IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

IEEE POWER & ENERGY SOCIETY SECTION

Received 7 July 2023, accepted 13 September 2023, date of publication 20 September 2023, date of current version 26 September 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3317695

SURVEY

Cyber Attacks on Power Grids: Causes and Propagation of Cascading Failures

VETRIVEL SUBRAMANIAM RAJKUMAR, (Student Member, IEEE), ALEXANDRU ŞTEFANOV, (Member, IEEE), ALFAN PRESEKAL, (Member, IEEE), PETER PALENSKY, (Senior Member, IEEE), AND JOSÉ LUIS RUEDA TORRES, (Senior Member, IEEE)

Department of Electrical Sustainable Energy, Delft University of Technology, 2628 CD Delft, The Netherlands

Corresponding author: Vetrivel Subramaniam Rajkumar (V.SubramaniamRajkumar@tudelft.nl)

This work was supported in part by the EU H2020 Project, ERIGrid 2.0, under Agreement 870620; and in part by the DeSIRE Program of 4TU Centre for Resilience Engineering.

ABSTRACT Cascading effects in the power grid involve an uncontrolled, successive failure of elements. The root cause of such failures is the combined occurrence of multiple, statistically rare events that may result in a blackout. With increasing digitalisation, power systems are vulnerable to emergent cyber threats. Furthermore, such threats are not statistically limited and can simultaneously occur at multiple locations. In the absence of real-world attack information, however, it is imperative to investigate if and how cyber attacks can cause power system cascading failures. Hence, in this work we present a fundamental analysis of the connection between the cascading failure mechanism and cyber security. We hypothesise and demonstrate how cyber attacks on power grids may cause cascading failures and a blackout. To do so, we perform a systematic survey of major historic blackouts caused by physical disturbances, and examine the cascading failure mechanism. Subsequently, we identify critical cyber-physical factors that can activate and influence it. We then infer and discuss how cyber attack vectors can enable these factors to cause and accelerate cascading failures. A synthetic case-study and software-based simulation results prove our hypothesis. This analysis enables future research into cyber resilience of power grids.

INDEX TERMS Blackout, cascading failures, cyber attacks, cyber resilience, cyber security.

I. INTRODUCTION

The electrical power grid is one of the most complex man-made systems, providing electricity worldwide. However, like any other large-scale system, it is prone to large-scale failures and catastrophes [1], [2]. This issue is exacerbated by the increasing interconnection of power grids across continents and countries. This in turn makes it vulnerable to failures with origins at different locations. Such failures can result in disruption of power supply, or failure to meet basic power quality requirements. Consequently, disruption of public services can occur, e.g., transportation, communications, domestic power supply, etc. Furthermore, these outages result in large penalties to system operators. Hence, it is of paramount importance to mitigate the effects of such failures and minimise damage caused [3].

The associate editor coordinating the review of this manuscript and approving it for publication was Ravindra Singh.

A. CASCADING FAILURES AND BLACKOUTS

The blackout state is defined by the European Network of Transmission System Operators for Electricity (ENTSO-E) as, *"the interruption of electricity generation, transmission, distribution and consumption processes, when operation of the transmission system or a part thereof is terminated."* The disastrous impacts of blackouts are well known, with severe technological and socioeconomic ramifications [1], [2], [3], affecting all spheres of societal functioning. It is seen that power outages are a persistent problem, caused by a multitude of reasons. Some of the most common reasons include, but are not limited to, extreme weather, high load demand, poor system planning, etc. Hence, a blackout is caused by a

combination of multiple, mutually exclusive, low probability events.

This brings into play the mechanism of cascading failures. A cascading failure is *"the uncontrolled successive loss of system elements triggered by an incident at any location"* [4]. Most blackouts are initiated by some major disturbances in the power grid, leading to a propagation of cascading failures across the entire system [4], [5], [6]. The number of affected users, country of origin, and year of occurrence of some major global blackouts in the time period 2003-2022 is shown in Figure 1. As can be seen from the figure, in the past 10 years, several significant blackouts have occurred worldwide. In 2003, USA and Canada experienced a 48-hour blackout affecting 50 million people, while Italy suffered a 12-hour blackout affecting 60 million people. In 2006, the ENTSO-E region had a 3-hour blackout impacting 15 million people. The largest blackout, in terms of affected consumers occurred in India in 2012 during severe 15-hour blackout, affecting a staggering 620 million people. Other notable blackouts include Turkey in 2015 for about 8 hours, affecting 70 million and Pakistan in 2021 (9 hours, 200 million people affected).

The most common reasons for these blackouts were adverse weather conditions, highly stressed systems or a combination of thereof. Increasing integration of renewable energy sources and the rapid digitalisation of the power system has significant implications on power system cascading failures. This combination creates a complex interplay between physical and cyber-physical aspects of the power system. The reliance on interconnected and interdependent systems may amplify the potential impact of cascading failures. A localised disturbance or failure in one part of the system can propagate through digital communication networks and physical components, leading to widespread outages and disruptions. This interplay between the cyber and physical worlds is subsequently discussed at length in the rest of the paper.

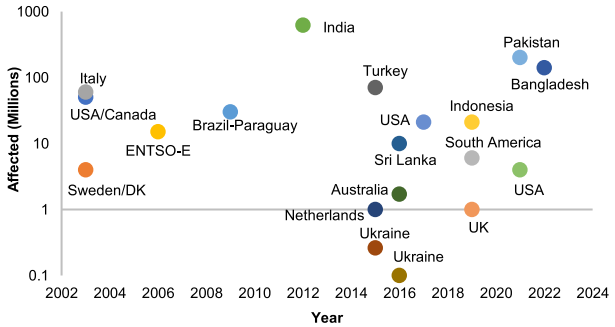


FIGURE 1. Recent global power system blackouts between 2003-2022 and their societal impact.

B. GRID DIGITALISATION AND CYBER SECURITY

Increasing power grid digitalisation has resulted in the convergence between Information Technology (IT) and Operational Technology (OT) systems. While offering greater monitoring and control capabilities, this has brought forth serious cyber security concerns. Malicious cyber attacks on power grids may trigger and accelerate cascading failures, leading to adverse consequences. A sophisticated and coordinated cyber attack across multiple locations may collapse the entire interconnected power grid of nations, or even continents. This is a real modern-day threat, as evidenced the cyber attacks on the Ukrainian power grid in 2015 and 2016 [7]. These are the first and only known cyber attacks to directly result in power outages.

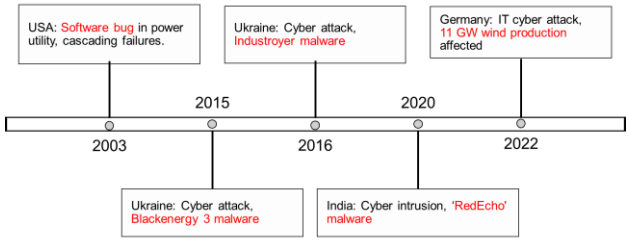


FIGURE 2. Timeline of power system related cyber security incidents from 2003 to 2022 [7], [8].

Figure 2 presents a brief timeline of cyber security incidents involving power systems in the past 5-6 years. It is evident that there is an ever increasing threat of cyber attacks on power systems. The attack in Ukraine in 2015 caused intermittent power outages, affecting more than 225,000 people. In 2016, a sophisticated malware was used that led to a disruption in the distribution network. This resulted in the loss of over 200 MW of load and a power outage. Meanwhile, on March 9, 2020, it was reported that the IT network of ENTSO-E was compromised in a cyber intrusion More recently, on October 12, 2020, Mumbai, a major Indian metropolis was affected by a power outage lasting over 12 hours. A recent study has revealed that the outage was related to 'RedEcho', an active hacker group. The attackers used sophisticated malware to target a regional control centre, in a campaign lasting over 6 months [8]. Thus, cyber security of power systems has emerged as a dynamic and critical area of research [9], [10].

Given this scenario, there is a pressing need to understand how cyber attacks can lead to cascading failures and blackouts in power systems. By conducting a thorough analysis of past blackouts, critical root causes of power system failures can be identified, with a focus on cyber-physical aspects. This can help to develop effective strategies for mitigating the impact of cyber attacks and minimising the likelihood of widespread power outages. Furthermore, by understanding the root causes of blackouts, appropriate measures can be taken at an early stage to avoid cascading failures and maintain the resilience of power systems in the face of cyber threats.

II. LITERATURE REVIEW

A. CLASSIFICATION OF STATE-OF-THE-ART

To identify the state-of-the-art research, a comprehensive literature review was undertaken, utilizing IEEE Xplore, Web of Science, and ScienceDirect databases. This review comprised

TABLE 1. Text search queries to find relevant literature on power system cascading failures and cyber security.

Objective	Text Search Queries
Part one: search relevant articles on power system cascading failures	*TS1*: ((power grids **OR** power system **OR** smart grid) **AND** *TS2*: ((cascading failure) **OR** (blackout) **OR** (outages))
Part two: search relevant articles on cyber security research in cyber-physical power systems	*TS1:* ((power grids **OR** power system **OR** smart grid **OR** SCADA) **AND** (cyber security))

TABLE 2. Classification and comparison with state-of-the-art literature.

Ref.	CF Analysis	C-P Factors	Cyber Security	Cyber Attacks	Validation	Remarks
[11]	L	M	M	L	L	Discussed vulnerability assessment and resilience aspects for CPPS.
[12]	L	L	H	M	L	Proposed a privacy conserving framework for intrusion detection.
[13]	L	M	H	H	L	Comprehensive review of CPPS attack vectors and defense mechanisms.
[14]	L	L	M	H	L	Explored methods to quantify resilience in CP power systems.
[15]	L	H	H	L	L	Advanced review on CPPS modelling and threat analysis.
[16]	L	L	H	H	L	Focused on CPS threats, attacks, and mitigation techniques.
[17]	M	L	M	L	L	Summary of CPS definition and metrics for quantification.
[18]	H	H	L	L	L	Comprehensive review of generalised cascading failure mechanism.
[19]	L	M	H	H	L	Thorough review of CPS modelling and cyber security
This paper	H	H	H	H	H	We provide a detailed review of major cascading failure incidents, identify common critical factors amongst them. Subsequently, based on reported cyber attack vectors, we infer how they can cause cascading failures.

Coverage: **L** - Low; **M** - Medium; **H** - High

two primary facets: power system cascading failures and cybersecurity for power systems. This is summarised through Table 1. Based on this review, five categories of interest were identified and a detailed comparison of reviews and surveys addressing these topics is provided in Table 2.

1) Cascading failure analysis: encompasses studies and research related to the modelling and analysis of cascading failures within power systems. This includes identifying vulnerabilities and potential points of failure. This category is chosen as it is crucial for understanding the fundamental aspects of power system reliability and resilience, and focuses on the root causes of cascading failures.

2) Cyber-physical factors: research that delves into the interplay between cyber and physical layers in power systems. This category is chosen to understand how cyber attacks can propagate and impact the physical infrastructure. Such knowledge is essential for devising strategies to safeguard power systems from cyber threats that can lead to cascading failures.

3) Cyber security of power grids: concentrates on the various cyber security threats, protocols, and technologies that can affect the power grid.

4) Cyber attacks: focuses on the different methods and strategies that cyber attackers employ to target power

systems, including malware, phishing, and Advanced Persistent Threats (APTs).

5) Experimental validation: This category deals with empirical studies and experiments aimed at validating the impact of cyber attacks on power system cascading failures and proposing suitable mitigation strategies.

B. CASCADING FAILURE RESEARCH

Cascading failures in smart power grids are a growing concern due to rapid digitalisation energy transition. Various modelling approaches for understanding the mechanisms behind cascading failures in power grids are discussed in [20]. The authors investigated the impact of different factors such as node connectivity, load distribution, and protection schemes on the likelihood of cascading failures. In [21], the authors analysed the vulnerability of power grids to cascading failures under different scenarios, including random failures and targeted attacks.

While the aforementioned works provide valuable insights into cascading failures in power grids, they do not address the cyber-physical factors that can influence such failures. In [22], the authors discuss the resilience of cyber-physical systems against natural hazards and cyber attacks. They consider human and societal factors that can affect system resilience, such as organisational structure and communication patterns. The impact of cyber attacks on the power system, however, is not discussed in detail, nor are the critical cyber-physical factors that can influence the cascading failure mechanism. Overall, further research is needed to fully understand the complex interplay between cyber and physical components in power grids and their impact on system stability. Hence, our work seeks to address this gap.

C. CYBER SECURITY FOR POWER GRIDS

Review of cyber security for power systems is well reported in the literature [16], [19]. In [23], the authors provide a comprehensive review of cyber attacks and defence mechanisms for improving smart grid security. This work provides an overview of all the topics in this research domain, i.e., cyber security, modelling, interplay between cyber and physical layers in CPS, etc. Similarly, [16] discusses vulnerability assessment for cyber-physical power systems. More importantly, this work reviewed methods to assess vulnerability and resilience and identified existing gaps. Meanwhile, cyber-physical security and cyber-physical attack scenarios are discussed in depth in [24]. All these works seek to provide a better understanding of vulnerabilities in cyber-physical systems and propose suitable resilience solutions. However, they miss connecting the cyber and physical worlds, i.e., how cyber threats can affect the power system cascading failure mechanism, which forms the focus of our work.

D. MOTIVATION AND CONTRIBUTIONS

In this work, we present a fundamental analysis of the connection between the cascading failure mechanism and cyber security. We hypothesise that cyber attacks at multiple locations in the power grid can induce cascading failures and a blackout. Cyber attacks can exploit vulnerabilities in the system's digital infrastructure, compromising control systems, disrupting communication networks, or manipulating data, thereby triggering or amplifying cascading failures. The novelty of such an analysis is the exploration of how reported cyber attack vectors can influence the critical factors and exacerbate the cascading failure mechanism. By examining documented instances of cyber attacks on power systems, we aim to demonstrate the correlation between cyber attacks and their effects on critical factors. This is visualised through Figure 3. The key scientific contributions of this work are summarised as follows:

1) A comprehensive state-of-the-art review of major recent power system blackouts caused by cascading failures is performed. Furthermore, the mechanism and propagation of cascading failures is critically examined. Based on this study, the critical cyber-physical factors that can lead up to the point of no return in a cascading failure sequence are identified.

2) Hypothetical cyber-physical attack scenarios are developed to analyse cyber attack induced blackouts. The scenarios aim to exploit the previously identified critical cyber-physical factors through various cyber attack vectors reported in the literature, to initiate cascading failures.

