Dynamical Analysis of Power System Cascading Failures Caused by Cyber Attacks

Rajkumar, Vetrivel S.; Stefanov, Alexandru; Rueda, José L.; Palensky, Peter

DOI
10.1109/TII.2024.3372024

Publication date
2024

Document Version
Final published version

Published in
IEEE Transactions on Industrial Informatics

Citation (APA)
Rajkumar, V. S., Stefanov, A., Rueda, J. L., & Palensky, P. (2024). Dynamical Analysis of Power System Cascading Failures Caused by Cyber Attacks. *IEEE Transactions on Industrial Informatics*, *20*(6), 8807-8817. https://doi.org/10.1109/TII.2024.3372024

Dynamical Analysis of Power System Cascading Failures Caused by Cyber Attacks

Vetrivel S. Rajkumar, Alexandru Ştefanov, *Member, IEEE*, José Luis Rueda Torres, *Senior Member, IEEE*, and Peter Palensky, *Senior Member, IEEE*

***Abstract*—Cascading failures in power systems are extremely rare occurrences caused by a combination of multiple, low probability events. The looming threat of cyberattacks on power grids, however, may result in unprecedented large-scale cascading failures, leading to a blackout. Therefore, new analysis methods are needed to study such cyber induced phenomena. In this article, we propose a data-driven method for dynamical analysis of power system cascading failures caused by cyberattacks. We provide experimental proof on how attacks may accelerate the cascading failure mechanism, in comparison to historically observed blackouts. Using a dynamic power grid model, consisting of multiple, coordinated protection schemes, we define and analyze the point of no return in a cascading failure sequence by applying the Hilbert–Huang transform for time-frequency analysis. Numerical results indicate, cyberattacks may accelerate cascading failures at least by a factor of 3x. This is due to the excitation and non-damping of multiple frequency modes greater than 1 Hz in a short time span. The proposed method is tested using time domain simulations conducted through a modified IEEE 39-bus test system, which can simulate cascading outages using coordinated protection schemes.**

***Index Terms*—Blackout, cascading failures, cyberattacks, cyber security, power system dynamics.**

I. Introduction

THE ongoing energy transition and power grid digitalization has resulted in the convergence of information and operational technologies. While offering advanced monitoring and control capabilities, these developments have brought forth serious cyber security concerns [1], [2], [3]. Cyberattacks on power grids are a real modern-day threat with considerable ramifications. They are no longer a figment of imagination, considering recent real-world events. The most famous and well-known examples of cyberattacks targeting power grids are the attacks in Ukraine in 2015 and 2016. The former caused a power outage, directly affecting nearly 225 000 customers [4], while the latter employed an advanced malware, i.e., Industroyer, resulting in a loss of 200 MW of load in the distribution network [5]. More recently, on October 12, 2020, Mumbai, a major Indian metropolis, was affected by a power outage lasting over 12 hours that may be related to *"RedEcho,"* an active hacker group.

The attackers used sophisticated malware to target the regional control centre, in an active campaign lasting over six months. In April 2022, in Germany, a reported cyberattack caused malfunctions in the communication systems used for monitoring and control of 2000 wind turbines. All these incidents point to the urgency of addressing evolving challenges such as cyber security and resilience of power system operational technologies.

Historically, cascading failures in power systems are extremely rare occurrences caused by a combination of multiple, low probability events. However, the looming threat of cyberattacks on power grids may result in unprecedented large-scale cascading failures, leading to a blackout. Therefore, new analysis methods are needed to study such phenomena.

II. State-of-the-Art and Contributions

A. Related Work

Analysis of power system cascading failures and blackouts is extensively documented in the literature [6], [7], [8]. Most existing work focuses on steady-state methods, such as DC [9], [10], [11] and AC [12], [13] power flow models that capture overloading conditions and voltage violations. Given the complexity of the electrical power system, however, such methods only provide a partial view of the cascading failure mechanism. Furthermore, a major drawback of such methods is the inability to study nonlinear and dynamic phenomena that have been observed in real-world cascading failures. For example, loss of synchronism and voltage collapse. Other techniques include statistical methods based on historical data [14] and graph theory models to describe the generalized behavior of cascading effects [15], [16]. While offering broad mathematical and analytical insights, however, both methods are limited in capturing the power system physics.

In other related work, extensive research has been conducted with dynamic grid models to simulate system instability caused by large disturbances [17], [18], [19]. Such numerical studies, however, consider only a particular type of instability

Manuscript received 20 March 2023; revised 1 November 2023; accepted 24 February 2024. Date of publication 27 March 2024; date of current version 5 June 2024. This work was supported in part by the EU H2020 Project, ERIGrid 2.0 under Grant 870620 and in part by the DeSIRE Program of 4TU Centre for Resilience Engineering. Paper no. TII-23-1711. *(Corresponding author: Vetrivel S. Rajkumar.)*

The authors are with the Department of Electrical Sustainable Energy, Delft University of Technology, 2628 CD Delft, The Netherlands (e-mail: v.subramaniamrajkumar@tudelft.nl; a.i.stefanov@tudelft.nl; j.l.ruedatorres@tudelft.nl; p.palensky@tudelft.nl).

Color versions of one or more figures in this article are available at https://doi.org/10.1109/TII.2024.3372024.

Digital Object Identifier 10.1109/TII.2024.3372024

phenomena and just highlight when the power system becomes unstable, e.g., rotor swings and oscillations. Major cascading outages consist of two distinct phases [20]. The slow phase is in the order of a few minutes to hours, while the fast phase occurs in the order of a few milliseconds to seconds. In the latter, various nonlinear and dynamic phenomena dominate, e.g., transient, frequency, and voltage stability. Hence, research into dynamic modeling and RMS simulations of cascading failures has gained increased attention [19].

The study and analysis of cascading failures due to cyberattacks is a relatively emergent topic of research, in the wake of the cyberattacks in Ukraine in 2015 and 2016. The role and impact of cyberattacks on power system stability and cascading failures is discussed in [1]. The authors present a screening method for the initiating cyber events and perform dynamic simulations for the identified critical study cases. This article, however, stops when the power system is deemed unstable, thereby ignoring the sequence of cascading events. In other related work, Atat et al. [21] presents a cascading failure vulnerability analysis by studying the interdependence between cyber and physical layers. Similarly, Tu et al. [22] discusses vulnerability analysis of cyberphysical power systems considering cyberattacks using a percolation-based approach to quantify both system and component vulnerabilities. However, both these works do not study the cascading failure mechanism itself.

Closer to our work is the Markov-chain based dynamical probabilistic model developed in [23]. This model partially captures the dynamics of cascading failures in the power grid but does not analyze the point of no return (PNR) or global instability, which is the focus of our work. Multiple recent studies have been conducted to model and analyze cascading failures in smart grids [24], [25] based on power flow analysis. Such studies analyze the impact of line overloads or loss of equipment, but do not capture the dynamics of the fast-cascading failure mechanism. Hence, it can be summed up that limited work has been carried out in employing detailed dynamic RMS models with comprehensive and coordinated protection schemes for analysis of power system cascading failures caused by cyberattacks.

The work in [26] serves as the foundation for our article. The authors provide a comprehensive analysis of major blackouts, with a particular emphasis on the cascading failure mechanism. This article delves into the intricate dynamics and root causes of cascading failures, offering invaluable insights into the factors that trigger them and the subsequent chain reactions that lead to blackouts. Most importantly, the authors coined the term, PNR. This signified a point of global instability beyond which power system collapse was imminent. However, the authors did not formalize nor quantify it which is the focus of our work.

B. Motivation and Contributions

Cyberattacks on power systems may instigate multiple, unprecedented excitation modes, and lead to an accelerated PNR in the cascading failure sequence. Hence, the impact of a cyberattack on power system dynamics can be fundamentally different from the consequences of physical faults or contingencies. This can lead to unprecedented *N-k* contingencies. Consequently, there is a compelling need for the development of newer analysis methods that are specifically tailored to the distinctive characteristics of cyberattacks on power systems. Furthermore, as described earlier, one of the key limitations of most existing methods is the analyses based on power flows or network topology. Thereby, such studies do not take dynamical behavior of the power system into account. This results in an incomplete view of the underlying mechanisms that govern power system cascading failures.

