panels or batteries, are included in the simulation to account for any energy supply variability or demand variability. Overall, setting up a test bed for a village of 7,000 people requires careful consideration of the load and energy requirements and the appropriate energy sources and management strategies. Figure 1 shows the block diagram that shows the overview of all the business case scenarios used for simulation. The following sections describe the business cases and their scenarios for our simulation studies.

4.1.1 Business case 1: remote access to smart meter circuit breakers

This scenario uses Advanced Metering Infrastructure (AMI) which enables frequent bidirectional communication for real-time processing of electrical consumption data. Essential for demand-side management and grid optimization, AMI, including smart meters, aids energy suppliers in understanding consumption patterns and customer behavior. Remote access to smart meters circuit breakers (CB) provides consumers with a more efficient way of managing their electricity usage. However, this also creates potential vulnerabilities that can be exploited by hackers. To evaluate the security and reliability of the remote access system, the following scenarios are simulated.

- Turn off Smart Meter power remotely: The first scenario involves switching off the power remotely. In this scenario, the power supply to the smart meter is switched off remotely, and the impact on the overall power grid is evaluated. It is essential to determine if there is any damage to the circuit breakers and other components of the smart meter and how quickly the power can be restored.
- Rhythmic turn on-off Smart Meter CB: The second scenario involves on-off switching of the circuit breakers. Here, the impact of the frequent on-off switching of the circuit breakers on the overall system is evaluated. It is essential to determine if the switching leads to any damage to the circuit breakers or other components of the smart meter and if there is any impact on the stability and reliability of the power grid.
- AMI operator intrusion: In addition to the above scenarios, a third scenario involves the case where the AMI operator is compromised and gains access to all the smart meters in the houses. In this scenario, the operator can shut off power to all the smart meters, leading to a massive blackout. It is essential to determine the response time of the system to such an attack and how quickly power can be restored.

TABLE 1 The 10 smart grid enabled business cases with the highest perceived consequence rank from (Toftegaard et al., 2023).

Nr	Business case	Consequence scenario
1	Digital twins	Adversaries able to access grid-related digital twins may use them to identify vulnerabilities, optimize damage or disturb operations, resulting in large outages. Digital twins may also be used in building energy management systems, where manipulation may result in financial consequences and physical damage
2	Remote access to smart meters circuit breakers	Adversaries may gain remote access to circuit breakers. May lead to small to large outages
3	Flexibility and balance management for the grid	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. May lead to injuries or death, grid imbalance, or small to large outages
5	Centralized storage of personal data	The scenario assumes future storage with very high resolution. Potential consequences of cyberattacks are privacy breaches, various financial consequences, or data being used for purposes we are unaware of today
6	SCADA and sensorics communication integration	Adversaries with access to sensors may inject false data. May lead to disconnections of power and outages due to bad decisions, e.g., if the false data indicates high risk
7	Virtual powerplants	Digital attacks on management systems of virtual powerplants may lead to grid instability and in worst case outages
8	Battery-parks management system	Adversaries with access to battery management systems may manipulate or disconnect the load. Consequences may be grid imbalance and potential fire in batteries. The worst case may be outages, especially if other loads are disconnected simultaneously
9	System integration and IT/OT digitization of OT	Adversaries gaining access to the OT environment may increase or decrease production and manipulate or delete data. The results may be grid disturbances and in the worst case outages
10	Smart meter consumption data	Consumption data of end-users may reveal military movements and preparations and thus be a threat to national security. Consumption data may also be manipulated by adversaries, leading to financial impacts for victims

4.1.2 Business case 2: flexibility and balance management for the grid

The introduction of weather-dependent energy resources makes it harder for grid operators to balance production and consumption. Consequently, a new energy market player role known as aggregators has emerged. An aggregator's role is to gather a pool of adjustable electricity demand and then adjust these flexibility resources based on the demand of grid operators. These flexibility resources may be appliances like water heaters, heaters, heat pumps, electric vehicles, and air conditioners. All these appliances are connected to the aggregator, which can then sell the user's flexibility to the grid operator through Demand Response. However, if the aggregator's systems used to control the loads are attacked, it can have severe consequences. The following scenarios are considered for simulation.

- Switching off the demand remotely during peak consumption hours: In this scenario, the power consumption of the flexibility resources is switched off remotely, and the impact on the overall power grid is evaluated. It is essential to determine if there is any peak in grid voltage that affects power quality and may damage user or grid components or even cause outages.
- Rhythmic on-off switching of all the flexibility resources: Here, the impact of the frequent on-off switching of the flexibility

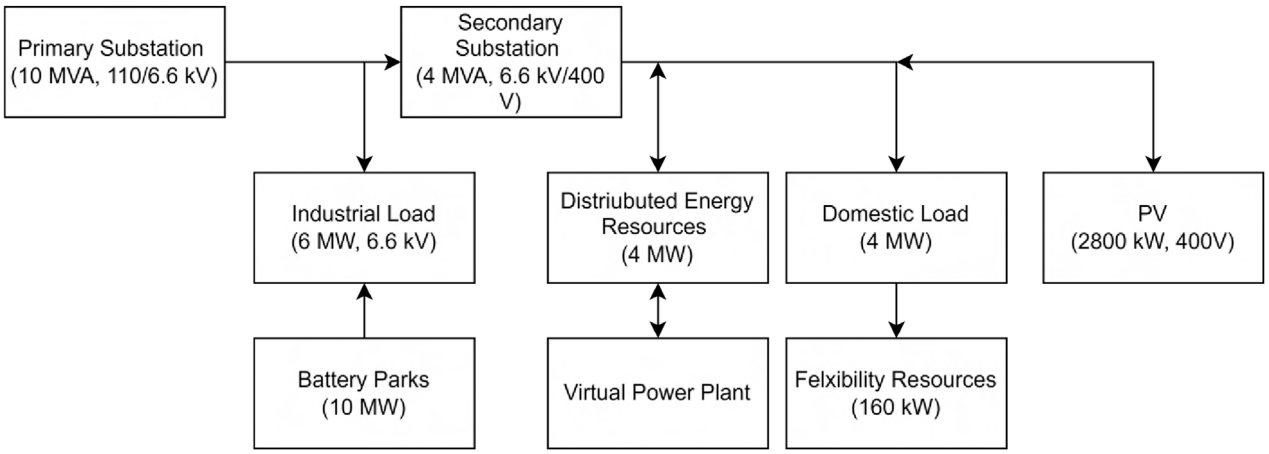

FIGURE 1
Overview of business cases for simulation.

resources on the overall system is evaluated. It is essential to determine if the switching of consumption affects power quality and may damage user or grid components or even cause outages.

- Switching on all appliances at maximum load at peak low hours: In this scenario, the power consumption of the flexibility resources is switched on remotely, and the impact on the overall power grid is evaluated. It is essential to determine if there is any peak drop in grid voltage that affects power quality and may damage user or grid components or even cause outages.

4.1.3 Business case 3: substation automation circuit breakers

A business case based on Substation Automation CB could be a cyber-attack on the substation management software. The attacker gains access to the software and tries to manipulate the CB to disrupt the power flow in the substation. The scenarios for this business case are as follows.

- Turn off Substation CB: The attacker tries to turn off the CB, which would cut off the power supply to the connected consumers. This could result in a power outage in the affected area.
- Rhythmically turn on-off CB: The attacker tries to rhythmically turn on and off the CB, which would cause frequent power outages and fluctuations in the power supply. This could damage the electrical equipment and appliances of the consumers.
- Removing electricity from the grid by opening extra CB (production side): The attacker tries to remove electricity from the grid by opening extra CB on the production side. This could cause a sudden drop in the power supply, leading to power outages and damages to electrical equipment.
- Removing consumption by opening CB (consumption side): The attacker tries to remove the consumption by opening the CBs on the consumption side. This could result in a sudden loss of power for the connected consumers, causing damages to electrical equipment and appliances.

4.1.4 Business case 4: virtual power plants

Virtual Power Plants (VPP) can be implemented in a scenario where industries and houses produce energy, which is all connected to the VPP. The VPP controller manages the distributed energy resources (DER). To evaluate the performance and reliability of the VPP, it is important to simulate the following three scenarios.

- DER shut-off: The first scenario involves an immediate DER shut-off by the hacker, which would test the response of the VPP when a DER needs to be shut off immediately. The VPP controller would need to manage the system to ensure that the energy demand is still met.
- DER on-off switching: The second scenario involves DER on-off switching, which would test if the switching can disturb the voltage. Additionally, the sub-scenario would aim to determine if the DER components would be destroyed if the voltage is manipulated. It would be important to evaluate the effect of DER switching on the overall performance of the VPP and its ability to manage DER effectively
- Disable PV: In the third scenario, an attack on PV is simulated, where the attacker disables the PV during night and then starts the feed from PV into the grid at for example, 13:00 in the afternoon. This can cause an excessive feed into the grid, which can increase the frequency voltage. In this scenario, it would be necessary to find the upper limit of the frequency voltage before the CB opens. By simulating this scenario, it would be possible to evaluate the ability of the VPP controller to manage a situation where an attacker attempts to manipulate the energy supply in the system.

4.1.5 Business case 5: battery parks managements system

Battery parks, also known as energy storage parks or battery energy storage systems (BESS), are facilities that store electrical energy during periods of low demand or when renewable sources generate excess power, and release it back into the grid during peak demand or when renewable generation is low Daggett et al. (2017). They play

a crucial role in grid stability, providing services such as frequency regulation, peak shaving, and backup power, and contribute to the integration of renewable energy sources and the enhancement of grid reliability Zhou et al. (2021). The Battery Parks Management System can be implemented in a scenario where a village with heavy industry needs power, but setting up more distribution grid capacity would be expensive. The system would allow the industry to charge at night and supply power during the day from the battery parks, which would save money for grid operators. During the day, the maximum capacity would be flowing through both the grid cables and the battery parks. The battery parks would be connected to a substation, and the effects of cutting off the battery parks from the substations could be simulated in three scenarios.