3) A synthetic case study and software-based simulation results demonstrate how cyber attacks can cause a blackout. The case study uses one of the aforementioned attack scenarios, to highlight how cyber attacks can trigger multiple critical cyber-physical factors and cause a blackout. Such an analysis can provide crucial know-how for grid operators and asset owners to manage and prioritise the maintenance and investment in securing their critical infrastructures. Furthermore, this study can help to develop suitable mitigation measures against cyber attacks on power systems.

The remainder of this paper is structured as follows. Section III provides a review of major power system blackout events between 2003-2021, to identify and highlight key causes/ critical events discussed in literature. A detailed analysis of the cascading failure mechanism in power systems, and identification of critical factors is carried out in Section IV. How these various factors can be exploited through different cyber attack scenarios to cause cascading failures is discussed in Section V, while Section VI presents experimental results to illustrate the same. Finally, conclusions are drawn and future work is discussed in Section VII.

III. REVIEW OF MAJOR BLACKOUTS

This section summarises major blackout events in the period 2003-2021. A summary of the sequence of events leading up to the blackout is provided, based on available literature. Through this summary, we identify the critical factors that initiated the cascading failures, leading to the blackout.

A. ITALY, 2003

On September 28, 2003, the Italian power system experienced a major blackout. The outage affected an area housing around 60 million people. The triggering event began at 03:01:00

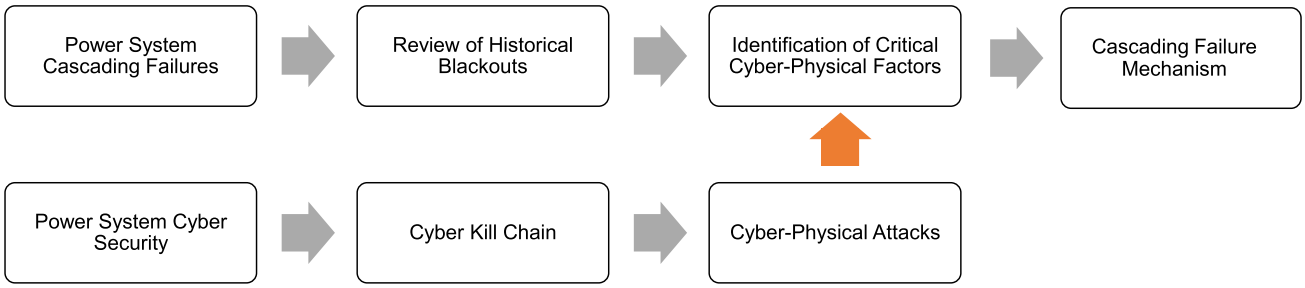


FIGURE 3. Connection between power system cascading failures and cyber security.

and proceeded up to 03:28:00. Power was restored after three hours in the North and later in the day in the rest of Italy. In total, approximately 6.4 GW of load was left unmet. This was deemed to be the largest blackout in the country's history, and one of the biggest within the EU. The blackout was initiated by a fault originating in neighbouring Switzerland, triggering a chain of cascading events. This eventually resulted in the Italian power grid being cut off from the rest of Europe [25].

The entire sequence of events can be summarised as follows. A tree flashover caused a 380 kV tie line trip in Switzerland near the Italian border, resulting in failed breaker controls and power transfer to Italy through neighbouring lines. Despite a 300 MW import reduction, a second tie line also tripped near the Swiss-Italian border due to poor operator response and inadequate power redistribution. Additional power was imported from France without prior planning. This overloading of tie-lines to France led to a drop in system frequency, triggering under-frequency relays, generator disconnections and a complete blackout. The major identified reasons were inadequate coordination, lack of real-time monitoring, reduced security margins, increased parallel flows, and angular and voltage instabilities, causing system collapse [26].

B. NORTH AMERICA, 2003

On August 14, 2003, a blackout occurred in North America involving eight U.S. states and two Canadian provinces. Approximately 50 million people were affected and around 63 GW of load was lost or interrupted [27]. This equated to roughly 11% of the total load served in the Eastern Interconnection of the North American system. Over the course of the entire event, more than 400 transmission lines and 531 generating units at 261 power plants tripped [28].

The blackout resulted from a combination of multiple unrelated events. Due to weather conditions and excess vegetation, flashovers took place on overhead transmission lines. A previously unknown and critical software bug, i.e., a race condition in the alarm system at the control room of the system operator, First Energy (FE) [4] led to inadequate situational awareness. This blindsided system operators who were unaware of actual ground conditions and the need to take remedial actions after the tripping of multiple transmission lines. This set of a chain of major cascading failures, culminating in one of the largest blackouts in American history [28].

A brief summary of the sequence of events. A generator outage occurred due to overexcitation caused by high reactive power output from other generators Northern Ohio service area. Unrelated, multiple 345 kV transmission lines experienced flashovers and trips due to vegetation contact, despite not being overloaded. Lack of situational awareness caused by a software bug at FE resulted in no operational actions being taken, leading to cascading line trips and severe under voltage conditions. A critical transmission line tripped in Ohio, triggering cascading failures in other nearby transmission and tie-lines with similar settings. This sudden loss of major tie lines caused power transfer between the U.S. and Canada to reverse, resulting in a huge power flow of around 3700 MW from Canada to Michigan and Ohio. This unplanned exchange caused voltage collapse due to overloaded transmission lines, leading to cascading failures of other lines and generators, resulting in a blackout [28].

C. EUROPE, 2006

The European transmission system experienced a major blackout on November 4, 2006, affecting around 15 million people. The origin of the events leading up to the blackout took place in Germany, but quickly spread throughout the continent. The main causes of the blackout were identified as the non-fulfilment of the *N-1* criterion and insufficient coordination amongst Transmission System Operators (TSO) [29]. The *N-1* criterion was violated when appropriate security analysis and application of pre-defined remedial actions were not performed. In addition, the compliance with the criterion was evaluated by a TSO regardless of the situation in the neighbouring systems. Furthermore, results of security analysis between TSOs were not robust and wide enough. The crucial factors that influenced the blackout were limited range of actions for handling grid congestions, lack of coordination throughout the event and generator related issues [29].

D. INDIA, 2012

The largest blackout in terms of people affected, occurred in July 2012, in India [30]. Extremely hot weather conditions led to a very high system demand, placing tremendous stress on

the power system. On 30 July 2012, around 02:00 local time, a 400 kV tie-line interconnecting the western and northern regions tripped, initiating a chain of events, culminating in a large-scale blackout. Successive line trips after the initial event led to a power imbalance of around 32 GW. This left around 300 million Indians in the dark. The socioeconomic ramifications were disastrous, affecting core sectors such as transport, healthcare, finance, etc. As per the post incident report, the root causes for the blackout were identified to be weaker transmission line corridors and protection malfunction. Other critical factors such as lack of coordination for outages, frequency control and islanding methods aggravated the effects [31], [32].

E. TURKEY, 2015

The Turkish power system experienced a blackout on March 31, 2015 that lasted for over 8 hours. The blackout was initiated by a major tie-line trip due to overload. This disconnected the eastern and western regions. Subsequently, other lines became overloaded and tripped in succession (violation of *N-1* criterion). Thus, the eastern and western parts were separated resulting in a major power mismatch [33]. The eastern region had excess supply, resulting in an over frequency condition leading to protection trips. Conversely, the western part suffered from under frequency, leading to load shedding. However, power plants could not operate at reduced frequencies for extended durations, leading to a blackout. The most critical factors in this event were found to be the lack of real-time monitoring and contingency preparedness. Furthermore, a lack of awareness about the effects of angular stability, distance relay settings, and grid code compliance compounded the issue [33], [34].

F. UNITED KINGDOM, 2019

On August 9, 2019, a major power outage in the UK affected over 1 million consumers' electricity supply. Several interdependent services were disrupted due to the outage. Rail services were severely affected, causing major socioeconomic disruptions. The event was found to be caused by a lightning strike prior to the blackout that triggered a process known as vector shift protection. This automatically reduced power output by 150 MW to ease the strain on the network. These outages also triggered a collapse in the frequency, which plummeted to 48.8 Hz during the blackout. This caused load shedding schemes to activate and disconnect about 350 MW of power from grid, allowing the frequency to recover. This unintentional load shedding however, had an adverse impact on electricity reliant critical services such as railways and hospitals [35].

G. PAKISTAN, 2021

The entire nation of Pakistan was plunged into darkness in the wee hours of January 9, 2021. The blackout was caused by electrical fault in southern Pakistan at 23:41 local time, which prompted a series of cascading outages. The total restoration process took around 20-22 hours in some areas. The post incident analysis report mentions a permanent bolted earth fault and unstable power swings as the root causes [36]. Furthermore, lack of operator experience and negligence also played a key role.

H. SUMMARY

Based on the above incidents, the anatomy of a power system blackout can be summarised as follows:

i. **Preconditions:** refer to the underlying conditions or vulnerabilities in the power system that may exist prior to a blackout. These can include factors like inadequate infrastructure, insufficient maintenance, or operational limitations.
ii. **Triggers:** events or factors that initiate the blackout. They can be external events such as severe weather conditions, natural disasters, equipment failures, or human errors. Triggers can also be internal factors like system overloads or voltage instability.
iii. **Emergency condition and remedial actions:** once the triggers occur, the power system enters an emergency condition. At this stage, various remedial actions need to be undertaken to stabilise the system and prevent a complete blackout. These actions may include load shedding, generation adjustments, or rerouting of power flows.
iv. **Other triggers:** apart from the initial triggers, there can be additional factors that contribute to the escalation of the blackout. These can include secondary equipment failures, lack of contingency plans, or ineffective actions by the system operator.
v. **Slow and fast cascading failures:** cascading failures refer to the progressive and interconnected failures that occur in a power system. They can be categorised as slow or fast depending on the speed at which they propagate. Slow cascading failures are characterised by a gradual deterioration of the power system, where the failure of one component leads to increased stress on others, eventually resulting in system-wide disruptions. Fast cascading failures, on the other hand, exhibit a rapid and simultaneous collapse of multiple components, leading to a sudden and severe blackout. Sometime between these two phases, the Point of No Return (PNR) is reached. This denotes an inflexion point between the stages and results in a blackout, i.e., loss of power supply to a significant portion or the entire power system.

This mechanism can also be visualised through the following Figure 4. In summary, all electrical power grids are designed to comply with the *N-1* criterion, i.e., a single component/element failure does not result in the collapse of the entire system. Nonetheless, a unique combination of failures can induce a cascading effect through the system [37], [38]. Effects such as such as Hidden Failures (HF) in relays [39], [40] and operational errors can worsen system conditions and amplify the effects of a single failure.

TABLE 3. Summary of major blackouts in the past two decades.

Year	Location	Duration (hours)	Affected (million)	Major Causes	Refs.
2003	USA/Canada	48	50	Critical software bug, protection malfunction	[28]
2003	Sweden/Denmark	6	4	Major faults, line overloads	[27]
2003	Italy	12	60	Frequency and voltage instability	[25], [26]
2006	Europe	3	15	*N-1* violation, lack of coordination	[29]
2009	Brazil-Paraguay	7	60	Extreme weather	[43]
2012	India	15	620	Overloading, protection malfunction	[30], [31], [32]
2015	Ukraine	6	0.26	Cyber attack	[7]
2015	Turkey	8	70	System failures, lack of coordination	[33]
2016	Australia	6.1	1.7	Extreme weather	[44]
2017	USA	11	21	Weather and protection issues	[45]
2019	UK	2	1	Lightning and major fault	[35]
2019	Indonesia	9	21	Power plant disruptions	[46]
2021	Pakistan	9	200	Electrical fault	[36]
2021	USA	6	4	Winter storm	[47]
2022	Bangladesh	10	140	Transmission line trip	[48]

Hence, cascading failures involve complicated mechanisms and interactions between phenomena on different timescales and domains [41], [42].

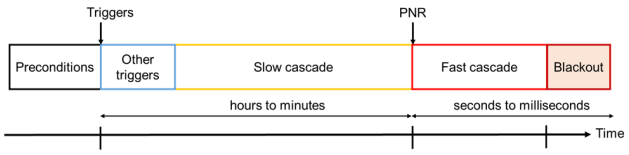


FIGURE 4. Simplified anatomy of the cascading failure mechanism.

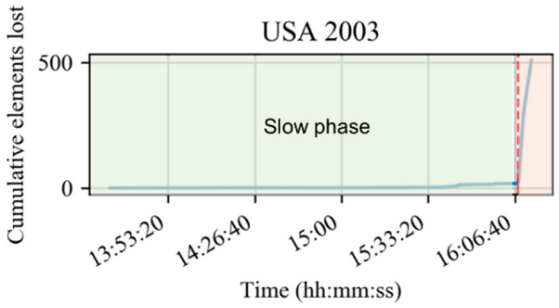


FIGURE 5. Loss of elements during the USA-Canada 2003 blackout. The slow phase continued on for a couple of hours (in green), while the fast phase lasted only a few minutes (in red).

IV. CYBER-PHYSICAL FACTORS

Large disturbances in power system operations can be followed by a series of events. If these events are not managed or controlled, they can lead to cascading failures and even a blackout. For a given power system with n components and k successive failures, the number of successive failure of components is given by n^k combinations [6]. Thus, it is infeasible to check every combination. Nevertheless, cascading failure induced blackouts share some recurrent characteristics, such as: 1) Extreme weather and natural disasters [49], 2) Hidden Failures [39], [40], 3) System-level failures, and 4) Human errors.

The focus of this work is limited to points 2 and 3, and how they may be triggered by cyber attacks. In a cascading failure sequence, power system dynamics plays a crucial role [50], [51]. A major disturbance or critical event in the power grid can cause a mismatch between power generation and demand, leading to the insecure operation of the system. Consequently, generators and transmission lines can get overloaded, causing the system frequency and voltages to drop. To keep the frequency and voltage within permissible limits, load shedding is often undertaken. However, if the curtailed load is not sufficient or if the action is delayed, additional transmission lines and generators may trip, leading to a domino cascading effect.

