Journal of Electrical Engineering, Electronics, Control and Computer Science – JEEECCS, Volume 8, Issue 30, pages 21-32, 2022

Stochastic Quantification of Cyber Attacks Impact on Smart Grid Contingency Analysis

*Lukumba Phiri[1]
Department of Electrical and Electronic Engineering, School of Engineering, University of Zambia, Lusaka, Zambia
phirilukumba@gmail.com

Simon Tembo
Department of Electrical and Electronic Engineering, School of Engineering, University of Zambia, Lusaka, Zambia

Kumbuso Joshua Nyoni
College of Science and Engineering, School of Geosciences, University of Edinburgh, UK

Umair Shahzad
Department of Electrical and Computer Engineering, University of Nebraska-Lincoln, Lincoln, Nebraska, USA

***Abstract* – A cyberattack on a power grid facility could have repercussions for other infrastructure in the chain, causing a domino effect if the repercussions are not addressed, damaging the entire power system. Our objective was the investigation and quantification of the impact of cyberattacks on interdependent power systems facilities. In this paper, a novel technique based on Stochastic Petri Nets is presented, as well as a comprehensive model of the major impacts of blackouts and cascading events in the power systems of the IEEE 24 bus system is presented in form of loss of revenue. The paper also hypothesizes cyberattacks or digital control system failure as possible causes for cascaded power blackouts. Furthermore, the limitations of current preventive methods and research gaps in the area of power system blackouts and cascade occurrences are identified. Future power system blackout studies and risk assessments shall take this into account as well.**

Keywords-Cascade, Cyberattacks, False Data Injection Attacks (FDIA), Domino effect, Impact, Stochastic Petri Nets

I. INTRODUCTION

Power Systems, which serve as the economic and security backbone of modern digital society, are among the most intricate and critical infrastructures. As a result, protecting one's activities from cyber threats and attacks is in everyone's best interests [1]. Cybersecurity threats could have cascade repercussions, resulting in property damage, power disruptions, and personal data breaches [2-3].

Situational awareness is required for smart power grids, which is aided by real-time monitoring and exact system status evaluation via Phasor Measurement Units (PMUs) [4]. Unfortunately, false data assaults can exploit the PMUs' communication design. False data attacks include the injection, blocking, deletion, and manipulation of data and status, as well as a combination of any of the foregoing devices or communication network routes that jeopardize the reliable operation of power systems [5].

Three essential functions can be used to evaluate online physical security in power system operations: (1) state estimation (SE), (2) contingency analysis (CA), and (3) security-constrained optimum power flow (SCOPF) [6]. SE's goal is to process data from a supervisory control and data acquisition (SCADA) system (for example, power injection/flow, bus voltage magnitude, and circuit breaker on/off status), calculate the best estimate of the power system's state and build real-time network models based on the estimate [7].

Power systems' capacity to maintain stability and provide a continuous supply of electrical power to clients in the case of disruption is crucial [8–10]. The power system network spans a large geographic area, and the probability of facing different types of faults and failures is relatively high. [5–9]. Attackers could exploit potential cyber weaknesses in the power grid, posing a significant threat to the system stability managed by power utilities. When the configuration restrictions are insufficiently enforced, attackers can sneak in through bidirectional remote access between substations and control centers, as well as protective limitations across the border firewalls [11].

According to hypothetical drill exercises undertaken by [12-14], a combination of 9 major substations would be sufficient to cause a widespread power outage in the USA. This and many other combinations of cases proved sufficient enough to initiate cascading consequences to the grid [12-16].

Every electrical system should be operated in such a way that the failure of a single component does not overload the other components, according to the North American Electric Reliability Corporation (NERC) [17]. In power networks, this is known as the N-1 rule [2].

The formulation of the network equations determines how long traditional contingency analyses take to compute. Iterative approaches like Gauss-Seidel[18], New-ton-Raphson[19], and the quick decoupling method[20] are used to solve power flow equations in power systems.

This creates computational difficulties when it comes to creating effective attack mitigation measures. Because of these difficulties, most tools are only useful for analyzing contingencies induced by the breakdown of one or two components in the power system [21].

Furthermore, existing contingency analysis techniques[18,19,20], ignore strategic and intelligent attackers, treating distinct attack profiles as flaws in the system. Smart attackers, on the other hand, can take advantage of such naive protection techniques and cause severe harm to the system.

In this paper, we look at the problems that arise as a result of higher-order contingency conditions caused by cyber-attacks. Our method provides effective tools for considering higher-order cyber-physical contingency analysis in a stochastic framework. Furthermore, we present computationally efficient techniques for dealing with higher-order contingency conditions.

Several assumptions underpin this study. Each assumption is evaluated in terms of its impact on power system operations. These interpretations are presented in this section.

a) For the safe operation of electrical energy networks, contingency analysis and risk assessment are critical activities. The knowledge of possible contingency events in a system can be used in the system state forecast estimation.

b) Performing a load-flow study to estimate contingency risk is a time-consuming and complex process.

c) When working with a big power system, the load-flow analysis is a time-consuming technique. The performance of power-flow outcomes, on the other hand, is valued in this work and is utilized as a benchmark for model performance and design.

d) The statistical technique is applied to time-consuming contingency analysis functions, resulting in a reduction in the contingency analysis process' overall calculation time.

The major contribution of this work is to i) re-establish the cyber-based contingency approach to extensively enumerate (the sum of S-k contingencies) by incorporating overloaded lines based on hypothesized substation outages, and (ii) develop a Semi-Markov Process (SMP) to model the impact of cyber attacks on the power system contingency analysis.

The remainder of this work is arranged in the following manner. Section II gives an overview of the traditional contingency analysis. Section III presents a new principle for power system contingency analysis. The proposed SMP model is introduced in Section IV. Case studies are conducted, and the findings are described in Section V. This paper's final observations are found in Section VI.

II. Review of Power Systems Analysis

The notion of power systems analysis is explained in detail in this chapter. This project's purpose is to create a model of the power grid and its accompanying control systems that may be used to analyze cyber security assaults. We're searching for large-scale power-grid consequences that are manifested through aggressive manipulation with control systems in particular. The basic power system flow is depicted in Fig. 1, which includes power generation, power distribution, and power consumption.

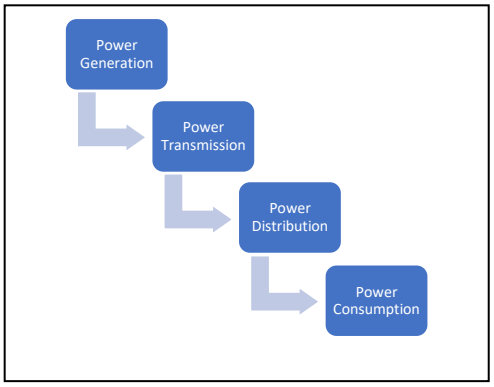

Fig. 1. Basic Concept of Power Systems flow

A. Review of the Four-Bus Test System

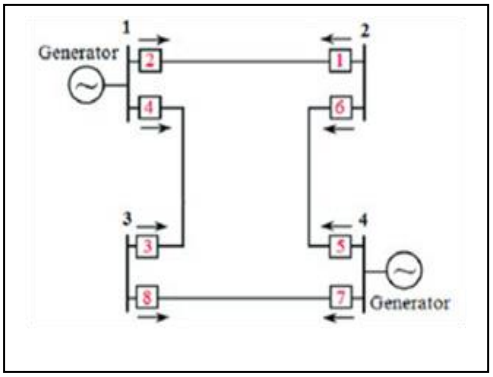

Fig.2. IEEE Four Bus system

The basic equation for power-flow analysis is derived from the nodal analysis equations of the power system: Take, for example, the four-bus system shown in Fig. 2.