- Battery Park shut-off: The first scenario involves a potential attack on the control system of the battery park, which would result in power shut off. If the total voltage reduces it would be a risk to the system. If the voltage does not drastically reduce, there would be no need to worry about the battery parks.
- Battery Park on-off switching: The second scenario involves on/off switching to test if it can disturb the voltage and damage some components. It is also interesting to determine if the on-off switching would destroy the battery pack components.
- Turn on Battery Park when distribution feed is off: The third scenario involves turning on the battery parks when the feed from the distribution is off, to see if it can provide sufficient power to meet the demand of the heavy industry. By simulating these three scenarios, it is possible to evaluate the performance and reliability of the Battery Parks Management System in this business case.

5 Simulation setup and results

This section describes the experimental setup for the simulation for all the business cases and the results obtained. The scenarios involving cyber threats on the power system infrastructure were simulated using MATLAB (The MathWorks Inc, 2022a), specifically focusing on utilizing Simulink (The MathWorks Inc, 2022b) for accurate representation and analysis. This approach allowed for a detailed examination of various cyber-attack scenarios and their potential impacts on critical components of the power grid. By leveraging the comprehensive modelling and simulation capabilities of Simulink, the study provided valuable insights into the complex interplay between cyber threats and the intricate elements of the power grid. The use of Simulink in the analysis ensured a high degree of accuracy and realism in depicting the potential consequences of cyber threats on the power system, enabling a thorough understanding of the vulnerabilities and risks associated with such attacks.

5.1 Business case 1: remote access to smart meter circuit breakers

The power distribution system under consideration in this business case comprises of two substations: Substation one and Substation 2. Substation 1, the primary substation, operates at an input voltage of 110 kV and an output voltage of 6.6 kV. The transformer in Substation 1 has a power capacity of 10 MVA and is equipped with three breakers: S1, S2, and S3. This substation has two feeders, one for industrial purposes and the other for residential use. The maximum load capacity of the industrial feeder is 6 MW, whereas the residential feeder has a total load capacity of 4 MW. Substation 2, on the other hand, is the secondary substation, with a power capacity of 4 MW. It operates at a primary voltage of 6.6 kV and a secondary voltage of 400 V. The simulation model for this scenario in Matlab is depicted in Figure 2, which is the primary simulation model for this study. In addition, this business case involves the integration of photovoltaic (PV) systems into the domestic load, as shown in Figure 3. The three scenarios under consideration in this study utilize the setup mentioned above.

5.1.1 Turn off smart meter power remotely

- Simulation Method: In this scenario, four household loads are deactivated concurrently at 0.1, 0.3, 0.5, and 0.8 s. These houses are equipped with PV systems capable of collectively generating an aggregate load of 2,800 kW.
- Results: The attacker compromises and cut off the power randomly at the smart meters in the houses. When the breaker for smart meters is off, it results in changes in the current supplied to the domestic load as shown in Figure 4A. From 0 to 0.1 s all the loads are on. So the total load current is 5268 A. This is calculated as follows:

$$\frac{\text{Maximum load current (7450)}}{\sqrt{2}}$$

From 0.1 to 0.3 s, the attacker turns off one of the feeder. This results in load current reducing to 3951 A. From 0.3–0.5 s, the next feeder is turned of hence reducing the load current to 2634 A. Subsequently from 0.5–0.8 s, when the next feeder is turned off, the load current is reduced to 1317 A. So, even though there is supply voltage, the attack results in interruptions in the power supply to houses from substation. When the smart meter is accessed by the attacker, the breaker of the smart meter opens the circuit causing the grid supply isolation from the load. At 0.8s, the grid failure happens (as shown in Figure 4B) and the source of power generation to domestic load is only from PV. Since only PV is delivering power, it is observed from Figure 4B that inverter output current is increasing from 0.8–0.9 s. At the same time it is observed that, there is a dip in inverter voltage from 0.8–0.9 s (Figure 4B). This means that the PV alone will not be able to deliver sufficient power to domestic load. For this scenario, the time taken to switch back the breaker on is taken as 100 m (0.8–0.9 s).

5.1.2 Rhythmic turn on-off smart meter CB

- Simulation Method: To simulate rhythmic activation and deactivation of the Circuit Breaker (CB), the primary CB is activated for a duration of 0.125 s and subsequently deactivated for 0.125 s.
- Results: Figure 4C, shows that when each time a turn-off of CB happens, there is an injection of Direct Current (DC) components of currents which is not much noticeable as it

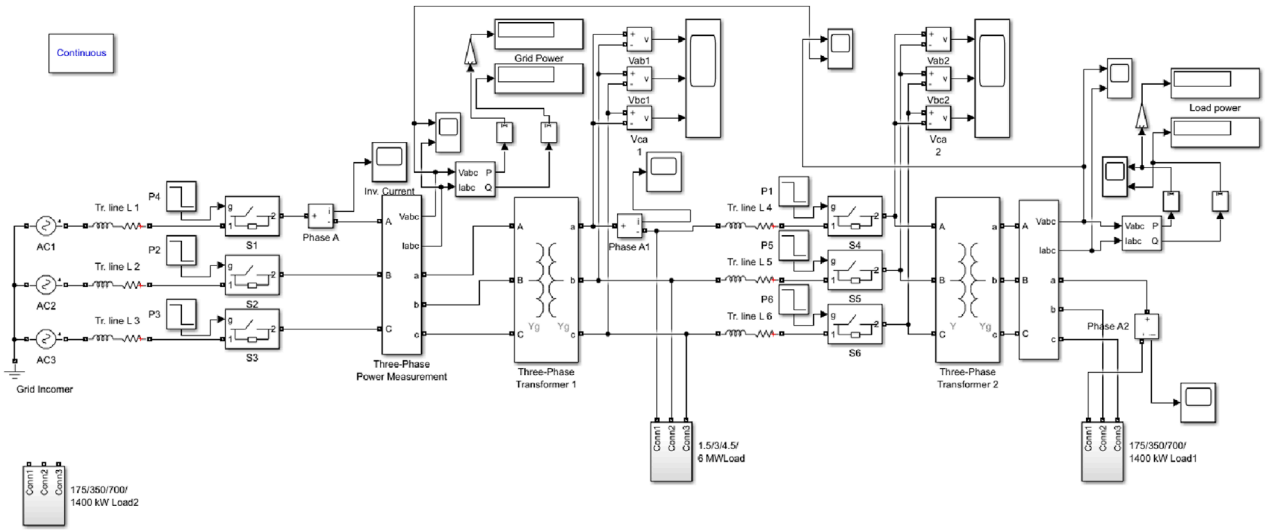

FIGURE 2
Matlab model for Business Case 3.

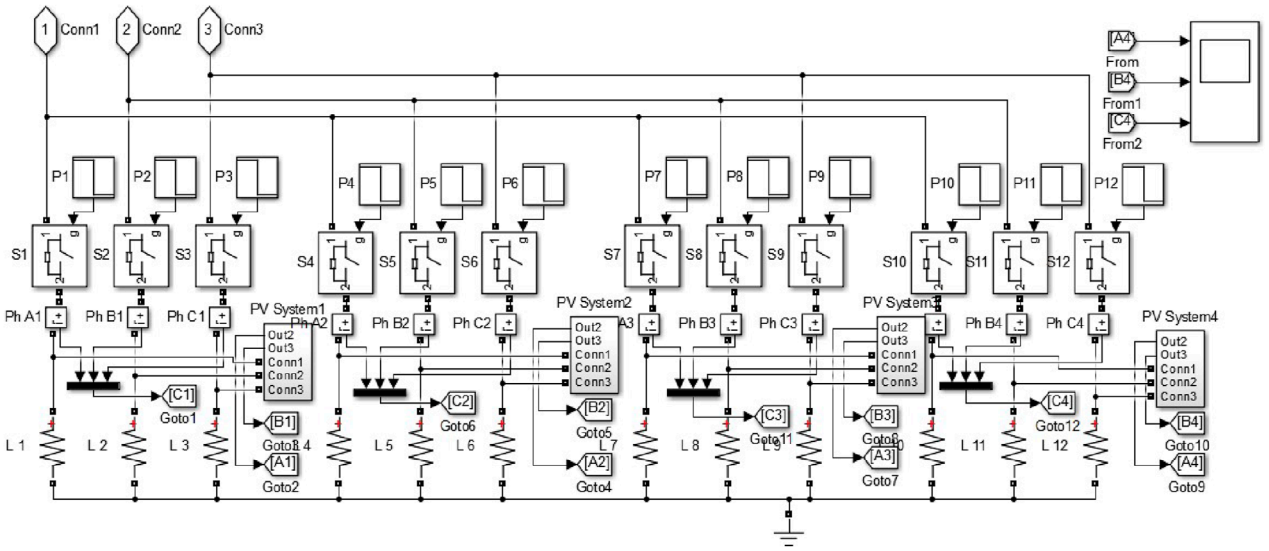

FIGURE 3
Matlab model for Domestic Load setup.

happens for a very short period. Overall, the injection of DC components into an (Alternating Current) AC system can lead to several issues, including distortion of the AC waveform, increased losses in the system, and potential damage to equipment.

5.1.3 AMI operator intrusion

- Simulation Method: The simulation scenario is executed for 0.5s, with the activation of CB shutdown initiated by the attacker at the 0.2s mark.
- Results: AMI operator is compromised, and all the load goes off at same time (at 0.2s as shown by current in the domestic load in Figure 4D). So the domestic load is off from 0.2–0.3 s. Figure 4D also shows the voltage of the domestic load. It can be seen that the system will automatically turn the domestic load on again after 0.1s (this happens at 0.3s), if the previous status of the system is normal (prior to the attack). Voltage will remain the same even though the smart meter is turned off.

5.2 Business case 2: flexibility and balance management for the grid

The experimental setup is similar to Business Case 1. In addition, flexibility resources like water heaters, heat pumps, electric vehicles, and air conditioners for domestic loads have been considered. The flexibility resources have an aggregate load of 160 kW.

