Power System Security With Cyber-Physical Power System Operation

Oyewole, Peju Adesina; Jayaweera, Dilan

DOI:
10.1109/ACCESS.2020.3028222

Document Version
Publisher's PDF, also known as Version of record

Citation for published version (Harvard):
Oyewole, PA & Jayaweera, D 2020, 'Power System Security With Cyber-Physical Power System Operation', *IEEE Access*, vol. 8, pp. 179970-179982. https://doi.org/10.1109/ACCESS.2020.3028222

IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received August 18, 2020, accepted September 19, 2020, date of publication October 1, 2020, date of current version October 13, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3028222

Power System Security With Cyber-Physical Power System Operation

PEJU ADESINA OYEWOLE, (Member, IEEE), AND DILAN JAYAWEERA, (Senior Member, IEEE)
Department of Electronic, Electrical, and Systems Engineering, University of Birmingham, Birmingham B15 2TT, U.K.
Corresponding author: Peju Adesina Oyewole (pxo669@bham.ac.uk)

This work was supported by the University of Birmingham.

ABSTRACT Cyber-attacks on a cyber-physical power system could lead to significant data failure, false data injection and cascading failure of physical power system components. This paper proposes an advanced approach based on a ternary Markovian model of cyber-physical components interactions to capture the subsystem layers' interactions of the cyber-physical power system and to quantify the interdependency impacts on physical power system security. The approach models cyber-physical interactive operation based on interactions and characteristics of three subsystem layers of the system with the presence of random and unforeseen contingencies, load demand variations and then quantify the impacts with Monte Carlo simulation. The viability of the approach is investigated by simulating a set of scenarios, representing realistic physical power system operating conditions with the cyber network interactions. Findings justify the presence of cyber-attacks in a cyber-physical power system components operation could lead to severe insecurities. However, the impacts on physical power system security does not always correlate with the severity of cyber-attacks.

INDEX TERMS Cyber-physical power system, cyber-physical power system reliability assessment Interdependency, Markov model, Monte Carlo simulation, power system security, reliability assessment, smart grid, subsystem layers' interactions, ternary Markovian model.

I. INTRODUCTION

Growing reliance on information and communication technology (ICT) and advanced automation systems in power systems has created cyber physical power (CPP) system paradigm. A CPP system is a series of components connected by power infrastructure, information and communication infrastructure and decision-making infrastructure. CPP system is a sophisticated intelligent power system architecture that integrates advanced control and modern communication technologies applicable to a power system. It is a modern-day smart power system with various systems and component interactions. In a CPP system, the normal operation of one subsystem depends on the interactive functions of other components or subsystems within the CPP system.

The information, communication and decision-making infrastructures execute the monitoring, control and decision-making processes. The communication and decision-making infrastructures are to ensure that a better reliability of CPP system is achieved [1]. Authors in [2], [3] state that communication and decision-making infrastructures support the transfer of power from generation to end-users in a reliable and secure manner. Also, authors in [4], [5] argue that use of real-time communications support dynamic flow of power and information data to ensure a reliable power supply.

However, growing reliance on cyber systems makes CPP system more susceptible to component failure, cyber network failure, software failure and human errors. These failures could cause failure propagation that could affect interdependencies within the CPP system, adversely, impacting power system security. References [6], [7] state that extensive reliance of the power system on cyber systems may leads to new threats and makes the CPP system more vulnerable to malicious attacks, information and data failure.

Authors in [8] state that any failure can transmit or spread more rapidly and extensively, and as a result the system reliability could be reduced.

Reference [5] argues that loss of monitoring and control of power system components may influence the real-time operation of the whole power system. Reference [2] argues

The associate editor coordinating the review of this manuscript and approving it for publication was Arup Kumar Goswami.

that communication system failures may cause lack of controllability and observability of a power system which may result in succession of failures in the system. For instance, accidental shutdown of a power station in Italy (2003 blackout) led to failures of the communication network nodes and the supervisory control and data acquisition (SCADA) system of the power grid. This incident led to more failures in the power grid and subsequently led to a sequence of tragic cascading failure in the system [9]. The combination of power components failures, lack of real-time information and diagnostic support, local decision-making without regard to interconnectivity, computer and human errors that resulted in cascading failures eventually led to the huge blackout in the Northeast of United States in 2003 [10]. The Northeast blackout affected almost 50 million customers in seven US states and Ontario, Canada. The blackout caused a sudden shutdown of over 100 power plants at a localized generating plant [4], [11].

Considering the likelihood of failure propagations and interdependency failure due to uncertainties and unpredictability in a CPP system, interdependency assessment and system modelling are important in order to assess true impacts. Relevant studies on interdependencies in a CPP system has been proposed in [12]–[15] for reliability assessment of the system. Reference [16] develops a mathematical model to evaluate the impacts of interdependencies in a cyber-physical system quantitatively. It concludes that the intelligent devices of the cyber-physical network could experience failures in two ways: direct and indirect interdependencies that might have effects on the reliability of a power system. An interdependency Markov-chain framework is proposed in [4] to investigate and forecast resilience to cascading failures and to study interdependency impacts on system reliability. It concludes that interdependencies among systems with reliable systems may lead to an unreliable system. A mathematical model to assess interdependency in power and communication systems of smart grid components is proposed in [17] for system vulnerability analysis. The model reveals interdependency between components and system vulnerabilities induced by system dynamics. Reference [18] proposes an analytical reliability model to capture effects of cyber-physical interdependencies and effects of failures from both physical and cyber components in a smart grid system. The results argue that cyber infrastructure can have less reliability than a conventional power grid. An analytical reliability assessment considering both power and cyber component failures is proposed in [19] to investigate impact of direct cyber network failures on a power network. The results show that is very important to consider cyber negative impacts on power grid for reliability assessment. Though impacts of interdependency in a CPP system reliability have been explored, a unified framework that reflect characteristics of three subsystem functional layers' interactions of the CPP system is missing.

Other frameworks have been established in CPP system modelling to analysis CPP system operation [20]–[25]. Authors in [26] analyze electrical cyber-physical systems operation by modelling communication network associated in a power transmission grid using a mesh topology to characterize the networks interdependency based on various types of information channels. The model investigates vulnerability of electrical cyber-physical systems under various cyber-attacks. Reference [27] proposes a CPP system equivalent model to quantitatively evaluate effect of improper control commands due to cyber contingencies on the power system of a CPP systems. Hierarchical control systems of cyber networks were designed as directed branches and directed graph with data nodes. The model effectively evaluates the impact of cyber contingencies without entire system simulations. An hierarchical CPP model based on flocking theory considering transient stability associated problems is proposed in [28] to maintain a transient stability during severe disturbances. The model facilitates identification of distributed control approaches that improve resiliency in power grid operation. An hybrid simulation model of CPP system considering time delay in predictive control model with low frequency oscillation damping controller is proposed in [29] to simulate CPP system operation. The model demonstrates good performance with improved cyber control systems. Lastly, a dynamic transmission model and a static connection model are proposed in [30] to evaluate effect of cyber components failure and quality of information transmission on CPP distribution system. These two models are developed to create CPP model based on service restoration, fault location and isolation of the CPP distribution system operation. The results show a significant failure rates of the cyber components causing considerable impact on the CPP distribution system reliability.

Most CPP system modelling focuses on a single dynamic characteristic of the CPP system operation. The CPP system model proposed in [21] is based on delay, dynamic routing and communication error. The approach in [27] is an hierarchical control system of a cyber network based on directed branches and directed graph with data nodes. Reference [31] models a unified electrical cyber physical system framework considering information flows and routers. These studies implement dynamic of the communication network in the CPP system modelling, the dynamic characteristics of the decision-making layer and power network are missing.

Some approaches explore the CPP system modelling as separate models. CPP system operation in [30] is modelled as two separate models: the static connection model and the dynamic transmission model based on service restoration, fault location isolation and of the CPP distribution system operation. This study does not reflect a single unified framework modelling.

The framework proposed in [26] models cyber physical electrical power systems with integration of both power grids and communication networks, based on power transmission grid characteristics: high-voltage levels, long transmission distances and node importance in transmission grids. This approach models the communication network as a meshed

topological network with each node linked to a physical node within the power transmission grid. The hierarchical CPP model in [28] is based on flocking theory considering transient stability associated problems. However, each of these studies does not reflect the characteristics of the three subsystem functional layers' interactions of the CPP system. As stated by authors in [1], it is very important in CPP system modelling to establish single unified model that combine series of consequences of events from the decision-making subsystem layer, the communication and coupling subsystem layer to the power subsystem layer. Therefore, the aim of this paper is to investigate the CPP system modelling as a single unified model considering interactions and characteristics of the three subsystem functional layers of the CPP system and then to propose an advanced algorithm to assess global impacts of the power system interacting with the cyber network processes. The three subsystem layers are decision-making layer, communication and coupling layer and power layer.

Taking into account the gap from the state of the art of the problem, this paper proposes a unified ternary Markovian model based on interactions and characteristics of three subsystem layers of the CPP system to capture dynamics of subsystem layers' interactions in the system for the assessment of interdependency impacts on power system security under various cyber-attacks and foreseen contingencies. The approach models impact of interdependency of CPP system operation through state transitions using non-sequential Monte Carlo simulation.