Hence, to overcome these drawbacks, in this article, we analytically show how cyberattacks can cause cascading failures and blackouts and lead to a quicker PNR. This is achieved through detailed modeling and simulation of power system dynamics and multiple, coordinated protection schemes for lines, generators, and loads. It allows us to analyze in time domain the entire sequence of cascading events, i.e., protection trips of transmission lines and generators. Consequently, the scientific contributions of this article are summarized as follows:

1) We propose a data-driven method for dynamical analysis of power system cascading failures caused by cyberattacks. The method is used to investigate the fast phase of the cascading failure mechanism initiated by cyberattacks and associated power system dynamics. It uses time-frequency analysis of simulation data through the Hilbert–Huang transform to estimate instantaneous damping and modal instabilities. The variation in singular values of the instantaneous damping matrix's decomposition is used to identify and quantify a point of global instability, i.e., the PNR [26] for a cascading failure sequence.
2) We provide experimental proof based on the proposed method, to demonstrate and explain how cyberattacks accelerate the cascading failure mechanism. Numerical results show that cyberattacks may accelerate cascading failures at least by a factor of 3x. This is attributed to the excitation and nondamping of multiple frequency modes greater than 1 Hz in a short time span, in comparison to historically observed blackouts.

One of the key novelties of this article is to formalize and quantify the PNR for a cascading failure sequence. To the best knowledge of the authors, this article is the first of its kind to detect and quantify the PNR, more so for cyberattack induced cascading failures. Therefore, a comparison with established techniques or traditional methods to detect and quantify the PNR may be difficult or not feasible. As a result, comparative experiments are not conducted.

III. Cyber-Physical Attacks on Power Grids

Various types of cyberattacks on power grids are already well reported in the literature. In this article, we consider attack vectors with maximum impact and scenarios that can severely affect system dynamics, thereby leading to cascading failures and a blackout.

A. Spoofing Attacks

These cyberattacks target the setpoints of control devices and mechanisms of generators, e.g., governors for load frequency control (LFC) and automatic voltage regulators (AVRs). This is also applicable to controllers for power electronics interfaced generation, such as photovoltaics or windfarms. The attacks aim to send malicious control signals that result in equipment or component malfunctions [17]. A resonance cyberattack targeting LFC of generators is discussed in [27]. In this type of attack, an adversary modifies the input signals to generator governors based on a resonance source, e.g., rate of change of frequency (ROCOF). This results in a negative feedback on LFC, such that the targeted generator loses stability, resulting in unexpected loss of generation. Similarly, in the event of over or under excitation AVRs of generators can trip for safety reasons. This can cause voltage stability issues and lead to a voltage collapse. Thereby, spoofing attacks can initiate or worsen an ongoing cascading failure process.

B. Switching Attacks

These types of cyberattacks aim to maliciously open multiple circuit breakers to impact power system operation. Let us consider a power system with n circuit breakers. We assume an attacker has access to m of these circuit breakers such that $m \subseteq (n)$. This is possible through communication network exploits or digital substation based attack vectors. Then, the attack vector for switching is given by the following relation where sw corresponds to a binary variable indicating connection or disconnection

$$\mathrm{SW} = [\mathrm{sw}_1, \mathrm{sw}_2 \ldots \mathrm{sw}_m]^T = [0, 0, \ldots 0]^T . \tag{1}$$

Thereby, the attacker can disconnect multiple transmission lines and other power system components. For instance, the unexpected loss of lines causes equipment to be disconnected as well as system parameters like voltage and frequency to exceed limits. As demonstrated during the 2015 cyberattack in Ukraine, lines can be put out of service by gaining unauthorized access to the substation automation systems and simultaneously opening multiple circuit breakers [4]. This results in overloading of parallel lines, setting off a cascade that could result in a voltage collapse. As observed in Italy and the United States-Canada in 2003, this can have a particularly catastrophic impact on the power system, leading to a blackout.

C. Data Integrity Attacks

False data injection (FDI) attacks are the most frequently discussed cyberattack on power systems in the literature. An FDI attack assumes that an attacker may gain access to knowledge about the existing configuration of the power system and alter measurements at substations. As a result, they might secretly insert arbitrary biases to some state variables. Hence, the majority of FDI attacks reported in the literature target state estimate methods and measurements [28] to result in data integrity issues and potential line overloading or even cascading failures. Another form of data integrity attack reported in the literature targets power system protection equipment. Communication-based protection schemes are vulnerable to data integrity attacks that can manipulate the data sensed by protection relays, causing them to maliciously trip or malfunction [29], [30]. This is summarized by the following relation which highlights the spoofing of the relay pickup current

$$I^{*}_{\text{pickup}} = I_{\text{pickup}} \pm \beta \tag{2}$$

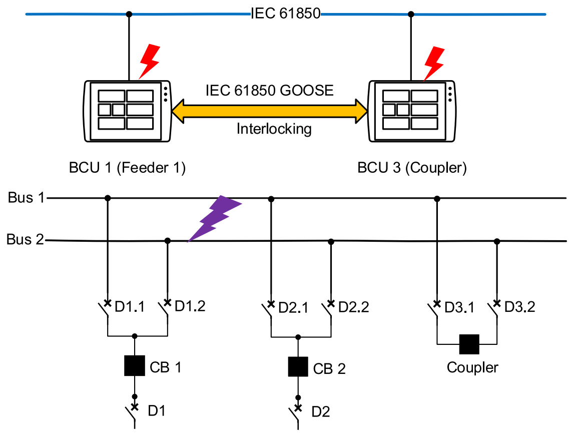


Fig. 1. Interlocking scheme in digital substations.

where β represents the bias added as a result of the cyberattack. Such sophisticated cyberattacks can lead to malicious tripping of relays, while remaining undetected. This can have crippling consequences for power system operation as the attacks can result in unwanted opening of circuit breakers, leading to transient and/or voltage instabilities. Another possibility is a denial-of-service 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 unwanted relay tripping, thereby triggering a chain of cascading events [25].

D. Cyber-Physical Attacks

Interlocking is an important safety mechanism that is commonly used in digital substations to ensure the safe operation of switchgear equipment. It involves the use of a software-based scheme that uses IEC 61850 GOOSE to exchange information between control units in different parts of the substation. For example, in a two-busbar single breaker arrangement with two feeder bays and a coupler, as shown in Fig. 1, the coupler and circuit breaker statuses are communicated to the feeder bay control unit to prevent the inadvertent opening of disconnects when the circuit breaker is closed. However, despite its importance, interlocking is vulnerable to cyberattacks that can compromise the system's security. In particular, attack vectors reported in the literature [31], [32] can allow disconnects to be operated in the feeder bays even when the circuit breakers of the feeders are closed, putting the system at risk. This can result in a bolted busbar fault and electric arc in the substation. Coupled with a denial of service attack which may inhibit protection functionality [32], this can cause massive system instabilities and lead to a blackout.

IV. Dynamical Analysis of Cascading Failures

A. Power System Dynamics

Power system dynamical behavior is characterized by two main properties, i.e., nonlinearity and nonstationarity [33]. This makes a detailed analytical study of such behavior complex.

Hence, modern-day power system studies involve modeling the power grid and associated components as a set of differential algebraic equations (DAEs) to be numerically solved in the time-domain. The continuous time behavior of the dynamical power system can be generally described by a general set of DAEs, wherein, the states and the dynamic behavior of the power system at any time instant t is given by three vectors *x*(*t*)*,* *y*(*t*)*,* and *z*(*t*), such that

$$\dot{x} = \mathrm{f}\left(\mathrm{x}\left(t\right),\ \mathrm{y}\left(t\right),\ \mathrm{z}\left(t\right)\right) \tag{3}$$

$$\mathrm{g}(t, (\mathrm{x}\left(t\right),\ \mathrm{y}\left(t\right),\ \mathrm{z}\left(t\right)) = 0 \tag{4}$$

$$\mathrm{h}\left(t,\ \mathrm{x}\left(t\right),\ \mathrm{y}\left(t\right),\ \mathrm{z}\left(t\right)\right) < 0 \tag{5}$$

x represents the vector of all state variables and *y* represents a vector of continuous state variables with algebraic associations to all other system variables. This includes the standard power flow equations and algebraic equations for all dynamic devices such as motors, converters, condensers, etc., and *z* represents the vector of discrete state variables, i.e., z ∈ [0, 1]. It captures the dynamics associated with discrete actions, such as protection and controls.