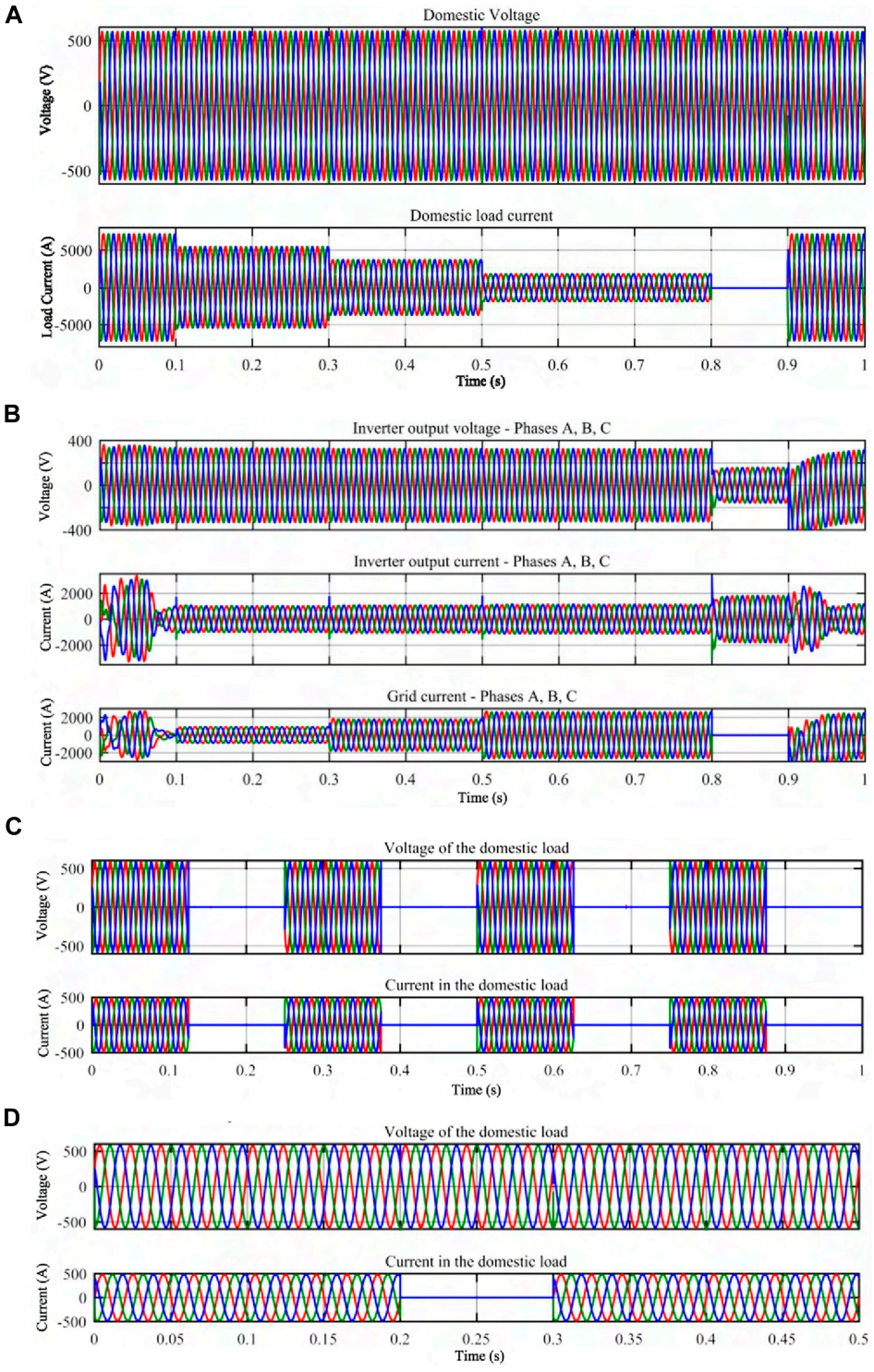

FIGURE 4
Results of Business Case 1 (Remote access to Smart Meter circuit breakers) Simulations. **(A)** Voltage and Current supplied to domestic load. **(B)** Effect of grid failure on PV power generation. **(C)** Voltage and Current when CB turns on and off frequently. **(D)** Voltage and Current in AMI operator intrusion.

5.2.1 Switching off the demand remotely during peak consumption hours

- Simulation Method: This scenario has four loads for houses (including flexibility resources) that are set to be turned off at 0.4 s, 0.6s, 0.8 s and 0.9 s simultaneously. The homes also have PV attached to them, which can generate an aggregate load of 700 kW.
- Results: The attacker compromises and turns off the flexibility resources in the houses. The load varies from 0.4–0.6 s,

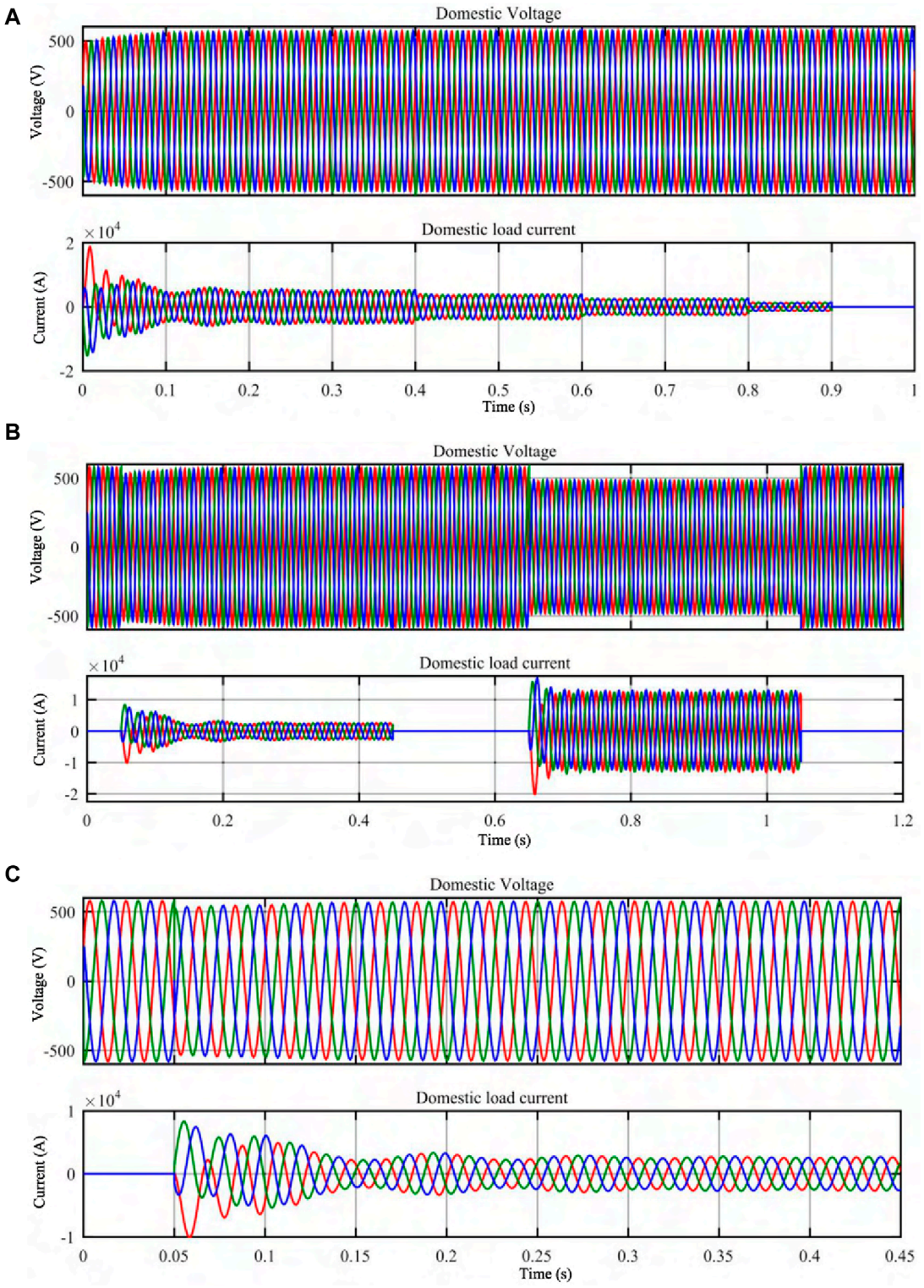

FIGURE 5
Results of Business Case 2 (Flexibility and balance management for the grid) Simulations. **(A)** Effect of attack on flexibility resources. **(B)** Effect of rhythmic attack on flexibility resources. **(C)** Effect of turn-on of flexibility resources at peak low hours.

0.6–0.8 s, 0.8–0.9 s simultaneously. For each variation in the load, it is observed that there is a decrease in domestic load current (Figure 5A). The domestic voltage increases for each variation by 1.25% which is not significant. The current also deviates and then reaches the steady state in accordance with the load.

5.2.2 Rhythmic on-off switching of all the flexibility resources

- Simulation Method: The domestic load is turned on at 0.05s and then off at 0.45s to simulate a rhythmical turn-on and off of the flexibility resources. The load is turned on again at 0.65s and again turned off at 1.05s.
- Results: It is observed that there are only slight variations in voltage and inrush currents (spikes of current for short duration). Figure 5B shows these current and voltage variations. The voltage is reduced to 354 V, which is calculated as follows:

$$\frac{\text{Peak Value (500)}}{\sqrt{2}}$$

This from time period 0.65–1.15s. During same duration load current increases to 9900 A. This current is abnormally high hence the reduction in voltage.

5.2.3 Switching on all appliances at maximum load at peak low hours

- Simulation Method: This scenario is simulated with a simulation time of 0.45s. The attacker triggered the turning on of the flexibility device at 0.05s.
- Results: At the point of switching on of the devices, transients in domestic load current are observed for a short period of time (0.05–0.2s) and then steady state is attained. During the same time period, a small reduction in terminal voltage (17 V) is also observed. Figure 5C shows these observations.

5.3 Business case 3: substation automation circuit breakers

Two substations, denoted as Substation 1 and Substation 2, are considered in this business case. Substation 1 operates at 110 kV (input) and 6.6 kV (output) with a transformer power capacity of 10 MVA. The associated circuit breakers are labeled as S1, S2, and S3. Substation 1 accommodates two feeders: one serving the industrial sector with a maximum load of 6 MW and the other catering to residential areas with a combined load of 3.5 MW. The secondary substation features a power capacity of 4 MW, a primary voltage 6.6 kV, and a secondary voltage of 400 V. The simulation model for this specific scenario is implemented using Matlab, and a visual representation is provided in Figure 2 for reference.

5.3.1 Turn off substation CB

- Simulation Method: In this scenario, the CB for houses are switched off at 0.1 s.
- Results: The attacker compromises and cuts off the power randomly at the CB to substation. It is observed that the power supply to the domestic consumers is turned off as indicated by Figure 7A. This CB cut off is from 0.1 s as expected.