$$\begin{bmatrix} Y11 & Y12 & Y13 & Y14 \\ Y21 & Y22 & Y23 & Y24 \\ Y31 & Y32 & Y33 & Y34 \\ Y41 & Y42 & Y43 & Y44 \end{bmatrix} \begin{bmatrix} V1 \\ V2 \\ V3 \\ V4 \end{bmatrix} = \begin{bmatrix} I1 \\ I2 \\ I3 \\ I4 \end{bmatrix} \quad (1)$$

where *Yij* is the elements of the bus admittance matrix, *Vi* is the bus voltages, and *Ii* is the currents injected at each node. The node equation at bus *i* can be written as

$$\boldsymbol{I_i} = \sum_{j=1}^{n} \boldsymbol{Y_{ij} V_j} \quad (2)$$

The per-unit real and reactive power provided to the system at bus I and the per-unit current injected into the system at that bus have the following relationship:

$$S_i = V_i \, I_i^* = P_i + \mathrm{j} Q_i \quad (3)$$

where *Vi* is the per-unit voltage at the bus; I_i^* - the complex conjugate of the per-unit current injected at the bus; Pi and Qi are per-unit real and reactive powers. Therefore,

$$I_i^* = (P_i + jQ_i)/V_i \quad (4)$$

$$I_i = (P_i - jQ_i)/V_i^* \quad (5)$$

$$P_i - jQ_i = V_i^* \sum_{j=1}^{n} Y_{ij} V_j \quad (6)$$

Let $\boldsymbol{Y_{ij}} = |\boldsymbol{Y_{ij}}|\angle\boldsymbol{\theta_{ij}}$ *and* $\boldsymbol{V_i} = |\boldsymbol{V_i}|\angle\boldsymbol{\delta_i}$

$$\boldsymbol{P_i} - j\boldsymbol{Q_i} = \sum_{j=1}^{n} |\boldsymbol{V_j}|\,|\boldsymbol{Y_{ij}}||\boldsymbol{V_i}|\angle(\boldsymbol{\theta_{ij}} + \boldsymbol{\delta_j} - \boldsymbol{\delta_i}) \quad (7)$$

$$\boldsymbol{P_i} = \sum_{j=1}^{n} |\boldsymbol{V_j}|\,|\boldsymbol{Y_{ij}}||\boldsymbol{V_i}|\boldsymbol{cos}(\boldsymbol{\theta_{ij}} + \boldsymbol{\delta_j} - \boldsymbol{\delta_i}) \quad (8)$$

$$\boldsymbol{Q_i} = -\sum_{j=1}^{n} |\boldsymbol{V_j}|\,|\boldsymbol{Y_{ij}}||\boldsymbol{V_i}|\boldsymbol{sin}(\boldsymbol{\theta_{ij}} + \boldsymbol{\delta_j} - \boldsymbol{\delta_i}) \quad (9)$$

Each bus is associated with its respective variable:

(i) P, (ii) Q (iii) V (iv) δ

In the meantime, each bus is linked to two power flow equations. In a power flow study, two of the four variables are known, while the other two are unknown. As a result, the number of equations equals the number of unknowns. The known and unknown variables differ depending on the bus type.

Each bus in a power system is classified into one of three types:

1. Load bus (P-Q bus) – a bus with defined real and reactive power and for which the bus voltage will be computed Load buses are those that do not have generators. V and δare unknown in this case.

2. Generator bus (P-V bus) – a bus on which the magnitude of the voltage is defined and maintained by modifying the synchronous generator's field current. According to the economic dispatch, we also assign real power generation to each generator. Q and δ are unknown in this case.

3. Slack bus (swing bus) – As the reference bus, a dedicated generator bus is used. The magnitude and phase of its voltage are presumed to be fixed (for instance, $1\angle 0^{\circ}$ pu). Here, P and Q are unknown.

Formulation of power-flow

Because the power flow equations are non-linear, they are impossible to solve analytically. Solving such equations necessitates the use of a numerical iterative procedure. The following is a standard procedure:

1. For the power system, create a Ybus bus admittance matrix;

2. Calculate the voltages (both magnitude and phase angle) at each bus in the system;

3. Plug in the power flow equations and calculate the deviations from the answer.

4. Use several well-known numerical procedures to update the estimated voltages (e.g., New-ton-Raphson or Gauss-Seidel).

5. Repeat step 5 until the deviations from the solution are as small as possible.

B. Applications of State Estimation

The output of the SE is the starting point for all essential applications in the EMS, such as optimal power flow (OPF) and economic dispatch, load forecast, and voltage security. To meet customer demand while lowering operational costs, the line power flow is computed using the OPF analysis and economic dispatch. This is done by solving a set of nonlinear power balance equations, which comprise generation, load, and network equations [22]. The security-constrained optimum power flow (SCOPF)[6] is a variant of the optimal power flow solution that incorporates additional constraints such as generator power restrictions, transmission line capacity, and contingency constraints. The SCOPF assures that the system is stable both before and after a disaster, with no system operating limits (SOL) breaches. [23–25].

The results of OPF assist the real-time contingency analysis (RTCA) to determine the binding thermal and voltage constraints, ensuring N-1 or N-1-1 reliability of the power system under all real-time operating conditions [26]. In other words, this means system operating limits (SOL) are satisfied at every instant. In general, three types of SOL are defined as - 24 hours (normal), 4 hours long-term emergency (LTE), and 15 minutes short-term emergency (STE). Depending on the currently estimated states and the load demand, transfer analysis helps determine the extent to which the current operating system can be moved before being bounded by SOL. To ensure safety and continuous operation, actions against SOL violations range from generation dispatch, and load curtailment to other appropriate emergency control actions.

In the electricity market [27], the information from SE and OPF/SCOPF is used to determine Locational Marginal Prices (LMP). The LMP compensates for the customer load pattern, cost of generation, and transmission line congestion while reflecting the price of power across different geographies. The electricity market allows generating power plants to sell power at a specified bidding price in the day-ahead (ex-ante market) and the real-time market (ex-post market) while simultaneously satisfying the customer need [27], [28]. The operation of AVC can be briefly explained as follows - first, the output of the SE, i.e., voltages and angles, are fed as an input to the OPF block. Once the OPF converges to a valid solution, the results are used to issue trigger commands to vary generator reactive power to maintain voltages within the prescribed margin of 0:9 – 1.1 p.u [29-30].

The SE output also drives the power system's automated generation control (AGC) [31–33], basic control, and operating block. By limiting generator output power and lowering area control error, the AGC ensures a nominal grid frequency and tie-line power flow within a designated control area. In addition, the estimated system states, along with the OPF, are used to calculate generating reserves to guarantee grid frequency is maintained in the case of a power outage.

C. Related Works

The stochastic hybrid system (SHS) is a mixture of the linearized differential-algebraic equation (DAE) model and the CTMC, as described in [34]. They claim that active/reactive power injections are governed by a continuous-time Markov chain (CTMC), while power system dynamics are governed by the standard DAE model. To linearize the DAE model, a hypothetical set of active/reactive power injections is used. The authors

of [35] suggested solving the resulting bilinear programming model using the big – M technique and giving the decomposition method. Both the advantages of RO and stochastic programming are combined in the suggested technique. Zhou and his associates. [36] investigated the application of the stochastic response surface method (SRSM) to small-signal stability analysis of coupled solar and load systems with probabilistic uncertainty. The impact of false data integration attacks (FDIA) on power systems was investigated in [37].