A complete cascading failure however, can take anywhere between minutes to hours, comprising of two distinct phases, i.e., 'slow' and 'fast' [42], [52]. This can be visualised through Figure 5 that illustrates the two phases for the USA-Canada 2003 blackout. The maximum damage is caused in the 'fast' phase, resulting in a domino effect which involves rapid tripping and disconnection of components. This phase typically occurs at the end of a cascading sequence, with a point of no return. It involves highly non-linear and dynamic phenomena, such as: 1) transmission line overloading, 2) generator disconnections, 3) frequency variations, 4) voltage instabilities, and 5) loss of synchronism. All these physical phenomena play a major role in the propagation of cascading failures. Power system dynamics can also be significantly affected by ICT infrastructure [53], [54]. This includes substation automation and protection systems, generator controls, protective relays, etc. With the looming threat of cyber attacks on power systems, impact assessment of cyber attacks on power system dynamics is a crucial topic [19].

Hence, a detailed analysis of the key dynamic factors and phenomena influencing cascading failures is provided in the subsequent subsection.

A. CRITICAL CATEGORIES AND FACTORS

1) LOSS OF TRANSMISSION LINES

In almost all major blackouts, loss of transmission lines has played a major role [50], [55]. The main IEs before the cascade include excessive or unplanned power transfers, extreme weather conditions, contact with vegetation, etc. There are various critical factors within this category that have contributed to real-world cascading failures.

(i) Zone 3 distance protection operation: a crucial factor that has been repeatedly observed in many severe cascading outages is the erroneous operation of transmission line zone 3 distance protection. Under heavy loading, coupled with relatively low system voltage, a distance relay may confuse the overloading situation for an uncleared zone 3 fault as the impedance enters the third zone of protection. Such a phenomenon has been reported in the literature [57] and witnessed in real-world cascading failures and blackouts such as USA-Canada 2003 [28] and Turkey 2015 [33]. Such a critical factor can be influenced by cyber attacks that spoof measurements of communication assisted protection schemes [53]. By altering the voltage and/or current measurements sensed by relays, it may be possible to maliciously trip them. Additionally, in the event of switching attacks and loss of multiple lines, this factor can be indirectly activated.

(ii) Line overloading: when transmission lines are overloaded beyond their nominal limits, due to increased I^2R losses, they start to sag and dissipate massive heat. This involves both thermal and electrical phenomena. If left unchecked beyond a certain time duration, they are automatically tripped by overload protection. In the worst case, overhead lines can sag, come in contact with vegetation, and trip due to flashovers. Therefore, line overloading can set off a cascading chain; other parallel lines in the system may get overloaded as well and trip [55], thereby severely compromising system integrity. It is be noted that overhead line overloading is a 'slow' phenomenon, in comparison to other dynamic parameters and categories discussed subsequently. Line sags and flashovers can take anywhere from between minutes to hours. Interestingly, the cascading failures propagate non-locally, i.e., the initiating event could be a significant distance away from subsequent line trips [4].

This loss of lines not only disconnects equipment but also leads to system parameters such as voltage and frequency going out of their limits. By gaining access to the substation controls and opening multiple circuit breakers at once, lines can be put of service, as seen during the Ukraine 2015 attack [7]. Consequently, parallel lines will be overloaded. If the original lines are not put back into service in a timely manner, the overloaded parallel lines can also trip, initiating a domino effect and possibly a voltage collapse. This can have a particularly devastating effect on the entire power system, as observed in Italy and USA-Canada in 2003 [27].

2) VOLTAGE STABILITY

Maintaining the system voltage at nominal values is crucial to ensure secure system operation. The fundamental reason for voltage instability is the inability to satisfy reactive power demands. Consequently, reactive power losses can increase, leading to voltage sags. During a cascading failure process, due to sudden and rapid tripping of elements, bus voltages can change drastically, causing severe voltage instabilities. Also, changes in active or reactive power outputs of generators can cause power swings and reactive power issues, respectively. Therefore, either primary or backup protection relays can trip, setting off a voltage collapse. This typically activates Under-Voltage Load Shedding (UVLS) or protection schemes that disconnect elements due to extremely low voltage levels. In the absence of sufficient voltage levels, the entire power system collapses, resulting in a blackout [56]. The critical factors affecting voltage stability during a cascading failure are as follows:

(i) Reactive power compensation: the crux of voltage instability is improper reactive power compensation. Devices for reactive power support such as Static VAr Compensators (SVCs) and Static Compensators (STATCOMs) can be targeted by Man-in-the Middle (MiTM) or data modification attacks to alter reactive power injections [16], [24], [58]. In the worst case, this can induce severe voltage instabilities and lead to a voltage collapse.

(ii) Voltage regulation: mechanisms to regulate voltage such as tap changers can also be compromised to impact voltage stability. In future power systems, the increased presence of Distributed Energy Resources (DERs) also provides an additional attack surface. These DERs are expected to be networked to the grid edge, via IoT that are also vulnerable. For example, [59] and [60] discuss the exploitation of vulnerabilities in photovoltaic inverters to cause abnormal voltages, and associated remedial measures to avoid this situation.

(iii) Line overloading: transmission lines can be heavily loaded due to increased reactive power flows, causing voltage drops. Subsequently, they can be tripped due to overload or distance protection, compounding the issue further. The influence of cyber security on this factor is discussed in the previous category.

(iv) Generator excitation: for any grid-tied synchronous generator, voltage/VAr control is provided by the Automatic Voltage Regulator (AVR) by varying field excitation current. Therefore, generators can be under or over excited, depending on voltage support requirements [56]. In the event of over or under excitation, the AVRs of generators can trip for safety reasons. This can potentially instigate voltage stability issues in the case of other contingencies. Such an advanced cyber attack scenario, targeting generator AVRs is discussed in [60] and [61].

3) TRANSIENT STABILITY

The most impactful event in a cascading failure is the disconnection of generator units and loss of synchronism.

TABLE 4. Summary of cyber attacks targeting critical factors.

Categories	Factors	Cyber Attacks						Refs.
		MiTM	DoS	Replay	Switching	Spoofing	Economic	
Loss of transmission lines	Zone 3 distance protection		✓		✓	✓		[40], [57]
	Line overloading	✓			✓	✓	✓	[49], [55]
	Protection malfunction	✓		✓		✓		[54]
Voltage instability	Reactive power compensation	✓		✓		✓		[58]
	Voltage regulation	✓		✓		✓		[59], [60]
	Line overloading	✓			✓	✓	✓	[49], [55]
	Generator excitation controls			✓		✓		[61]
Transient instability (Loss of synchronism)	Fault clearing times	✓	✓			✓		[54], [58]
	Loss of generation	✓			✓			[62], [63]
	Generator excitation controls			✓		✓		[61], [64]
Frequency instability	Islanding	✓			✓	✓		[65], [66], [67]
	Power mismatch	✓					✓	[68], [69], [70]
	Load shedding		✓	✓			✓	[71], [72]

Without sufficient power production, the power grid can destabilise rapidly. The major factors contributing to transient instabilities in cascading failures are the following.

(i) Fault-clearing times: the primary requirement for transient stability is the satisfaction of the equal-area criterion, i.e., the kinetic energy absorbed by the generator rotor during acceleration or fault conditions must equal the kinetic energy dissipated during deceleration, post-fault. Hence, it is crucial that faults must be cleared as quickly as possible to prevent loss of synchronism.

Therefore, a cyber attack that manipulates protection schemes and their associated communications to cause increased fault clearing times can lead to loss of synchronism. This may be possible through Denial-of-Service (DoS) attacks which delay the communication of critical control commands, as discussed in [54] and [58].

(ii) Loss of generation: in cascading failure events, angular instabilities may arise due to sudden large component disconnections or system changes, resulting in rotor angle instabilities. The sudden loss of a large generator or line switching can induce transient instabilities. As discussed in [62] and [63], targeting the breaker controls of a generator and rapidly switching them out of phase can result in transient instabilities. Consequently, the generator can lose synchronism and get disconnected or even damaged.

(iii) Generator controls: crucial aspect to ensure transient stability is the terminal voltage of generators, controlled by the AVR through field excitation. Hence, a cyber attack altering the field excitation parameters can affect transient stability of the system. This is especially true in the case of coordinated attack, leading to loss of multiple components. Typically, generators are equipped with several interface protection relays, and schemes to safeguard them in the event of major fault conditions. However, during a cascading failure process, the very same protection relays, while ensuring the safety of the generator can compromise the rest of the system. This directly worsens the cascading process in the rest of the system [61].

Switching attacks on generators are extensively discussed in [64]. This research shows how cyber attacks can disconnect generators and initiate cascading failures. Furthermore, [63] demonstrates the physical implications of such cyber attacks

on the machine and power system. Hence, a cyber attack seeking to compromise transient instability can rapidly connect and disconnect the generator's main circuit breaker. Such an advanced attack can destabilise the entire power system in a matter of a few seconds [64]. This can result in a loss of synchronism in the remaining parts of the system. Subsequently, other generator units may be tripped, resulting in a large-scale blackout, possibly requiring significant amounts of restorative efforts.

4) FREQUENCY INSTABILITY

The root cause of frequency instability is a mismatch between supply and demand. This can manifest in multiple ways, as follows.

(i) Islanding: cascading failures involve transmission line overloading and tripping of connected generators. This may result in islanding, i.e., creation of areas with a large mismatch between power supply and demand. As a result, the frequency within the islanded systems can differ vastly. This can also occur due to sudden large load disconnections. Depending on the inertia of the synchronous generators within the system, such a mismatch can activate Rate of Change of Frequency (ROCOF) protection to protect the generator units. With the influx of more renewable power generation, system inertias are expected to reduce further [65]. Therefore, ROCOF protection is a critical parameter with regard to frequency stability and cascading failure analysis.

A resonance cyber attack targeting ROCOF and load frequency control of generators is discussed in [66]. In this type of attack, the adversary modifies the input signals to generator controllers based on a resonance source, e.g., ROCOF. This results in a negative feedback on load frequency control, such that the targeted generator loses stability. Furthermore, the authors conclude that the maliciously modified inputs still lie within the normal operating range, thereby making the attack highly stealthy.

(ii) Supply-demand mismatch: to cause a mismatch between supply and demand, multiple cyber attack strategies are possible. Some sophisticated cyber attacks to induce such mismatches are discussed in literature. In [67], the authors explain how botnets may be used to rapidly increase power demand before frequency control mechanisms can react. Using a hypothetical example of continental Europe, they show how this can lead to loss of load and generation. Likewise, [68] presents a cyber attack scenario to artificially manipulate power demand through a spoofed market price signal. The net result in both cases is that of sudden frequency variations, prompting remedial actions such as load shedding.

(iii) Load shedding: to prevent scenarios such as islanding, corrective actions such as Under Frequency Load Shedding (UFLS) techniques are undertaken, leading to a loss of load. thereby creating a power imbalance. Such techniques must be fast enough to restrict the frequency drop, otherwise, the system can further destabilise. Sustained under frequency or over frequency conditions can cause generators to automatically trip [69]. Therefore, a DoS cyber attack which causes a delay in communication of load shedding commands can have an adverse effect on frequency stability, as discussed in [70] and [71].

It is to be pointed out that all of the aforementioned and discussed categories and factors are not mutually exclusive, but intertwined [72], [73]. For example, transient and voltage instabilities are strongly linked and usually occur together [56]. Likewise, frequency instability and transient instability also influence each other. It is worth mentioning that cyber attacks exploiting even one of the critical categories may induce cascading failures due to the strong interplay between all the phenomena. Extending this line of thought, a coordinated cyber attack can therefore accelerate the cascading failure mechanism. A recent study has confirmed this acceleration mechanism being observed in major historical cascading outages [52]. As a result, in the event of a coordinated cyber attack, the power grid may reach a point of no return sooner, triggering a massive collapse.

B. DISCUSSION AND SUMMARY

Based on the thorough analysis of past blackouts and critical root causes of power system cascading failures, the key points of the analysis are as follows:

1) Most cascading failures are caused by cyber-physical factors initiated by a set of events.
2) Typically, these events are physical in nature, e.g., extreme weather, human errors, etc. Nevertheless, it is possible for such events to be initiated by cyber attacks.
3) Such types of cyber attacks are scalable, i.e., they can result in abrupt $N - k$ contingencies. Therefore, existing power system planning, centred around $N - 1$ or $N - 2$ contingencies, must also account for cyber contingencies. This gives rise to a combined cyber-physical contingency evaluation.
4) With greater power grid interconnections, research on the impact analysis of cyber attacks on power system operation and stability is the need of the hour. Thus, future research can focus on carrying out cyber-physical simulations to understand how many cyber events can initiate a cascade, leading to a collapse, and therefore develop response strategies. Subsequently, future research is needed to answer the following:
   (i) How to detect cyber attacks in early-stages, before action on objectives results in any impact?
   (ii) Which OT assets are the most vulnerable and how to secure them?

V. CYBER ATTACKS ON POWER GRIDS

Cyber attacks on power grids have emerged as a sophisticated modern-day threat with wide-ranging ramifications. They are High-Impact Low-Frequency (HILF) events that can severely impact power system operation and stability. Table 4 lists some well-reported cyber attack exploits from literature, specifically targeting power systems. Such attack vectors are mainly inspired by the real-world cyber attacks in Ukraine

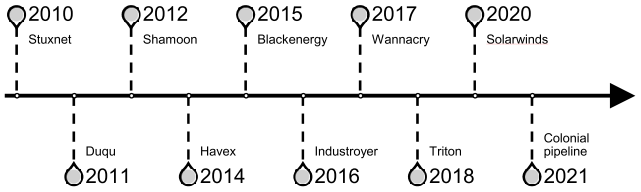


FIGURE 6. A timeline of major cyber attacks on ICS.

in 2015 and 2016. Figure 6 depicts a brief timeline of major cyber attacks on industrial control systems.

A. UKRAINE 2015 AND 2016

In 2015, the attack originated from the peripheral IT systems of the power grid operator. The adversaries successfully intruded into the system through hacking mechanisms such as phishing emails, malware operations, and credential theft. The entry point of the attack was a targeted spear phishing campaign on employees of the system operator in Ukraine. The phishing email contained weaponised Microsoft office files. Through macros located within the office files, the adversaries infiltrated the power grid operator's system using Black Energy 3 malware. From this point on, they had gained backdoor access to the core operational system of the system operator.

An alarming point is that the infiltration went undetected until the attackers launched a remote desktop session to access and control the Supervisory Control and Data Acquisition (SCADA) system. Subsequently, they opened multiple circuit breaker switches through the SCADA user interface. The system operator's employees could only watch in horror as they were locked out of their systems. The attack resulted in the blackout of seven 110 kV and twenty-three 25 kV substations. Roughly, more than 225,000 customers were affected by the blackout for several hours [7]. This attack is the first known, real-world example of a cyber attack to directly impact power grid operations.