In this article, a dynamic RMS model of the power system with multiple, coordinated protection schemes is developed. It includes: protection schemes for lines, i.e., distance and overload protection; interface protection schemes for generators, i.e., over/under frequency, over/under voltage, ROCOF, over flux, and pole-slip (out of step); and underfrequency and undervoltage load shedding schemes. If the input parameter sensed by a protection I_s exceeds a specified pickup or threshold value over a specified time period, the relay produces a trip signal to open the associated circuit breaker. A binary variable K_s determines the trip status of the relay and can be generalized by the following logic, with 1 being the trip state

$$K_{\mathrm{s}} = \begin{cases} 0, & 0 < I_{\mathrm{s}} \le I_{\mathrm{pickup}} \qquad t < t_{\mathrm{lim}} \\ 1, & I_{\mathrm{pickup}} < I_{\mathrm{s}} < I_{\mathrm{lim}} \qquad t > t_{\mathrm{lim}}. \end{cases} \tag{6}$$

This logic is incorporated into the developed dynamic RMS model. Hence, it can simulate cascading failures and associated dynamic system response. With increasing system size, purely analytical studies of power grids are challenging and numerical simulations are needed. Hence, we perform time-domain simulations and use the dynamic system response for further analysis.

B. Time-Frequency Analysis

To capture both nonlinear and nonstationary system behavior, we employ a modified Hilbert–Huang transform (HHT) and study the PNR. It is a signal processing technique for data analysis of nonlinear and nonstationary processes and consists of an iterative empirical mode decomposition (EMD). In this article, an EMD process for power systems is used to decompose an input signal, i.e., power system measurement, into a series of individual amplitude and frequency-modulated components, i.e., intrinsic mode functions (IMFs) [34]. The IMFs are computed based on the sifting process. IMFs are characterized by being nearly monotonic, i.e., consisting of a single frequency component. Consequently, we apply the Hilbert transform (HT) on IMFs, which allows for a detailed analysis into the temporal modal properties of the input signals. As a result, an in-depth interpretation of nonlinear and nonstationary phenomena is achieved. For a given time-series signal input, $u(t)$, we first compute the major IMF using EMD [34] and then compute its HT as follows:

$$\mathrm{H}[u(t)] = -\frac{1}{\pi}\lim_{\varepsilon\to 0}\int_{\varepsilon}^{\infty}\frac{u(t+\tau)-u(t-\tau)}{\tau}d\tau. \tag{7}$$

Two of the known limitations of the HHT are mode mixing, i.e., close proximity of frequency components and presence of low frequency components. To overcome these limitations, in this research, we apply a modified EMD procedure with an iterative-EMD technique [35]. This technique automatically identifies the best masking signal frequencies based on the inherent dynamics of the input data signal. Based on the HT, the analytical signal of the input is computed and expressed as an exponential, i.e.,

$$u_a\left(t\right) = u\left(t\right) + j\ \mathrm{H}\left[u\left(t\right)\right] \tag{8}$$

$$u_a\left(t\right) = A\left(t\right)e^{j\omega\left(t\right)}. \tag{9}$$

Using the above, it becomes possible to calculate instantaneous parameters such as amplitude, as follows:

$$A\left(t\right) = \sqrt{u^2\left(t\right) + H^2\left[u\left(t\right)\right]}. \tag{10}$$

Knowledge of the instantaneous amplitude and phase information allows to estimate the instantaneous damping. This allows for a deeper stability analysis of the system. The damping is calculated as the ratio of the differential of the instantaneous amplitude to itself, i.e.,

$$\alpha\left(t\right) = -\frac{\dot{2}A(t)}{A(t)}. \tag{11}$$

This opens up interesting possibilities for analysis of dynamic system response, while preserving temporal properties, as explained in the subsequent subsections.

C. Instantaneous Damping Correlation

The analysis of the PNR in this article is inspired by the analogy and similarities between nonlinear mechanical and electrical systems [18]. When such dynamic systems are subject to systemic failures, points of global instability may surface. For example, consider a simple example of a mass-spring system with a single degree of freedom, governed by the following differential equation:

$$m\frac{d^2x}{dt^2} + c\frac{dx}{dt} + kx = 0 \tag{12}$$

where x is the system state, m is the spring mass, c is the damping coefficient, and k is the spring constant. Calculating its system and damping response is quite straightforward. More interestingly, however, this equation bears close resemblance to the well-known swing equation [19], governing fundamental

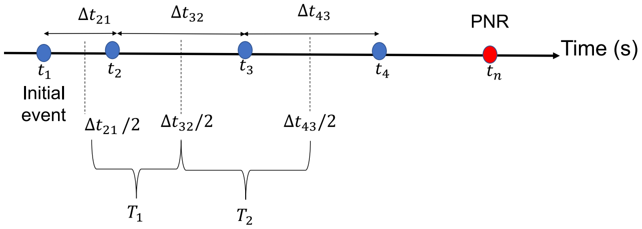


Fig. 2. Sliding time windows for cascading failures analysis.

power system dynamics:

$$\frac{d\left(\Delta\bar{\omega}_r\right)}{dt} = \frac{1}{2H}\left(\bar{T}_m - \bar{T}_e - K_D \Delta\bar{\omega}_r\right). \tag{13}$$

The above equation is the so called classical swing equation with two state variables—the generator rotor angle (δ) and angular speed (ω_r). This simple and elegant relation provides powerful analytical insights into grid dynamics. Inspired by the similarities between (12) and (13), the proposed algorithm in this article seeks to leverage the properties of instantaneous damping, to characterise and study the PNR.

Any cascading failure sequence involves loss of multiple elements, captured through the discrete relay trip events K_s. Thereby, the order and time of tripping serves as an important input to identify and quantify PNR. The observation time window around each trip event K_s is dependent on the timing of the discrete relay actions at t_i. The proposed sliding time window T_{i-1} around each discrete relay action at t_i is given by

$$T_{i-1} = \left\{\frac{\Delta t_{i,i-1}}{2}, \frac{\Delta t_{i+1,i}}{2}\right\}. \tag{14}$$

Fig. 2 summarizes the calculation of $T\ \forall\{\,T_1,\ T_2, \ldots T_n\}$. It captures the continuous dynamical variations occurring in the power system due to sequential relay tripping events, which indicate cascading failures. Therefore, the sliding time window T allows us to analyze the entire sequence of cascading failures.

For each time window, the we estimate the instantaneous damping, based on (11). Subsequently, a cross-correlation matrix R is formed, for n number of time-series signals, i.e.,

$$\mathrm{R} = \begin{bmatrix} \mathrm{E}\left[X_1 Y_1\right] & \mathrm{E}\left[X_1 Y_2\right] & \cdots & \mathrm{E}\left[X_1 Y_n\right] \\ \mathrm{E}\left[X_2 Y_1\right] & \mathrm{E}\left[X_2 Y_2\right] & \cdots & \mathrm{E}\left[X_2 Y_n\right] \\ \vdots & \vdots & \ddots & \vdots \\ \mathrm{E}\left[X_m Y_1\right] & \mathrm{E}\left[X_m Y_2\right] & \cdots & \mathrm{E}\left[X_m Y_n\right] \end{bmatrix} \tag{15}$$

where $\mathrm{E}(\mathrm{X}_i, \mathrm{Y}_i)$ represents the correlation between the two variables, i.e., $E(X, Y) = -\frac{1}{n}\sum_{i=1}^{n}(x-\mu_x)(y-\mu_y)$. This a measure of how two variables change with respect to each other. Hence, R contains the combination of correlations between all values of instantaneous damping and is of size $n \times n$. These values lie in the range [−1, 1].