The key contributions of this paper are as follows: Firstly, this paper establishes a single unified ternary Markovian model of CPP system operation based on three subsystem functional layers: decision-making layer, communication and coupling layer and power layer. Secondly, the model reflects dynamic operation of subsystem layers' interactions of communication and coupling layer, decision-making layer and power layer. This is demonstrated as an embedded three subsystem layers interactions that capture each operation of subsystem layer in the CPP system. Each of the subsystem layer is characterized as three states to capture time varying behaviour under various cyber-attacks or unforeseen contingencies. Lastly, the model with Monte Carlo simulation is embedded into the security assessment algorithm and quantitatively assess realistic impacts of subsystem layers' interactions on power system security.

The rest of this paper is organized as follows: Section II presents different CPP system layers; Section III presents the proposed approach in detail; The implementation of the approach, results and analysis are detailed in Section IV; and conclusions are given in Section V.

II. CYBER PHYSICAL POWER SYSTEM

A CPP system integrates advanced control, intelligent electronic devices(IEDs) and ICT to advance the performance of the composite system to achieve prime and other objectives. CPP system is an interconnected and complex cyber-physical system which forms a multi-dimensional heterogeneous system [18]. The complex interconnections and interactions in CPP system is considered as a system with three subsystem functional layers (FL) (see Fig.1): FLI is the decision-making intelligent subsystem layer, FLII is the information, communication and coupling subsystem layer and FLIII is the physical power subsystem layer. Both the decision-making intelligent layer and the information, communication and coupling layer make up the cyber layer.

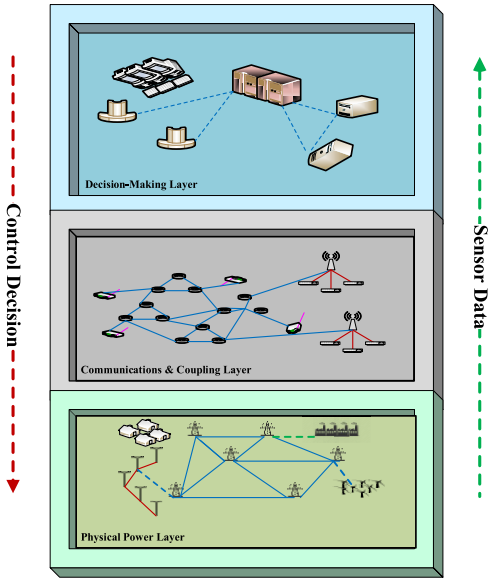

FIGURE 1. Cyber-physical power system representation.

A. DECISION MAKING INTELLIGENT SUBSYSTEM LAYER

Generally, the decision-making intelligent layer determines the smartness of a CPP system. The decision-making intelligent subsystem layer (DISL) is made up of various programs or functions; substation automation system, control centre, control of renewable power generation, energy and demand management system of computer programs for relays, IEDs etc. These functions are for continuous operation of the power system. They process information received from sensors or disseminate information from the communication infrastructure to others. Control directives or business process decisions exhibited in the physical layer is achieved in this layer [32].

Malfunctioning in the DISL such as DISL tools failure (including servers), incorrect decision-making and malicious intention might generate incorrect state estimation [33], [34]. Various malicious intention could introduce cyber-attacks through sensor(s) hacking and measurement distortions [1], [35]. This may lead to decision errors that could cause failures or lead to a blackout.

B. COMMUNICATION AND COUPLING SUBSYSTEM LAYER

The communication and coupling subsystem layer (CCSL) contain communication networks and interface devices such as remote terminal units (RTU). The communication

networks are generally categorized into three: wide-area network, field area network and home area network. They consist of various communication devices. The interface devices convey control directives and decision programs from DISL to the power layer and measurements from the power layer to the DISL. The communication networks connect the interface devices and the links between them. Any malfunction or error in the communication networks or interface devices will affect the accuracy of the DISL functions [1], [36]. However, communication networks and links are susceptible to wrong data injection attacks which may alter measurements during data transmission [37]. This might also cause wrong decisions from DISL and invariably could cause system malfunctions or lead to a blackout.

C. PHYSICAL POWER SUBSYSTEM LAYER

The physical power subsystem layer (PPSL) is simply the physical power network consists of all physical devices generally, the power generation, power transmission and distribution assets including protection systems, power electronic interface devices, and storage technologies, and traditional and smart grid loads. The power system is usually grouped into three functional zones of generation, transmission and distribution. Power devices are connected to the communication and coupling layers via state awareness sensors and program execution devices.

III. THE APPROACH

A. INTERDEPENDENCY IN CYBER PHYSICAL POWER SYSTEM

Interdependency in a CPP system is a mutual reliance of components or subsystems within a system. The states of a component or a subsystem in a system can potentially influence the performance of other subsystems. The successful operation of a power system with a significant integration of cyber infrastructure depends on the cyber network security. Consideration of interdependency of cyber and power system is extremely important [1]. Moreover, loss of interdependency due to uncertainty, unpredictability and failure in the CPP system could affect effective operation of the power system thus, the power system security could be jeopardized.

B. FAILURES IN CYBER PHYSICAL POWER SYSTEM

In a CPP system either the cyber system or the power system could be the source of failure from failures of their components, software failures, human errors, etc. All these failures may be categorized into three: component failure, cyber unavailability, and cyber intrusion. Component Failure is the loss of functionality in component(s) of the decision-making and intelligent layer, information, communication and coupling layer or power layer such as routers, servers, generators, etc., may malfunction or fail. This might cause interruption in communication networks or incorrect decision-making which could affect the security of the whole system. Cyber Unavailability is the loss of functionality in information & communication networks as a result of interruption such as link unavailability, packet loss, packet delay, etc., which may affect the decision-making process thus, jeopardizing the power system security. Cyber intrusion is the loss of functionality due to malicious attacks, false data-injection attacks, etc. which may affect the decision-making process.

C. MARKOV APPROACH

Markov process is defined as a stochastic process. Markov chain is a form of Markov process with some finite states (V1, V2, V3.... V_n) which make the process to occur at any given time. Transition probability y_{ij} is the probability of the process moving from state Vi to state V_j. Transition probability y_{ii} is the probability of the process remaining in the same state. Markov processes is utilized in the analysis of systems' reliability, maintainability and availability [38]–[41]. A typical system consists of n components with one or all the components operating effectively or ineffectively at any given time. The entire system successful operation depends on the availability or unavailability of its components.

D. TERNARY MARKOVIAN MODEL

Markov modelling is a modelling method with common application in reliability analysis of systems. Markov modelling offers better insight into dynamic behavior of a system or component [1], [4]–[44]. It is a type of stochastic process where system behavior varies with time and space randomly [42], [45].

The proposed approach is established using a ternary Markovian model (TMM) to incorporate the influence and interoperability of subsystems within the CPP system to capture the dynamics of subsystems' interactions in the CPP system. TMM is a single integrated probabilistic framework modelled as an embedded three subsystem interactions. Each subsystem layer(SL) is characterized with three states to capture time varying behavior under various cyber-attacks or unforeseen contingencies. The interactive operation and sequence of events in each of DISL, CCSL and PPSL of the CPP system is modelled as a subsystem which exist in three states within a system (see Fig. 2).

The TMM is formed as an embedded three SL interactions: the DISL, the CCSL and the PPSL. Each of the SL is formed to interact with each other. The DISL is formed as a SL with various procedures and functions including substation automation system, control of renewable power generation, operation of IEDs etc. for continuous operation of the physical power system. To capture time varying behavior under various cyber-attacks and unforeseen contingencies the DISL is further characterized to operate in three states: available without error state indicated as "A", available with error state indicated as "E" or unavailable state indicated as "F".

The CCSL is formed as an interface and coupling SL with various interface devices (e.g. RTU) and communication network to convey control directives and decision programs from the DISL to the PPSL and measurements from the PPSL to the DISL. To capture time varying behavior under various

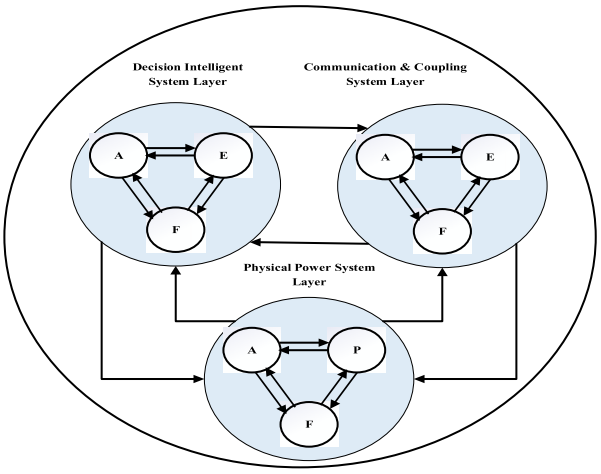

FIGURE 2. Ternary Markovian model of a cyber-physical power system.

cyber-attacks and unforeseen contingencies the CCSL is further characterized to operate in three states: available without error state indicated as "A", available with error state indicated as "E" or unavailable state indicated as "F".