In the following year, 2016, a more advanced and sophisticated cyber attack was launched, exploiting vulnerabilities present in power system communication protocols. Whilst the 2015 attack involved using remote desktop access to control SCADA remotely, the 2016 attack was performed through Industrial Control System (ICS) software manipulation using 'CRASHOVERRIDE/Industroyer' malware. This software manipulation required greater know how about ICS functioning, to launch a more sophisticated attack. The malware mainly targeted power system communication protocols such as IEC 101, IEC 104, and IEC 61850. By tampering with the protocols and their messages, the attackers could influence physical parameters such as the state of circuit breakers.

Luckily, the attack was not very successful and only resulted in small-scale impact, in comparison to the previous year. Nevertheless, the particular attack technique was quite alarming. By employing a similar technique, i.e., exploitation of power grid communication protocol vulnerabilities, it is possible that an advanced cyber attack can have catastrophic effects on the power grid.

B. CYBER KILL CHAIN

In this work, we focus our discussions on cyber attacks aimed at causing large-scale cascading failures and blackouts. Such cyber attacks can broadly categorised be into four categories [10]: 1) Attacks affecting physical equipment. 2) Attacks targeting communication networks. 3) Application centric attacks. 4) Data centric attacks. All the subsequently discussed cyber attacks fall into one of the four categories.

As previously discussed, most cascading failure induced blackouts consist of a multitude of factors. However, the critical factors that influence system dynamics and lead to the domino effect are limited. Therefore, in subsequent subsections we discuss how said factors can be exploited through different hypothetical 'nightmare' cyber attack scenarios. These scenarios are aimed at initiating or accelerating cascading failures, by influencing system conditions. The type and nature of the exploits are based on cyber attacks on power grids, already reported in the literature. The goal of this discussion is to highlight how such attacks can lead to cascading failures and a blackout. Hence, most advanced cyber attacks on ICS follow a similar chain of events, with the following steps:

1) Reconnaissance. This is the first stage in the cyber attack kill chain and involves conducting investigations of the target. Through this step, the adversary collects sensitive/critical information that can be used to jeopardise the target. An example for such information could be network data, critical equipment locations, etc.

2) Weaponisation. The information collected from the first stage is then used to develop an appropriate attack vector or payload. This is referred to as the weaponisation stage. An example of such a payload could be a malware or a bot.

3) Delivery. The third stage in the kill chain is the delivery stage. Once the payload is ready, the victim is targeted through suitable means. This may include mechanisms such as phishing emails, corrupted file attachments, malicious hyperlinks, etc. The goal of this stage is to successfully infect one or more machines of the target with the malicious payload.

4) Exploitation. The fourth stage entails exploitation of system resources through the delivered payload. An attacker can exploit known vulnerabilities in the target environment through the payload, to gain backdoor access to entire critical infrastructures.

5) Execution. This is the actual attack phase of the kill chain. Having gained unauthorised access, an adversary can then run their malicious code, remotely, to wreak havoc on the target.

6) & 7) Command and Control. These stages involve the adversary taking over controls of critical infrastructures and manipulating them to cause serious damages. Such actions could include changing operating set points, shutting down entire components or systems, thereby leading to catastrophic

damages. Examples of such unauthorised actions with respect to power grid operations can include malicious opening of circuit breakers and manipulation or spoofing of controller set points of generator AVRs and governors. The cyber attack kill chain and associated stages are illustrated through Figure 7.

C. MALWARE ATTACK

There are well known examples of malware targeting and compromising functioning of ICS. This includes the Stuxnet virus [74], Blackenergy 3 [7], and 'Crashoverride/ Industroyer' [8]. The last two were responsible for the cyber attacks, specifically targeting the power grid in Ukraine in 2015 and 2016, respectively. In April 2022, cyber attacks caused a malfunction in the communication systems used for monitoring and control of nearly 2000 wind turbines in Germany [75].

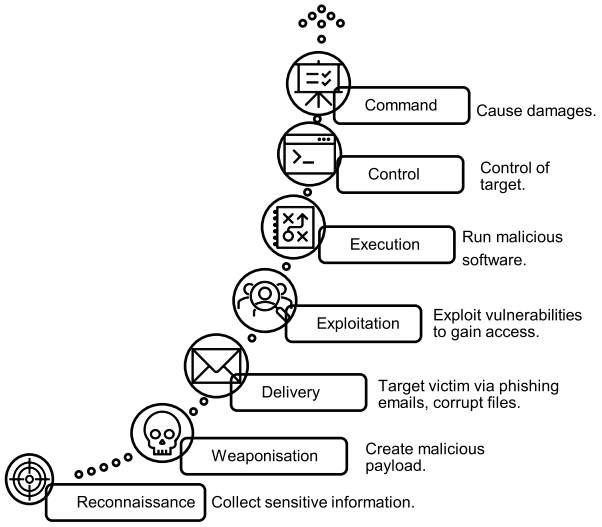


FIGURE 7. ICS cyber attack kill chain.

Around the same time, the Ukrainian computer emergency response team confirmed that high-voltage electrical substations in Ukraine were targeted by Industroyer2 malware [76]. These incidents highlight the evolving ICS cyber threat landscape. Malware attacks on physical equipment can affect the availability and integrity of signals, thereby compromising the system integrity. For example, a compromised critical device may continue to operate slowly than what is required by the corresponding application, even though the signals produced are reflective of the actual system, which triggers usability concerns. Hence, an advanced malware attack can wreak havoc on power system operations.

It is assumed that the adversary has gained access to the IT/OT infrastructure of the target power grid operator through malicious hacking activities, similar to the Ukraine 2015 attack [7]. The adversary then stays within the system, monitoring and recording system operations to pick an appropriate attack target and timing. This corresponds to stages 1, 2, and 3 in the cyber kill chain. In the summer, the power system is operating close to its limits due to a high demand. This prompts the attackers to launch their attack.

The attackers having conducted reconnaissance are familiar with the grid topology and operational conditions. They execute the first stage of the attack by planting a sophisticated malware, similar to Industroyer that initiates a race condition, given their access to the IT/OT infrastructure. This results in a critical software bug that goes unnoticed. It is assumed that the first stage is carried out well in advance. Hence, most, if not all regional control centres are infected by the malware. The goal of this stage is to blindside the system operator and cause lack of situational awareness. The malware prevents timely remedial actions in case of major faults or disturbances. Consequently, even a single IE can become a critical event, setting off a catastrophic cascading effect.

In the second stage of the attack, at a major transmission substation, where some lines are out of service for maintenance, the attackers take over the substation controls. They initiate automatic opening of all circuit breakers, even going to the extent of blocking all manual overrides. This corresponds to the execution and control stages of the cyber kill chain. Due to the malware, the system operator is fed misinformation that the system is in a healthy state. By opening all breakers in this substation, the already stressed system is pushed close its limits. Parallel lines in neighbouring substations are soon overloaded, causing line sags and eventual flashovers. A critical transmission line interconnecting the northern and southern regions is put out of service due to the cyber attack.

This forms the critical event and sets off a domino effect. Due to the sudden power imbalance and frequency instability, islands are formed. Consequently, under frequency relays of generators start to trip. This worsens system conditions and causes huge load disconnections. Subsequently, the lack of generation and extremely poor voltage levels leads to a blackout. The entire sequence of events is summarised in Table 5. The blackout from the initial event takes ∼1 hour. The critical cascading events happen in a matter of a few minutes. A similar sequence of events is what transpired during the USA- Canada blackout of 2003 [28].

D. OT HIJACKING ATTACK

As shown by the cyber attack in Ukraine, 2015, malicious takeover of substations and SCADA system can lead to catastrophic consequences [7], [64], [77]. Through lateral movement from IT to the OT system, attackers hijacked the substation OTs and maliciously disconnected multiple circuit breakers from the control centre. Such an attack vector is possible due to the use of legacy power system communication protocols with limited or no cyber security implementations. These communication protocols used by utilities, such as Distributed Network Protocol 3 (DNP3) and IEC 104 are vulnerable [77], [78], [79]. Particularly, through eavesdropping and active reconnaissance, attackers can jump from the substation to the control centre. In a

TABLE 5. Sequence of events due to malware attack.

Time (hrs.)	Event
22:10:05	Cyber attack at a transmission substation. Five circuit breakers are disconnected and manual override is disabled. This forms an *N-k* contingency. The system is highly stressed.
22:10:05	Critical transmission line is put out of service due to the cyber attack. Power flows are rerouted through other parallel lines.
22:50:07	Automatic Under frequency Load Shedding (UFLS) initiated. System operator finally realises situation due to load disconnections and emergency calls.
22:55:10	Cascading failures propagate and affect generating units. Under frequency protection automatically disconnects multiple generators due to sustained low frequency conditions.
23:00:00	Extremely poor voltage profile leads to voltage collapse and blackout.

critical ICS infrastructure, such attacks can have serious consequences, as timely operation is strictly necessary. This is shown Figure 8, wherein, critical messages/commands between control centre and substations can be sniffed or hijacked to gain unauthorised access. In the worst-case, such attacks can maliciously disconnect lines and equipment in the power grid. This can set off a chain of contingencies that may lead to cascading failures and even a blackout.

In the imagined attack scenario, it is assumed that the cyber attackers have gained backdoor access to the gateway server in multiple substations through spear phishing or malware attack [78]. This server acts as the medium of communication between the control centre and substation. Thereby, by gaining access to the server, the communication channel is compromised, allowing the adversaries to monitor and inspect all traffic. This corresponds to steps 1 and 2 in the cyber kill chain. The attackers inspect the type and content of all packets exchanged between the control centre and compromised substations, over an extended period of 3-4 months.

In stage two, with this knowledge, the attackers launch their cyber attack. The particular target utility uses IEC 104 for their SCADA communications. The attackers jump from the substation to the control centre by exploiting known IEC 104 vulnerabilities [80]. From the control centre, the attackers disable manual overrides, launch spoofed packets that tamper with the tap positions of the transformers within the substations. This has a severe effect on the voltage stability of the entire system as voltage levels are severely affected. A sustained low-voltage condition results in UVLS schemes being activated. Additionally, the attackers also maliciously

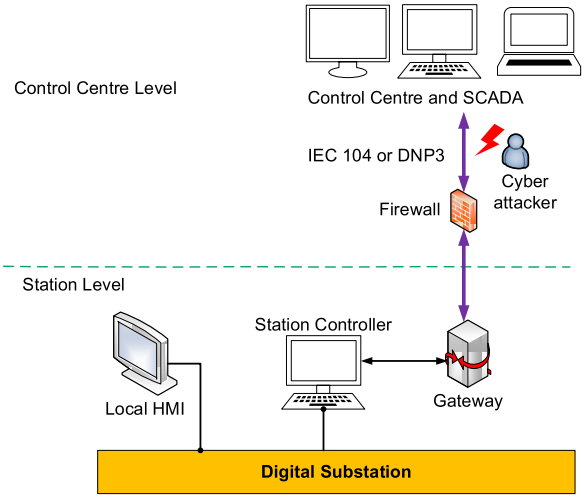


FIGURE 8. OT hijacking attack.

open multiple circuit breakers, thereby disconnecting several transmission lines and loads. Such a coordinated attack has an acute effect on voltage and frequency stability, initiating a voltage collapse. Generators are tripped by their over exciters due to high reactive power outputs. The cascading event propagates rapidly, causing successive line overloads and trips, resulting in a blackout.

TABLE 6. Sequence of events due to OT hijacking cyber attack.

No.	Event
1.	Cyber attack at three substations. Transformer tap positions are tampered causing changes to voltages.
2.	Generators automatically increase VAr outputs. System operator is sent spoofed packets from compromised substations.
3.	Automatic UVLS is activated to alleviate low voltages.
4.	Attackers open multiple feeder circuit breakers at once, disconnecting numerous lines and loads.
5.	Sudden disconnections cause power swings and frequency instabilities. Generators are tripped by automatic overexcitation protection due to voltage instabilities.
6.	UFLS is activated to arrest frequency drop due to loss of generation.
7.	Three parallel overhead lines are overloaded beyond thermal limits and trip.
8.	Severe frequency and voltage instabilities cause cascading failures and blackout.

E. MAN-IN-THE-MIDDLE ATTACK

An example of the MiTM attack is the exploitation of the IEC 61850 standard for digital substations. Owing to operational constraints, the standard does not implement any encryption, making it susceptible to a wide-range of cyber attacks, e.g., packet sniffing and replay attacks. The two protocols of

importance within the standard, i.e., Generic Object-Oriented Substation Event (GOOSE) and Sampled Values (SV) can be tampered with and spoofed [81], [82], [83]. As a result, protection equipment and components within a digital substation can be compromised or put out of service [83]. Subsequently, this can trigger a cascading failure due to the sudden loss of multiple components.

In a doomsday scenario, attackers can trigger a blackout by compromising critical digital substations, causing catastrophic damage. Figure 9 shows the typical layout of a digital substation communication network. This comprises of station, bay, and process levels. Each bay is controlled by a Bay Control Unit (BCU). A local area network enables the communication between engineering workstations, station control systems, and communication servers with control centres. It is to be noted that IEC 61850 traffic on the local operating network is not encrypted. This is to ensure real-time performance of protection equipment. All commands and measurements are communicated using the process bus. Hence, by gaining access to the substation communication network, the attacker can cause significant disruption and abnormal functioning of equipment within the digital substation, i.e., maliciously open circuit breakers, block or disable protection devices, or collapse the substation communication network itself.

To mitigate such attack threats, the IEC 62351-6 standard focuses on securing the protocols defined in IEC 61850. It introduces an additional field in the GOOSE and SV data payloads to incorporate security-related information. This field includes an Rivest Shamir Adelman (RSA)-based digital signature to ensure the integrity of the Protocol Data Unit (PDU). Similarly, the standard recommends using a Message Authentication Code (MAC) generated using a Secure Hash Algorithm (SHA-256) to verify the integrity of GOOSE and SV messages. By calculating and comparing HMAC values, the authenticity of the messages and the identity of the publisher can be verified. The use of RSA and HMAC algorithms, however, for message authenticity and integrity is not suitable for applications requiring a response time of four milliseconds or lower due to their computational demands. Additionally, the standard lacks guidance on certificates related to RSA keys used for signing extended PDUs, and the use of RSA and HMAC authentication keys for Intelligent Electronic Devices (IEDs) necessitates a key management infrastructure within the digital substation. As a result, these security mechanisms have not been widely adopted.