D. PNR and Singular Value Decomposition (SVD)

SVD is a linear algebraic technique to factorize any $m \times n$ matrix and generalize its eigen decomposition. In our case, the matrix R is symmetric, therefore, its SVD yields

$$R = USV^T \tag{16}$$

Algorithm 1: Identification of Point of No Return.

```
 Inputs: time window vector $T$ and signals $x(t)$
 1:  estimate sliding time window using (14)
 2:  for each time window do
 3:    compute instantaneous damping $\alpha(t)$
 4:    form cross-correlation matrix $R$
 5:    calculate $\sigma_0$ , $\sigma_1$ using (16)
 6:    obtain $\Delta\sigma = \sigma_0 - \sigma_1$
 7:    if $\Delta\sigma > \epsilon$ do
 8:      possible PNR. set smaller $T$ and repeat 3 to 6
 9:    else
10:      $T = T_{next}$
11:    end if
12:  end for
```

where U and V are distinct orthogonal matrices, and S is a sparse diagonal matrix containing the singular values of R, i.e.,

$$S = \begin{bmatrix} \sigma_i & 0 & \cdots & 0 \\ 0 & \sigma_j & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \sigma_n \end{bmatrix} \tag{17}$$

where $\sigma_i\ \ldots \sigma_n$ are the singular values of R descending order, i.e., $\sigma_1 > \sigma_2 \ldots \sigma_{n-1} > \sigma_n$. Essentially, SVD helps to identify dimensions along which data is best preserved by the largest singular values [36]. Hence, under nominal operations, matrix R is a zeros matrix and consequently $\sigma_1 = 0$. If the power system suffers a major disturbance, however, for e.g., an electrical fault, it will suffer undamped oscillations, i.e., $\alpha(t) \rightarrow \{-1\}$. Subsequently, post fault, the system will reach a new equilibrium point and oscillations will be over/critically damped, i.e., $\alpha(t) \rightarrow \{1\}$. In case of an unchecked cascading sequence, however, the system will move between highly unstable operating points, reach a PNR and collapse. Consequently, the system-wide oscillations are undamped across multiple time-windows, i.e., $\alpha(t) \rightarrow \{-1\}$. As a result, we hypothesise that σ_1 of R will drop below the theoretical threshold, i.e.,

$$\Delta\sigma = \sigma_{1_{t2}} - \sigma_{1_{t1}} \gg 0 \tag{18}$$

where t_1 and t_2 represent successive time windows (only for notation). Hence, (18) forms the limit criterion and theoretical basis to identify the smallest/earliest PNR and is summarized by the following algorithm. The proposed algorithm is meant to be used for postmortem analysis and takes time occurrence of events and time-series measurements as inputs. Subsequently, it application yields an estimation of the earliest PNR value, which is nontrivial, as noted in [26]

V. Experimental Results

To verify the proposed method, numerical simulations are conducted on a modified IEEE-39 bus test system, consisting of multiple, coordinated protection schemes using DIgSILENT PowerFactory 2021, as depicted in Fig. 3. Furthermore, automated scenario handling and data collection is done through

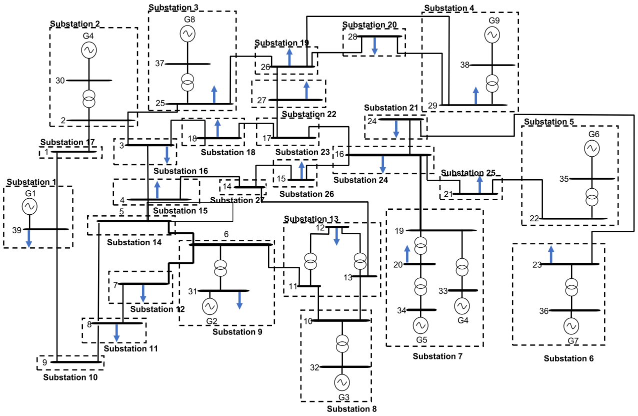


Fig. 3. IEEE 39-bus test system.

Python 3.7. The time-frequency and PNR analysis is implemented in Python using NumPy, SciPy, and EMD libraries. Meanwhile, the cyberattacks are modeled through the Mininet network emulator, interfaced to PowerFactory via OPC unified architecture. This results in a cyberphysical co-simulation experimental setup. We also assume that voltage magnitudes from 13 PMU locations, i.e., buses 2, 6, 9, 10, 11, 14, 17, 19, 20, 22, 23, 25, and 29 are available for system observability, as described in [37]. Moreover, we assume that no remedial actions are undertaken during the evolution of the cascading failures.

In all simulations, a single operational point is used, i.e., fixed generation and load profile. This is because most numerical solvers used for dynamic power system simulations are typically designed to work well when initiated from a stable operating point. These simulations involve solving complex sets of nonlinear DAE. Fixed operational points help maintain the numerical stability of the simulation as significant deviations from this point, especially in highly nonlinear systems can lead to numerical instabilities or nonconvergence of simulation. Furthermore, more crucially, our analysis is in the order of milliseconds to seconds, while generation and load profiles are typically in the order of minutes to hours. We must also however, emphasise, changes in the system due to normal operations, i.e., loading and generation, do not affect the results of the proposed method. This is because, the proposed method seeks to analyse a point of global instability, i.e., PNR, around which the system response is distinctly unique, in comparison to variations around nominal operating points.

To simulate the impact of cyberattacks, a detailed *N-2* contingency analysis on IEEE 39-bus test system is carried out. The system comprises of 10 generators and 34 lines, i.e., 44 components. Therefore, the total number of contingency combinations is given by $C(44,2) = 946$. For each combination, a DC power flow is calculated to obtain the bus voltages and line overloading. Furthermore, critical combinations are defined as dc power flows that result in line thermal overloading $>$ 125% for two more lines and/or voltage violations outside the limits of [0.9 p.u, 1.05 p.u] at least two busbars. For such cases, in addition to DC power flow, AC power flows using Newton Raphson method are calculated. From this analysis, it is observed that line 05–06 and bus 09 are critical components with a high occurrence of 327 and 42, respectively, amongst all studied contingency combinations. Hence, we consider cyberattack scenarios involving these two locations. A summary of each simulation scenario and cyberattack type is given in Table I.

TABLE I
SUMMARY OF SIMULATION SCENARIOS AND CYBERATTACK TYPES

Scenario	Cyber attack Type
Scenario 1	Data-integrity and Cyber-physical
Scenarios 2 and 3	Switching Attacks
Scenario 4	Spoofing