In [38-39], the authors described an integrated operational simulation tool that includes different stochastic unit commitment (SUC) and economic dispatch models that take stochastic loads and variable generation into account across multiple operational timescales. The program included customizable sub-models for day-ahead security-constrained unit commitment (SCUC), real-time SCUC, real-time security-constrained economic dispatch (SCED), and automatic generation control (AGC).

Milano and Minano [40] present a broad and systematic framework for modeling power systems as continuous stochastic differential-algebraic equations. This was accomplished in the paper by providing a theoretical background on stochastic differential-algebraic equations and advocating for the use of stochastic models in power system research. Similarly, [41], [42], and [44] recommended the use of stochastic differential equations (SDEs), a sort of power system model. [41] looks at quasi-Hamiltonian power systems with losses and SDEs in the first section. Second, an unique analytical method for studying the stability of the power system with losses under SDEs is proposed, based on the stochastic averaging method. [42] examines the stability of the quantity of uncertainty in a power system using the noise-to-state stability (NSS) and NSS Lyapunov function (NSS-LF).

[43] designs Dynamic Load Altering Attacks to counter smart grid demand response algorithms (D-LAA). The D-LAAs are described in great depth. Open-loop vs. closed-loop assaults, single-point vs. multi-point attacks, feedback type, and attack controller type are all examples of D-LAAs. The attacker uses feedback from the power system frequency to manage changes in the victim load, which is defined and assessed, in a closed-loop D-LAA against power system stability. Zhang et al [44], proposed a forced outage rate (FOR) model to study the reliability of the generators and transmission lines. Authors in [45], used the Bayesian networks to model the attack propagation process and inferred the probabilities of sensors and actuators being compromised. The probabilities were fed into a stochastic hybrid system (SHS) model to predict the evolution of the physical system being controlled. [46, 47,48], also attempted to study the impacts of cyberattacks on the physical components of the power systems such as circuit breakers.

Several methods to model cascading failures in power systems have been proposed in the literature review; however, the strategies proposed do not include overloaded lines based on hypothesized substation outages, or a Semi-Markov Process (SMP) to model the impact of cyberattacks on power system contingency analysis.

III. Methodology

Fig. 3 depicts the method employed in this experiment.

The failure of a target unit in a power system domino effect research is determined by the dynamic properties of the escalation vectors (physical effects), threshold values, target unit category, system parameters, and the robustness of the mitigation/intervention systems. Following a successful breach into a substation network, attackers can use their domain-specific abilities to produce traffic manipulation. To maximize the impact of an attack, important cyber-physical security understanding between established communication protocols and the interface with physical equipment is critical. The attacker would need to understand software settings and how device addresses in power control centers correspond to user interfaces. The most obvious manipulation is to add delay to each signal, which has an impact not only on the protection system but also on the SCADA capability of the control center. The breaker in a damaged part of the transmission line is delayed when a trip signal is blocked for a specified period, which might cause a system failure. This section contains a collection of credible clever attack strategies that have successfully penetrated a substation network.

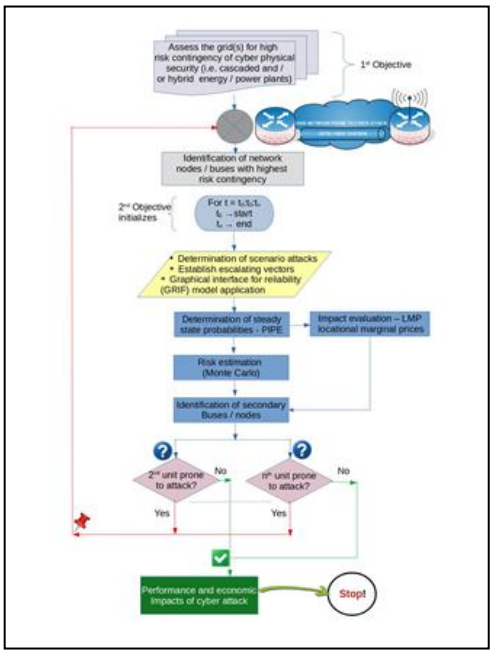

Fig. 3. Methodology Flow Diagram

A. Representation of system states (state of each unit)

An industrial system is made up of several subsystems or units (*U1, U2, ..., Un*). The domino effect analysis framework divides each unit into four stages:

1. State1, Normal state (N),

2. State2, Vulnerable state (V),
3. State3, Failure state (F)
4. State4, Restored state (R).

Masked compromised state, undiscovered compromised state, triage state, fail-secure state, and graceful degradation state are examples of intermediate stages between Normal and Restored [49]. The intermediate phases are merged into the failed state for the sake of simplicity.

B. Transition between system states

Considering two units, the transitions may take place from state 1 to state 2,3, and/or state 4.

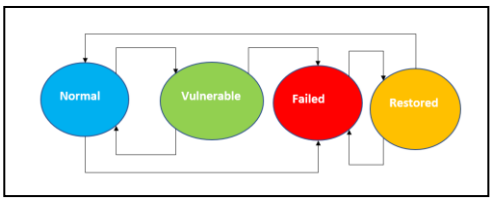

Fig. 4. Description of system states

Given the stochastic nature of attacks, a transition into state V can be characterized as an exponential distribution with the rate λ_{NV} when the system is in state N (commonly referred to as zero-day attacks). This is because once the system's security is compromised (state V), the chances of a serious attack increase, and the system goes to state F. To replicate the duration spent in state V, which simulates a generally increasing rate of failure, a Weibull distribution (shape parameter θ, scale parameter β) with $\theta_{VF}, \beta_{VF} > 1$ is utilized.

On the other hand, unsuccessful attacks mimic a decreasing failure rate, and the transition from V to N is modeled as a Weibull distribution with $\theta_{VN}, \beta_{VN} < 1$. The change from N to F reflects an insider assault based on past system information, which is likewise considered to be stochastic and described using exponential distributions with λ_{WF}. When system operators uncover malicious attempts, they disconnect the systems and install fixes to address the vulnerabilities. The system now enters the recovery phase. Transitions from F to R or R to F are considered stochastic for both successful and unsuccessful patch installations.

Given the sophistication and novelty of zero-day attacks, a rapid mitigation method may not be easily available. An exponential distribution is used to modify the transition from R to W. The fundamental idea is to use non-exponential distributions to model activities involving increasing or decreasing the rate of failures, and exponential distributions to model stochastic actions.

Table I summarizes the cumulative distribution functions (CDF) of time spent in various states. The steady-state probability π_i is derived using the state transitions.

TABLE I. DESCRIPTION OF TRANSITIONS

CDF	Distribution	Parameters	Expression
$\mathbf{P_{NV}}$	Exponential	λ_{NV}	$1\text{-}e^{-\lambda NVt}$
$\mathbf{P_{NF}}$	Exponential	λ_{NF}	$1\text{-}e^{-\lambda NFt}$
$\mathbf{P_{VN}}$	Weibull	θ_{VN}, β_{VN}	$1\text{-}e^{-(t/\beta VN)\theta VN}$
$\mathbf{P_{VF}}$	Weibull	θ_{VN}, β_{VN}	$1\text{-}e^{-(t/\beta VF)\theta VF}$
$\mathbf{P_{FR}}$	Exponential	λ_{FR}	$1\text{-}e^{-\lambda FRt}$
$\mathbf{P_{RF}}$	Exponential	λ_{RF}	$1\text{-}e^{-\lambda RFt}$
$\mathbf{P_{RN}}$	Exponential	λ_{RN}	$1\text{-}e^{-\lambda RNt}$

The steady-state probabilities describe the fraction of time the system spends in different states over the whole assault horizon, i.e. The semi-Markov Process is then meticulously mathematically modeled.