The PPSL is modelled as physical power system with of all physical devices generally. To capture time varying behavior under various cyber-attacks and unforeseen contingencies the PPSL is further characterized to operate in three states: available state indicated as "A", partial operated state indicated as "P" or unavailable state indicated as "F".

Fig. 2 shows that the DISL and CCSL can either exist as available without error state indicated as "A", available with error state indicated as "E" or unavailable state indicated as "F". PPSL can either exist as available state indicated as "A", partial operated state indicated as "P" or unavailable state indicated as "F". Available without error state "A" is when each subsystem (DISL CCSL or PPSL) is working as expected. Available with error state "E" is presence of error or incorrect data as a result of cyber intrusion, malicious attack, false data injection, etc., in the system that may affect the functionality of each/both DISL and CCSL which might impact the power system layer and whole system functionality. Unavailable state "F" is a failed state of the subsystem layer as a result of component failure, packet loss, packet delay, etc. which might impact the system security. Partial operated state "P" state is when the subsystem is operating partially or operating at a reduced-capacity.

TMM is conceptualized as varying with respect to time and space with state transition probabilities [44] as expressed in (1):

$$\mathrm{p_{ij}}\forall \mathrm{i}, \quad \mathrm{j} \in \mathrm{X} = 1, 2, 3 \ldots . \mathrm{n} \tag{1}$$

where: X is set of possible states, n and p_{ij} is state transition probability from state i to state j. The state transition probabilities represent all the transitions from one state to another. Stochastic transitional probability matrix P consist of all the transition probability values for the system states as expressed in (2):

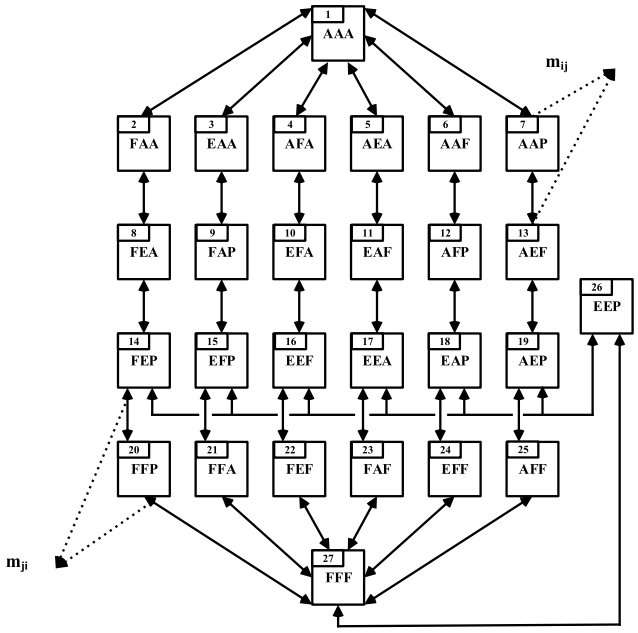

FIGURE 3. TMM state space transition representation of the CPP system.

$$P_{k,k+1} = \begin{bmatrix} p_{11} & p_{12} & \cdots & p_{1n} \\ p_{21} & p_{22} & \cdots & p_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ p_{n1} & p_{n2} & \cdots & p_{nn} \end{bmatrix} \tag{2}$$

where: $P_{k,k+1}$ is state transition probability matrix, k and $k+1$ is the current and next state respectively, n is number of states and p_{ij} is the transition probability that depict the probability of transiting from state i to state j during a given time interval. Within the transition probability matrix, the rows are the current state of the system while the columns are the next state, the sum of each row in the transition probability matrix must be 1, that is, from a given state, the transition probabilities must equal to unity [42] as expressed in (3):

$$\sum_{\mathrm{j}\in \mathrm{X}} \mathrm{p_{ij}} = 1 \tag{3}$$

The TMM state space diagram (see Fig. 3) collectively represents the possible states of the CPP system due to operational consequences of events in the DISL, CCSL and PPSL. There are three state variables in each of the subsystem layer. "A", "E" and "F" (see Fig. 2) state variables indicate that each of the DISL and CCSL could either be in available-without-error state, available-with-error state or failed state respectively. "A", "P" and "F" state variables indicate that the PPSL could either be in available state, partial operation state or failed state respectively.

Each subsystem layer state is denoted by a ternary variable $x_i = 2, 1, or 0$ such that, subsystem layer i is either available, error/partial or failed, respectively.

Let consider C_i as set of states for subsystem, i with a cardinality of N_i. For a system with n subsystems, the system

state can be represented as a vector W:

$$\mathrm{W} = (\mathrm{w_i}), \quad \text{where } w_i \in C_i \; 1 \leq \mathrm{i} \leq \mathrm{n} \tag{4}$$

Also, the states of all subsystems can be described by a ternary vector:

$$\mathrm{x} = (\mathrm{x_1}, \mathrm{x_2}, \ldots . \mathrm{x_n}) \tag{5}$$

With standard assumptions, state of a system depends on combination of all components states [46], [47], the ternary system state model is described by y and is subject to subsystems state vector x:

$$\mathrm{y} = \mathrm{y}\,(\mathrm{x}) \tag{6}$$

The system can be in any different state since $w_i \in C_i$ therefore N is:

$$\mathrm{N} = \prod_{\mathrm{i}=1}^{\mathrm{n}} \mathrm{N_i} \tag{7}$$

And the system state space express as:

$$\mathrm{SS} = \{\mathrm{W_j} | 1 \leq j \leq N\}$$

Likewise, let Ω_i represent the state transition due to subsystem i operation and from 6, the system state transition can be expressed approximately as:

$$\Omega = \prod_{i=1}^{n} \Omega_i \tag{8}$$

Hence, as depicted in (2) the ternary Markovian CPP system stochastic transitional probability matrix is modelled as:

$$\mathrm{M_{k,k+1}} = \begin{bmatrix} \mathrm{m_{11}} & \mathrm{m_{12}} & \cdots & \mathrm{m_{1}}n \\ \mathrm{m_{21}} & \mathrm{m_{22}} & \cdots & \mathrm{m_{2}}n \\ \vdots & \vdots & \vdots & \vdots \\ \mathrm{m}n1 & \mathrm{m}n2 & \cdots & \mathrm{m}nn \end{bmatrix} \tag{9}$$

where: $M_{k,k+1}$ is the state transition probability matrix, m_{ij}, m_{ji} *and* m_{ii} are the transition probabilities.

Considering subsystem layers' interactions and dynamics of one subsystem layer influence the dynamics of the other subsystem layer. The system may operate in either of any of the N possible states. Generally, the most likely state begins with the system fully-functional. This is when each of the subsystem layers of the CPP system and the whole CPP system is available and working as expected. However, operational uncertainty and unpredictability may cause any of the subsystem layers to transit from its fully functional state to another state, which might impact the whole system. One or multiple transitions of subsystem layer(s) can cause one step transition of the whole CPP system. In Fig. 3 state "AAA" of TMM can transit to state "AAP" as a result of the DISL and CCSL remaining fully functional and the PPSL transits to partial operation state, individual subsystem transitions cause the TMM state transition as stated in (5) and (6).

To reduce design complexity and to ensure effective implementation, the state space representation in Fig. 3 is truncated to smaller number of states by excluding states with very low probability of occurrences. Hence, the reduced number of state space transition representation of the CPP system is shown below (see Fig. 4).

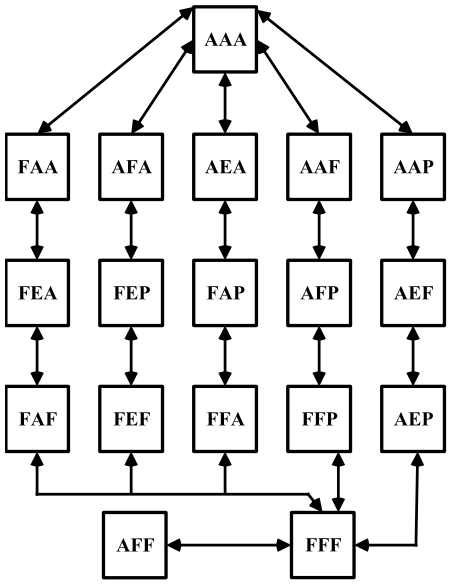

FIGURE 4. Truncated TMM state space transition representation of the CPP system.

Fig. 4 shows the TMM truncated state space transition reflecting subsystems interactions and their dynamics within a whole CPP system as result of one or more transitions of subsystem layer(s). All the possible N states of the TMM is categorized as fully functional, functional, fully blackout, blackout, conventional, conventional partial operation, conventional error partial operation and conventional error.