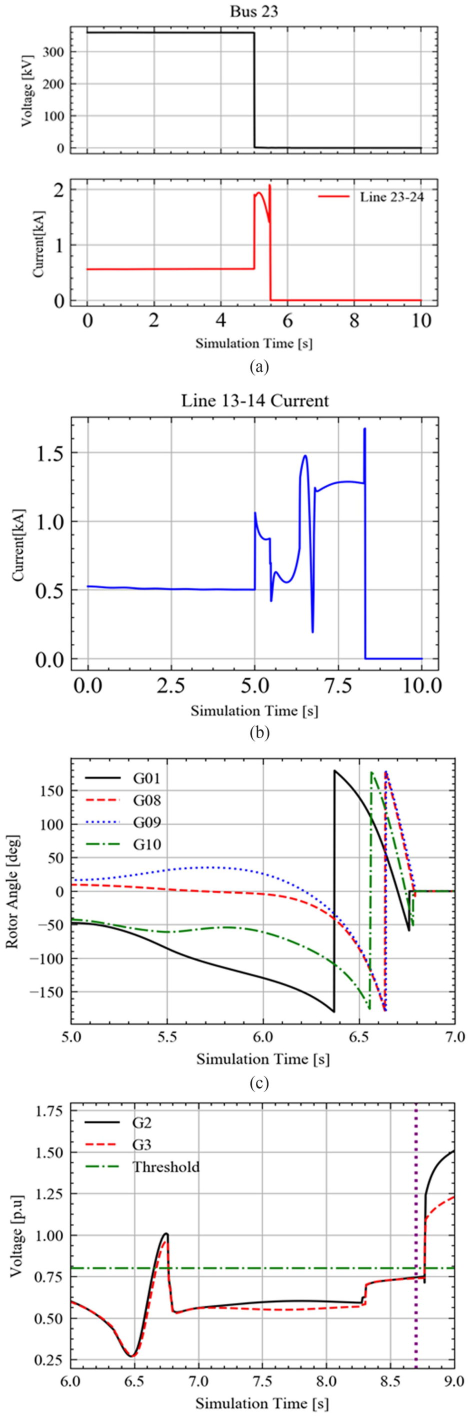
TABLE II
SEQUENCE OF CASCADING FAILURES IN SCENARIO 1

No.	Time	Event
1.	5 s	Cyber attack causes busbar fault on bus 23.
2.	5.5 s	Multiple lines in vicinity of attack location tripped by distance protection, i.e., lines 21–22 and 23–24.
3.	6.1 s	Generator G6 is islanded and tripped by ROCOF protection.
4.	6.1–6.3 s	Multiple lines tripped by distance protection, i.e., lines 22–23 and 16–19. **PNR is reached.**
5.	6.6–6.7 s	Lines 13–14 and 04–05 tripped by distance protection.
6.	6.8 s	Multiple generators, i.e., G1, G8, and G9 lose synchronism.
7.	7.3 s	Generator G10 is islanded and tripped by ROCOF protection.
8.	8.7 s	Generators G3 and G2 are disconnected by under voltage protection.
9.	10 s	End of simulation. Cyber attack results in loss of load ~ 6000 MW.

A. Cascading Failure Simulation

A cyberphysical attack scenario is simulated to test the proposed method. Attack scenario 1 exploits vulnerabilities in interlocking schemes within a digital substation, as explained in Section III. Furthermore, all protection functionality within the substation is inhibited due to a data modification attack. The malicious opening of a disconnect under loading, coupled with the lack of protection action results in a busbar fault on bus 23 at 5 s simulation time. Subsequently, the nontimely clearance of the fault induces cascading failures throughout the system, resulting in a blackout. The sequence of events in the cascading failure is given in Table II.

As the protection equipment within the substation is inhibited due to the cyberattack, neighboring lines are tripped by distance protection at 5.5 s simulation time. The loss of line 13–14 due to distance protection maloperation, as previously explained, is depicted in Fig. 4(b)and (b). As a result, the system is split into multiple islands with generator G6 being tripped by ROCOF protection at 6.2 s simulation time. The cascading loss of elements continues with the loss of other transmission lines. Subsequently,



(a)

(b)

(c)

(d)

Fig. 4. Power system dynamics during cascading failures in scenario 1. (a) Busbar fault on bus 23. (b) Distance protection tripping of lines 13–14 at 8.3 s simulation time. (c) Loss of synchronism of multiple generators. (d) Under voltage trip of G2 and G3 at 8.7 s simulation time. Protection setting is < 0.8 p.u. and $t > 2$ s.

at around 6.8 s simulation time, multiple generators lose synchronism and are disconnected from the grid. This is visualized in Fig. 4(c). The loss of multiple generators and lines destabilizes the power system with a lack of reactive power generation and extremely poor voltage profile. Finally, generators G2 and G3 trip due to sustained under voltage conditions of 0.8 p.u over 2 sat 8.7 s simulation time, resulting in a blackout. This is illustrated in Fig. 4(d).

B. Point of No Return Identification

1) Switching Attacks: To verify the efficacy of the proposed method, two simulation case studies are compared. Scenario 2 is the opening of line 05–06 and scenario 3 is the disconnection of all lines in substation 2. Both cases have initiating events at $t = 5$ s simulation time.

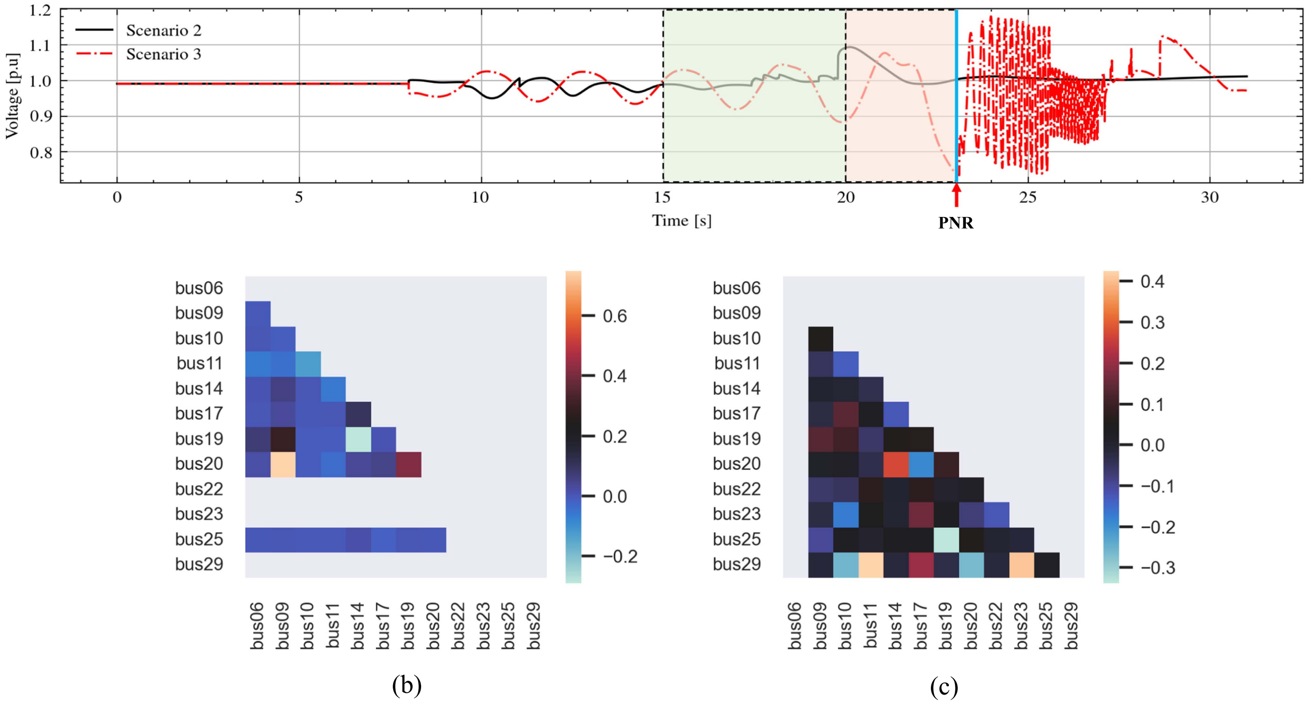
Owing to the system topology, scenario 3 results in cascading failures, while the scenario 2 results in system disturbances. This is visualized through the voltage plot of bus 20 in Fig. 5(a). For ease of explanation and analysis, sliding time windows are chosen as $T_1 = [15, 20]$, $T_2 = [20, 23]$. Subsequently, the instantaneous damping is calculated to form the correlation matrix using (15).

For scenario 2, in T_1, the system suffers significant oscillations, which are, however, well-damped, i.e., $\alpha(t) \gg 0$. On the other hand, for scenario 3, as can be seen, the oscillations are undamped and rising, i.e., $\alpha(t) < 0$. In time window T_2, however, the system reaches a new equilibrium point in scenario 2. This is visualized through Fig. 5(b) which illustrates the correlation matrix R of damping values as a heatmap. As can be seen, most of the elements do not exhibit any correlation, shown in shades of blue. Furthermore, the difference in largest singular values between the successive time windows is infinitesimally small, i.e., $\Delta\sigma_1 << 0$.

Conversely, for scenario 3, during the propagation of cascade, the system moves from one instability point to another. This is indicated by an increase in positive correlations, as indicated by the heatmap in Fig. 5(c). More importantly, for scenario 3, the difference in largest singular values between time windows T_1 and T_2 is greater than zero, i.e., limit criterion (18) is violated. This is confirmed by a large positive shift of ~ 0.89 in $\Delta\sigma_1$ and can be visualized in Fig. 6 (in red). Hence, it is concluded that the PNR is reached at ca 23 s simulation time. Therefore, in scenario 3 from the initiating event, the PNR is reached in $\sim$16 s.