F. FALSE DATA INJECTION ATTACK

The most commonly reported type of cyber attack on power systems in literature is the False Data Injection (FDI) attack. An FDI attack operates under the assumption that an attacker can access current power system configuration information and manipulate the measurements of meters at physically protected locations such as substations. Thereby, they may introduce arbitrary errors into certain state variables without being detected. Most FDI attacks reported in literature are aimed at targeting state estimation algorithms and measurements [84], [85]. Related work also discusses data-driven attacks that target power flow measurements [86], [87].

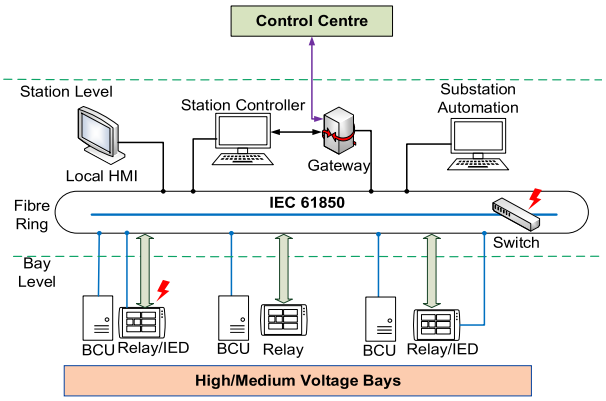


FIGURE 9. Digital substation communication network.

Such attacks however, are limited or restricted to boundaries of one substation. Hence, we focus our attention on data integrity attacks that target specific components of power systems to cause widespread damages.

Data integrity attacks targeting power system protection, i.e., relays and communication are of serious concern. It is critical to ensure security of supply and maintain power system health. With rapid developments in ICT and digital technologies, conventional protection systems are being upgraded into communication-assisted protection schemes [88]. Such communication-assisted protection schemes provide high-speed tripping at either ends of a protected line. Traditional multi-zone distance protection lacks such capabilities, as noted in [89]. Furthermore, reduced fault clearing times can minimise power system instability conditions and improve system reliability. Such high-speed fault clearing is achieved through dedicated communication between line terminals. Each line terminal communicates its status as a data bit to the remote end(s), over a dedicated communication channel. The data bit can represent either a trip or block command, depending on the protection scheme being employed. The most commonly used schemes are Permissive Overreaching Transfer Trip (POTT) and Permissive Under-reaching Transfer Trip (PUTT) [88]. While offering aforementioned advantages, this digitalisation of protection raises cyber security concerns [90], [91].

Cyber attacks considering the role of protection systems are extensively discussed in [90]. Typically, the most commonly used protection schemes are distance and differential protection for protection of transmission lines and transformers, respectively. Cyber attack vectors targeting these schemes are reported in [53] and [91]. Such sophisticated cyber attacks manipulate the parameters sensed by protection relays to calculate trip conditions. Thus, a successful cyber attack can lead to malicious tripping of relays, while remaining undetected.

Such attacks can have crippling consequences on power system operations. They can directly result in unwanted opening of circuit breakers, leading to transient instabilities. Another possibility is a 'sleeper cell' attack. In this scenario, the protection equipment is inhibited or blocked from normal functioning. Hence, during a fault condition, the relay may not operate, causing other zones of protection to be activated. This can subsequently cause other unwanted relay trips, triggering a cascading effect. While sounding far-fetched, such cyber attack scenarios are worrisome, since protection issues and malfunctions are directly/indirectly involved in about 70% of cascading failure incidents [49].

In the attack scenario, we consider two types of attack manipulations. The first one is focused on directly modifying the relay parameters used to issue tripping commands. The second is inhibition of protection functionality. The latter can achieved by carrying out DoS attacks on the communication channel used by communication-assisted protection [92], [93]. In the considered cyber attack scenario, attackers have gained access to the communication channel used by the communication-assisted protection system at three substations. This corresponds to steps 1-3 in the cyber kill chain. Execution of a DoS or FDI attack requires a malicious device with access to communication channels used by the relay. By remotely introducing such a device into the network, attackers can access the communication channel which enables fast breaker actions during faults. By launching a cyber attack when timely breaker action is necessary, however, they cause substantial disturbances to the power grid. This forms the crux of the discussed cyber attack scenario.

The attackers launch a DoS attack by flooding the communication channel with packets through their own malicious device. This results in blocking of permissive trip communications, i.e., prolonged fault clearing times. Subsequently, transient instabilities may arise in case of major faults. As the second stage of the attack, the cyber attackers execute an FDI attack to modify the trip signals. The attackers issue spoofed permissive trip signals that cause malicious tripping of relays. Now, when a fault occurs in the associated transmission line, due to the DoS attack, it is not cleared on time. Simultaneously, through the FDI attack, multiple relays are maliciously tripped, causing sudden opening of circuit breakers. Both these conditions put together induce massive system instabilities, initiating a domino effect, i.e., cascading failures and a blackout. The sequence of events is summarised in Table 7.

TABLE 7. Sequence of events due to DoS and FDI attacks.

No.	Event
1.	DoS attack on communication-assisted protection of a critical transmission line. Timely protection functionality is jeopardised.
2.	During short circuit, due to the DoS attack, zone 1 tripping is blocked. Zone 2 and 3 protection activated. Results in transient instabilities.
3.	FDI attack is executed, and multiple relays issue malicious permissive trip signals. Multiple transmission lines suddenly disconnected, resulting in an *N-k* contingency.
4.	Two or more regions are islanded by ROCOF protection as a consequence of the cyber attack.
5.	Mismatch between generation and demand in the regions causes frequency drops. Automatic UFLS is activated in steps. System is split into two asynchronous regions and partially blacked out.

G. ADVANCED PERSISTENT THREATS

Advanced Persistent Threats (APTs) represent a significant cyber security challenge for critical infrastructures, such as power systems. APTs are highly sophisticated and stealthy forms of cyber attacks conducted by well-funded and persistent threat actors. In the context of power systems, APTs pose a grave risk due to their potential to disrupt essential services, compromise data integrity, and even inflict physical damages. They are characterised by three main aspects. 1) Persistence: APTs are carried out over a long-term, with stealthy presence in a targeted OT network or system. Threat actors maintain access and continue their reconnaissance over an extended period, often remaining undetected. 2) Sophistication: APTs employ advanced techniques, including zero-day exploits, custom malware, and social engineering tactics. They adapt to network defences and conditions, making them difficult to detect and mitigate. 3) Targeted: APTs are not opportunistic attacks but rather meticulously planned and specifically aimed at high-value targets and critical infrastructures, such as power grids.

APTs pose a grave threat to the power system operation, as shown in the Ukraine 2015 and 2016 cyber attacks. Unlike cyber attacks on IT systems, attacks on cyber-physical power systems can lead to operational disruptions, with physical impact such as cascading failures and power outages [94], [95]. In conclusion, APTs on power systems represent a serious and evolving threat that necessitate proactive cyber security measures. By understanding their characteristics, motivations, and potential impacts, utilities can better prepare and defend against these sophisticated cyber threats.

VI. CASE STUDY AND SIMULATION RESULTS

In this section, we discuss a simulation case study involving cyber attacks conducted on a transmission system digital substation. The simulations are carried out on a modified IEEE-39 Bus test system simulated on DIgSILENT PowerFactory. The OT network is emulated using Mininet, based on operating-system-level virtualisation. The entire emulated OT network runs on 10 virtual servers and consists of 27 user-defined substations, 118 measurement devices, and over 800 data points for the entire simulated power system. SCADA device functionality within the OT network is realised through custom Python code. To analyse

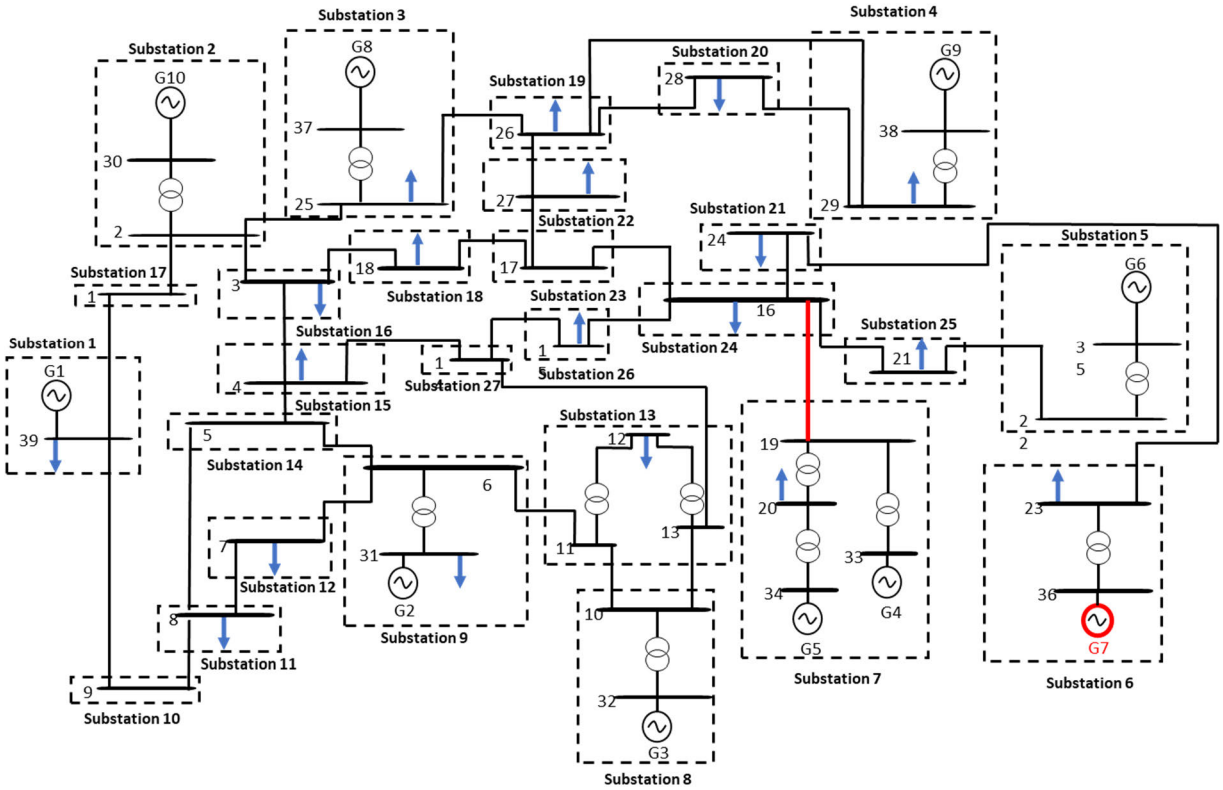


FIGURE 10. IEEE-39 bus test system with cyber attack locations highlighted in red.

TABLE 8. Protection schemes implemented.

Protection scheme	Component
Over/Under Frequency Over/Under Voltage ROCOF Over flux Out of step	Generators
Underfrequency Load Shedding Undervoltage Load Shedding	Loads
Distance Overload	Lines

the impact of cascading failures, multiple coordinated protection schemes are implemented. These include interface protection for generators in the form of under/over-frequency, ROCOF, loss of synchronism, and under/overvoltage. For the transmission lines, distance protection along with line overloading protection is enabled. Stress mitigation includes under frequency and under voltage load shedding. This is summarised by the following Table 8.

A. ATTACK SCENARIO

In the presented attack scenario, a coordinated cyber attack leads to manipulation of generator AVRs and opening of circuit breakers. The latter is achieved through IEC 61850 GOOSE cyber attacks. The attack locations are indicated in Figure 10. The cyber attack is launched at 5s simulation time to maliciously alter the AVR set-point for generator G6, as visualised through Figure 12. It is observed that the traffic is zero at some instants. This is due to variability of latency and delays in distributed communication systems, leading to variations in the packet arrival time. The attack causes an abrupt increase in the terminal voltage of the generator by 10%.

B. CYBER-PHYSICAL FACTORS

The cyber attack affects the voltage regulation and reactive power compensation factors. Subsequently, circuit breakers on the line 19-16, at substation 7 are also maliciously opened at 10s simulation time. As a result, the two generators in substation 7, i.e., G4 and G5 are islanded from the rest of the system and disconnected by ROCOF protection. This can be visualised through Figure 13, wherein the threshold of 2 Hz/s over 500 ms is crossed. Consequently, due to the sudden loss of generation, multiple transmission lines are overloaded and trip due to zone-3 distance protection. The sustained overcurrent and low voltage is misinterpreted as an uncleared zone-3 fault, resulting in an overreach of distance protection. This is depicted in Figure 14 as a plot of bus voltages and line currents highlighting sustained under voltage and overcurrent conditions.