Table 1 shows the reduced states considering design complexity and implementation. The fully functional state refers when each subsystem (DISL, CCSL and PPSL) of the system is fully available and in working state, functional state refers to when both subsystems DISL and CCSL of the system is fully available and in working state with subsystem PPSL in partial operation state. The fully blackout state is when each subsystem DISL, CCSL and PPSL of the system failed, not in working condition, and not available. The blackout state is when subsystem PPSL failed and either DISL or CCSL is available, error or failed state. The conventional state refers to when the PPSL is fully available and in working state with either subsystem DISL or CCSL in error state or failed state. The conventional partial state refers to when the PPSL is not fully available but in partial operational state with either subsystem DISL or CCSL in the error state or failed state. The conventional error state is when the PPSL is fully available and is in working state with either subsystem DISL in failed state or available state with CCSL in error state. The conventional error partial operational state refers to when the PPSL is in partial operated state with either subsystem DISL in failed or available state with CCSL in error state.

TABLE 1. CPP system truncated TMM states.

States	States Names	Status
AAA	Fully Functional	CPPS Operation
AAP	Functional	
FFF	Fully Blackout	Non Functional
AAF	Blackout	
AEF	Blackout	
AFF	Blackout	
FAF	Blackout	
FEF	Blackout	
FFP	Conventional Partial Operation	Conventional Operation
FAP	Conventional Partial Operation	
AFP	Conventional Partial Operation	
FFA	Conventional Operation	
FAA	Conventional Operation	
AFA	Conventional Operation	
FEP	Conventional Partial Operation	
AEP	Conventional Partial Operation	
FEA	Conventional Operation	
AEA	Conventional Operation	

E. TERNARY MARKOVIAN MODEL IN MONTE CARLO SIMULATION

Fig. 5 illustrates the basic steps of the approach proposed in this paper. Monte Carlo simulation (MCS) examines and predicts various system states in simulated time to obtain energy not supplied (ENS) and to estimate expected value of the ENS. With different states of the TMM as stated above, MCS steps were coded in MATLAB to model the states of the CPP system applying state sampling technique. In this technique, system states are determined based on probability distributions of system states and generated random numbers (RN). RN comprises of a uniform distribution over a specified range of values [47]–[49]. This study assumes a uniform distribution of RN within [0,1]. The states for different samples of state probability of the TMM system are sampled and a non-sequential system states achieved for the system.

At each MCS sample trial, if the system is considered to be in fully functional state or functional state, then that complete the MCS sample trial. If the system is considered failed either as a result of DISL failure(or error) or CCSL failure(or error) or PPSL failure, the corresponding energy lost due to the failure is considered and logged. If PPSL fails, corresponding total ENS, and value of lost load (VoLL) are noted and logged against the sample trial of MCS. If DISL and/or CCSL fails, component randomization is performed

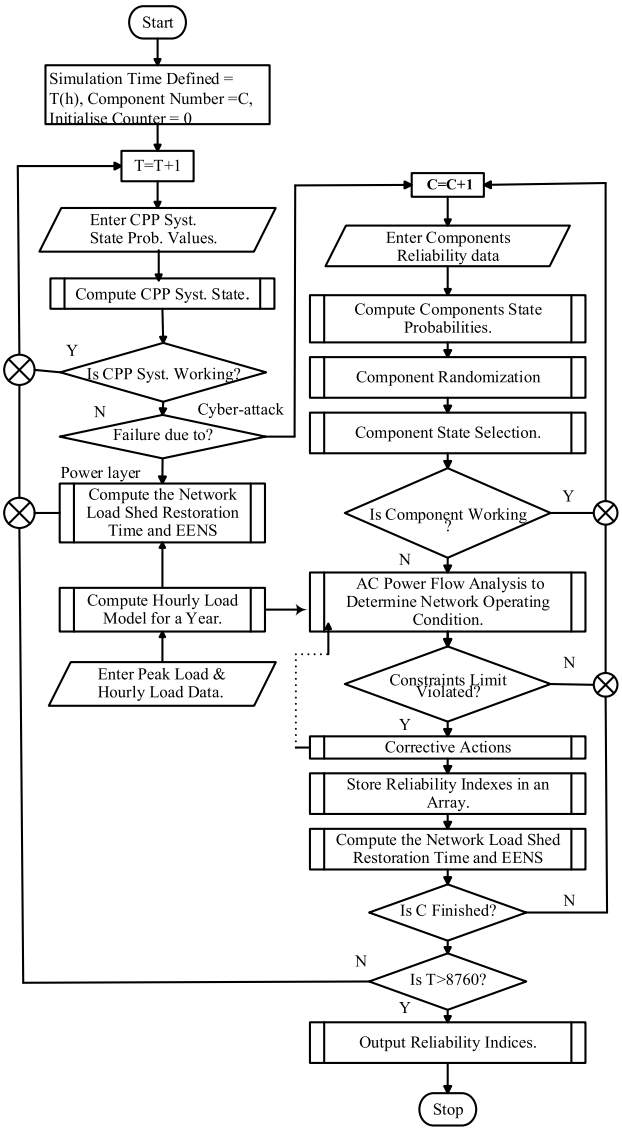

FIGURE 5. Basic flow chart of Ternary Markovian Model with Monte Carlo Simulation.

to determine which physical power component is affected with DISL and/or CCSL failure. Then a Newton-Raphson A/C power flow is simulated to check the network operating condition. If power flow convergence is established and constraint violations are rectified, then MCS sample trial is completed. However, if any constraint is violated, then it is rectified through corrective actions to prevent network collapse or to alleviate sustained violations. The incorporated and developed corrective actions in this study are reactive power compensation, on-load-tap changing, generation re-dispatch and shedding of loads.

Cyber failure and power layer failure and their corresponding ENS and VoLL [50]–[52] are logged and recorded against the individual sample trial of MCS considering the magnitude of load shedding, restoration time of the loads that were being shed, and sector customer damage functions. At the end of each sample trial of MCS, mean value of the curtailed load

and corresponding of cost of lost load of all the processed samples are estimated, with maximum number of samples trials, the expected energy not supplied(EENS) is calculated as:

$$\mathrm{EENS} = \frac{1}{\mathrm{y}} \sum_{\mathrm{i}}^{\mathrm{y}} \mathrm{K_i x T_i} \tag{10}$$

where, y is the processed samples, K_i is the magnitude of curtailed or shed load at the sample i and T_i is the restoring time of K_i. The VoLL is calculated as:

$$\mathrm{VoLL} = \frac{1}{\mathrm{y}} \sum_{\mathrm{i}}^{\mathrm{y}} \mathrm{ENS_i x C_i\,(T_i)} \tag{11}$$

where, C_i is sector customer damage function (SCDF) [52] for Residential, Commercial, Industrial and large user in £/MWh for the interruption duration T_i and $\mathrm{ENS_i}$ is energy not supplied for the sample i.

F. FAILURE FREQUENCE INDEX

It is important to understand effects of individual subsystem on the whole system for operational system security, hence, [1], [53]–[55] identified some measures that quantify the effect of subsystem activities on CPP system operation. Thus, power layer failure, cyber failure and error frequency index and their corresponding ENS and VoLL are considered as an indication of unreliability that could jeopardize power system security. Specific definitions of those indices are as follow:

Average Power Layer Failure Frequency Index: This is measure of interruption or disturbance on the CPP system due to failure of the power layer as a fraction of the total processed samples:

$$\mathrm{APFFI} = \frac{\text{Total power layer failure}}{\text{Total processed samples}}$$

Power layer failure include all uncertainties and failure in the physical power layer.

Average Cyber Failure Frequency Index: This is measure of lost decisions on the CPP system due to failure of cyber layer (CCSL and DISL) as a fraction of the total processed samples:

$$\mathrm{ACFFI} = \frac{\text{Total Cyber Failure}}{\text{Total processed samples}}$$

Cyber failure is any uncertainties that affect the functionality of cyber layer such as, malicious intention, cyber tool failure, etc.

Average Cyber Error Frequency Index: This is measure of lost decisions on the CPP system due to error in the cyber layer as a fraction of the total processed samples:

$$\mathrm{ACEFI} = \frac{\text{Total Cyber Error}}{\text{Total processed samples}}$$

Cyber error is any error that affect the functionality of cyber layer such as incorrect decision-making, wrong data injection, etc.

TABLE 2. ICT components' reliability data.

ICT Components	MTTF (h)	MTTR (h)	Failure Rate (yr)
Protection Panels	438000	48	0.02
Merging Units	438000	48	0.02
Ethernet Switches	876000	48	0.01

IV. CASE STUDIES

A. NETWORKS

The IEEE 24-Bus Reliability Test System (RTS) [56] is used for the viability assessment of the proposed approach. MATLAB codes were developed to stimulate the network characteristics and other eventualities. The transmission system consists of 24 buses, 33 lines and 5 transformers. There are 10 generator buses of connecting 32 generating units and 17 load buses in the system. The transmission lines are at two voltages, 230 kV and 138 kV. The 138 kV system is in the lower part of the power system. The buses 11, 12, and 24 represent the 230/138 kV tie-stations. Bus 14 and bus 6 have a synchronous condenser and a reactor connected respectively as voltage corrective devices. The data of the system components are given in [56] with annual peak active power load of 2850 MW and reactive power load is 580MVAr. The hourly load variations model is created from the technical data given in Table 4 and Table 5 of [56].