Starting with the failure of at least one unit as the starting event, one can study the domino effect sequence. At least one unit, according to the assumption, has failed.

C. Sojourn Time and Transition Probability of Semi-Markov Process

The semi-Markov Process is then meticulously mathematically modeled. The steady-state probabilities describe the fraction of time the system spends in different states over the entire assault horizon.

The domino effect sequence can be studied by starting with the failure of at least one unit as the initiating event. According to the presumption, at least one unit has failed.

According to the presumption, at least one unit has failed.

(1) J = $(\boldsymbol{J_m})\mathbf{m} \in \mathbf{N}$ where $(\boldsymbol{J_m})$ is the system state at the m^{th} time,

(2) S = $(\boldsymbol{S_m})\mathbf{m} \in \mathbf{N}$ where $(\boldsymbol{S_m})$ is the m^{th} transition time and

(3) X = $(\boldsymbol{X_m})\boldsymbol{m} \in \boldsymbol{N}$ where $(\boldsymbol{X_m}) = (\boldsymbol{S_m}) - (\boldsymbol{S_{m-1}})$ is the sojourn time in state $(\boldsymbol{J_{m-1}})$. The chain $(\boldsymbol{J_m}, \boldsymbol{S_m})\mathbf{n} \in \mathbf{N}$ is a Markov renewal chain if $\forall$ m $\in$ N,

$$P((\boldsymbol{J_{m+1}}) = j, \boldsymbol{S_{m+1}} - \boldsymbol{S_m} = k/\boldsymbol{J_0}, \boldsymbol{S_0}, \ldots, \boldsymbol{J_m}, \boldsymbol{S_m})$$

$$P((\boldsymbol{J_{m+1}}) = j, \boldsymbol{S_{m+1}} - \boldsymbol{S_m} = k/\boldsymbol{J_m}) \quad (10)$$

Equation (10) shows that the next transition state and time spent in the current state are completely dependent on the system's current state. The semi-Markov chain is a type of Markov chain. $Z = (\boldsymbol{Z_k})\mathbf{k} \in \mathbf{N}$ associated with the Markov renewal process (J, S) is $\boldsymbol{Z_k} = \boldsymbol{J_{N(k)}}$. N represents the number of transitions that occur during time k. The average sojourn period for the SMP in each state is derived using the formula:

$$\boldsymbol{t_i} = \int_0^{\infty} (\mathbf{1} - \boldsymbol{P_{ij(k)}})\,(\mathbf{1} - \boldsymbol{P_{ik(k)}})\,dk \quad (11)$$

where j; k is reachable states from i and $(\mathbf{1} - \boldsymbol{P_{ij(k)}})$ is the duration of sojourn in state i's survival function.

With an exponential distribution, the sojourn time in state N can be expressed as, for example, using equation (11).

$$\boldsymbol{t_i} = \int_0^{\infty} (\boldsymbol{P_{NV}})\,(\boldsymbol{P_{NF}})\,dt = \int_0^{\infty} (\boldsymbol{e^{-(\lambda NV + -\lambda NF)t}}\,dt \quad (12)$$

Sojourn times for states V, F, and R can be written similarly.

A transition probability matrix Q is defined for the evolution of this SMP. The elements of Q = Qij(k) are defined as, and they indicate the likelihood of transitioning from a state I to state j within time k.

$$\boldsymbol{Q_{ij}(k)} = P\,(\boldsymbol{J_{n+1}} = j, \boldsymbol{X_{n+1}} \leq k \boldsymbol{J_n} = \boldsymbol{i}) \quad (13)$$

The constituents of the kernel Q can be evaluated as Pij signifies the cumulative distributions of the sojourn time in state I corresponding to the following state j.

$$\boldsymbol{Q_{ij}(k)} = \int_0^{k} (\mathbf{1} - \boldsymbol{P_{ik(k)}})\; d\boldsymbol{P_{ik(k)}} \quad (14)$$

where j; k is reachable states from I and (1 - Pij(k)) is the sojourn time survival function in state i. The transition probability matrix Q can be written as, as seen in (15).

$$Q = \begin{vmatrix} 0 & QNV & QNF & 0 \\ QVN & 0 & QVF & 0 \\ 0 & 0 & 0 & QFR \\ QNV & 0 & QRF & 0 \end{vmatrix} \quad (15)$$

The one-step transition probability matrix in the steady-state analysis of the SMP is computed as $M = Q(\infty)$, assuming state transitions are time-independent. After that, by solving the set of linear equations with M, the steady-state probability vector of the embedded Markov chain $v = \{\boldsymbol{v_1}, \boldsymbol{v_2}, \text{----}\boldsymbol{v_n}\}$ may be obtained. $v = vM$ with $\sum_{i=1}^{n} \boldsymbol{v_i} = \mathbf{1}$. The steady-state probabilities $\boldsymbol{\pi_i}$ are then evaluated as

$$\boldsymbol{\pi_i} = \frac{\boldsymbol{v_i t_i}}{\sum_{\delta} \boldsymbol{v_i t_i}},\ i \in \delta \quad (16)$$

D. Simplified Generalised Stochastic Petri Nets (GSPN) Model

Each unit can be described by a state graph represented by a basic (elementary) Stochastic Petri Nets as a result of the preceding procedures. The units in place P1 are in normal operation. The vulnerable buses are housed in P2. P3 is where the buses that have been recovered are kept. P4 is the location of the failed buses, and it is a source of hazard for the adjacent apartments (see Fig. 5).

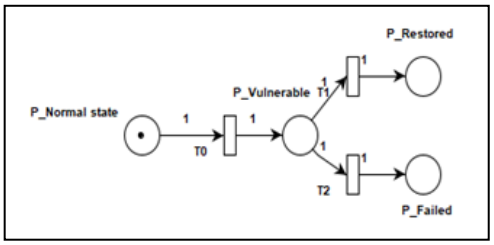

Fig. 5. GSPN model for the defined state

E. Firing conditions

According to the preceding procedures, a primary scenario resulted in the catastrophic failure of one bus, which may have generated a system disruption that impacted other nearby units. The firing of transitions simulates the evolution of system behavior, with each transition firing matching the occurrence of an event. Similarly, an event alters the system state, causing transition fires and, eventually, changes to the Stochastic Petri Net marking.

F. Failure probability/mitigation probability

According to Fig. 5, the failure probability (PCFi) for each bus may be calculated as the firing probability of the transition T2. The mitigation probability of the unit Bi is the firing probability of the transition T1 knowing that the transition T0 is fired.

G. Domino scenario probability

While the failure probability, PBi, is known for each unit, The chance of a domino effect can be computed for the entire system. The likelihood of each domino scenario (domino sequence) can be calculated as follows:

$$\boldsymbol{P_{CF}} = \prod_{j=1}^{n} \boldsymbol{P_{Bi}} \quad (17)$$

$\boldsymbol{P_{CF}}$ is the joint probability that each unit in sequence I fail, and n is the number of failed units in the domino sequence, where n is the number of failed units in the domino sequence.