5.3.2 Rhythmically turn on-off CB

- Simulation Method: To simulate rhythmically turning and off the breakers, the main CB is on for 0.1 s and off for 0.1 s.
- Results: Figure 7B shows the currents and voltages when CB is rhythmically turned on and off. The observations shows that each time when the CB is switched off, there is a short spike in voltage at each breaking times (0.15 s, 0.35 s, 0.55 s, 0.75 s and 0.95 s). Voltage spikes can cause arcing between the contacts of the circuit breaker. This arcing can generate high temperatures and pressures, damaging the contacts, insulation, and other breaker components.

5.3.3 Removing electricity from the grid by opening extra CB (production side)

- Simulation Method: An additional generator was incorporated to simulate this scenario, resulting in an augmented power generation source and an extra CB. The schematic representation of this configuration is illustrated in Figure 6. The simulation is conducted for 0.4s in steady state.
- Results: In substations that is fed from one or more incoming generators, if anyone of the incoming generator is turned off, the other generator may not be able to supply the required load demanded by subsequent substations or consumers. This is as shown in Figure 7C from 0.2 s. It is observed that when all the incoming feeders are available (up to 0.2 s), the voltage is nominal at 63.5 kV per phase. Then at 0.2 s, when one of the incoming feeder is turned off, the grid voltage is reduced to 42.5 kV per phase and current is reduced to 21.3 A per phase.

5.3.4 Removing consumption by opening CB (consumption side)

- Simulation Method: Simulation of the total system is done for 0.4 s. The operation is regular for 0.2 s and then switched off for the industrial load. The shorter time duration is taken to view the output clearly.
- Results: The attacker attacks breaker to industrial load which will cause power loss into industrial consumers. Figure 7D shows this power loss at 0.2 s in the grid current to the substation. The current is reduced to 6 A which results in under-utilization of the transmission line to industrial consumers.

5.4 Business case 4: virtual power plants

The experimental setup is similar to Business Case 2, with the inclusion of battery storage units as a component of the DER. The combined output of the grid and DER is 10 MW, which is sufficient to fulfill the domestic load of 4 MW and the industrial load of 6 MW. The capacity of the grid is 6 MW, while the DER has a capacity of 4 MW.

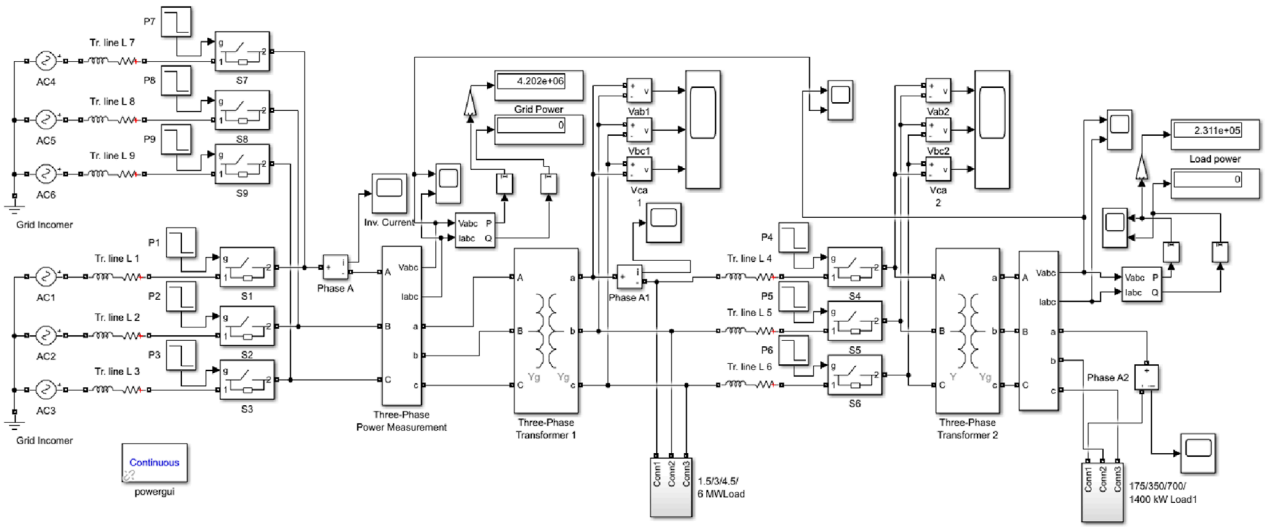

FIGURE 6
Matlab model for Business Case 3 with additional CB.

5.4.1 DER shut-off

- Simulation Method: The total simulation time is for 1s. The attacker shuts off the DER at 0.5s.
- Results: It is observed that the total load is maintained even though the DER is shut off by the attacker. Figure 8A shows the results. At 0.5s, when the DER is turned off, the load current still remains the same. The reduction in DER current is compensated by increase in grid current by equal amount (Figure 8A).

5.4.2 DER on-off switching

- Simulation Method: To simulate rhythmically turn-on and off the DER, the DER is on for 0.5 s, off for 0.25 s and then again on for 0.25 s.
- Results: It is observed that there is a small transient period before the DER current is settled. The first half-cycle of the transient current is 2.5 times the nominal value when the DER is turned on again at 0.75 s. Figure 8B shows the results.

5.4.3 Disable PV

- Simulation Method: The PV panel is off for a duration of 0.5s while other resources (battery, grid and load) are on. Then at 0.5s, the load becomes off-peak and is slightly reduced. The PV system is synchronized to the grid at 0.6s.
- Results: When the system is operating normally till 0.6s, the grid voltage and the voltage of the DER is at its nominal value of 400 V. After 0.6s, the excess generation of the PV system is sent back to the grid as shown in Figure 8C. The power that is sent back to the grid is reflected with an increase in the current magnitude at 0.6s. It was observed that the system voltage has no significant increase. This is because, the grid is strong enough to absorb the injected power or deliver the power demand. Figure 8C shows the observations.

5.5 Business case 5: battery parks managements system

The experimental setup is similar Business Case 3. In addition, battery park have been added to secondary side of primary substation with capacity of 10 MW. This battery park can supply power for approximately 1 day when there is no supply from grid.

5.5.1 Battery park shut-off

- Simulation Method: Attacker shuts off the power to the battery park at 0.25 s. The total simulation time is 0.5 s.
- Results: The attacker compromises and cuts off the power of the Battery Park. Until the battery is on (before 0.25 s), the voltage at the point of common coupling (PCC) is slightly above (6.73 kV) the rated value (6.6 kV). After the attack (at 0.25 s), it is observed that the voltage and current of the total load is reduced. Line voltage is 6.47 kV and load current is 510 A (before shut-off the load current is 530 A). This is as shown in Figure 9A. The power system will still deliver power but at a reduced voltage.

5.5.2 Battery park on-off switching

- Simulation Method: To simulate rhythmically turn-on and off of the battery, the CB before the battery is turned off at 0.2 s, then turned on at 0.4 s, turned off at 0.6 s, turned back on at 0.8 s.
- Results: Figure 9B shows the currents and voltages of the battery park when it rhythmically turned on and off. It can be seen that, there are large transient currents during the initial period

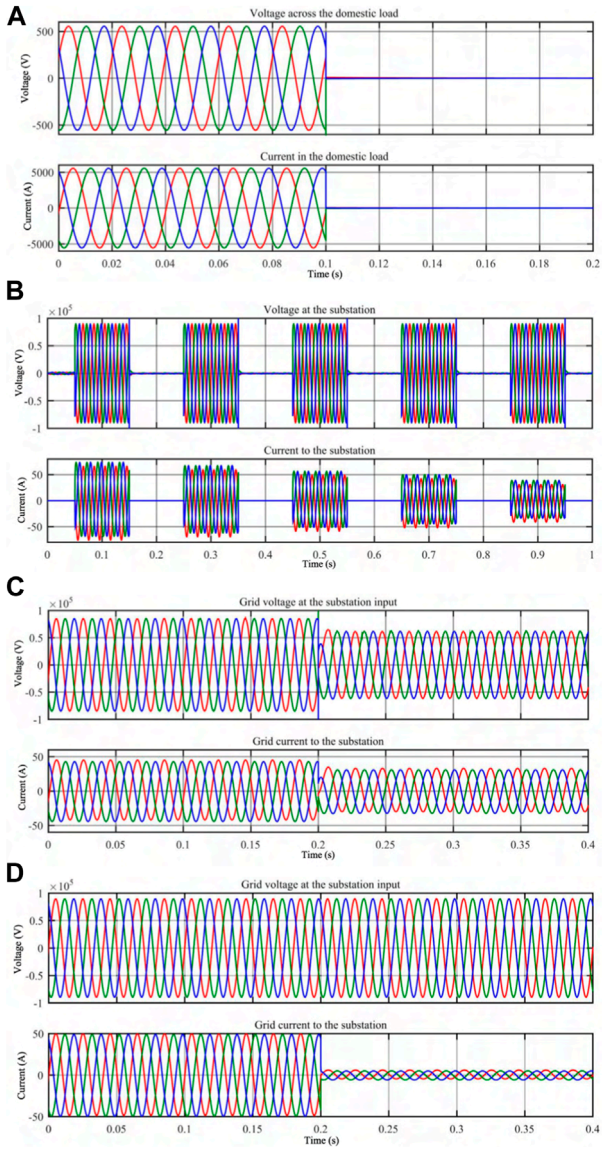

FIGURE 7
Results of business case 3 (substation automation circuit breaker) simulations. **(A)** Voltage and Current when attacker turns off power. **(B)** Voltage and Current when attacker rhythmically. **(C)** Power loss in subsequent substations. **(D)** Power loss for Industrial consumers.

of turn-on time of the circuit breaker (0–0.06 s, 0.4–0.46 s, 0.8–0.86 s). This rhythmic turn on and turn off will lead to injection of DC components of currents and voltages into the load which is also observed as shown in 8b.

5.5.3 Turn on battery park when distribution feed is off

- Simulation Method: The scenario is simulated with simulation time of 1s, with turn off of the grid triggered by the attacker at 0.5s. At this time, the battery park will still be on.
- Results: The battery park is intended to supply to the grid as shown in Load current in Figure 9C. When the grid is switched off, the battery park only delivers power to domestic households and industries as in shown in Inverter and Grid current. It is observed that even if the grid fails, battery parks can deliver the power and maintain current. Figure 9C also shows these observations.