Authors in [57] developed a benchmark CPP reliability test system to establish a reliability test system that incorporates ICT components into 24-Bus RTS. The study suggests that portion(s) of the 24-Bus RTS may be extended with ICT configurations. Therefore, in this study all generator buses of the 24-Bus RTS are incorporated with ICT components to achieve a comprehensive cyber-physical test system [57]. The 24-Bus RTS power network with selected buses (substations) of cyber part of the system (ICT configurations) is shown in Fig. 6. Each of these selected buses is integrated with ICT features, such as Merging Units (MUs), Ethernet Switches (ESs) and line protection panel (LPP) with their connections, are shown in Fig. 7 below. Mean time to failure (MTTF) and mean time to repair (MTTR) values of ICT components used in this study for reliability assessments are from [57]–[59] and are shown in Table 2.

It is also to be noted that although the reliability is a combined reflection of adequacy and the security of the system, the paper investigates the security part of the system and impacts on the physical power system from the cyber-physical interactive operation.

B. SCENARIOS

Various failure rates of cyber-attacks are considered in this study in order to explore any abnormal transitions within the CPP system. Having such leverage can ensure extra planning in the events of unforeseen contingencies in the CPP

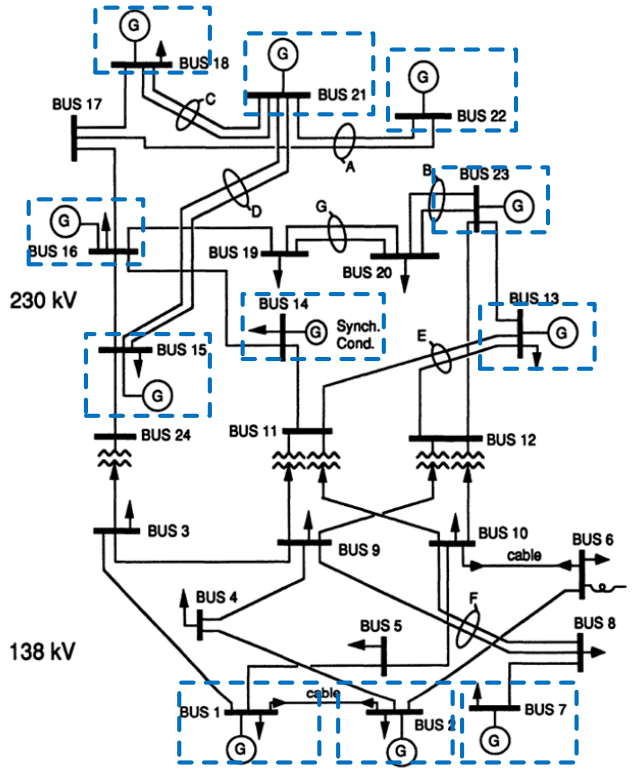

FIGURE 6. IEEE RTS physical network with selected buses indicating cyber system [56].

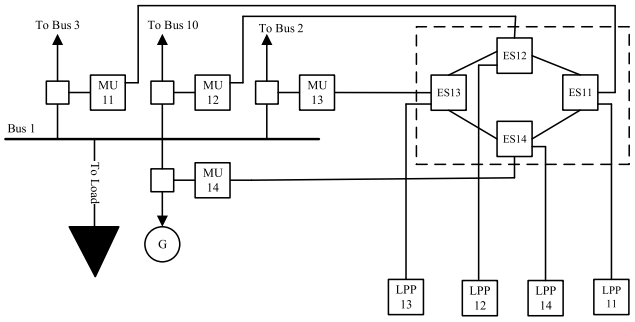

FIGURE 7. Cyber configurations extension on bus 1 [57].

system. However, such data may not be available in reality, but it is important to be aware of such transitions to mitigate unexpected contingencies. Hence, the study is performed to investigate the TMM performance and to assess the interdependency in a CPP system operation in the presence of the power system failure or cyber system failure (components failure, cyber-attacks, malicious attacks and false data-injection attacks). Thus, for every CPP system failure caused by cyber-attacks some scenarios were considered.

First scenario set A contains five clusters scenarios: A1, A3, A5, A7 and A9. Each of the scenario in scenario Set A is designed by incorporating the base case (BC) operating condition given in section IV A and then applying different failure rates of cyber-attacks on all generator substations and associated transmission lines for each failure due to cyber-attacks on the system. The probabilities of failure due to cyber-attacks on all the generators were increased in the scale 20% and simultaneously applying the failures rates of cyber-attacks at 10%, 30%, 50%, 70% and 90% on generator associated transmission lines for each failure due to cyber-attacks on the CPP system. The scenario cluster A1 is formed by simulating 10%, 30%, 50%, 70% and 90% failure rates (FR) of cyber-attack on all effective generator substations with FR of cyber-attack on all the generator associated transmission lines maintained at 10% each. The scenario cluster A3 is formed by simulating 10%, 30%, 50%, 70% and 90% FR of cyber-attack on all effective generator substations with FR of cyber-attack on all the generator associated transmission lines maintained at 30% each. Scenario cluster A5, A7 and A9 maintain the same procedure as A1 and A3.

The objectives of these scenarios are to investigate any significant transitions of impacts and sensitivities in the eventualities of significant increase in the failure rates due to cyber-attacks because it is vital to know the extreme situations and plan remedial actions accordingly.

Second scenario set B contains five clusters scenarios: B1, B3, B5, B7 and B9. Scenario set B is designed by incorporating the base case operating condition given in section IV A and then applying different levels of failure on all transformer substations and associated transmission lines for each failure is due to cyber-attacks on system. The probabilities of failure due to cyber-attacks on all the transformer substations were increased in the scale of 20% and simultaneously applying the failures rates of cyber-attacks at 10%,30%, 50%, 70% and 90% on transformer associated transmission lines for each failure due to cyber-attacks on the CPP system. The scenario cluster B1 is formed by simulating 10%, 30%, 50%, 70% and 90% FR of cyber-attack on all effective transformer substations with FR of cyber-attack on all the transformer associated transmission lines maintained at 10% each. The scenario cluster B3 is formed by 10%, 30%, 50%, 70% and 90% FR of cyber-attack on all effective transformer substations with FR of cyber-attack on all the transformer associated transmission lines maintained at 30% each. Scenario cluster B5, B7 and B9 are designed following the same procedure as in B1 and B3.

The objectives of scenario set B are the same as in scenario set A but considering the transformer substations and lines instead of power generators.

Scenario set C contains ten scenarios: CA1 to CA9 and CB1 to CB9. Scenario set C collectively group largest EENS value from each of the cluster scenario. CA1 is the largest EENS of cluster scenario A1, CA3 is the largest EENS of cluster scenario A3, CA5 is the largest EENS of cluster scenario A5, CA7 is the largest EENS of cluster scenario A7 and CA9 is the largest EENS of cluster scenario A9. CB1 to CB9 have been designed following the same procedure as in CA1 to CA9.

The objectives of scenarios in set 'C' are to investigate any significant transitions of impacts and sensitivities in the eventualities of significant increase in the failure rates of cyber-attacks with various power system components.

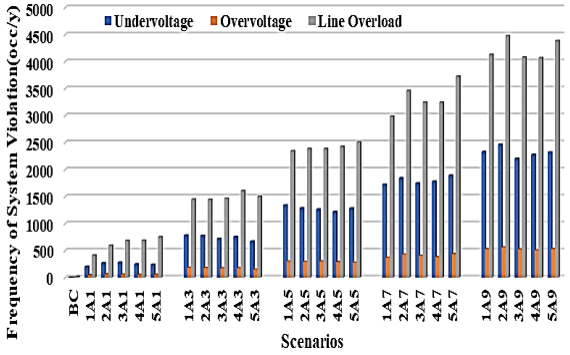

FIGURE 8. System violations for scenario set A.

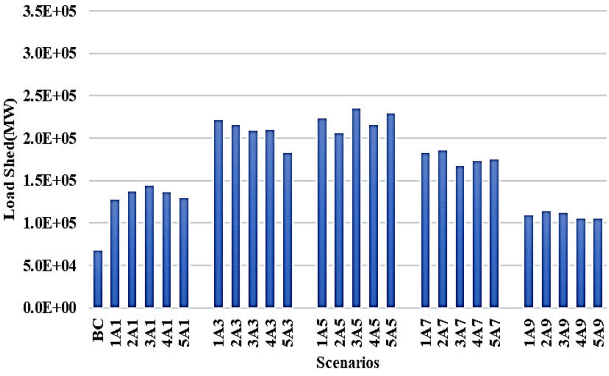

FIGURE 9. Annual load shed for scenario set A.

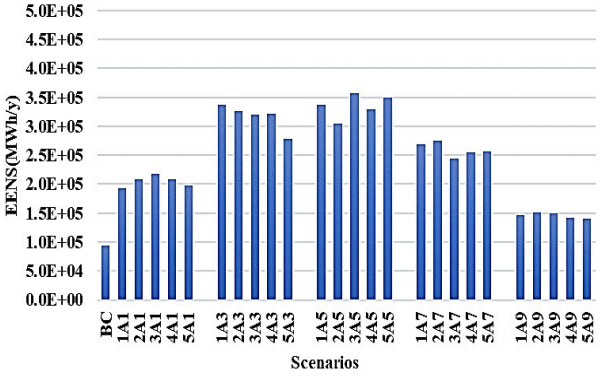

FIGURE 10. Annual EENS for scenario set A.