IV. CASE STUDY

The defined methodology in chapter 3 was used in the case study to assess the domino effect in the case of an IEEE 4 Bus system.

A. Scenario 1: Bus 1 to Bus 2 cascade propagation Considering both Physical and Cyber Failures

Figure 6 depicts the layout that was evaluated during the analysis. We suppose that the breakdown of generator number 1 was caused by both a physical failure and a cyberattack scenario, affecting bus 1. The latter can cause escalation vectors, which can affect nearby units. For buses 1 and 2, we convert Fig. 2 into a state-space graph or generalized stochastic model.

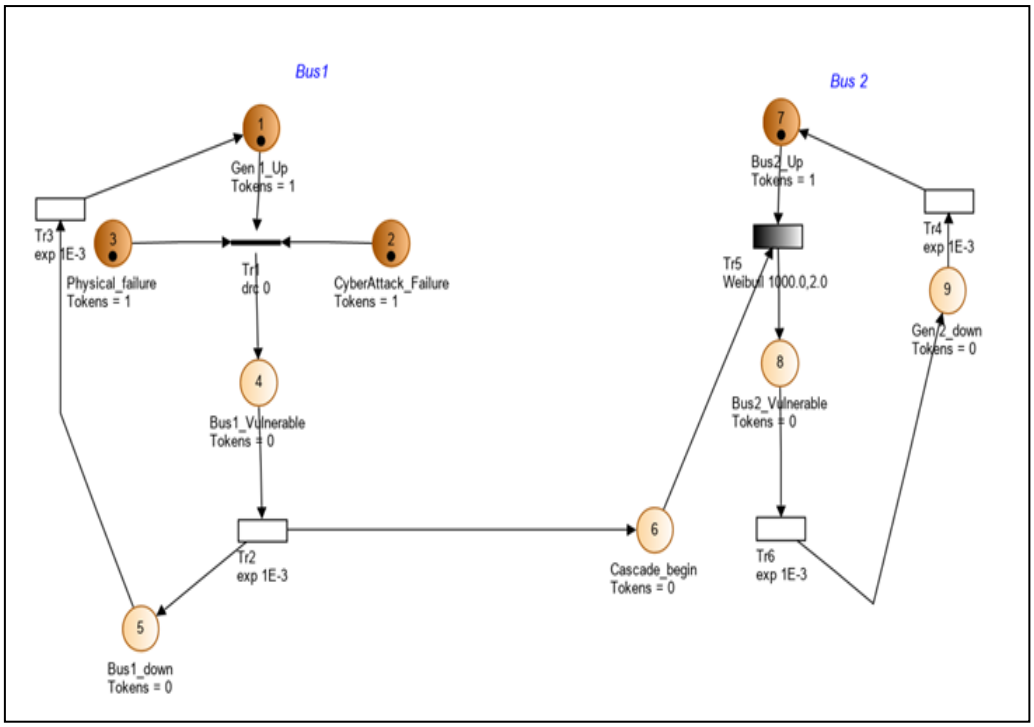

Fig. 6. Considering Both Physical and Cyber failures

In which its initial state, there is a token each in the places Gen1_Up, Physical_failure, CyberAtack_Failure, and Bus2_Up. The transition Tr1 once enabled changes the state of bus 1 from normal to vulnerable without any delay based on the protection settings of the transmission line intelligent electronic device (IED). The vulnerability of bus 1 has a cascading or domino effect on bus 2 if the vulnerability is sustained, and Tr2 is an exponentially distributed transition is enabled, then bus 1 fails. The failure propagates an effect on bus 2 which falls into a vulnerable state once Tr5 gets enabled. Similarly, if no action is applied bus 2 equally fails when the CDF transition Tr6 is enabled. The transitions Tr3 and Tr4 are restoration transitions for bus 1, and bus 2 respectively.

B. Scenario 2: Bus 1 to Bus 2, Bus 3, and Bus 4 cascade propagation

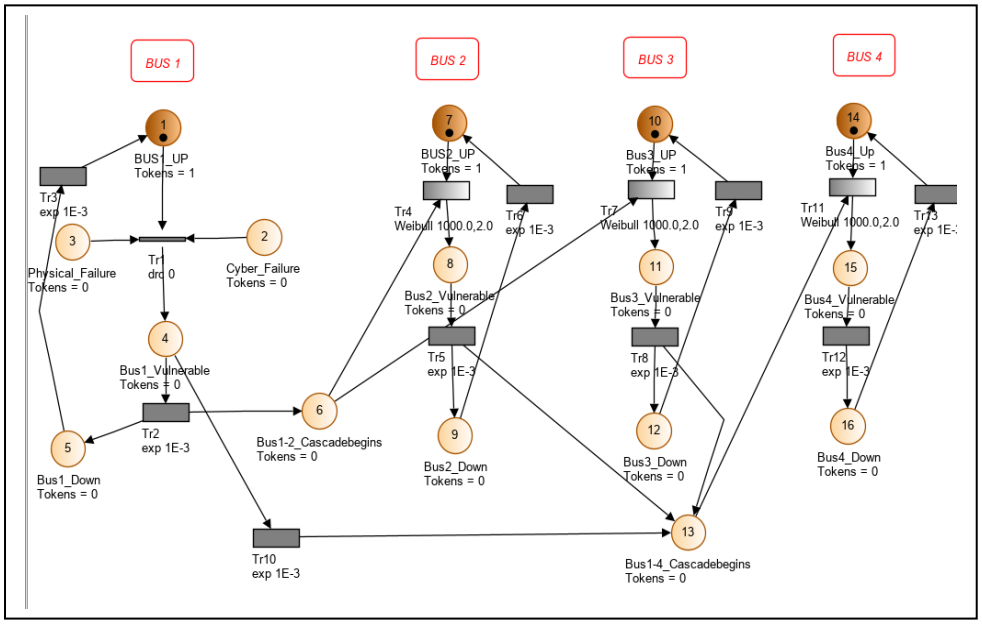

Fig. 7. Equivalent Stochastic model for for a Four Bus System

The final scenario depicted in Fig. 7, is a GSPN model for the entire 4 bus system. Tokens in places Bus1_Up, Bus2_Up, Bus3_Up, and Bus4_Up indicate that the four buses are in their normal operating state. The presence of tokens in places 2, and 3 introduce vulnerabilities in the form of physical and cyber failures. Firing or enabling of the transition Tr2 initiates a failure in Bus 1, and propagates cascaded effects to mostly buses 2 and 3, bus 4 is reliant mostly on power supply from generator 2 but it's equally vulnerable to a domino effect due to the loss of loads on the other busses if load curtailment is not initiated

C. Performance and Economic Impact of Attacks

The power system reliability worth evaluating in this study is the monetary loss. We adopted the formulation proposed in [50,51,52], letting Co be the optimal operating cost of the system under normal conditions (no cyber-attack). Let C_{Ln} denote the optimal cost of the system under n^{th} (N-1) line outage due to a cyber-attack.

Then, deviation from optimal cost under this condition is given by ΔC_{Ln}. Mathematically, we can write it as follows

$$\Delta C_{Ln} = C_{Ln} - C_O \quad (18)$$

The average cost deviation due to the (N-1) line an outage is given by ΔC_L. Mathematically,

$$\Delta C_L = \sum_{n=1}^{NL} \Delta C_{Ln} / N_L \quad (19)$$

Let σ denote the net economic impact due to both (N-1) lines by cyber-attack. Then:

$$\sigma = \Delta C_L \quad (20)$$

Further letting R_i denote the risk due to outages, then Risk is;

$$R_i = P_i x \sigma \quad (21)$$

where P_i denotes the probability of a cyber-attack (on single bus i).