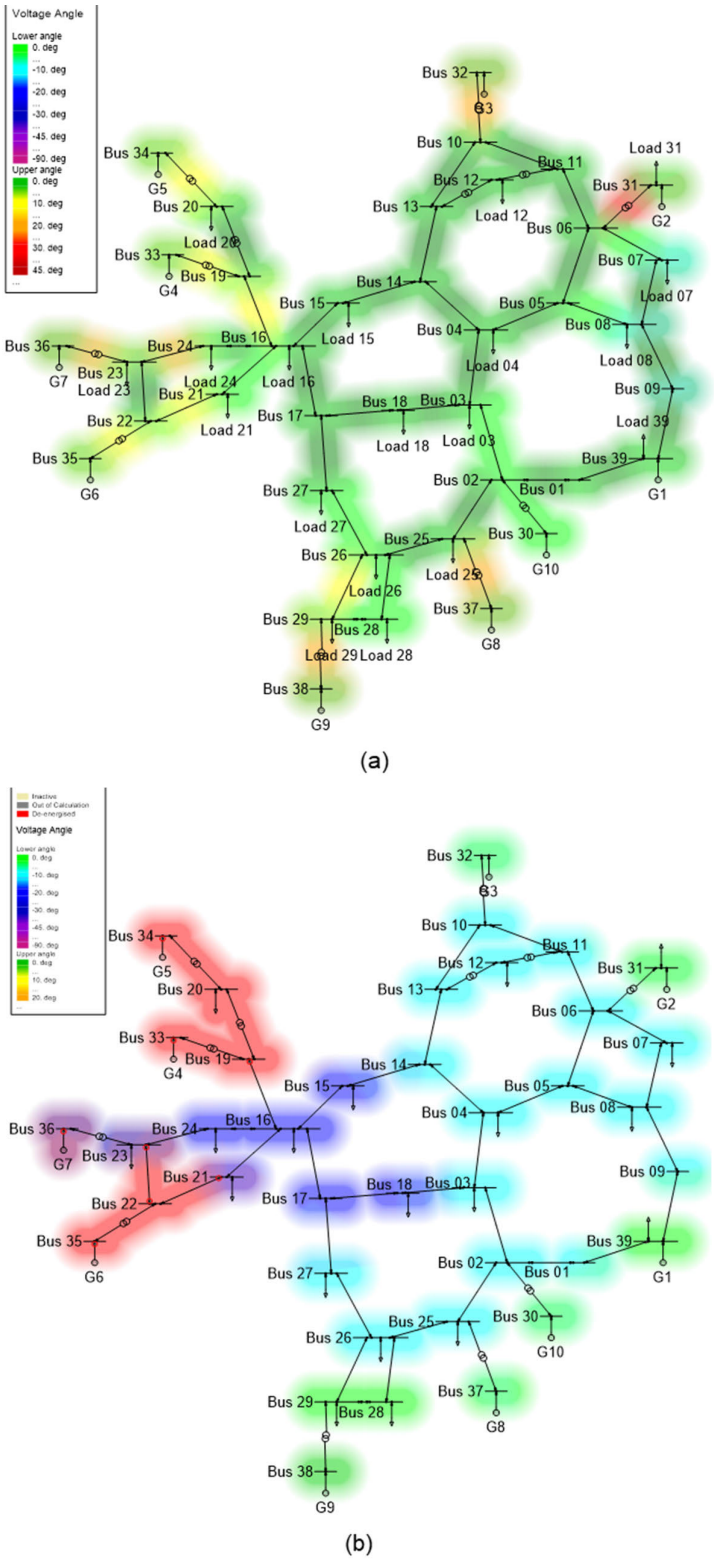
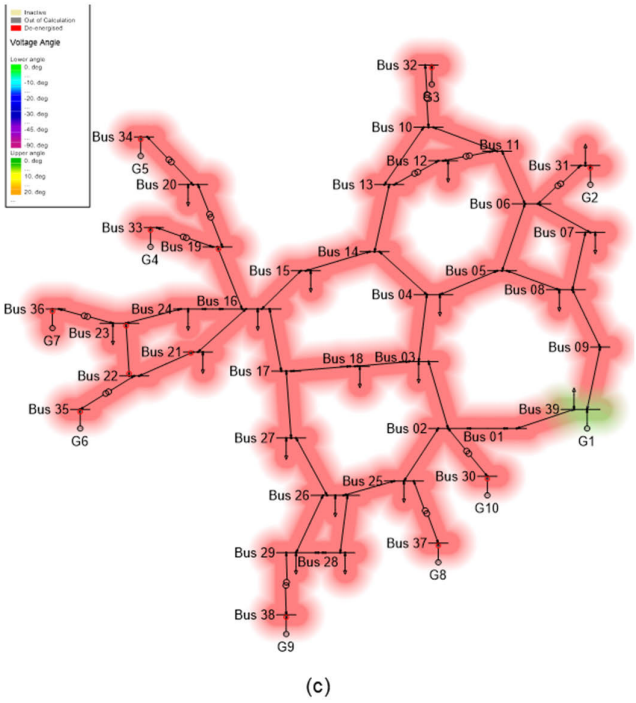


FIGURE 11. Propagation of cyber induced cascading failure on the IEEE 39-bus test system, visualised as heat maps of voltage angles. Figs. 11(a) , 11(b) and 11(c) depict start of simulation (0s), 15s and 20s simulation time, respectively. At the start of the simulation, most areas are healthy, i.e., with minimal voltage angle deviations (shown in green). Over the course of the cyber attack simulation, areas in red are de-energised, while the areas indicated by purple and blue suffer from power swings with significant variations in voltage angles, in excess of 30 to 40 degrees. The cyber attack results in a blackout in a matter of 20s with ∼5.2 GW load lost.



(c)

FIGURE 11. *(Continued.)* **Propagation of cyber induced cascading failure on the IEEE 39-bus test system, visualised as heat maps of voltage angles. Figs. 11(a) , 11(b) and 11(c) depict start of simulation (0s), 15s and 20s simulation time, respectively. At the start of the simulation, most areas are healthy, i.e., with minimal voltage angle deviations (shown in green). Over the course of the cyber attack simulation, areas in red are de-energised, while the areas indicated by purple and blue suffer from power swings with significant variations in voltage angles, in excess of 30 to 40 degrees. The cyber attack results in a blackout in a matter of 20s with ∼5.2 GW load lost.**

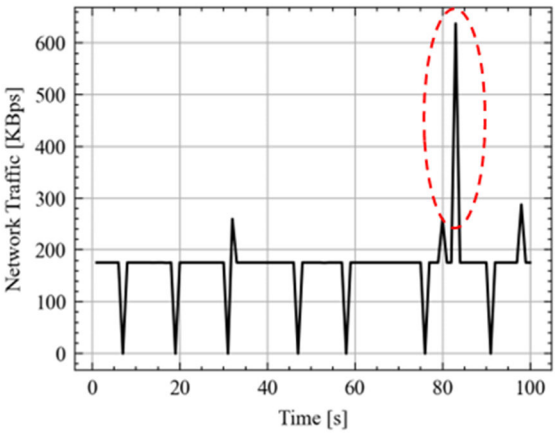


FIGURE 12. **Illustration of cyber attack via change in network traffic of substation 6 gateway.**

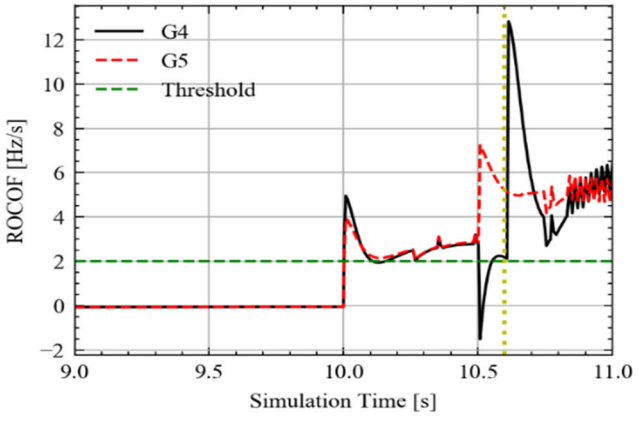


FIGURE 13. **ROCOF trip of generators G4 and G5. Protection setting limit is 2 Hz/s over 500 ms.**

C. CASCADING FAILURES AND BLACKOUT

Eventually, the generator targeted by the cyber attack, i.e., G6 is disconnected due to voltage instability around 13s, as predefined voltage limits (1.1 p.u) are exceeded. This is illustrated in Figure 15. Therefore, the system is heavily stressed and the last remaining generator G7 in the vicinity of the attack location cannot cover all the loads and is islanded by ROCOF protection at 13.28s. This results in major system-wide frequency and voltage instabilities due to the loss of multiple elements. Consequently, system frequency is severely affected due to the prolonged power mismatch, prompting emergency under frequency load shedding, as shown through Figure 16. Following, multiple lines are tripped by zone- distance protection overreach. Thus, the

TABLE 9. Sequence of cascading failures due to cyber attack.

No.	Time	Event
1.	0s	Start of simulation.
2.	5s	Spoofing cyber attack on substation 5. Generator G6 AVR set point increased by 10%
3.	10s	Cyber attack at substation 7. Line 19-16 maliciously disconnected.
4.	10.5-10.6s	Generators G4 and G5 are islanded and disconnected by ROCOF protection.
5.	11.2-12.7s	Lines 21-22, 22-23, and 23-24 trip due to distance protection.
6.	12.8s	Generators G2 and G6 are disconnected by overvoltage protection.
7.	13.27s	Generator G7 is islanded and disconnected by ROCOF protection.
8.	14s-14.2s	Under frequency load shedding of 6.7% at all loads.
9.	14.28s	Line 02-03 trips due to distance protection.
10.	14.3-17.3s	Load shedding
11.	17.31s	Multiple lines trip due to distance protection, i.e., lines 04-05, 10-13, and 13-14.
12.	17.52s	Line 01-39 disconnects due to distance protection.
13.	18.01s	Generator G9 is tripped by ROCOF protection.
14.	20s	End of simulation. Cyber attacks result in a blackout with loss of load amounting to ~5250 MW.

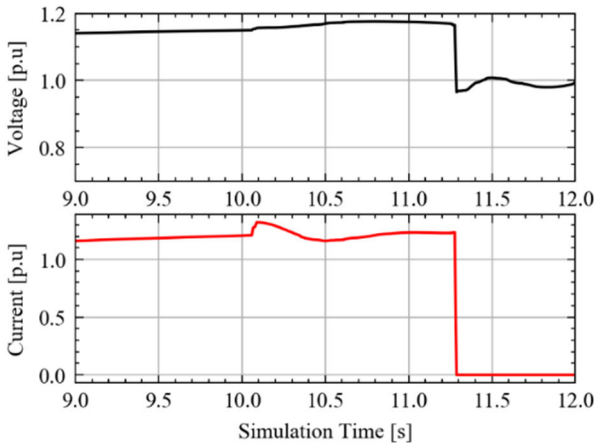


FIGURE 14. Under voltage at bus 21 and overcurrent on line 21-22, highlighting trip of zone 3 distance protection.

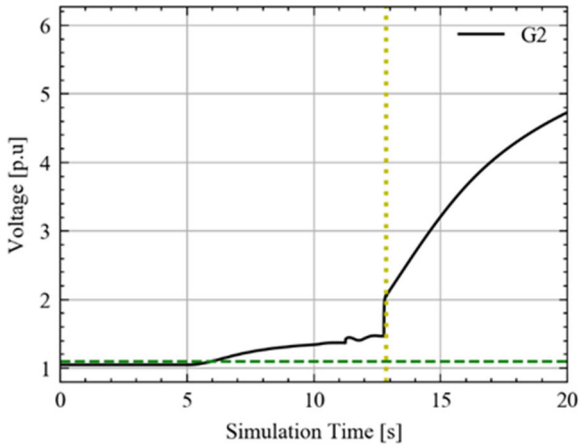


FIGURE 15. Over voltage trip of generator G2 at 12.8 s. Protection setting limit is 1.1 p.u as shown by the green dashed line.

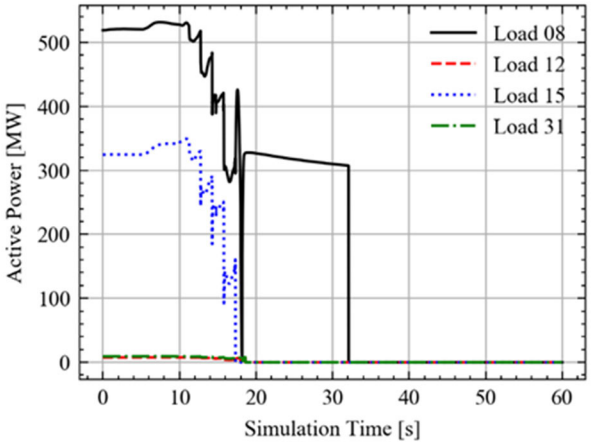


FIGURE 16. Load shedding and loss of load due to cyber attack.

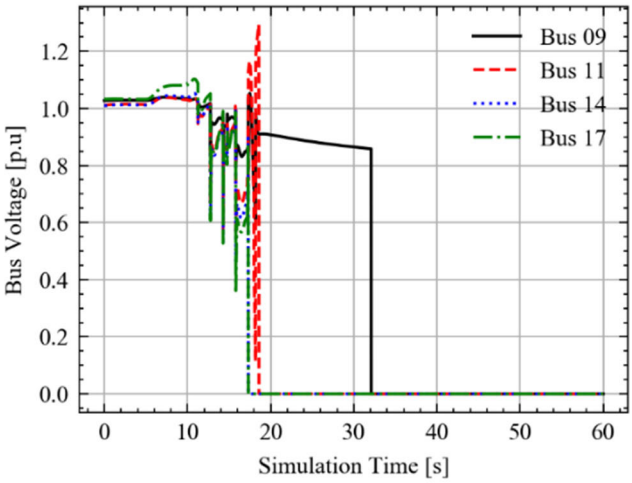


FIGURE 17. Voltage collapse caused by cyber attack.

system reaches a point of no return at ∼ 20s and the cyber attack results in a blackout with ∼5.2 GW load lost. The evolution of the cascade is better visualised through Figure 11 that illustrates variations in voltage angles over the course of the simulation. Areas in red are de-energised, while the areas indicated in purple and blue suffer from power swings

with significant variations in voltage angles, in excess of 30 to 40 degrees. The entire sequence of events is summarised in Table 8. As observed, the cyber attacks trigger multiple critical cyber-physical factors and influence the cascading failure mechanism. This results in a blackout, thereby confirming our hypothesis.

VII. CONCLUSION AND OUTLOOK

As power systems become increasingly digitalised, the importance of cyber security cannot be overstated. With the looming threat of cyber attacks on power grids, in this work, we presented a fundamental analysis of the link between the power system cascading failure mechanism and cyber security. This was achieved through a comprehensive state-of-the-art review of major historic power system blackouts caused by physical disturbances. Based on this, critical cyber-physical factors that enable and influence the cascading failure mechanism were identified. Furthermore, hypothetical cyber-physical attack scenarios were developed to analyse the effects of the critical factors through different cyber attack vectors. A systemic evaluation of the scenarios revealed how cyber attacks can initiate cascading failures, leading to a widespread blackout. A synthetic case study and software-based indicate that cyber attacks can not only cause, but also accelerate the cascading failure mechanism.

Our findings in this paper highlight the direct link between cyber attacks and their influence on critical factors in the cascading failure mechanism. Based on this study, our future work will focus on developing an analytical method to prove how cyber attacks can cause cascading failures and accelerate them compared to physical disturbances. Through this, we will analyse how cyber attacks have the potential to cause widespread power outages. Furthermore, impact of social factors such as operator actions and decisions on cascading failures can also be researched. This research will emphasise the urgent need for robust cyber security measures to safeguard power systems from malicious cyber threats and mitigate their potentially catastrophic impact. This can aid in securing and ensuring cyber resilience of future power systems.

REFERENCES

[1] S. Imai, D. Novosel, D. Karlsson, and A. Apostolov, "Unexpected consequences: Global blackout experiences and preventive solutions," *IEEE Power Energy Mag.*, vol. 21, no. 3, pp. 16–29, May 2023.

[2] H. M. Merrill, M. A. Hossain, and M. Bodson, "Nipping blackouts in the bud: Introducing a novel cascading failure network," *IEEE Power Energy Mag.*, vol. 18, no. 4, pp. 64–75, Jul. 2020.