To further analyse the active modes during these extended periods of instability, a detailed frequency analysis is carried out and is illustrated in Fig. 7. This corresponds to the time window T_2 for bus 10. A similar result can be obtained for the other twelve PMU locations. Typical inter-area oscillations in power systems are observed to be in the range of 0.1 to 0.7 Hz [26]. As can be observed from Fig. 7, closer to the PNR, the major oscillatory modes correspond to 1.2 and 1.5 Hz. Hence, these higher frequency oscillation modes correspond to the excitation brought about by cyberphysical events. These oscillations, if left unchecked, can lead to a system wide instabilities. Thus, such insights are useful when designing power system stabilisers or damping controllers.

2) Spoofing Attacks: To verify and validate the applicability and accuracy of the method, a spoofing and switching attack, i.e., scenario 4, as described in Section III is simulated. In this attack scenario, the voltage reference setpoints for the AVR of generator G6 are maliciously spoofed by $+10\%$ at 5 s simulation time.



(b)

(c)

Fig. 5. Identification of PNR. Subfigure (a) depicts the voltage waveform for bus 20. (b) and (c) depict the correlation matrix R as a heatmap in time windows, $\boldsymbol{T}_1$ and $\boldsymbol{T}_2$, respectively.

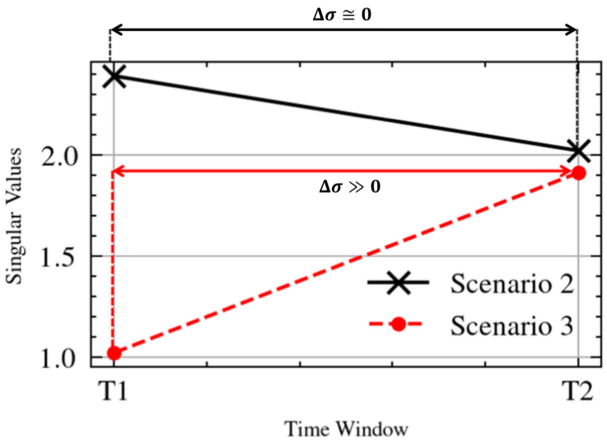


Fig. 6. Identification of PNR.

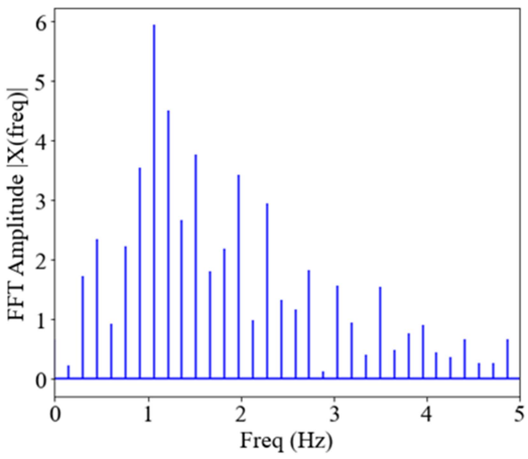


Fig. 7. Frequency spectrum of bus 10 voltage HHT in time window $\boldsymbol{T}_2$.

Simultaneously, two transmission lines, i.e., 16–19 and 16–24, are maliciously disconnected via a switching attack. These unexpected events result in the propagation of cascading failures throughout the system. Fig. 8 shows the plot of the voltage and time windows considered for analysis, using the proposed method. Similar to the analysis of the previous case, sliding time windows are chosen as $T_1 = [5, 12]$, $T_2 = [12, 17]$. Subsequently, the instantaneous damping is calculated to form the correlation matrix using (15). Due to the abrupt setpoint change and line disconnections, the system undergoes severe voltage stability issues. Crucially, $\Delta\sigma_1 \approx 1$ in T_1 and $\Delta\sigma_1 \approx 1.28$ in T_2. Therefore, $\Delta\sigma_1 \gg 0$ indicates that the PNR lies in time window T_2. As can be seen from Fig. 9, due to the cyberattack, a voltage collapse is triggered and significant load is shed. Eventually, the cyberattacks result in a blackout with 3000 MW load left unserved. The entire sequence of events of the cascading failure is given in Table III.

C. Acceleration Mechanism

To study the acceleration of cascading failures, we analyse the Italy 2003 blackout. Fig. 10 illustrates the observed cumulative loss of elements, based on the post incident report. As seen, until the PNR, a linear behaviour is observed. Beyond this, an exponential rise in loss of elements occurs. Hence, it is concluded that the PNR was reached approximately in ∼28

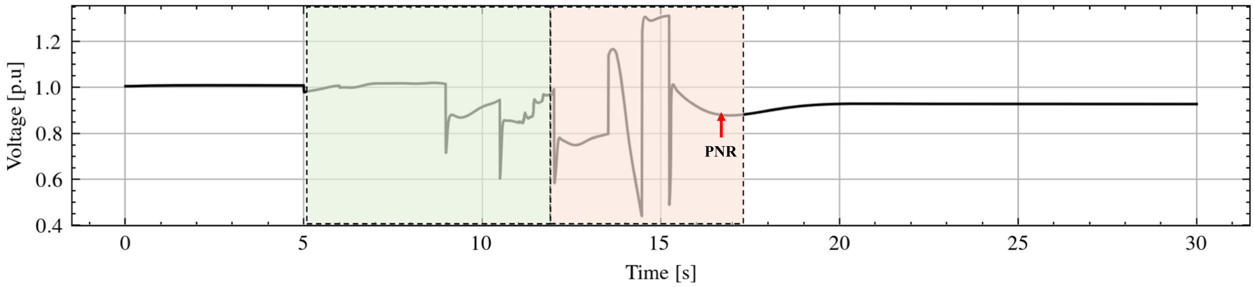


Fig. 8. Voltage plot of bus 6. Time window T_1 from 5 to 12 s is shown in green, while T_2 from 12 to 17 s is shown in orange and the PNR at ∼16.5 s is highlighted.

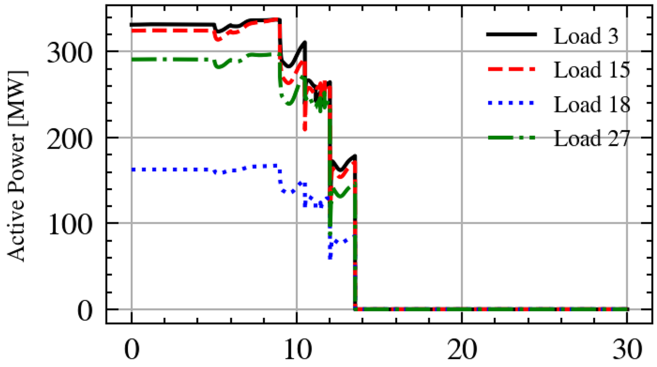


Fig. 9. Active power of four loads, highlighting the voltage collapse at 14 s and subsequent blackout at ∼16 s simulation time.

TABLE III
SEQUENCE OF EVENTS LEADING TO BLACKOUT DUE TO SPOOFING AND SWITCHING ATTACKS

No.	Time	Event
1.	5 s	Spoofing cyber attack causes AVR voltage setpoint of generator G6 to increase by 10%
2.	5–6 s	Lines 16–19 and 16–24 disconnected by switching attacks.
3.	9 s	Line 21–22 tripped by distance protection.
4.	9.5 s	Generator G6 and G7 are islanded and tripped by ROCOF protection.
5.	11 s	Underfrequency load shedding by 7%.
6.	12–13.5 s	Multiple lines tripped by distance protection, i.e., lines 26–27, 04–05, and 05–06
7.	14.3 s	Generator G9 is islanded and tripped by ROCOF protection.
8.	14.8–15 s	Generators G6 and G7 tripped by frequency protection. **PNR is reached.**
9.	20 s	End of simulation. Cyber attacks result in blackout with loss of load ~ 3000 MW.