6 Discussions

The power system is an essential infrastructure that underpins modern society, providing electricity for homes, businesses, and critical services. However, this system is increasingly vulnerable to cyber threats, which can disrupt its operations and cause severe economic and operational consequences. Simulations were conducted to illustrate the effects of various cyber attacks on critical components of the power system to understand the impacts of these threats better and devise strategies for mitigating them. Following are some of the direct consequences for each business case and its scenarios as a result of the attacks simulated in Section 5.

6.1 Business case 1: remote access to smart meter circuit breakers

The cyber attack described involves opening the circuit breaker of smart meters, effectively isolating the grid supply from the load as observed in Section 5.1 results. The immediate consequence is power outages for affected households, disrupting daily life and impacting essential services such as lighting, heating, cooling, and electronic devices. These outages can lead to safety hazards and financial losses, as overloading circuits can cause electrical fires, endangering lives and property, and unplanned power outages disrupt businesses, manufacturing processes, and critical infrastructure, contributing to economic losses. The cascading effect of multiple smart meters being compromised can escalate to widespread power disruptions, potentially causing large-scale blackouts. Additionally, the attack can lead to reduced utility revenues, as interruptions caused by attackers can lead to under-reporting of energy usage, resulting in reduced revenues for utility companies and affecting the sustainability and operation of the utility grid. Unauthorized access or manipulation of smart meters by attackers compromises customer privacy, leading to legal and ethical concerns and eroding public trust in the utility provider. Overall, the attack highlights vulnerabilities in the smart grid's network and process aspects, emphasizing the importance of addressing these vulnerabilities to maintain a robust and reliable power distribution system.

The injection of DC components (observed in Section 5.1 results) into the grid disrupts the alternating current (AC) balance, leading to asymmetry in the current waveform and the potential for harmonics, voltage fluctuations, and oscillations. These oscillations can propagate through the network, affecting neighbouring substations and loads, potentially leading to grid instability or blackouts. Grid components designed for AC may experience stress and premature ageing when exposed to DC components, including transformer core saturation and increased losses. The electromagnetic fields generated by DC components

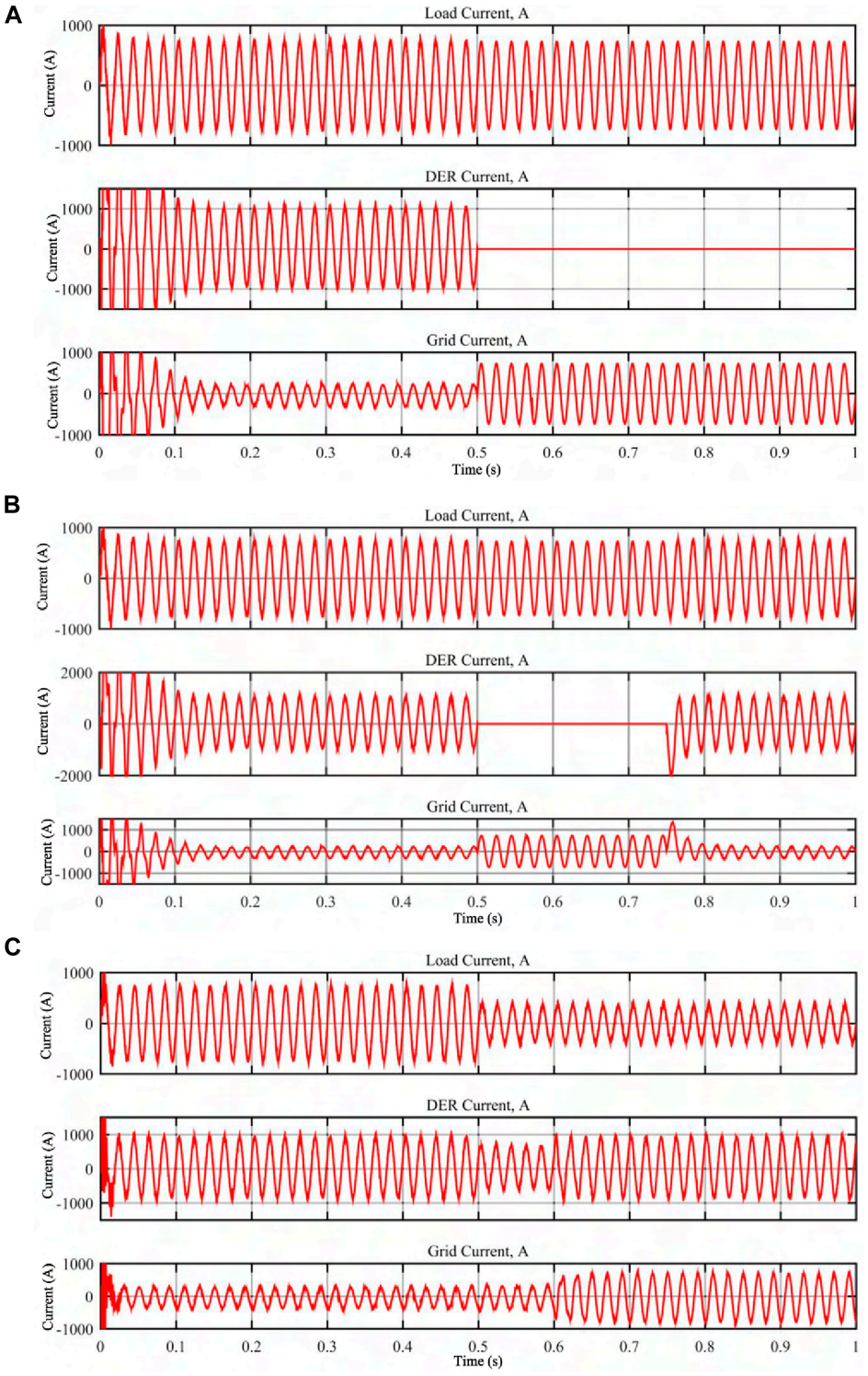

FIGURE 8
Results of business case 4 (virtual power plants) simulations. **(A)** Load, DER and Grid Currents. **(B)** Load, DER and Grid Currents. **(C)** Load, DER and Grid Currents.

can interfere with communication systems, control circuits, and sensitive electronic devices, disrupting data transmission and compromising grid control mechanisms. Protection relays, which rely on AC characteristics for fault detection and coordination, can be confused by DC components, resulting in false tripping or delayed responses during faults, necessitating specialized algorithms and settings to ensure reliable protection.

The compromise of the AMI operator could lead to several direct consequences for the smart grid. Firstly, it could cause immediate load shedding, potentially leading to grid instability

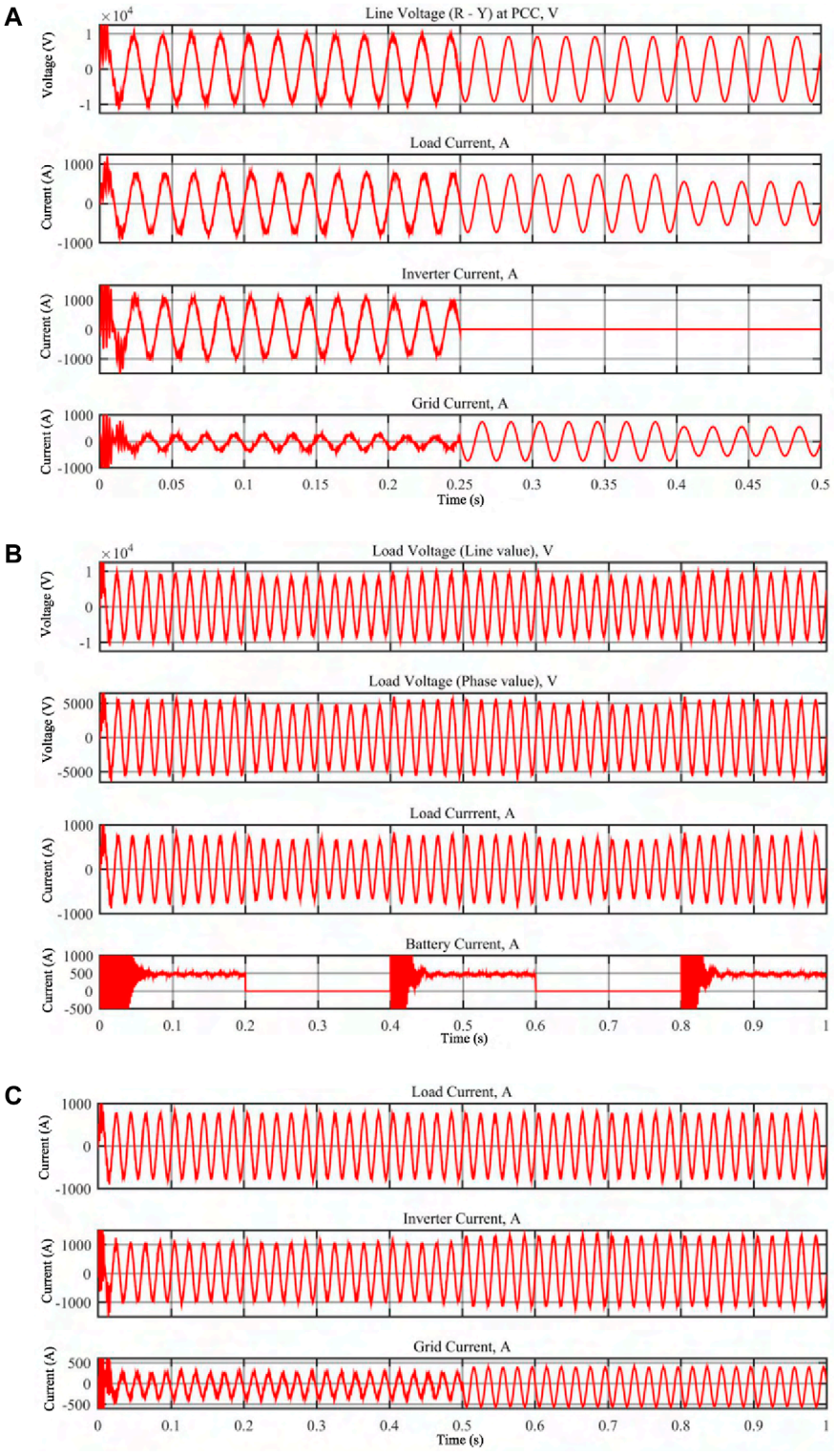

FIGURE 9
Results of business case 5 (battery parks managements system) simulations. **(A)** Voltage and Current when attacker turns off battery. **(B)** Voltage and Current when attacker rhythmically. **(C)** Voltage and Current when attacker rhythmically.

or even a blackout if the grid is unprepared for such a sudden change. Additionally, the rapid restoration of load after a brief interruption could cause further disturbances in the smart grid, potentially leading to oscillations and voltage dips or spikes that can harm electrical equipment. The attack also raises significant security concerns, as it implies a significant security breach that could allow

the attacker to manipulate the load in a way that causes maximum disruption or damage. Furthermore, in the long term, such an attack could undermine confidence in the security and reliability of the smart grid, potentially slowing down the adoption of smart grid technologies and increasing costs due to the need for enhanced security measures.