Scenario D is a power system security assessment in the presence of component failure without considering cyber-attacks and subsystem layers' interactions of CPP system.

C. RESULTS AND ANALYSES

Fig. 8, Fig. 9 and Fig. 10 show annual estimated results of system violations, load shed and EENS respectively for the scenario set A. In Fig. 8, the levels of CPP system violations (undervoltage, overvoltage and line-overload) increased simultaneously with increase in failure rates of cyber-attacks on all generator substations and associated transmission lines

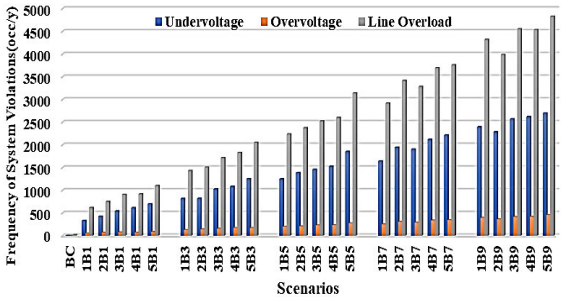

FIGURE 11. Annual system violations for scenario set B.

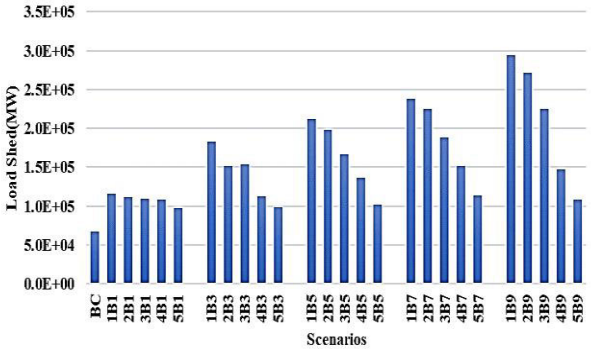

FIGURE 12. Annual Load Shed for scenario set B.

with respect to the base case. Fig. 8 indicates that the increase in failure rates of cyber-attacks on all generator substations and associated transmission lines imposed same increased rate of system disturbance and stress thus, making the system to be more unbalanced which subsequently affects the CPP system performance which is demonstrated in different increased levels of system violations.

Fig. 9 shows different increased levels of load shed with respect to the base case. The increased load shed experienced at each of the scenario set A with respect to the base case indicates that the increase in failure rates of cyber-attack on all generator substations and associated transmission lines cause various degrees of load shed in order to maintain the sustained constraint violations and the power balance of the CPP system to avoid system breakdown. Also, with respect to the increased failure rates of cyber-attack on all generator substations and associated transmission lines both Fig. 9 and Fig. 10 show a consistent increase in the load shed amount and EENS respectively from cluster scenario A1 through cluster scenario A5 but cluster scenario A7 and cluster scenario A9 show a decrease in the load shed and EENS. Cluster Scenario A9 in Fig. 9 experiences a less total blackout thus, the level of load shed is reduced compare to scenario cluster A5 which experiences a more total blackout. This depicts nonlinearity behaviour of some power system components in response to system violations in order to maintain power balance of the system.

Fig. 12 and Fig. 13, shows different increased levels of load shed and EENS respectively with respect to the base case.

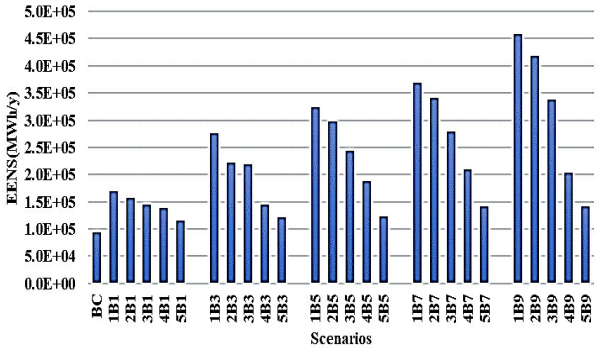

FIGURE 13. Annual EENS for scenario set B.

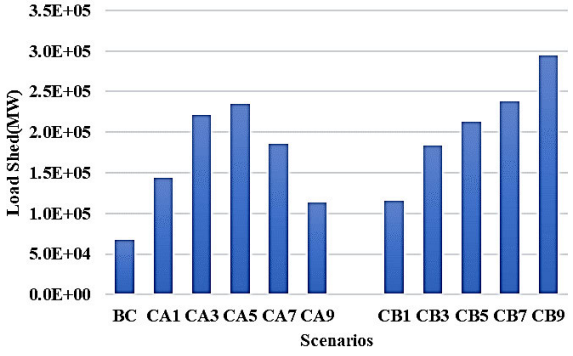

FIGURE 14. Annual Load Shed for scenario set C.

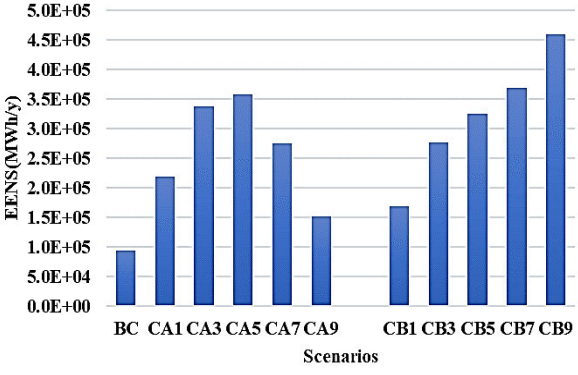

FIGURE 15. Annual EENS for scenario set C.

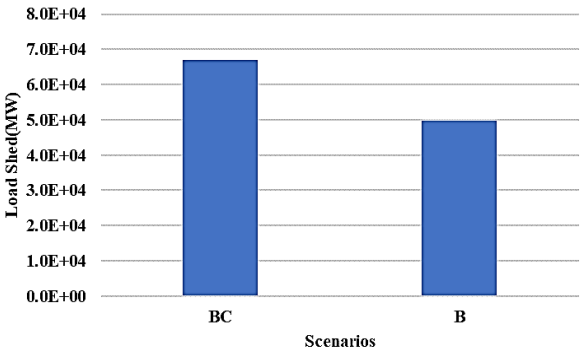

FIGURE 16. Annual Load Shed for base case and scenario D.

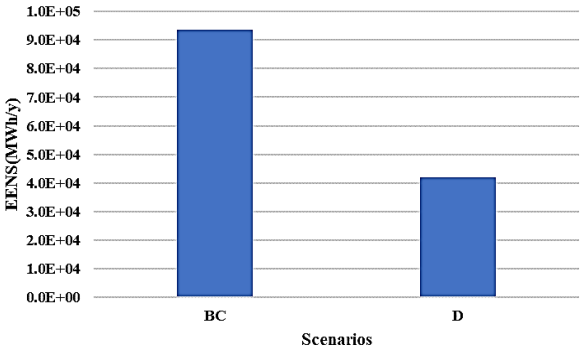

FIGURE 17. Annual EENS for base case and scenario D.

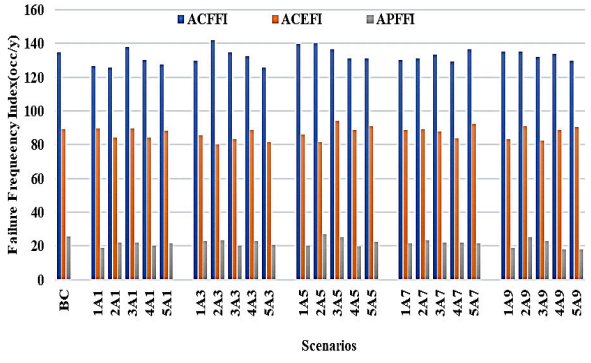

FIGURE 18. Failure Frequency Index for scenario A.

This increased load shed and EENS experienced at each of the scenario set B with respect to the base case indicates that the increase in failure rates of cyber-attacks on all the transformer substations and associated transmission lines cause various increase levels of load shed and EENS in order to maintain the sustained constraint violations and the power balance of the CPP system to avoid system breakdown. However, rate of increase of the load shed and EENS is not consistent with the rate of increase of the cyber-attacks on all the transformer substations and associated transmission lines. This depicts nonlinearity behaviour of some power system components in response to system violations to maintain the power balance of the CPP system.

Fig. 14 and Fig. 15 show the scenario set C load shed and EENS respectively with respect to the base case. In Fig. 14 there is a considerably increase in the load shed. Increased effect level of 50% failure rates of cyber-attacks on all generator substations and associated transmission lines is 250% in scenario CA5. The increased effect level of 50% failure rates of cyber-attacks on all transformer buses and associated transmission lines is 117% in scenario CB5. The rate of increase of the load shed in scenario CA and scenario CB with respect to base case depicts that load shed increases regardless, of part or section of the network affected with cyber-attacks but rate of increase in different part of the network varies. Increased failure rate of a cyber-attack on the CPP system impacts the CPP system considerably however, value of impact varies with various power system components.