V. VULNERABILITY EVALUATION AND IMPACT DISCUSSIONS

A. Scenario 1: Results

To model the domino effect, GRIF's PN module [53] was used by applying the transitions described in Table I, (14), and finally applying the instances described in Table II below. The resultant probabilities are depicted in Tables III and IV for scenarios 1 and 2 respectively.

TABLE II.SIMULATION SCENARIOS

	Number of histories	**First random number**	**Maximum calculation time**
Instance 1	10	12345681	10
Instance 2	100	12345681	10
Instance 3	1000	12345681	10
Instance 4	10,000	12345681	10

The results show that generator number 1 or bus 1 has a higher probability of being in a running state compared to bus 2. Conversely, a probability of 0.1497 compared to 0.112 shows that bus 1 is highly likely to be in a failed state. The sojourn times for the places depicting the escalation vectors are zero, and hence the steady-state probabilities for places CyberAttack_Failure and Physical_failure are zero.

TABLE III. STEADY-STATE PROBABILITIES SCENARIO 1

State	Instance Probabilities	Instance 2 Probabilities	Instance 3 Probabilities	Instance 4 Probabilities
Gen 1_Up	0.218912037	0.16771764	0.15347399	0.141604717
CyberAttack_Failure	0	0	0	0
Physical_failure	0	0	0	0
Bus1_Vulnerable	0.158933134	0.110965197	0.106574945	0.10042471
Bus1_down	0.149654942	0.117068243	0.106371085	0.10017746
Cascade_begin	0.036801102	0.048744505	0.047475634	0.046191394
Bus2_Up	0.144268051	0.159321881	0.148026631	0.138944834
Bus2_Vulnerable	0.050134476	0.109162418	0.104100555	0.099417391
Gen 2_down	0.112241987	0.109186027	0.104415866	0.098710829

TABLE IV. STEADY-STATE PROBABILITIES SCENARIO 2

State	Steady-State Probability	Instance 2 Probabilities	Instance 3 Probabilities	Instance 4 Probabilities
BUS1_UP	0.433850811	0.43452249	0.431120969	0.432954469
Cyber_Failure	0	0	0	0
Physical_Failure	0	0	0	0
Bus1_Vulnerable	0.085838129	0.057241576	0.051214666	0.048893878
Bus1_Down	0.05369558	0.083681461	0.091316239	0.085387221
Bus1-2_Cascadebegins	0.047193387	0.041509163	0.038681341	0.038476318
BUS2_UP	0.168198255	0.131439965	0.126147693	0.112466913
Bus2_Vulnerable	0.124942457	0.070541997	0.075268742	0.067284266
Bus2_Down	0.066882864	0.085536671	0.073917414	0.065913581
Bus3_UP	0.088703859	0.114639195	0.111429556	0.109050511
Bus3_Vulnerable	0.028640047	0.069577334	0.069194784	0.066200892
Bus3_Down	0.060073606	0.058586149	0.061599753	0.064143721
Bus1-4_Cascadebegins	0.045620111	0.050869293	0.04724814	0.046404441
Bus4_Up	0.139295519	0.151801784	0.146124909	0.138172721
Bus4_Vulnerable	0.117320166	0.11057571	0.105408834	0.099395137
Bus4_Down	0.060704225	0.099873658	0.099526062	0.097858459

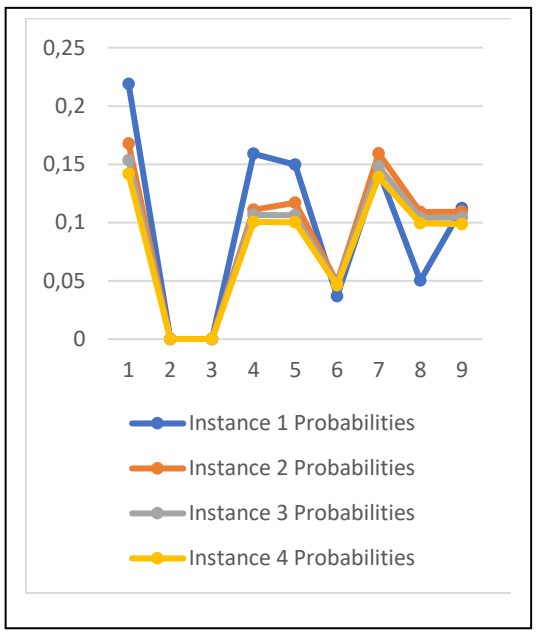

Fig. 8. Comparison of instances for scenario 1

B. Scenario 2: Results

Maintaining the argument introduced in sections III, and V, the steady-state probabilities for scenario 2 are depicted in Table IV.

The result suggests that the probability of buses being in the running state is higher for bus 1, seconded by bus2, third is bus 4 and last is bus 3. Concerning cascaded vulnerabilities; bus 2 has a higher likelihood of falling due to escalating vectors emanating from bus1, while bus1 is less likely to be affected by a cascaded vulnerability. States Bus1-2_Cascadebegins and Bus1-4_Cascadebegins depict the initiation of the cascading effects with the steady-state probabilities of 0.0471 and 0.0456 respectively.

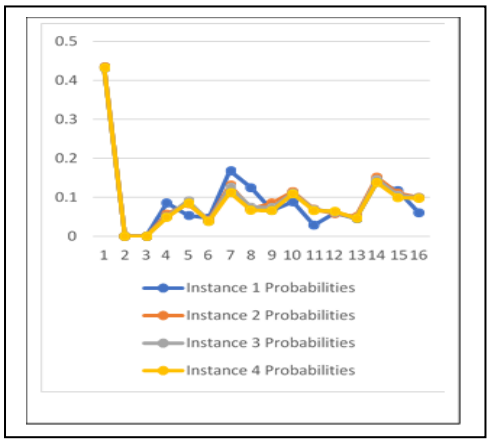

Fig. 9. Comparison of instances for scenario 2

C. Numerical Analysis of Performance and Economic Impact of Attacks on a 24 Bus System

Based on the computation procedure described in section IV and applied to the IEEE 24 bus [54]. The corresponding Locational Marginal Pricing (LMP) tabular results are shown in Table V. In this case, a data integrity attack on the transmission line and buses was modeled.

TABLE V. LMP CALCULATED IN MODIFIED IEEE 24 BUS TEST SYSTEM

BUS	LMP ($/hr)	BUS	LMP ($/hr)
1	56.3169	**13**	58.6915
2	56.5817	**14**	67.3583
3	52.6700	**15**	44.2975
4	57.2618	**16**	44.5828
5	59.8611	**17**	40.5909
6	60.5628	**18**	41.5488
7	46.1486	**19**	52.5032
8	58.4498	**20**	54.0081
9	57.8183	**21**	42.4102
10	59.0814	**22**	41.6976
11	61.6508	**23**	54.8289
12	57.8578	**24**	47.4390

From Table V, it is determined that buses 14, 11, and 6 have the highest LMP. As a result, these three elements are regarded as the most important when estimating the consequences of a cyber-attack. System designers must pay special attention to these components so that suitable rules and procedures may be developed to safeguard their integrity and make the system as dependable as possible. Evaluation of the economic impact is based on the LMP given in Table V above. As a result, the cyber-net attack's risk owing to bus outages (line) is calculated using (21).

$$R_{14} = 0.060 \times 67.3583 = \$\ 4.041/hr \quad (22)$$

$$R_{11} = 0.060 \times 61.6508 = \$\ 3.939/hr \quad (23)$$

$$R_{6} = 0.060 \times 60.5628 = \$\ 3.633/hr \quad (24)$$

VI. RECOMMENDATIONS AND FURTHER WORK

Results from this research can be used as a design guideline for the real-time system for the contingency analysis process in large power systems. The results obtained in section V can be postulated to the Zambian 330kV power system to conduct the actual monetary aspects**.** This study has demonstrated a novel way of quantifying the impacts of cyberattacks on power

systems infrastructure and the economic impacts they possess. The results can further be used by actuarial scientists for calculating the true risk that cyber failures introduce in power systems.