6.2 Business case 2: flexibility and balance management for the grid

The compromise of flexibility resources in smart grids leads to various direct consequences. Firstly, there is a noticeable increase in voltage across the overall load, though it is not significant as observed in Section 5.2 results. This can cause current deviations, leading to potential disturbances in the grid, especially if the infrastructure is not designed to handle such fluctuations. However, the current eventually reaches a steady state, indicating the presence of some regulatory system within the grid to maintain stability. Despite this, the initial disturbances can damage sensitive electrical equipment that is unsuitable to tolerate such changes. Overall, the security breach from the compromise raises concerns about the vulnerability of other grid components and the potential for attackers to manipulate the system for maximum disruption or damage.

An attacker's rhythmic on-off switching of flexibility resources can have several direct consequences. Firstly, it can lead to slight variations in voltage as observed in Section 5.2 results. Although these variations might be subtle, they can still disturb the power grid, especially if it is not equipped to manage such changes. Additionally, this switching can cause inrush currents, which are brief current spikes. These currents can harm electrical equipment connected to the grid, especially if it is not designed to handle high currents, even if they are transient. Lastly, the rhythmic switching can result in oscillations within the smart grid, further destabilizing it and potentially damaging sensitive grid-connected equipment.

Switching on all appliances at maximum load during peak low hours directly affects the smart grid. It leads to transients (indicated by Section 5.2 results), which are short-lived, high-energy disturbances that can damage electrical equipment not designed to handle them. However, the system eventually reaches a steady state, indicating a regulatory mechanism in place. Despite this, a slight reduction in terminal voltage could affect equipment performance. Additionally, the potential for overloading the grid during peak low hours raises concerns about grid instability and possible blackouts.

6.3 Business case 3: substation automation circuit breakers

Several significant consequences emerge if an attacker compromises and cuts off power at a substation circuit breaker. Firstly, power outages would occur in areas serviced by the substation, varying in severity based on the outage's extent and duration. Secondly, critical infrastructure like hospitals, emergency services, water treatment facilities, and transportation systems dependent on a constant power supply would be severely disrupted, potentially jeopardizing public safety and health. Thirdly, prolonged outages could result in significant economic impacts, including business losses due to interrupted operations, spoilage of perishable goods, equipment damage, and productivity loss. Lastly, in the digital age, power outages could lead to data loss in computer systems, which would be catastrophic for businesses and individuals.

Frequent switching of substation circuit breakers can lead to significant consequences. Firstly, injecting DC components into the power transformer is a considerable concern. Even minor DC bias can lead to half-cycle saturation of the transformer core (Bachinger et al., 2013). This saturation can result in several adverse effects like:

- Increased Noise Levels: Even small direct currents can increase the noise level by more than 10 dB A), and in the case of a transformer with a low general noise level, it can increase by more than 20 dB A) (Ricketts, 2020).
- Reactive Power Consumption: The DC bias can lead to high reactive power consumption, which can reach a critical level for the power grid.
- Overheating: The higher harmonic stray flux caused by strong direct currents can lead to additional losses in metallic parts, causing overheating.
- Corrosive Effects: DC injection can accelerate the corrosion of the network cabling.

Secondly, frequent opening and closing circuit breakers under loaded conditions can lead to excessive wear on the contacts. This is due to the arc created by opening and closing the circuit breaker (Bachinger et al., 2013). The consequences include:

- Reduced Lifespan: The circuit breaker's life can be shortened due to the excessive wear.
- Safety Risks: Operating a circuit breaker during high current conditions can cause the breaker to deteriorate internally. The intense heat of the arc can deteriorate the surrounding materials, and the lubricant applied to the circuit breaker's contact pivot points can dry out over time, eventually becoming gummy and causing the breaker to freeze.
- Fire Risk: If the circuit breaker is frequently reset, the wiring gets hotter and hotter, and the breaker is out of sync with just how hot it is. This can lead to a fire

Lastly, the impact on production and consumption is substantial, with interruptions leading to downtime in production facilities and equipment damage on the consumption side.

Opening extra circuit breakers (CB) on the production side to remove electricity from the grid can lead to various potential consequences. Firstly, it can result in insufficient power supply (observed in Section 5.3 results), as one of the incoming generators in a substation may not be able to meet the demand, potentially causing power outages, voltage fluctuations, and increased operational costs. Secondly, it can lead to grid instability, as the grid needs to maintain a balance between power supply and demand to ensure quality and reliability. Thirdly, it can impact the integration of renewable energy sources, as removing a generator could disrupt the balance between renewable and non-renewable energy, making it more challenging to manage and potentially reducing the effectiveness of renewable energy integration. Lastly, it

can have significant economic impacts, particularly in sectors like manufacturing, where consistent power supply is crucial.

Removing consumption by opening circuit breakers (CB) on the consumption side, particularly in an attack leading to power loss for industrial consumers (observed in Section 5.3 results), can have several potential consequences. Firstly, the immediate disruption of industrial operations is significant, with production lines abruptly halting, machinery breaking down, and the entire supply chain becoming disrupted. This leads to substantial financial losses in the form of lost work in process, additional labour costs, and missed shipment dates. Furthermore, power loss can result in power quality issues, damage equipment, and increase maintenance costs. Over time, the cumulative impact of power loss can damage a company's reputation and increase operational costs.

6.4 Business case 4: virtual power plants

In the event of an attack on a VPP resulting in the shutdown of DER, several immediate implications emerge. Firstly, the ability of the VPP to sustain the total load despite the DER shutdown demonstrates a high level of resilience in the system, potentially due to backup power sources or efficient load management strategies. However, this scenario also exposes security vulnerabilities, indicating weaknesses in the cybersecurity defences of VPP. While the ability of VPP to maintain the load during the shutdown is commendable, questions arise regarding its long-term reliability, primarily if it relies heavily on DER. Economic impacts could also result, as purchasing additional power from the grid or using backup sources may incur higher operational costs. Furthermore, there may be regulatory implications if it is discovered that the VPP operator did not sufficiently protect against cyber attacks, potentially leading to fines or new cybersecurity standards for VPP.

Rhythmic activation and deactivation of Distributed Energy Resources (DER) in a Virtual Power Plant (VPP) can have several direct consequences. Firstly, transients caused by this rhythmic switching can result in power quality issues such as voltage sags or swells, harmonics, and flicker. These disturbances can affect the performance of electrical equipment connected to the VPP and may even cause equipment damage in severe cases. Secondly, the high transient current observed, 2.5 times the nominal value (as indicated in Section 5.4 results), raises stability concerns. These high currents can stress the electrical system and potentially trigger protective devices, leading to power outages. Thirdly, managing these transients may pose operational challenges for the VPP, necessitating advanced control strategies or using energy storage systems to smooth out the transients. Finally, these transients can result in efficiency losses, as the energy used during the transient period is not effectively utilized for power generation, leading to increased operational costs for the VPP.

In a VPP where PV system is disabled, several direct consequences can arise. Firstly, the system's voltage remains stable, suggesting a robust and resilient grid capable of absorbing excess power. However, increased current magnitudes may result in power quality issues, impacting devices connected to the grid. Economically, if the PV system consistently supplies excess power, there may be opportunities to sell this surplus to the grid operator, generating additional revenue. Conversely, inefficient operations may result in constant over-generation, necessitating adjustments to generation schedules or load forecasts. Regulatory compliance is also a concern, with potential penalties for exceeding power injection limits set by local regulations. Turning off a PV system in a VPP has multifaceted impacts on grid stability, power quality, economic operations, and regulatory compliance.

6.5 Business case 5: battery parks managements system

The scenario of a compromised battery park resulting in reduced voltage and current of the total load has several direct consequences. Firstly, the reduction in voltage at PCC could lead to a decrease in power quality, as most electrical devices operate optimally at a specific voltage. This reduction can also significantly increase power loss in the system. Additionally, some devices may malfunction or become damaged due to the reduced voltage, leading to increased maintenance costs and potential system downtime. A sudden change in voltage could also cause instability in the power grid, potentially resulting in power outages. These consequences could lead to increased operational costs for the power company, ultimately impacting consumers through higher electricity bills.

Several direct consequences arise when an attacker rhythmically turns a battery park on and off, injecting DC components of currents and voltages into the load. Firstly, large transient currents (observed in Section 5.5 results) can cause thermal stress on electrical components, leading to premature ageing and failure. Secondly, injecting DC components into an AC system can cause transformer saturation, increased losses, and overheating, distorting power system measurements and protections. Thirdly, the rhythmic switching can introduce harmonic distortion, which can increase losses and heating in the power system and cause maloperation of sensitive electronic equipment. Fourthly, these factors can lead to a significant degradation in power quality, affecting the performance of electrical devices and potentially causing their failure. Lastly, the increased losses and potential for equipment failure can result in increased operational costs for the power company.

When an attacker turns on a battery park while the distribution feed is off, it has several direct consequences. Firstly, the battery park continues to deliver power to domestic households and industries, ensuring uninterrupted operations even when the grid is off. This also reduces the dependence of these entities on the grid, which can be beneficial in areas with an unreliable grid. However, if the battery park is designed to handle only some of the load, it could become overloaded, potentially leading to overheating and failure. Moreover, the increased demand on the battery park could deplete the batteries faster, resulting in higher replacement costs. Finally, when the grid comes back online, there could be a sudden surge in power as the load shifts back from the battery park to the grid, potentially causing grid instability.