Fig. 16 and Fig. 17 show the base case and scenario D load shed and EENS respectively. In Fig. 16, the base case results show a significant increased level of load shed than the scenario D load shed. The results depict that there is a

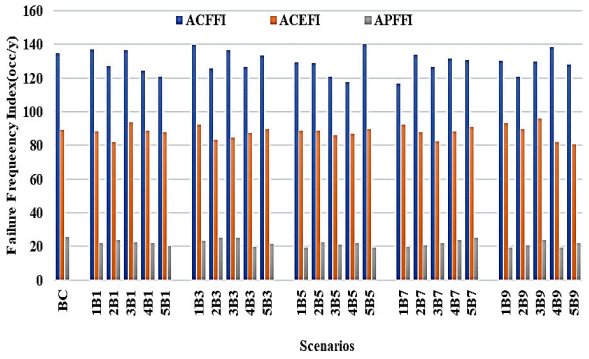

FIGURE 19. Failure Frequency Index for scenario B.

considerable increase in load shed due to interdependency operation in a CPP system caused by subsystem layers' interactions and dynamics of one subsystem layer influence the dynamics of the other subsystem layer. This makes CPP system more unreliable than the traditional power system.

Fig. 18 and Fig. 19 show failure frequency index result for base case, scenario A and scenario B respectively.

V. CONCLUSION

The paper proposes a unified ternary Markovian model (TMM) based on interactions and characteristics of three subsystem layers of the CPP system to capture the dynamics of subsystem layers' interactions in a CPP system.

The results suggest that the TMM effectively captures the dynamics of subsystem layers' interactions in a CPP system. The extended investigations suggest that the presence of cyber-attacks in a CPP system can considerably impacts the security of the physical power system. The severity of the attacks that lead to component outages does not necessarily correlate with the level of security impacts on the physical power system. Non-linearity of power system operating characteristics could make barriers for attackers in targeting power system stations that could lead to severe disturbances in the physical power system.

The proposed approach provides holistic assessment of interactions in the decision-making layer, information, communication and coupling layer and power system layer in a CPP system and offers innovative pathway to quantify the security impacts of interdependency of components in a CPP system effectively.

REFERENCES

[1] V. Aravinthan, T. Balachandran, M. Ben-Idris, W. Fei, M. Heidari-Kapourchali, A. Hettiarachchige-Don, J. N. Jiang, H. Lei, C.-C. Liu, J. Mitra, M. Ni, M. Papic, M. Parvania, M. Sephary, C. Singh, A. Srivastava, A. Stefanov, H. Sun, and S. Tindemans, "Reliability modeling considerations for emerging cyber-physical power systems," in *Proc. IEEE Int. Conf. Probabilistic Methods Appl. Power Syst. (PMAPS)*, Jun. 2018, pp. 1–7.

[2] Y. Xue, M. Ni, J. Yu, J. Hu, and W. Yu, "Study of the impact of communication failures on power system," in *Proc. IEEE Power Energy Soc. Gen. Meeting*, Jul. 2015, pp. 1–5.

[3] C. Singh and A. Sprintson, "Reliability assurance of cyber-physical power systems," in *Proc. IEEE PES Gen. Meeting*, Jul. 2010, pp. 1–6.

[4] M. Rahnamay-Naeini and M. M. Hayat, "Cascading failures in interdependent infrastructures: An interdependent Markov-chain approach," *IEEE Trans. Smart Grid*, vol. 7, no. 4, pp. 1997–2006, Jul. 2016.

[5] B. Falahati, A. Kargarian, and Y. Fu, "Impacts of information and communication failures on optimal power system operation," in *Proc. IEEE PES Innov. Smart Grid Technol. Conf. (ISGT)*, Feb. 2013, pp. 1–6.

[6] D. Kundur, X. Feng, S. Liu, T. Zourntos, and K. L. Butler-Purry, "Towards a framework for cyber attack impact analysis of the electric smart grid," in *Proc. 1st IEEE Int. Conf. Smart Grid Commun.*, Oct. 2010, pp. 244–249.

[7] M. Panteli and D. S. Kirschen, "Assessing the effect of failures in the information and communication infrastructure on power system reliability," in *Proc. IEEE/PES Power Syst. Conf. Expo.*, Mar. 2011, pp. 1–7.

[8] M. N. Albasrawi, N. Jarus, K. A. Joshi, and S. S. Sarvestani, "Analysis of reliability and resilience for smart grids," in *Proc. IEEE 38th Annu. Comput. Softw. Appl. Conf.*, Jul. 2014, pp. 529–534.

[9] A. Veremyev, A. Sorokin, V. Boginski, and E. L. Pasiliao, "Minimum vertex cover problem for coupled interdependent networks with cascading failures," *Eur. J. Oper. Res.*, vol. 232, no. 3, pp. 499–511, Feb. 2014.

[10] M. Čepin, *Assessment of Power System Reliability: Methods and Applications*. London, U.K.: Springer, 2011.

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

[12] Z. Huang, C. Wang, M. Stojmenovic, and A. Nayak, "Characterization of cascading failures in interdependent cyber-physical systems," *IEEE Trans. Comput.*, vol. 64, no. 8, pp. 2158–2168, Aug. 2015.

[13] K. Marashi, S. S. Sarvestani, and A. R. Hurson, "Quantification and analysis of interdependency in cyber-physical systems," in *Proc. 46th Annu. IEEE/IFIP Int. Conf. Dependable Syst. Netw. Workshop (DSN-W)*, Jun. 2016, pp. 149–154.

[14] J. H. Kazmi, A. Latif, I. Ahmad, P. Palensky, and W. Gawlik, "A flexible smart grid co-simulation environment for cyber-physical interdependence analysis," in *Proc. Workshop Modeling Simulation Cyber-Phys. Energy Syst. (MSCPES)*, Apr. 2016, pp. 1–6.

[15] L. Xu, Q. Guo, T. Yang, and H. Sun, "Robust routing optimization for smart grids considering cyber-physical interdependence," *IEEE Trans. Smart Grid*, vol. 10, no. 5, pp. 5620–5629, Sep. 2019.

[16] B. Falahati and Y. Fu, "A study on interdependencies of cyber-power networks in smart grid applications," in *Proc. IEEE PES Innov. Smart Grid Technol. (ISGT)*, Jan. 2012, pp. 1–8.

[17] B. Moussa, P. Akaber, M. Debbabi, and C. Assi, "Critical links identification for selective outages in interdependent power-communication networks," *IEEE Trans. Ind. Informat.*, vol. 14, no. 2, pp. 472–483, Feb. 2018.

[18] K. Marashi, S. S. Sarvestani, and A. R. Hurson, "Consideration of cyber-physical interdependencies in reliability modeling of smart grids," *IEEE Trans. Sustain. Comput.*, vol. 3, no. 2, pp. 73–83, Apr. 2018.

[19] A. H. Ahangar and H. A. Abyaneh, "Improvement of smart grid reliability considering various cyber network topologies and direct interdependency," in *Proc. IEEE PES Asia–Pacific Power Energy Eng. Conf. (APPEEC)*, Oct. 2016, pp. 267–272.

[20] M. H. Cintuglu, O. A. Mohammed, K. Akkaya, and A. S. Uluagac, "A survey on smart grid cyber-physical system testbeds," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 1, pp. 446–464, 1st Quart., 2017.

[21] W. Liu, Q. Gong, H. Han, Z. Wang, and L. Wang, "Reliability modeling and evaluation of active cyber physical distribution system," *IEEE Trans. Power Syst.*, vol. 33, no. 6, pp. 7096–7108, Nov. 2018.

[22] M. A. A. Faruque and F. Ahourai, "A model-based design of cyber-physical energy systems," in *Proc. 19th Asia South Pacific Design Autom. Conf. (ASP-DAC)*, Jan. 2014, pp. 97–104.

[23] T. Facchinetti and M. L. Della Vedova, "Real-time modeling for direct load control in cyber-physical power systems," *IEEE Trans. Ind. Informat.*, vol. 7, no. 4, pp. 689–698, Nov. 2011.

[24] M. D. Ilic, L. Xie, U. A. Khan, and J. M. F. Moura, "Modeling of future cyber–physical energy systems for distributed sensing and control," *IEEE Trans. Syst., Man, Cybern. A, Syst., Humans*, vol. 40, no. 4, pp. 825–838, Jul. 2010.

[25] J. Dang, Y. Liang, L. Huang, L. Zhu, Y. Tang, Q. Wang, and B. Lv, "Accurate modeling method of power system load based on online measurement under CPS environment," in *Proc. IEEE 7th Annu. Int. Conf. CYBER Technol. Autom., Control, Intell. Syst. (CYBER)*, Jul. 2017, pp. 1361–1366.