[3] M. Mahzarnia, M. P. Moghaddam, P. T. Baboli, and P. Siano, "A review of the measures to enhance power systems resilience," *IEEE Syst. J.*, vol. 14, no. 3, pp. 4059–4070, Sep. 2020.

[4] P. Pourbeik, P. S. Kundur, and C. W. Taylor, "The anatomy of a power grid blackout," *IEEE Power Energy Mag.*, vol. 4, no. 5, pp. 22–29, Sep./Oct. 2006.

[5] M. Noebels, R. Preece, and M. Panteli, "AC cascading failure model for resilience analysis in power networks," *IEEE Syst. J.*, vol. 16, no. 1, pp. 374–385, Mar. 2022.

[6] R. Baldick, B. Chowdhury, I. Dobson, Z. Dong, B. Gou, D. Hawkins, H. Huang, M. Joung, D. Kirschen, F. Li, and J. Li, "Initial review of methods for cascading failure analysis in electric power transmission systems," in *Proc. IEEE Power Energy Soc. Gen. Meeting*, Jul. 2008, pp. 1–8.

[7] D. E. Whitehead, K. Owens, D. Gammel, and J. Smith, "Ukraine cyber-induced power outage: Analysis and practical mitigation strategies," in *Proc. 70th Annu. Conf. Protective Relay Eng. (CPRE)*, Apr. 2017, pp. 1–8.

[8] Recorded Future. (2022). *Continued Targeting of Indian Power Grid Assets by Chinese State-Sponsored Activity Group*. Accessed: Dec. 7, 2022. [Online]. Available: https://go.recordedfuture.com/hubfs/reports/ta-2022-0406.pdf

[9] C.-C. Liu, A. Stefanov, J. Hong, and P. Panciatici, "Intruders in the grid," *IEEE Power Energy Mag.*, vol. 10, no. 1, pp. 58–66, Jan. 2012.

[10] C. Peng, H. Sun, M. Yang, and Y.-L. Wang, "A survey on security communication and control for smart grids under malicious cyber attacks," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 49, no. 8, pp. 1554–1569, Aug. 2019.

[11] S. Paul, F. Ding, K. Utkarsh, W. Liu, M. J. O'Malley, and J. Barnett, "On vulnerability and resilience of cyber-physical power systems: A review," *IEEE Syst. J.*, vol. 16, no. 2, pp. 2367–2378, Jun. 2022.

[12] I. A. Khan, D. Pi, N. Khan, Z. U. Khan, Y. Hussain, A. Nawaz, and F. Ali, "A privacy-conserving framework based intrusion detection method for detecting and recognizing malicious behaviours in cyber-physical power networks," *Appl. Intell.*, vol. 51, pp. 7306–7321, Feb. 2021.

[13] H. Zhang, B. Liu, and H. Wu, "Smart grid cyber-physical attack and defense: A review," *IEEE Access*, vol. 9, pp. 29641–29659, 2021.

[14] S. Colabianchi, F. Costantino, G. D. Gravio, F. Nonino, and R. Patriarca, "Discussing resilience in the context of cyber physical systems," *Comput. Ind. Eng.*, vol. 160, Oct. 2021, Art. no. 107534.

[15] M. Abdelmalak, V. Venkataramanan, and R. Macwan, "A survey of cyber-physical power system modeling methods for future energy systems," *IEEE Access*, vol. 10, pp. 99875–99896, 2022.

[16] M. M. Hossain and C. Peng, "Cyber-physical security for on-going smart grid initiatives: A survey," *IET Cyber-Phys. Syst., Theory Appl.*, vol. 5, pp. 233–244, Mar. 2020.

[17] A. Clark and S. Zonouz, "Cyber-physical resilience: Definition and assessment metric," *IEEE Trans. Smart Grid*, vol. 10, no. 2, pp. 1671–1684, Mar. 2019.

[18] L. D. Valdez, L. Shekhtman, C. E. La Rocca, X. Zhang, S. V. Buldyrev, P. A. Trunfio, L. A. Braunstein, and S. Havlin, "Cascading failures in complex networks," *J. Complex Netw.*, vol. 8, no. 2, Apr. 2020, Art. no. cnaa013.

[19] R. V. Yohanandhan, R. M. Elavarasan, P. Manoharan, and L. Mihet-Popa, "Cyber-physical power system (CPPS): A review on modeling, simulation, and analysis with cyber security applications," *IEEE Access*, vol. 8, pp. 151019–151064, 2020.

[20] A. Salehpour, I. Al-Anbagi, K.-C. Yow, and X. Cheng, "Modeling cascading failures in coupled smart grid networks," *IEEE Access*, vol. 10, pp. 81054–81070, 2022.

[21] R. Meyur, A. Vullikanti, M. V. Marathe, A. Pal, M. Youssef, and V. Centeno, "Cascading effects of targeted attacks on the power grid," in *Complex Networks and Their Applications VII* (Studies in Computational Intelligence), vol. 812, L. Aiello, C. Cherifi, H. Cherifi, R. Lambiotte, P. Lió, and L. Rocha, Eds. Cham, Switzerland: Springer, 2019, doi: 10.1007/978-3-030-05411-3_13.

[22] M. Z. Islam, Y. Lin, V. M. Vokkarane, and V. Venkataramanan, "Cyber-physical cascading failure and resilience of power grid: A comprehensive review," *Frontiers Energy Res.*, vol. 1, Feb. 2023, Art. no. 1095303.

[23] M. Ghiasi, T. Niknam, Z. Wang, M. Mehrandezh, M. Dehghani, and N. Ghadimi, "A comprehensive review of cyber-attacks and defense mechanisms for improving security in smart grid energy systems: Past, present and future," *Electr. Power Syst. Res.*, vol. 215, pp. 108975–108985, Feb. 2023.

[24] L. Xu, Q. Guo, Y. Sheng, S. M. Muyeen, and H. Sun, "On the resilience of modern power systems: A comprehensive review from the cyber-physical perspective," *Renew. Sustain. Energy Rev.*, vol. 152, pp. 111642–111672, Dec. 2021.

[25] S. Corsi and C. Sabelli, "General blackout in Italy Sunday September 28, 2003, h. 03:28:00," in *Proc. IEEE Power Eng. Soc. Gen. Meeting*, Jul. 2004, pp. 1691–1702.

[26] (Aug. 2004). *Final Report of the Investigation Committee on the September 3 Blackout in Italy*. UCTE. Accessed: Dec 7, 2022. [Online]. Available: http://ns2.rae.gr/old/cases/C13/italy/UCTE_rept.pdf

[27] G. Andersson, P. Donalek, R. Farmer, N. Hatziargyriou, I. Kamwa, P. Kundur, N. Martins, J. Paserba, P. Pourbeik, J. Sanchez-Gasca, R. Schulz, A. Stankovic, C. Taylor, and V. Vittal, "Causes of the 2003 major grid blackouts in North America and Europe, and recommended means to improve system dynamic performance," *IEEE Trans. Power Syst.*, vol. 20, no. 4, pp. 1922–1928, Nov. 2005.

[28] (2003). *U.S.-Canada Power System Outage Task Force: Causes of the August 14th Blackout in the United States and Canada*. Accessed: Dec. 7, 2022. [Online]. Available: https://www.energy.gov/oe/downloads/us-canada-power-system-outage-task-force-final-report-implementation-task-force

[29] J. W. Bialek, "Why has it happened again? Comparison between the UCTE blackout in 2006 and the blackouts of 2003," in *Proc. IEEE Power Tech.*, Jul. 2007, pp. 51–56.

[30] V. Rampurkar, P. Pentayya, H. A. Mangalvedekar, and F. Kazi, "Cascading failure analysis for Indian power grid," *IEEE Trans. Smart Grid*, vol. 7, no. 4, pp. 1951–1960, Jul. 2016.

[31] L. L. Lai, H. T. Zhang, S. Mishra, D. Ramasubramanian, C. S. Lai, and F. Y. Xu, "Lessons learned from July 2012 Indian blackout," in *Proc. 9th IET Int. Conf. Adv. Power Syst. Control, Operation Manage. (APSCOM)*, Nov. 2012, pp. 1–6.

[32] J. J. Romero, "Blackouts illuminate India's power problems," *IEEE Spectr.*, vol. 49, no. 10, pp. 11–12, Oct. 2012.

[33] Project Group Turkey. (Apr. 2016). *Report on Blackout in Turkey on 31 March 2015*. Accessed: Dec 7, 2022. [Online]. Available: https://docs.entsoe.eu/dataset/ops-report-turkey-blackout-march-2015/resource/08fb8ed2-5b40-4b94-90b0-5682bcd618cb

[34] B. Schäfer and G. C. Yalcin, "Dynamical modeling of cascading failures in the Turkish power grid," *Chaos, Interdiscipl. J. Nonlinear Sci.*, vol. 29, no. 9, Sep. 2019, Art. no. 093134.

[35] S. Wilde. *9 August 2019 Power Outage Report*. Accessed: Dec. 7, 2022. [Online]. Available: https://www.ofgem.gov.uk/sites/default/files/docs/2020/01/9_august_2019_power_outage_report.pdf

[36] National Electric Power Regulatory Authority (NEPRA). (Feb. 2021). *Inquiry Report Regarding Total Power System Collapse*. Accessed: Dec 7, 2022. [Online]. Available: https://www.nepra.org.pk/Standards/2021/Inquiry%20Report%20regarding%20total%20power%20system%20collapse%20on%2009%20Jan%202021.PDF

[37] I. Dobson and D. E. Newman, "Cascading blackout overall structure and some implications for sampling and mitigation," *Int. J. Electr. Power Energy Syst.*, vol. 86, pp. 29–32, Mar. 2017.

[38] Z. Ma, C. Shen, F. Liu, and S. Mei, "Fast screening of vulnerable transmission lines in power grids: A PageRank-based approach," *IEEE Trans. Smart Grid*, vol. 10, no. 2, pp. 1982–1991, Mar. 2019.

[39] D. Pal, B. Mallikarjuna, P. Gopakumar, M. J. B. Reddy, B. K. Panigrahi, and D. K. Mohanta, "Probabilistic study of undervoltage load shedding scheme to mitigate the impact of protection system hidden failures," *IEEE Syst. J.*, vol. 14, no. 1, pp. 862–869, Mar. 2020.

[40] J. De La Ree, Y. Liu, L. Mili, A. G. Phadke, and L. DaSilva, "Catastrophic failures in power systems: Causes, analyses, and countermeasures," *Proc. IEEE*, vol. 93, no. 5, pp. 956–964, May 2005.

[41] L. Liu, H. Wu, L. Li, D. Shen, F. Qian, and J. Liu, "Cascading failure pattern identification in power systems based on sequential pattern mining," *IEEE Trans. Power Syst.*, vol. 36, no. 3, pp. 1856–1866, May 2021.

[42] R. Yao, S. Huang, K. Sun, F. Liu, X. Zhang, and S. Mei, "A multi-timescale quasi-dynamic model for simulation of cascading outages," *IEEE Trans. Power Syst.*, vol. 31, no. 4, pp. 3189–3201, Jul. 2016.

[43] *Officials Search for Answers in Extensive Brazil Blackout*. New York Times, New York, NY, USA. Accessed: Dec. 7, 2022. [Online]. Available: https://www.nytimes.com/2009/11/12/world/americas/12brazil.html

[44] R. Yan, N.-A. Masood, T. K. Saha, F. Bai, and H. Gu, "The anatomy of the 2016 South Australia blackout: A catastrophic event in a high renewable network," *IEEE Trans. Power Syst.*, vol. 33, no. 5, pp. 5374–5388, Sep. 2018.

[45] Wall Street Journal (WSJ). *New York City Blackout Caused by Power Grid's Protection System Failing*. Accessed: Dec. 7, 2022. [Online]. Available: https://www.wsj.com/articles/cuomo-blasts-con-edison-for-role-in-nyc-blackout-11563220715

[46] British Broadcasting Corporation (BBC). *Indonesia Blackout: Huge Outage Hits Jakarta and Surrounding Area*. Accessed: Dec. 7, 2022. [Online]. Available: https://www.bbc.com/news/world-asia-49227033

[47] TIME. *5 Million Americans Have Lost Power From Texas to North Dakota After Devastating Winter Storm*. Accessed: Dec. 7, 2022. [Online]. Available: https://time.com/5939633/texas-power-outage-blackouts/#:~:text=5%20Million%20Americans%20Have%20Lost,on%20Feb.%2015%2C%202021

[48] Aljazeera. *Power Back in Bangladesh After Grid Glitch Forces 7-Hour Blackout*. Accessed: Dec. 7, 2022. [Online]. Available: https://www.aljazeera.com/news/2022/10/5/power-back-in-bangladesh-after-grid-glitch-forces-7-hour-blackout

[49] H. H. Alhelou, M. E. Hamedain-Golshan, T. C. Njenda, and P. Siano, "A survey on power system blackout and cascading events: Research motivations and challenges," *Energies*, vol. 12, no. 4, pp. 1–28, 2019.

[50] H. Guo, C. Zheng, H. H.-C. Iu, and T. Fernando, "A critical review of cascading failure analysis and modeling of power system," *Renew. Sustain. Energy Rev.*, vol. 80, pp. 9–22, Dec. 2017.

[51] C.-W. Ten, K. Yamashita, Z. Yang, A. V. Vasilakos, and A. Ginter, "Impact assessment of hypothesized cyberattacks on interconnected bulk power systems," *IEEE Trans. Smart Grid*, vol. 9, no. 5, pp. 4405–4425, Sep. 2018.

[52] M. Noebels, I. Dobson, and M. Panteli, "Observed acceleration of cascading outages," *IEEE Trans. Power Syst.*, vol. 36, no. 4, pp. 3821–3824, Jul. 2021.

[53] S. Amini, F. Pasqualetti, and H. Mohsenian-Rad, "Dynamic load altering attacks against power system stability: Attack models and protection schemes," *IEEE Trans. Smart Grid*, vol. 9, no. 4, pp. 2862–2872, Jul. 2018.

[54] A. A. Jahromi, A. Kemmeugne, D. Kundur, and A. Haddadi, "Cyber-physical attacks targeting communication-assisted protection schemes," *IEEE Trans. Power Syst.*, vol. 35, no. 1, pp. 440–450, Jan. 2020.