6.6 Perceived and simulated consequences comparison

The previous discussions show that the simulated consequences closely align with the perceived consequences, as illustrated in

TABLE 2 Business cases with the highest simulated consequence rank.

Ranking	Business case
1	Substation Automation Circuit Breakers
2	Remote Access to Smart Meter Circuit Breakers
3	Virtual Power Plants
4	Battery Parks Management System
5	Flexibility and balance management for the grid

Table 1. Another notable finding is the ranking of simulated consequences for each business case, as shown in Table 2. This ranking is based on the consequences as observed for each Business cases in the simulation.

An intriguing observation is the disparity in rankings between perceived and simulated consequences for specific business cases. Specifically, the Substation Automation Circuit Breakers case ranks higher in simulation than the perceived consequence. In contrast, the Flexibility and Balance Management for the Grid case ranks lower in simulation than the perceived consequence ranking. This is due to the consequences of the simulated business cases having higher impacts which is summarized as follows:

1. Substation Automation Circuit Breakers:

    - Power outages
    - Severely disrupted critical infrastructures causing harm to public safety and health
    - Significant economic impacts
    - Data loss causing disruptions for businesses and individuals
    - Transformer damage and production interruption
    - Corrosion of network cabling
    - Overheating
    - Increased noise levels in transformer
    - CB heating and damage
    - Reduced life span of CB
    - Grid instability
    - Reduction in effectiveness of renewable energy integration
    - Economic impacts
    - Disruption of industrial operations
    - Increased operational costs

2. Remote Access to Smart Meter Circuit Breakers:

    - Power outages for affected households impacting daily life
    - Safety hazards and financial losses
    - Endanger lives and property
    - Disrupt businesses and manufacturing processes
    - Potential equipment damage due to overloading
    - Reduced utility revenues
    - Violation of customer privacy
    - Affect neighbouring substations leading to grid instability.
    - Interfere with communication systems, control circuits, and sensitive electronic devices
    - Disrupt data transmission and compromising grid control mechanisms

3. Virtual Power Plants:

    - Grid instability and efficiency losses from DER shutdowns
    - Increased operational costs
    - Regulatory implications from cybersecurity breaches
    - Decreased power quality
    - Power outages
    - Over power production

4. Battery Parks Management System:

    - Reduced voltage and current
    - Power loss
    - Power outages
    - Potential equipment damage
    - Increased operational costs
    - Maloperation of sensitive electronic equipment
    - Decreased power quality
    - Overheating of battery parks
    - Grid instability

5. Flexibility and balance management for the grid:

    - Voltage fluctuations and potential equipment damage
    - Grid instability due to rhythmic switching
    - Economic losses from peak low-hour appliance usage
    - Reduced dependence on the grid

This underscores the significance of verifying perceived consequences with actual simulated results.

6.7 Implementing cybersecurity frameworks to enhance smart grid security

Adopting structured cybersecurity frameworks plays a critical role in pursuing a fortified smart grid. These frameworks provide the scaffolding for developing, implementing, and managing cybersecurity practices tailored to the unique needs of smart grids. Among the most pertinent frameworks are the NIST Cybersecurity Framework, ISO/IEC 27001, and IEC 62443, each offering distinct approaches and benefits.

- NIST Cybersecurity Framework: The NIST Cybersecurity Framework offers a flexible and cost-effective approach to enhancing critical infrastructure cybersecurity (Cybersecurity, 2018). Its applicability to smart grids lies in its comprehensive taxonomy of cybersecurity outcomes and the guidance it provides for managing cyber risks. Organizations can tailor the NIST framework to support the specific operational needs of smart grid environments, promoting resilience through its core functions: Identify, Protect, Detect, Respond, and Recover.

- ISO/IEC 27001: ISO/IEC 27001 sets forth requirements for establishing, implementing, maintaining, and continually improving an information security management system (ISMS) (Culot et al., 2021). This standard is particularly relevant for smart grids, where security management extends beyond physical devices to include information processes, making it integral to protecting against data breaches and ensuring data integrity.
- IEC 62443: Tailored for the security of industrial communication networks and system security, IEC 62443 addresses security for industrial control systems, a fundamental component of smart grids (International Electrotechnical Commission, 2010). The framework focuses on risk assessment and mitigation, providing guidelines covering security levels and system requirements crucial for maintaining operational continuity in smart grids.

6.8 Relevance and impact of the research on industry and society

The research addresses a critical and timely issue in smart grid technologies: cybersecurity vulnerabilities and their potential impacts on modern power systems. This study is particularly significant given the increasing integration of advanced communication networks and renewable energy sources into power grids, which also introduce new cybersecurity challenges while enhancing efficiency and sustainability.

- Industry Impact: In the energy industry, this research provides valuable insights into how cyber attacks can disrupt critical components of the power grid, such as smart meter circuit breakers, substation automation systems, and virtual power plants. By simulating various cyber-attack scenarios, the study highlights potential disruptions that can affect load interruptions and core infrastructure, leading to severe operational and economic consequences. For instance, attacks on smart meter circuit breakers can cause interruptions and damage to substations, requiring quick responses from AMI operators. This is crucial for industry stakeholders who must understand the risks and develop robust defence mechanisms to protect infrastructure and maintain grid stability.
- Community Impact: For the wider community, this research underscores the critical role of robust cybersecurity measures in ensuring the dependability and resilience of power supply systems. The findings underscore the need for agile responses to unforeseen cyber threats, which can have far-reaching effects on the entire grid and disrupt daily life. By pinpointing vulnerabilities in systems like virtual power plants and battery park management systems, the study advocates for the implementation of enhanced security protocols to shield these components from malicious attacks. This is of utmost importance in ensuring that households and businesses can count on an uninterrupted and secure power supply, thereby safeguarding public safety and economic stability.

7 Validity assessment

This section shows the validity assessment of the study Runeson and Höst (2009).

7.1 Construct validity

The simulations conducted in this study exhibit strong construct validity as they align with the primary objective of comprehensively assessing cyber attacks' impacts on the critical components of Smart Grid. The chosen scenarios, including smart meter circuit breaker attacks, flexibility resource failures, substation automation circuit breaker vulnerabilities, virtual power plant susceptibilities, and battery park management system risks, effectively capture the diverse range of cyber threats to the Smart Grid.

7.2 Content validity

The content validity of the simulations is robust, ensuring a thorough representation of the potential consequences of cyber attacks on the power system. The study provides a comprehensive and representative exploration of the subject matter by addressing various attack scenarios and their implications on both core and emerging grid elements.

7.3 Face validity

The face validity of the study is apparent, as the content of the simulations aligns intuitively with the aim of understanding and mitigating the impacts of cyber threats on the Smart Grid. The chosen scenarios and outcomes are suitable and relevant to the broader objectives of fortifying grid resilience against evolving cyber threats.

7.4 Criterion validity

The simulations demonstrate strong criterion validity by effectively measuring the outcomes they are designed to assess. For instance, in Business Case 1, the impact of smart meter circuit breaker attacks accurately measures interruptions and potential damage to substation equipment. Similarly, other business cases, such as flexibility resource failures, substation automation circuit breaker vulnerabilities, and virtual power plant susceptibilities, precisely measure their respective concrete outcomes, contributing to a robust evaluation of the power system's vulnerability to cyber threats.

In conclusion, the validity assessment indicates that the simulations conducted in this study are methodologically sound, aligning closely with the intended objectives of comprehensively evaluating the impacts of cyber threats on the power system. Incorporating diverse scenarios enhances the study's validity by providing a refined understanding of the intricate interplay between cyber threats and the various components of the Smart Grid.

8 Conclusion

The simulation of business case scenarios underscores the complex interactions between cyber threats and the sophisticated components in the smart grid. Our findings reveal the potential cascading effects of cyber attacks on smart meter circuit breakers and substation automation systems, not just theoretical possibilities but as real-world threats that can disrupt the grid's core infrastructure. These vulnerabilities extend beyond simple interruptions, affecting both domestic and industrial loads and posing significant risks to grid stability.

Moreover, our simulations show how the remote manipulation of flexible resources and the inherent vulnerabilities in virtual power plants and battery park management systems can lead to unexpected and severe consequences. These scenarios underscore the urgent need for robust cybersecurity measures to ensure the reliability of these emerging grid elements and to prevent severe economic and operational repercussions.

Comprehensive cybersecurity frameworks, such as NIST, ISO/IEC 27001, and IEC 62443, are not just tools but crucial to safeguarding grid stability. These frameworks not only help mitigate risks but also ensure proactive management of the dynamic landscape of cyber threats. The simulations also stress the importance of corroborating the perceived consequences of cyber attacks with those observed in simulated environments, providing valuable insights that support the ongoing efforts to fortify the resilience of modern power grids against evolving threats.

In conclusion, the simulations conducted in this study expose the escalating vulnerability of the Smart Grid to cyber threats, which poses significant risks to its stability and functionality. Exploring diverse attack scenarios on critical components like smart meter circuit breakers, flexibility resources, substation automation circuit breakers, virtual power plants, and battery park management systems discovers the landscape of potential disruptions. These findings highlight the imperative for robust cybersecurity frameworks and a swift, adaptive response to emerging threats. As the Smart Grid continues to evolve, our study emphasizes the necessity for proactive efforts in enhancing grid resilience, ensuring the reliable delivery of electricity to homes, businesses, and critical services. Future work will explore these business case scenarios to evaluate and mitigate the identified cybersecurity risks.

Data availability statement

The raw data supporting the conclusion of this article will be made available by the authors, without undue reservation.

Author contributions

DA: Conceptualization, Data curation, Formal Analysis, Investigation, Methodology, Project administration, Resources, Software, Validation, Visualization, Writing–original draft, Writing–review and editing. OT: Conceptualization, Investigation, Methodology, Writing–review and editing. BB: Methodology, Software, Validation, Visualization, Writing–review and editing. AG: Supervision, Validation, Writing–review and editing, SY: Supervision, Writing–review and editing.

Funding

The author(s) declare that no financial support was received for the research, authorship, and/or publication of this article.

Conflict of interest

The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Publisher's note

All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers. Any product that may be evaluated in this article, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.

References

Abraham, D., Toftegaard, Gebremedhin, A., and Yayilgan, S. (2023). "Consequence verification during risk assessments of smart grids," in *IFIP advances in information and communication technology in press*.