This study can be extended to accommodate future studies on hybrid energy systems such as hydro, floating photovoltaics and wind [56], concentrated solar power, ground-mounted photovoltaics, and battery storage [57]. This novel methodology shall be applied to large-scale IEEE bus systems. To model the cyber-based contingencies and their impact

REFERENCES

[1] SGTF EG2. Recommendations for the European Commission on Implementation of a Network Code on Cybersecurity, Second Interim Report, Smart Grid Task Force Expert Group. 2018. Available online: https://ec.europa.eu/energy/sites/ener/files/sgtf_eg2_2nd_interim_report_final.pdf (accessed on 29 January 2019).

[2] EECSP. Recommendations for the European Commission on a European Strategic Framework and Potential Future Legislative Acts for the Energy Sector, EECSP Expert Group. 2017. Available online: https://ec.europa.eu/energy/sites/ener/files/documents/eecsp_report_final.pdf (accessed on 29 January 2019).

[3] European Commission. Joint Communication to the European Parliament, the Council, the European Economic and Social Committee, and the Committee of the Regions. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, Report. 2013. Available online: https://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf (accessed on 29 January 2019).

[4] Basumallik, Sagnik, "Impact Assessment, Detection, And Mitigation Of False Data Attacks In Electrical Power Systems" (2021). Dissertations - ALL. 1301.https://surface.syr.edu/etd/1301.

[5] Emilie Bout, Valeria Loscri, Antoine Gallais. How Machine Learning changes the nature of cyberattacks on IoT networks: A survey. Communications Surveys and Tutorials, IEEE Communications Society, Institute of Electrical and Electronics Engineers, 2021.hal-03390359f.

[6] Bulat, H.; Frankovi´c, D.; Vlahini´c, S. Enhanced Contingency Analysis—A Power System Operator Tool. Energies 2021, 14, 923.https://doi.org/10.3390/en14040923.

[7] J. Kang, I. Joo, and D. Choi, "False Data Injection Attacks on Contingency Analysis: Attack Strategies and Impact Assessment," in *IEEE Access*, vol. 6, pp. 8841-8851, 2018, doi: 10.1109/ACCESS.2018.2801861.

[8] Salimian, M.R.; Aghamohammadi, M.R. A Three Stages Decision Tree-Based Intelligent Blackout Predictor for Power Systems Using Brittleness Indices. IEEE Trans. Smart Grid 2018, 9, 5123–5131.

[9] Zhang, Y.; Xu, Y.; Dong, Z.Y. Robust Ensemble Data Analytics for Incomplete PMU Measurements-Based Power System Stability Assessment. IEEE Trans. Power Syst. 2018, 33, 1124–1126.

[10] Amini, S.; Pasqualetti, F.; Mohsenian-Rad, H. Dynamic load altering attacks against power system stability: Attack models and protection schemes. IEEE Trans. Smart Grid 2018, 9, 2862–2872.

[11] Dharmesh Faquir, Nestoras Chouliaras, Vlachou Sofia, Kalopoulou Olga, Leandros Maglaras. Cybersecurity in smart grids, challenges, and solutions[J]. *AIMS Electronics and Electrical Engineering*, 2021, 5(1): 24-37. doi: 10.3934/electreng.2021002.

[12] "Reliability standards for the bulk electric systems of north america," May 2017. [Online]. Available: http://www.nerc.com/pa/Stand/Reliability Standards Complete Set/RSCompleteSet.pdf

[13] R. Kuckro, "Simulated cyberattack takes down u.s. power grid," Nov. 15, 2013. [Online]. Available: http://www.utilitydive.com/news/simulatedcyberattack-takes-down-us-power-grid/195153/

[14] M. Sahraei-Ardakani, X. Li, P. Balasubramanian, K. W. Hedman, and M. Abdi-Khorsand, "Real-time contingency analysis with transmission switching on real power system data," IEEE Trans. Power Syst., vol. 31, no. 3, pp. 2501–2502, May 2016.

[15] Y. Zhang, L. Wang, and Y. Xiang, "Power system reliability analysis with intrusion tolerance in SCADA systems," IEEE Trans. Smart Grid, vol. 7, no. 2, pp. 669–683, Mar. 2016.

[16] Y. Zhang, L. Wang, Y. Xiang, and C.-W. Ten, "Inclusion of SCADA cyber vulnerability in power system reliability assessment considering optimal resources allocation," IEEE Trans. Power Syst., vol. 31, no. 6, pp. 4379–4394, Nov. 2016.

[17] "Results   // ." NERC, https://www.nerc.com/search/Pages/results.aspx?k=N-1+contingency.

[18] "What Is a Gauss-Seidel Method? Circuit Globe." Circuit Globe, 8 Feb. 2021, https://circuitglobe.com/gauss-seidel-method.html.

[19] Rohit Yadav May. "What Is Newton Raphson Method? - Procedure & Flowchart." Circuit Globe, 8 Feb. 2021, https://circuitglobe.com/newton-raphson-method.html.

[20] A. Umunnakwe, H. Huang, K. Oikonomou, K.R. Davis, Quantitative analysis of power systems resilience: Standardization, categorizations, and challenges, Renewable and Sustainable Energy Reviews, Volume 149,2021,111252, ISSN 1364-0321,https://doi.org/10.1016/j.rser.2021.111252.

[21] J. De La Ree, V. Centeno, J. S. Thorp, and A. G. Phadke, "Synchronized Phasor Measurement Applications in Power Systems," IEEE Transactions on Smart Grid, vol. 1, no. 1, pp. 20–27, 6 2010.

[22] A. Monticelli, State estimation in electric power systems: a generalized approach. Springer Science & Business Media, 2012.

[23] F. Schweppe and J. Wildes, "Power System Static-State Estimation, Part I: Exact Model," IEEE Transactions on Power Apparatus and Systems, vol. PAS-89, no. 1,pp. 120–125, 1 1970.

[24] A. Monticelli, "Electric power system state estimation," Proceedings of the IEEE, vol. 88, no. 2, pp. 262–282, 2000.

[25] G. N. Korres and N. M. Manousakis, "State estimation and bad data processing for systems including PMU and SCADA measurements," Electric Power Systems Research, vol. 81, no. 7, pp. 1514–1524, 7 2011.

[26] V. Murugesan, Y. Chakhchoukh, V. Vittal, G. T. Heydt, N. Logic, and S. Sturgill, "PMU Data Buffering for Power System State Estimators," IEEE Power and Energy Technology Systems Journal, vol. 2, no. 3, pp. 94–102, 9 2015.

[27] "Financial Transmission Right." Financial Transmission Right - an Overview | ScienceDirect Topics, https://www.sciencedirect.com/topics/engineering/financial-transmission-right.