[55] F. Xue, E. Bompard, T. Huang, L. Jiang, S. Lu, and H. Zhu, "Interrelation of structure and operational states in cascading failure of overloading lines in power grids," *Phys. A, Stat. Mech. Appl.*, vol. 482, pp. 728–740, Sep. 2017.

[56] P. S. Kundur and O. P. Malik, *Power System Stability and Control*, 2nd ed. New York, NY, USA: McGraw-Hill, Jun. 2022.

[57] A. M. Abdullah and K. Butler-Purry, "Distance protection zone 3 misoperation during system wide cascading events: The problem and a survey of solutions," *Electr. Power Syst. Res.*, vol. 154, pp. 151–159, Jan. 2018.

[58] B. Chen, K. L. Butler-Purry, S. Nuthalapati, and D. Kundur, "Network delay caused by cyber attacks on SVC and its impact on transient stability of smart grids," in *Proc. IEEE PES Gen. Meeting | Conf. Expo.*, Jul. 2014, pp. 1–5.

[59] Y. Isozaki, S. Yoshizawa, Y. Fujimoto, H. Ishii, I. Ono, T. Onoda, and Y. Hayashi, "Detection of cyber attacks against voltage control in distribution power grids with PVs," *IEEE Trans. Smart Grid*, vol. 7, no. 4, pp. 1824–1835, Jul. 2016.

[60] F. Li, Q. Li, J. Zhang, J. Kou, J. Ye, W. Song, and H. A. Mantooth, "Detection and diagnosis of data integrity attacks in solar farms based on multilayer long short-term memory network," *IEEE Trans. Power Electron.*, vol. 36, no. 3, pp. 2495–2498, Mar. 2021.

[61] M. A. Rahman, M. S. Rana, and H. R. Pota, "Mitigation of frequency and voltage disruptions in smart grid during cyber-attack," *J. Control, Autom. Electr. Syst.*, vol. 31, no. 2, pp. 412–421, Apr. 2020.

[62] A. Farraj, E. Hammad, and D. Kundur, "A cyber-physical control framework for transient stability in smart grids," *IEEE Trans. Smart Grid*, vol. 9, no. 2, pp. 1205–1215, Mar. 2018.

[63] M. F. M. Arani, A. Abiri Jahromi, D. Kundur, and M. Kassouf, "Modeling and simulation of the Aurora attack on microgrid point of common coupling," in *Proc. 7th Workshop Modeling Simulation Cyber-Phys. Energy Syst. (MSCPES)*, Apr. 2019, pp. 1–6.

[64] M. Zhou, C. Liu, A. A. Jahromi, D. Kundur, J. Wu, and C. Long, "Revealing vulnerability of N-1 secure power systems to coordinated cyber-physical attacks," *IEEE Trans. Power Syst.*, vol. 38, no. 2, pp. 1044–1057, Mar. 2023.

[65] P. Du and J. Matevosyan, "Forecast system inertia condition and its impact to integrate more renewables," *IEEE Trans. Smart Grid*, vol. 9, no. 2, pp. 1531–1533, Mar. 2018.

[66] Y. Wu, Z. Wei, J. Weng, X. Li, and R. H. Deng, "Resonance attacks on load frequency control of smart grids," *IEEE Trans. Smart Grid*, vol. 9, no. 5, pp. 4490–4502, Sep. 2018.

[67] A. Dabrowski, J. Ullrich, and E. R. Weippl, "Grid Shock: Coordinated load-changing attacks on power grids the non-smart power grid is vulnerable to cyber attacks as well," in *Proc. 33rd Annu. Comput. Secur. Appl. Conf.*, Nov. 2017, pp. 303–314.

[68] G. Raman, B. AlShebli, M. Waniek, T. Rahwan, and J. C.-H. Peng, "How weaponizing disinformation can bring down a city's power grid," *PLoS One*, vol. 15, no. 8, pp. 1–10, Aug. 2020.

[69] X. Zhang, D. Liu, C. Zhan, and C. K. Tse, "Effects of cyber coupling on cascading failures in power systems," *IEEE J. Emerg. Sel. Topics Circuits Syst.*, vol. 7, no. 2, pp. 228–238, Jun. 2017.

[70] M. X. Ma and A. Lahmadi, "On the impact of synchronization attacks on distributed and cooperative control in microgrid systems," in *Proc. IEEE Int. Conf. Commun., Control, Comput. Technol. Smart Grids (SmartGridComm)*, Oct. 2018, pp. 1–6.

[71] I. L. Carreño, A. Scaglione, A. Zlotnik, D. Deka, and K. Sundar, "An adversarial model for attack vector vulnerability analysis on power and gas delivery operations," *Electr. Power Syst. Res.*, vol. 189, Dec. 2020, Art. no. 106777.

[72] L. Chen, D. Yue, C. Dou, J. Chen, and Z. Cheng, "Evaluation of cyber-physical power systems in cascading failure: Node vulnerability and systems connectivity," *IET Gener., Transmiss. Distrib.*, vol. 14, no. 7, pp. 1197–1206, Apr. 2020.

[73] P. Wang and M. Govindarasu, "Multi-agent based attack-resilient system integrity protection for smart grid," *IEEE Trans. Smart Grid*, vol. 11, no. 4, pp. 3447–3456, Jul. 2020.

[74] R. Langner, "Stuxnet: Dissecting a cyberwarfare weapon," *IEEE Secur. Privacy*, vol. 9, no. 3, pp. 49–51, May 2011.

[75] Deutsche Windtechnik. *Cyber attack on Deutsche Windtechnik*. Accessed: Dec. 7, 2022. [Online]. Available: https://www.deutsche-windtechnik.com/en/news/details/cyber-attack-on-deutsche-windtechnik/

[76] CERT-UA. *Cyber Attack of the Sandworm Group (UAC-0082) on Energy Facilities of Ukraine Using Malware Industroyer2 and CaddyWiper*. Accessed: Dec. 7, 2022. [Online]. Available: https://cert.gov.ua/article/39518

[77] R. Liu, C. Vellaithurai, S. S. Biswas, T. T. Gamage, and A. K. Srivastava, "Analyzing the cyber-physical impact of cyber events on the power grid," *IEEE Trans. Smart Grid*, vol. 6, no. 5, pp. 2444–2453, Sep. 2015.

[78] C.-C. Sun, A. Hahn, and C.-C. Liu, "Cyber security of a power grid: State-of-the-art," *Int. J. Electr. Power Energy Syst.*, vol. 99, pp. 45–56, Jul. 2018.

[79] A. Volkova, M. Niedermeier, R. Basmadjian, and H. de Meer, "Security challenges in control network protocols: A survey," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 1, pp. 619–639, 1st Quart., 2019.

[80] S. Hussain, J. Hernandez Fernandez, A. K. Al-Ali, and A. Shikfa, "Vulnerabilities and countermeasures in electrical substations," *Int. J. Crit. Infrastruct. Protection*, vol. 33, Jun. 2021, Art. no. 100406.

[81] J. Hoyos, M. Dehus, and T. X. Brown, "Exploiting the GOOSE protocol: A practical attack on cyber-infrastructure," in *Proc. IEEE Globe Work*, Dec. 2012, pp. 1508–1513.

[82] N. Kush, E. Ahmed, M. Branagan, and E. Foo, "Poisoned GOOSE: Exploiting the GOOSE protocol," in *Proc. Australas. Inf. Secur. Conf. (ACSW-AISC)*, Jan. 2014, pp. 17–22.

[83] V. S. Rajkumar, M. Tealane, A. Stefanov, and P. Palensky, "Cyber attacks on protective relays in digital substations and impact analysis," in *Proc. 8th Workshop Modeling Simulation Cyber-Phys. Energy Syst. (MSCPES)*, Apr. 2020, pp. 1–6.

[84] J. Zhang, Z. Chu, L. Sankar, and O. Kosut, "Can attackers with limited information exploit historical data to mount successful false data injection attacks on power systems?" *IEEE Trans. Power Syst.*, vol. 33, no. 5, pp. 4775–4786, Sep. 2018.

[85] D. Mukherjee, "Data-driven false data injection attack: A low-rank approach," *IEEE Trans. Smart Grid*, vol. 13, no. 3, pp. 2479–2482, May 2022.

[86] S. Lakshminarayana, A. Kammoun, M. Debbah, and H. V. Poor, "Data-driven false data injection attacks against power grids: A random matrix approach," *IEEE Trans. Smart Grid*, vol. 12, no. 1, pp. 635–646, Jan. 2021.

[87] V. C. Nikolaidis, E. Papanikolaou, and A. S. Safigianni, "A communication-assisted overcurrent protection scheme for radial distribution systems with distributed generation," *IEEE Trans. Smart Grid*, vol. 7, no. 1, pp. 114–123, Jan. 2016.

[88] *IEEE Guide for Power System Protective Relay Applications Over Digital Communication Channels*, Standard IEEE Std C37.236-2013, 2013, pp. 1–84.

[89] *IEEE Guide for Protective Relay Applications to Transmission Lines*, Standard IEEE Std PC37.113/D7.0, Aug. 2014, pp. 1–40.

[90] A. Ahmed, V. V. G. Krishnan, S. A. Foroutan, M. Touhiduzzaman, C. Rublein, A. Srivastava, Y. Wu, A. Hahn, and S. Suresh, "Cyber physical security analytics for anomalies in transmission protection systems," *IEEE Trans. Ind. Appl.*, vol. 55, no. 6, pp. 6313–6323, Nov. 2019.

[91] X. Liu, M. Shahidehpour, Z. Li, X. Liu, Y. Cao, and Z. Li, "Power system risk assessment in cyber attacks considering the role of protection systems," *IEEE Trans. Smart Grid*, vol. 8, no. 2, pp. 572–580, Mar. 2017.

[92] J. Hong, R. F. Nuqui, A. Kondabathini, D. Ishchenko, and A. Martin, "Cyber attack resilient distance protection and circuit breaker control for digital substations," *IEEE Trans. Ind. Informat.*, vol. 15, no. 7, pp. 4332–4341, Jul. 2019.

[93] A. Ameli, A. Hooshyar, and E. F. El-Saadany, "Development of a cyber-resilient line current differential relay," *IEEE Trans. Ind. Informat.*, vol. 15, no. 1, pp. 305–318, Jan. 2019.

[94] N. Costilla-Enriquez and Y. Weng, "Attack power system state estimation by implicitly learning the underlying models," *IEEE Trans. Smart Grid*, vol. 14, no. 1, pp. 649–662, Jan. 2023.

[95] M. Mohammadpourfard, Y. Weng, A. Khalili, I. Genc, A. Shefaei, and B. Mohammadi-Ivatloo, "Cyber-physical attack conduction and detection in decentralized power systems," *IEEE Access*, vol. 10, pp. 29277–29286, 2022.

VETRIVEL SUBRAMANIAM RAJKUMAR (Student Member, IEEE) received the B.Eng. degree in electrical engineering from Anna University, India, in 2013, and the M.Sc. degree in electrical engineering from the Delft University of Technology, The Netherlands, in 2019. He is currently a Doctoral Researcher with the Intelligent Electrical Power Grids Group, Department of Electrical Sustainable Technology, Delft University of Technology. His research interests include cyber security and resilience for power grids.

ALEXANDRU ŞTEFANOV (Member, IEEE) received the M.Sc. degree from the Politehnica University of Bucharest, Romania, in 2011, and the Ph.D. degree from University College Dublin, Ireland, in 2015. He is an Assistant Professor of intelligent electrical power grids with TU Delft, The Netherlands. He is also the Director of the Control Room of the Future (CRoF) Technology Centre. His research interests include cyber security for power grids, resilience of cyber-physical systems, and next generation grid operation. He holds the professional title of Chartered Engineer from Engineers Ireland.

ALFAN PRESEKAL (Member, IEEE) received the B.Eng. degree in computer engineering from Universitas Indonesia, in 2014, and the M.Sc. degree in secure software system from Imperial College, London, U.K., in 2016. He is currently pursuing the Ph.D. degree with the Department of Electrical Sustainable Energy, Delft University of Technology, The Netherlands. He was a Junior Lecturer with the Department of Electrical Engineering, Universitas Indonesia, from 2017 to 2019. He participated in an Exchange Research Program with the Department of Information and Communication Engineering, Tokyo Institute of Technology, from 2012 to 2013. His main research interests include cyber security, cyber-physical systems, and artificial intelligence for power system applications.

PETER PALENSKY (Senior Member, IEEE) received the M.Sc. degree in electrical engineering and the Ph.D. and Habilitation degrees from the Vienna University of Technology, Austria, in 1997, 2001, and 2015, respectively. He has co-founded Envidatec, a German startup on energy management and analytics. He joined the Lawrence Berkeley National Laboratory, Berkeley, CA, USA, as a Researcher, and the University of Pretoria, South Africa, in 2008. In 2009, he was appointed as the Head of the Business Unit on Sustainable Building Technologies, Austrian Institute of Technology (AIT), and later the first Principle Scientist of complex energy systems. In 2014, he was appointed as a Full Professor of intelligent electric power grids with TU Delft. His research interests include energy automation networks, smart grids, and modeling intelligent energy systems. He is active in international committees, such as ISO and CEN. He serves as an IEEE IES AdCom Member-at-Large in various functions for IEEE. He is also the Editor-in-Chief of *IEEE Industrial Electronics Magazine* and an associate editor of several other IEEE publications and regularly organizes IEEE conferences.

JOSÉ LUIS RUEDA TORRES (Senior Member, IEEE) received the Diploma degree (cum laude) in electrical engineering from Escuela Politécnica Nacional, Quito, Ecuador, in 2004, and the Ph.D. degree in electrical engineering from the National University of San Juan, San Juan, Argentina, in 2009, obtaining the highest mark 'Sobresaliente' (Outstanding). He is currently an Associate Professor, leading the Research Team on Stability, Control, and Optimization, Electrical Sustainable Energy Department, TU Delft, Delft, The Netherlands. From September 2003 to February 2005, he worked on industrial control systems and distribution network operation and planning in Ecuador. His research interests include the stability and control of power systems and multi-energy systems, power system operational planning and reliability, and probabilistic and artificial intelligence methods. He is currently a member of the Technical Committee on Power and Energy Systems and the International Federation of Automatic Control (IFAC), the Chairperson of the IEEE PES Working Group on Modern Heuristic Optimization, the Secretary of CIGRE JWG Evaluation of Voltage Stability Assessment Methodologies in Transmission Systems and the IEEE PES Intelligent Systems Subcommittee, and the Vice-Chair of IFAC TC 6.3 Power and Energy Systems on Social Media.