Alert, D. (2016). "Cyber-attack against Ukrainian critical infrastructure," in *Tech. rep. ics alert (ir-alert-h-16-056-01), Cybersecurity Infrastruct* (Washington, DC, USA: Secur. Agency).

Amani, A. M., and Jalili, M. (2021). Power grids as complex networks: resilience and reliability analysis. *IEEE Access* 9, 119010–119031. doi:10.1109/access.2021.3107492

Amin, B. R., Taghizadeh, S., Rahman, M. S., Hossain, M. J., Varadharajan, V., and Chen, Z. (2020). Cyber attacks in smart grid–dynamic impacts, analyses and recommendations. *IET Cyber-Physical Syst. Theory and Appl.* 5, 321–329. doi:10.1049/iet-cps.2019.0103

Bachinger, F., Hackl, A., Hamberger, P., Leikermoser, A., Leber, G., Passath, H., et al. (2013). Direct current in transformers: effects and compensation. *e i Elektrotechnik und Inf.*, 1–5. doi:10.1007/s00502-012-0114-0

Bronk, C., and Tikk-Ringas, E. (2013). The cyber attack on saudi aramco. *Survival* 55, 81–96. doi:10.1080/00396338.2013.784468

Case, D. U. (2016). Analysis of the cyber attack on the Ukrainian power grid. *Electr. Inf. Shar. Analysis Cent. (E-ISAC)* 388, 3.

Chen, Y., Hong, J., and Liu, C. (2016). Modeling of intrusion and defense for assessment of cyber security at power substations. *IEEE Trans. Smart Grid* 9, 2541–2552. doi:10.1109/tsg.2016.2614603

Culot, G., Nassimbeni, G., Podrecca, M., and Sartor, M. (2021). The iso/iec 27001 information security management standard: literature review and theory-based research agenda. *TQM J.* 33, 76–105. doi:10.1108/tqm-09-2020-0202

Cybersecurity, C. I. (2018). *Framework for improving critical infrastructure cybersecurity*. Available at: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP4162018.

Daggett, A., Qadrdan, M., and Jenkins, N. (2017). "Feasibility of a battery storage system for a renewable energy park operating with price arbitrage," in *2017 IEEE PES*

innovative smart grid technologies conference europe (Torino, Italy: ISGT-Europe), 1–6. doi:10.1109/ISGTEurope.2017.8260249

Ding, J., Qammar, A., Zhang, Z., Karim, A., and Ning, H. (2022). Cyber threats to smart grids: review, taxonomy, potential solutions, and future directions. *Energies* 15, 6799. doi:10.3390/en15186799

El Mrabet, Z., Kaabouch, N., El Ghazi, H., and El Ghazi, H. (2018). Cyber-security in smart grid: survey and challenges. *Comput. Electr. Eng.* 67, 469–482. doi:10.1016/j.compeleceng.2018.01.015

Elomari, Y., Norouzi, M., Marín-Genescà, M., Fernández, A., and Boer, D. (2022). Integration of solar photovoltaic systems into power networks: a scientific evolution analysis. *Sustainability* 14, 9249. doi:10.3390/su14159249

Espe, E., Potdar, V., and Chang, E. (2018). Prosumer communities and relationships in smart grids: a literature review, evolution and future directions. *Energies* 11, 2528. doi:10.3390/en11102528

Eto, J. H., Nelson-Hoffman, J., Torres, C., Hirth, S., Yinger, B., Kueck, J., et al. (2007). *Demand response spinning reserve demonstration*.

Fakhar, A., Haidar, A. M., Abdullah, M., and Das, N. (2023). Smart grid mechanism for green energy management: a comprehensive review. *Int. J. Green Energy* 20, 284–308. doi:10.1080/15435075.2022.2038610

Gunduz, M. Z., and Das, R. (2020). Cyber-security on smart grid: threats and potential solutions. *Comput. Netw.* 169, 107094. doi:10.1016/j.comnet.2019.107094

International Electrotechnical Commission (2010). *IEC 62443: Industrial Communication Networks—Network and System Security*. Geneva, Switzerland: IEC Central Office.

Jiang, Y., Chen, S., Liu, C.-C., Sun, W., Luo, X., Liu, S., et al. (2017). Blackstart capability planning for power system restoration. *Int. J. Electr. Power and Energy Syst.* 86, 127–137. doi:10.1016/j.ijepes.2016.10.008

Kayamboo, S., Ray, B., Das, N., and Tom, M. (2022). "Iot-based cyber-physical distribution system planning," in *2022 IEEE international IOT, electronics and mechatronics conference (IEMTRONICS)* (IEEE), 1–6.

Kirby, B. J. (2003). *Spinning reserves from responsive loads*.

Kirmani, S., Mazid, A., Khan, I. A., and Abid, M. (2023). A survey on iot-enabled smart grids: technologies, architectures, applications, and challenges. *Sustainability* 15, 717. doi:10.3390/su15010717

Kumar, N. M., Chand, A. A., Malvoni, M., Prasad, K. A., Mamun, K. A., Islam, F., et al. (2020). Distributed energy resources and the application of ai, iot, and blockchain in smart grids. *Energies* 13, 5739. doi:10.3390/en13215739

Kumar, S., Abu-Siada, A., Das, N., and Islam, S. (2022). "Comparison between wired versus wireless mode of digital protection scheme leveraging on prp topology," in *2022 IEEE sustainable power and energy conference (iSPEC)* (IEEE), 1–5.

Langner, R. (2011). Stuxnet: dissecting a cyberwarfare weapon. *ieee Secur. Priv.* 9 (3), 49–51. doi:10.1109/msp.2011.67

Mudgal, S., Pranjale, S., Balaji, T., Ahmed, S., Singh, N., Gupta, P., et al. (2022). Impact of cyber-attacks on economy of smart grid and their prevention. *U. Porto J. Eng.* 8, 51–64. doi:10.24840/2183-6493_008.002_0005

Nur-E-Alam, M., Basher, M. K., Iftekharuzzaman, Mostofa, K. Z., Islam, M. A., Haque, A. H. M. A., et al. (2022). Rooftop PV or hybrid systems and retrofitted low-E coated windows for energywise and self-sustainable school buildings in Bangladesh. *Solar* 2 (4), 540–558. doi:10.3390/solar2040032

O'Brien, J. G., Cassiadoro, M., Becejac, T., Sheble, G. B., Follum, J. D., Agrawal, U., et al. (2022). *Electric grid blackstart: trends, challenges, and opportunities*.

Olowu, T. O., Dharmasena, S., Hernandez, A., and Sarwat, A. (2021). "Impact analysis of cyber attacks on smart grid: a review and case study," in *New research directions in solar energy technologies*, 31–51.

Paidimukkala, N., Das, N., and Islam, S. (2022). "Power quality improvement of a solar powered bidirectional smart grid and electric vehicle integration system," in *2022 IEEE sustainable power and energy conference (iSPEC)* (IEEE), 1–6.

Rasheed, M., and Ahmed, S. F. (2022). Review of short-term load forecasting for smart grids using deep neural networks and metaheuristic methods. *Math. Problems Eng.* 2022, 1–14. doi:10.1155/2022/4049685

Rebours, Y., and Kirschen, D. (2005). *What is spinning reserve*. Manchester, United Kingdom: The University of Manchester 174.

Rice, E. B., and AlMajali, A. (2014). Mitigating the risk of cyber attack on smart grid systems. *Procedia Comput. Sci.* 28, 575–582. doi:10.1016/j.procs.2014.03.070

Ricketts, M. (2020). The case of the overloaded electrical circuit. *Prof. Saf.* 65, 52–63.

Rodríguez-Molina, J., Martínez-Núñez, M., Martínez, J.-F., and Pérez-Aguiar, W. (2014). Business models in the smart grid: challenges, opportunities and proposals for prosumer profitability. *Energies* 7, 6142–6171. doi:10.3390/en7096142

Runeson, P., and Höst, M. (2009). Guidelines for conducting and reporting case study research in software engineering. *Empir. Softw. Eng.* 14, 131–164. doi:10.1007/s10664-008-9102-8

Sgouras, K., Birda, A., and Labridis, D. (2014). "Cyber attack impact on critical smart grid infrastructures," in *Isgt 2014*, 1–5.

Sun, C., Sebastian Cardenas, D., Hahn, A., and Liu, C. (2021). Intrusion detection for cybersecurity of smart meters. *IEEE Trans. Smart Grid* 12, 612–622. doi:10.1109/tsg.2020.3010230

The MathWorks Inc (2022a). *MATLAB version: 9.13.0 (R2022b)*. Natick, Massachusetts, United States: The MathWorks Inc.

The MathWorks Inc (2022b). *Simulink version: 9.13.0 (R2022b)*. Natick, Massachusetts, United States: The MathWorks Inc.

Toftegaard, Abraham, D., Shenoi, S., and Bernhard, H. (2023). "Smart-grid-enabled business cases and the consequences of cyberattacks," in *IFIP advances in information and communication technology in press*.

Tweneboah-Koduah, S., Tsetse, A., Azasoo, J., and Endicott-Popovsky, B. (2018). "Evaluation of cybersecurity threats on smart metering system," in *Information technology-new generations: 14th international conference on information technology*, 199–207.

Vazquez, M. A. O. (2006). *Optimizing the spinning reserve requirements*. United Kingdom: The University of Manchester.

Wang, W., and Lu, Z. (2013). Cyber security in the smart grid: survey and challenges. *Comput. Netw.* 57, 1344–1371. doi:10.1016/j.comnet.2012.12.017

Waseem, M., and Manshadi, S. D. (2020). Electricity grid resilience amid various natural disasters: challenges and solutions. *Electr. J.* 33, 106864. doi:10.1016/j.tej.2020.106864

Zheng, T., Liu, M., Puthal, D., Yi, P., Wu, Y., and He, X. (2022). *Smart grid: cyber attacks, critical defense approaches, and digital twin*. arXiv preprint arXiv:2205.11783.

Zhou, K., Zhang, Z., and Lu, X. (2021). Optimal operation of battery energy storage system in industrial park. *2021 IEEE 5th Conf. Energy Internet Energy Syst. Integration* EI2, 1894–1898. doi:10.1109/EI252483.2021.9713459