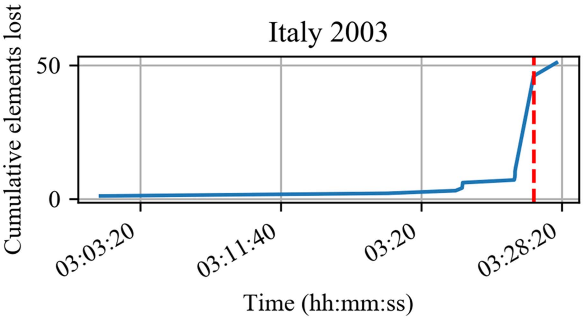


Fig. 10. Observed PNR in the Italy 2003 blackout.

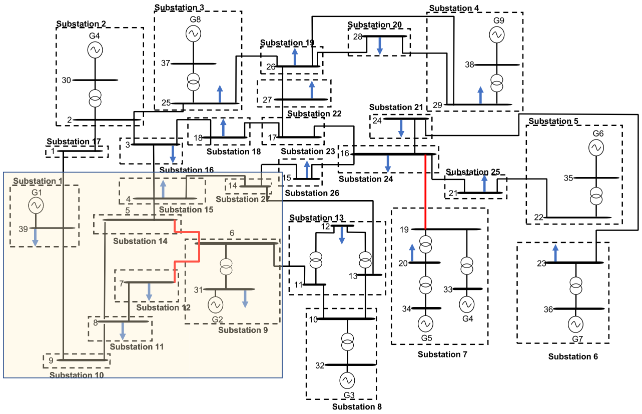


Fig. 11. Blackout simulation. The locations marked in red are disconnected, while the indicated area 1 is unserved.

minutes from the loss of the first element. Keeping this in mind, we simulate scenario 5 to mimic a similar sequence of events. In the considered scenario, routine maintenance causes line 05-06 to be put of service at 5 s simulation time. Shortly thereafter, due to contact with vegetation, lines 16–19 is also put of service at 10 s simulation time. Consequently, the system is stressed, and other lines start to be overloaded. Eventually, line 06-07 comes in contact with vegetation and is immediately tripped at 30 s simulation time. As a result, area 1 is blacked out as depicted in Fig. 11 .

A comparison of the loss of elements in the between scenarios 1, 3, and 5 is carried out. The initiating events in all three scenarios occur at 5 s simulation time and the cumulative loss of elements is depicted in Fig. 12. Furthermore, using the proposed method from this article, the PNR is calculated to be 10, 6.5, and 31 s for cyberattack scenarios 3, 1 and 5, respectively. This is shown by the red dots in Fig. 12. We use this information to define a rate of elements lost. The rate γ is

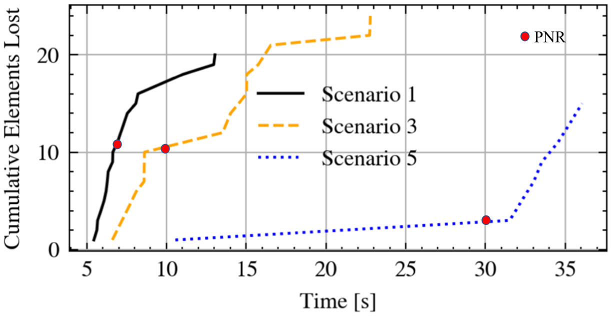


Fig. 12. Acceleration of cascading failures due to cyberattacks.

TABLE IV
COMPARISON OF CYBERATTACK SCENARIOS IMPACT

Scenario	PNR (s)	γ	Load Lost (MW)
Scenario 1	10	2.2	4000
Scenario 3	6.5	8.6	6000
Scenario 5	31	0.1	2500

defined as

$$\gamma = \frac{\sum \mathrm{EL}}{\Delta\, t} \tag{19}$$

where EL is the number of elements lost in a specific time period *t*. A comparison of the factor and final impact of the three cases is summarized in Table IV. As can be seen, attack scenario 1 is the quickest with a factor of almost 8.5, while scenarios 3 and 4 develop much slower. In case of the cyberattacks, multiple frequency modes $>$ 1 Hz are excited in a short time span, which when left unchecked lead to undamped system-wide oscillations. This can be attributed to the fact that cyberattacks can directly influence the occurrence of multiple events that are statistically improbable to occur together due to natural causes. Also, it can be seen that the ratio of PNR of scenario 4 to 1 is $\sim$3. This signifies an acceleration of 3x. Thus, we empirically conclude that cyberattacks can induce a significant speed-up in the cascading failure mechanism, by at least a factor of 3x.

VI. Conclusion and Discussions

In this article, a data-driven analysis method was proposed to study how cyberattacks on power systems can induce accelerated large-scale cascading failures and a blackout. This involved time-frequency analysis of dynamic simulation data using a modified Hilbert–Huang transform. Additionally, using the proposed method and a synthetic case-study, it was shown how cyberattacks may accelerate the cascading failure mechanism by at least a factor of 3x. This was due to the excitation of multiple high frequency modes in a short time span. The analysis method was tested using time domain simulations conducted on a modified IEEE-39 bus test system, consisting of multiple, coordinated protection schemes.

The proposed method can be used by utilities for cyber-physical system studies and assessment of cybersecurity and grid cyber resilience, which is currently of limited nature. Known limitations of the method include its a-priori nature and choice of the sliding time window. Nevertheless, it is tool agnostic and is designed for synchrophasor measurements and trip data from protection relays, post a major disturbance.

The choice to primarily utilize the IEEE 39-bus test system in our study was made considering several factors, particularly that it was a widely recognised benchmark for power system analysis. More importantly, modeling, coordination, and validation of protection schemes to simulate cascading outages on larger power systems is a nontrivial task due to increased complexity and computational demands. Our study aimed to establish the foundation for this approach, demonstrating its feasibility and effectiveness using the IEEE 39-bus system. Nevertheless, validating our proposed method on larger and more complex power systems, such as the 118-bus system will be the focus of our future work. Additionally, we will develop methods to mitigate the impact of the cyber induced cascading failures before the PNR is reached. Consequently, its knowledge for various scenarios aids in the development of resilience measures for shock absorption and system adaptation. Thereby, improved security analytics and defence methods can be developed to cybersecure the power system.

References

[1] D. Pliatsios, P. Sarigiannidis, T. Lagkas, and A. G. Sarigiannidis, “A survey on SCADA systems: Secure protocols, incidents, threats and tactics,” *IEEE Commun. Surv. Tut.*, vol. 22, no. 3, pp. 1942–1976, Jul.–Sep. 2020.

[2] N. Saxena, L. Xiong, V. Chukwuka, and S. Grijalva, “Impact evaluation of malicious control commands in cyber-physical smart grids,” *IEEE Trans. Sustain. Comput.*, vol. 6, no. 2, pp. 208–220, Apr.–Jun. 2021.

[3] 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.

[4] R. Lee et al., “Analysis of the cyber attack on the Ukrainian power grid,” *Electricity Inf. Sharing Anal. Center*, vol. 388, pp. 1–26, Mar. 2016.

[5] G. Liang, S. R. Weller, J. Zhao, F. Luo, and Z. Y. Dong, “The 2015 Ukraine blackout: Implications for false data injection attacks,” *IEEE Trans. Power Syst.*, vol. 32, no. 4, pp. 3317–3318, Jul. 2017.

[6] S. He, Y. Zhou, Y. Zhou, J. Wu, M. Zheng, and T. Liu, “Fast identification of vulnerable set for cascading failure analysis in power grid,” *IEEE Trans. Ind. Informat.*, vol. 19, no. 4, pp. 5645–5655, Apr. 2023.

[7] D. Liu, X. Zhang, and C. K. Tse, “A tutorial on modeling and analysis of cascading failure in future power grids,” *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 68, no. 1, pp. 49–55, Jan. 2021.

[8] P. Henneaux et al., “Benchmarking quasi-steady state cascading outage analysis methodologies,” in *Proc. Int. Conf. Probabilistic Methods Appl. Power Syst.*, 2018, pp. 1–6.

[9] M. J. Eppstein and P. D. H. Hines, “A ‘random chemistry’ algorithm for identifying collections of multiple contingencies that initiate cascading failure,” *IEEE Trans. Power Syst.*, vol. 27, no. 3, pp. 1698–1705, Aug. 2012.