[28] A. Monticelli, "Electric power system state estimation," Proceedings of the IEEE, vol. 88, no. 2, pp. 262–282, 2000.

[29] Ali Abur, Antonio Gómez Expósito. "Power System State Estimation: Theory and Implementation: Ali Abur." Taylor & Francis, Taylor & Francis, 24 Mar. 2004, https://www.taylorfrancis.com

[30] F. Capitanescu, M. Glavic, D. Ernst, and L.Wehenkel, "Contingency Filtering Techniques for Preventive Security-Constrained Optimal Power Flow," IEEE Transactions on Power Systems, vol. 22, no. 4, pp. 1690–1697, 11 2007.

[31] R. S.Wibowo, T. P. Fathurrodli, O. Penangsang, and A. Soeprijanto, "Security constrained optimal power flow incorporating preventive and corrective control," in 2014 Electrical Power, Electronics, Communications, Control, and Informatics Seminar (EECCIS). IEEE, 8 2014, pp. 29–34.

[32] Feng Dong, "Practical applications of Preventive Security Constrained Optimal Power Flow," in 2012 IEEE Power and Energy Society General Meeting. IEEE, 7 2012, pp. 1–5.

[33] S. Dhople, Y. Chen, L. DeVille, and A. D. Domínguez-García, "Analysis of Power System Dynamics Subject to

Stochastic Power Injections", IEEE Transactions on Circuits and Systems I: Regular Papers, vol. 60, no. 12, pp. 3341-3353, Dec. 2013.

[34] Y. Gu and L. Xie, "Stochastic Look-Ahead Economic Dispatch With Variable Generation Resources," IEEE Trans. Power Syst., vol. 32, no. 1, pp. 17-29, Jan. 2017

[35] Y. Zhou, Y. Li, W. Liu, D. Yu, Z. Li, and J. Liu, "The Stochastic Response Surface Method for Small-Signal Stability Study of Power System With Probabilistic Uncertainties in Correlated Photovoltaic and Loads," IEEE Trans. Power Syst., vol. 32, no. 6, pp. 4551-4559, Nov. 2017.

[36] Basumallik, Sagnik, "Impact Assessment, Detection, And Mitigation Of False Data Attacks In Electrical Power Systems" (2021). Dissertations - ALL. 1301. https://surface.syr.edu/etd/1301

[37] H. Wu, I. Krad, E. Ela, A. Florita, E. Ibanez, J. Zhang and B. Hodge, "Stochastic Multi-Timescale Power System Operations with Variable Wind Generation", IEEE Trans. Power Syst., vol. 32, no. 5, pp. 3325-3337, Sept. 2017.

[38] M. Khodayar, M. Shahidehpour and L. Wu, "Enhancing the Dispatchability of Variable Wind Generation by Coordination With Pumped-Storage Hydro Units in Stochastic Power Systems", IEEE Trans. Power Syst., vol. 28, no. 3, pp. 2808-2818, Aug. 2013.

[39] F. Milano and R. Zarate-Minano, "A Systematic Method to Model Power Systems as Stochastic Differential Algebraic Equations", IEEE Trans. Power Syst., vol. 28, no. 4, pp. 4537-4544, Nov. 2013.

[40] Li, H.; Ju, P.; Gan, C.; Wu, F.; Zhou, Y.; Dong, Z. Stochastic Stability Analysis of the Power System with Losses. Energies 2018, 11, 678. https://doi.org/10.3390/en11030678

[41] Xu Y, Wen F, Zhao H, Chen M, Yang Z, Shang H. Stochastic Small Signal Stability of a Power System with Uncertainties. Energies. 2018; 11(11):2980. https://doi.org/10.3390/en11112980

[42] Amini, S.; Pasqualetti, F.; Mohsenian-Rad, H. Dynamic load altering attacks against power system stability: Attack models and protection schemes. IEEE Trans. Smart Grid 2018, 9, 2862–2872.

[43] Adeen, Muhammad, and Federico Milano. "Modeling of Correlated Stochastic Processes for the Transient Stability Analysis of Power Systems." NASA/ADS, https://ui.adsabs.harvard.edu/abs/2021ITPSy..36.4445A/abstract.

[44] Y. Zhang, L. Wang, and W. Sun, "Investigating the impact of cyber attacks on power system reliability," IEEE International Conference on Cyber Technology in Automation, Control and Intelligent Systems, 2013, pp. 462-467.

[45] K. Huang, C. Zhou, Y.-C. Tian, S.-H. Yang, and Y. Qin, "Assessing the physical impact of cyberattacks on industrial cyber-physical systems," IEEE Transactions on Industrial Electronics, vol. 65, no. 10, pp. 8153-8162, Oct. 2018.

[46] T. Meraj, S. Sharmin, and A. Mahmud, "Studying the impacts of cyber-attack on smart grid," 2nd International Conference on Electrical Information and Communication Technologies (EICT), 2015, pp. 461-466.

[47] Y. Xiang, L. Wang, and Y. Zhang, "Power system adequacy assessment with probabilistic cyber attacks against breakers," IEEE PES General Meeting | Conference & Exposition, 2014, pp. 1-5.

[48] Boyaci, Osman, et al. "Spatio-Temporal Failure Propagation in Cyber-Physical Power Systems." 2022 3rd International Conference on Smart Grid and Renewable Energy (SGRE) (2022): 1-6.

[49] Liu, Zhaoxi, et al. "An Actuarial Framework for Power System Reliability Considering Cybersecurity Threats." IEEE Transactions on Power Systems 36 (2021): 851-864.

[50] P. Lau, W. Wei, L. Wang, Z. Liu and C. -W. Ten, "A Cybersecurity Insurance Model for Power System Reliability Considering Optimal Defense Resource Allocation," in *IEEE Transactions on Smart Grid*, vol. 11, no. 5, pp. 4403-4414, Sept. 2020, doi: 10.1109/TSG.2020.2992782.

[51] Lau, et al. "A Cybersecurity Insurance Model for Power System Reliability Considering Optimal Defense Resource Allocation." IEEE Transactions on Smart Grid, 1 Sept. 2020, https://par.nsf.gov/biblio/10189117-cybersecurity-insurance-model-power-system-reliability-considering-optimal-defense-resource-allocation.

[52] U. Shahzad, "Economic Impact Assessment of Cyber Attacks on the Smart Power System," Journal of Electrical Engineering, Electronics, Control, and Computer Science, vol. 8, pp. 39-46,2022.

[53] GRIF-Workshop, Retrieved from 2021. Satodev, Total. http://grif-workshop.com.

[54] Rastgou, Abdollah. Study of Transmission Expansion Planning with Security Considerations and High Penetration of Wind Energy. International Journal on Electrical Engineering and Informatics. 6. 460-478. 10.15676/ijeei.2014.6.3.2.

[55] Hindolo George-Williams, Nisrine Kebir, Stephanie Hirmer, Malcolm McCulloch. (2021). Sample Electricity Grid Outage Management Data. IEEE Dataport. https://dx.doi.org/10.21227/cwkn-9888

[56] Nyoni KJ, Maronga A, Tuohy PG, Shane A. Hydro–connected floating PV renewable energy system and onshore wind potential in Zambia. Energies. 2021 Jan;14(17):5330.

[57] Maronga A, Nyoni KJ, Tuohy PG, Shane A. Evaluation of PV and CSP systems to supply power in the Zimbabwe mining sector. Energies. 2021 Jan;14(13):3740