[10] J. Yan, Y. Tang, H. He, and Y. Sun, “Cascading failure analysis with DC power flow model and transient stability analysis,” *IEEE Trans. Power Syst.*, vol. 30, no. 1, pp. 285–297, Jan. 2015.

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

[12] D. P. Nedic, I. Dobson, D. S. Kirschen, B. A. Carreras, and V. E. Lynch, “Criticality in a cascading failure blackout model,” *Int. J. Elect. Power Energy Syst.*, vol. 28, no. 9, pp. 627–633, Nov. 2006.

[13] H. Cetinay et al., “Analyzing cascading failures in power grids under the AC and DC power flow models,” *Assoc. Comput. Machinery SIGMETRICS Perform. Eval. Rev.*, vol. 45, no. 3, pp. 198–203, Nov. 2017.

[14] I. Dobson, “Where is the edge for cascading failure?: Challenges and opportunities for quantifying blackout risk,” in *Proc. IEEE Power Eng. Soc. Gen. Meeting*, 2007, pp. 1–8.

[15] S. V. Buldyrev, R. Parshani, G. Paul, H. E. Stanley, and S. Havlin, “Catastrophic cascade of failures in interdependent networks,” *Nature*, vol. 464, no. 7291, pp. 1025–1028, Apr. 2010.

[16] B. Schäfer, D. Witthaut, M. Timme, and V. Latora, “Dynamically induced cascading failures in power grids,” *Nature Commun.*, vol. 9, no. 1, pp. 1–6, Dec. 2018.

[17] B. M. R. Amin et al., “Cyber attacks in smart grid-dynamic impacts, analyses and recommendations,” *Inst. Eng. Technol. Cyber-Phys. Syst., Theory Appl.*, vol. 5, no. 4, pp. 321–329, Dec. 2020.

[18] 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.

[19] J. Song, E. Cotilla-Sanchez, G. Ghanavati, and P. D. H. Hines, “Dynamic modeling of cascading failure in power systems,” *IEEE Trans. Power Syst.*, vol. 31, no. 3, pp. 2085–2095, May 2016.

[20] 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.

[21] R. Atat, M. Ismail, S. S. Refaat, E. Serpedin, and T. Overbye, “Cascading failure vulnerability analysis in interdependent power communication networks,” *IEEE Syst. J.*, vol. 16, no. 3, pp. 3500–3511, Sep. 2022.

[22] T. Tu, Y. Liao, X. Li, L. Wang, F. Zhang, and X. Guo, “Vulnerability assessment of cyber-physical power systems considering failure propagation: A percolation-based approach,” *Inst. Eng. Technol. Gener., Transmiss. Distrib.*, vol. 17, pp. 4344–4358, Apr. 2023.

[23] R. A. Shuvro, P. Das, J. S. Jyoti, J. M. Abreu, and M. M. Hayat, “Data-integrity aware stochastic model for cascading failures in power grids,” *IEEE Trans. Power Syst.*, vol. 38, no. 1, pp. 142–154, Jan. 2023.

[24] 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.

[25] 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.

[26] 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.

[27] 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.

[28] 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.

[29] S. Liu, B. Chen, T. Zourntos, D. Kundur, and K. Butler-Purry, “A coordinated multi-switch attack for cascading failures in smart grid,” *IEEE Trans. Smart Grid*, vol. 5, no. 3, pp. 1183–1195, Mar. 2014.

[30] 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.

[31] N. Kush, E. Ahmed, M. Branagan, and E. Foo, “Poisoned GOOSE: Exploiting the GOOSE protocol,” in *Proc. Australas. Inf. Secur. Conf.*, 2014, pp. 17–22.

[32] V. S. Rajkumar, M. Tealane, A. Ştefanov, A. Presekal, and P. Palensky, “Cyber attacks on power system automation and protection and impact analysis,” in *Proc. IEEE PES Innov. Smart Grid Technol. Eur.*, 2020, pp. 247–254.

[33] T. J. Browne, V. Vittal, G. Heydt, and A. R. Messina, “Practical application of Hilbert transform techniques in identifying inter-area oscillations,” in *Inter-Area Oscillations Power Systems*, Power Electronics Power Syst., Springer, Boston, MA, 2009. [Online]. Available: https://doi.org/10.1007/978-0-387-89530-7_4

[34] N. E. Huang et al., “The empirical mode decomposition and the Hilbert spectrum for nonlinear and non-stationary time series analysis,” *Proc. Roy. Soc. London. Ser. A, Math., Phys. Eng. Sci.*, vol. 454, no. 1971, pp. 903–995, Nov. 1998.

[35] M. S. Fabus, A. J. Quinn, C. E. Warnaby, and M. W. Woolrich, “Automatic decomposition of electrophysiological data into distinct nonsinusoidal oscillatory modes,” *J. Neurophysiol.*, vol. 126, no. 5, pp. 1670–1684, Nov. 2021.

[36] V. Klema and A. Laub, “The singular value decomposition: Its computation and some applications,” *IEEE Trans. Autom. Control*, vol. 25, no. 2, pp. 164–176, Apr. 1980.

[37] S. Chakrabarti and E. Kyriakides, “Optimal placement of phasor measurement units for power system observability,” *IEEE Trans. Power Syst.*, vol. 23, no. 3, pp. 1433–1440, Aug. 2008.

Vetrivel Subramaniam Rajkumar received the MSc. degree in electrical engineering from the Delft University of Technology, Delft, 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 University Politehnica of Bucharest, Bucharest, Romania, in 2011, and the Ph.D. degree from University College Dublin, Dublin, Ireland, in 2015.

He is currently an Assistant Professor in intelligent electrical power grids with the Department of Electrical Sustainable Energy, TU Delft, Delft, The Netherlands. He is also the Director of Control Room of the Future (CRoF) Technology Centre. He is leading the Cyber Resilient Power Grids (CRPG) research group. His research interests include cyber security of power grids, resilience of cyber-physical systems, and next generation grid operation.

Dr. Stefanov holds the professional title of Chartered Engineer from Engineers Ireland.

José Luis Rueda Torres (Senior Member, IEEE) was born in 1980. He received the Electrical Engineer Diploma (cum laude Hons.) from Escuela Politcnica Nacional, Quito, Ecuador, in 2004, and the Ph.D. degree (Sobresaliente) in electrical engineering from the National University of San Juan, San Juan, Argentina, in 2009.

He is currently an Associate Professor leading the research team on dynamic stability of sustainable electrical power systems with Intelligent Electrical Power Grids Section, Electrical Sustainable Energy Department, Delft University of Technology, Delft, The Netherlands. From 2003 to 2005, he worked in Ecuador, in the fields of industrial control systems and electrical distribution networks operation and planning. Between 2010 and 2014, he was a Postdoctoral Research Associate with the Institute of Electrical Power Systems, University Duisburg-Essen, Duisburg, Germany. His research interests include physics-driven analysis of stability phenomena, dynamic equivalencing of HVdc–HVac systems, probabilistic multisystemic reliability and stability management, and adaptive-optimal resilient multiobjective controller design.

Dr. Torres is a Member of the Technical Committee on Power and Energy Systems of IFAC (International Federation of Automatic Control), Chairman of the IEEE PES Working Group on Modern Heuristic Optimization, Secretary of CIGRE JWG C4/C2.58/IEEE “Evaluation of Voltage Stability Assessment Methodologies in Transmission Systems”, Vice-Chair of the IEEE PES Intelligent Systems Subcommittee, and Vice-Chair of the IFAC Technical Committee TC 6.3. Power and Energy Systems on social media.

Peter Palensky (Senior Member, IEEE) received the M.Sc. degree in electrical engineering and the Ph.D. and Habilitation degrees from Vienna University of Technology, Austria, in 1997, 2001, and 2015, respectively.

He is currently full Professor of intelligent electric power grids and the Head of the Electrical Sustainable Energy Department, TU Delft, Delft, The Netherlands. His research interests include energy automation networks, smart grids, and modeling intelligent energy systems.

Dr. Palensky is currently an IEEE IES AdCom Member-at-Large in various functions for IEEE. He is past Editor-in-Chief Editor-in-Chief of IEEE Industrial Electronics Magazine, an Associate Editor of several other IEEE publications, and regularly organizes IEEE conferences.