[26] Y.-N. Wang, Z.-Y. Lin, X. Liang, W.-Y. Xu, Q. Yang, and G.-F. Yan, "On modeling of electrical cyber-physical systems considering cyber security," *Frontiers Inf. Technol. Electron. Eng.*, vol. 17, no. 5, pp. 465–478, May 2016.
[27] S. Xin, Q. Guo, H. Sun, B. Zhang, J. Wang, and C. Chen, "Cyber-physical modeling and cyber-contingency assessment of hierarchical control systems," *IEEE Trans. Smart Grid*, vol. 6, no. 5, pp. 2375–2385, Sep. 2015.
[28] J. Wei, D. Kundur, T. Zourntos, and K. L. Butler-Purry, "A flocking-based paradigm for hierarchical cyber-physical smart grid modeling and control," *IEEE Trans. Smart Grid*, vol. 5, no. 6, pp. 2687–2700, Nov. 2014.
[29] X. Shi, Y. Li, Y. Cao, Y. Tan, Z. Xu, and M. Wen, "Model predictive control considering cyber-physical system to dampen low frequency oscillation of interconnected power systems," in *Proc. IEEE PES Asia–Pacific Power Energy Eng. Conf. (APPEEC)*, Nov. 2015, pp. 1–5.
[30] S. Wang, Z. Wu, A. Su, S. Jin, Y. Xia, and D. Zhao, "Reliability modeling and simulation of cyber-physical power distribution system considering the impacts of cyber components and transmission quality," in *Proc. 37th Chin. Control Conf. (CCC)*, Jul. 2018, pp. 6166–6171.
[31] Y. Wang, W. Li, G. Yan, and S. Song, "Towards a framework for cyber attack impact analysis of electric cyber physical systems," in *Proc. IEEE Int. Conf. Ind. Technol. (ICIT)*, Mar. 2017, pp. 638–643.
[32] E. Santacana, G. Rackliffe, L. Tang, and X. Feng, "Getting smart," *IEEE Power Energy Mag.*, vol. 8, no. 2, pp. 41–48, Mar./Apr. 2010.
[33] Y. Huang, J. Tang, Y. Cheng, H. Li, K. A. Campbell, and Z. Han, "Real-time detection of false data injection in smart grid networks: An adaptive CUSUM method and analysis," *IEEE Syst. J.*, vol. 10, no. 2, pp. 532–543, Jun. 2016.
[34] J. Jiang and Y. Qian, "Defense mechanisms against data injection attacks in smart grid networks," *IEEE Commun. Mag.*, vol. 55, no. 10, pp. 76–82, Oct. 2017.
[35] E. Hossain, Z. Han, and H. V. Poor, *Smart Grid Communications and Networking*. Cambridge, U.K.: Cambridge Univ. Press, 2012.
[36] K. Marashi and S. S. Sarvestani, "Towards comprehensive modeling of reliability for smart grids: Requirements and challenges," in *Proc. IEEE 15th Int. Symp. High-Assurance Syst. Eng.*, Jan. 2014, pp. 105–112.
[37] J. Hao, R. J. Piechocki, D. Kaleshi, W. H. Chin, and Z. Fan, "Sparse malicious false data injection attacks and defense mechanisms in smart grids," *IEEE Trans. Ind. Informat.*, vol. 11, no. 5, pp. 1–12, Oct. 2015.
[38] G. Levitin, *Computational Intelligence in Reliability Engineering: Evolutionary Techniques in Reliability Analysis and Optimization*, vol. 39. Berlin, Germany: Springer, 2006.
[39] B. S. Dhillon, *Applied Reliability and Quality: Fundamentals, Methods and Procedures*. London, U.K.: Springer, 2007.
[40] G. J. Anders, *Probability Concepts in Electric Power Systems*. New York, NY, USA: Wiley, 1989.
[41] D. J. Smith, *Reliability, Maintainability and Risk: Practical Methods for Engineers*. Oxford, U.K.: Butterworth-Heinemann, 2017.
[42] R. Billinton and R. N. Allan, *Reliability Evaluation of Engineering Systems*. New York, NY, USA: Springer, 1992.
[43] K. N. Smith, M. A. Taylor, A. A. Carroll, T. W. Manikas, and M. A. Thornton, "Automated Markov-chain based analysis for large state spaces," in *Proc. Annu. IEEE Int. Syst. Conf. (SysCon)*, Apr. 2017, pp. 1–8.
[44] C. Graham, *Markov Chains: Analytic and Monte Carlo Computations*. Hoboken, NJ, USA: Wiley, 2014.
[45] N. B. Fuqua, "The applicability of Markov analysis methods to reliability, maintainability and safety," *Sel. Top. Assur. Relat. Technol.*, vol. 10, no. 2, p. 8, 2003.
[46] I. B. Gertsbakh, Y. Shpungin, and R. Vaisman, "D-spectrum and reliability of a binary system with ternary components," *Probab. Eng. Informational Sci.*, vol. 30, no. 1, pp. 25–39, Jan. 2016.
[47] W. Li, *Reliability Assessment of Electric Power Systems Using Monte Carlo Methods*. New York, NY, USA: Springer, 2013.
[48] C. Singh and J. Mitra, "Monte Carlo simulation for reliability analysis of emergency and standby power systems," in *Proc. IAS Conf. Rec. IEEE Ind. Appl. Conf. 30th IAS Annu. Meeting*, Oct. 1995, pp. 2290–2295.
[49] M. Wadi, M. Baysal, A. Shobole, and M. R. Tur, "Reliability evaluation in smart grids via modified Monte Carlo simulation method," in *Proc. 7th Int. Conf. Renew. Energy Res. Appl. (ICRERA)*, Oct. 2018, pp. 841–845.
[50] R. Allan and R. Billinton, "Probabilistic assessment of power systems," *Proc. IEEE*, vol. 88, no. 2, pp. 140–162, Feb. 2000.
[51] D. Jayaweera and S. Islam, "Security of energy supply with change in weather conditions and dynamic thermal limits," *IEEE Trans. Smart Grid*, vol. 5, no. 5, pp. 2246–2254, Sep. 2014.
[52] K. K. Kariuki and R. N. Allan, "Evaluation of reliability worth and value of lost load," *IEE Proc. Gener. Transm. Distrib.*, vol. 143, no. 2, pp. 171–180, Mar. 1996.
[53] *IEEE Guide for Electric Power Distribution Reliability Indices—Redline*, Standard IEEE Std 1366-2012 (Revision of IEEE Std 1366-2003)—Redline, 2012, pp. 1–92.
[54] V. Aravinthan, B. Karimi, V. Namboodiri, and W. Jewell, "Wireless communication for smart grid applications at distribution level—Feasibility and requirements," in *Proc. IEEE Power Energy Soc. Gen. Meeting*, Jul. 2011, pp. 1–8.
[55] M. Benidris, J. Mitra, and C. Singh, "Integrated evaluation of reliability and stability of power systems," *IEEE Trans. Power Syst.*, vol. 32, no. 5, pp. 4131–4139, Sep. 2017.
[56] C. Grigg, P. Wong, P. Albrecht, R. Allan, M. Bhavaraju, R. Billinton, Q. Chen, C. Fong, S. Haddad, S. Kuruganty, W. Li, R. Mukerji, D. Patton, N. Rau, D. Reppen, A. Schneider, M. Shahidehpour, and C. Singh, "The IEEE reliability test system-1996. A report prepared by the reliability test system task force of the application of probability methods subcommittee," *IEEE Trans. Power Syst.*, vol. 14, no. 3, pp. 1010–1020, Aug. 1999.
[57] H. Lei and C. Singh, "Developing a benchmark test system for electric power grid cyber-physical reliability studies," in *Proc. Int. Conf. Probabilistic Methods Appl. Power Syst. (PMAPS)*, Oct. 2016, pp. 1–5.
[58] M. G. Kanabar and T. S. Sidhu, "Reliability and availability analysis of IEC 61850 based substation communication architectures," in *Proc. IEEE Power Energy Soc. Gen. Meeting*, Jul. 2009, pp. 1–8.
[59] J. Guo, Y. Wang, C. Guo, S. Dong, and B. Wen, "Cyber-physical power system (CPPS) reliability assessment considering cyber attacks against monitoring functions," in *Proc. IEEE Power Energy Soc. Gen. Meeting (PESGM)*, Jul. 2016, pp. 1–5.

PEJU ADESINA OYEWOLE (Member, IEEE) received the B.S. degree in electrical and electronic engineering from the University of Ibadan, Nigeria, in 2002, and the M.Sc. degree in electrical engineering from the University of Nottingham, U.K., in 2014. She is currently pursuing the Ph.D. degree with the Department of Electronic, Electrical, and Systems Engineering, University of Birmingham, U.K. She has more than ten years of industrial experience in project engineering management focusing on components and system specification, design, manufacturing, installation, and commissioning from initial concept to completion. Her research interests include cyber-physical power system modeling and reliability analysis, power system reliability, smart grids, renewable energy, and system modeling.

DILAN JAYAWEERA (Senior Member, IEEE) received the Ph.D. degree in electrical power engineering from the University of Manchester Institute of Science and Technology (UMIST), Manchester, U.K., in 2003. He is currently a Senior Lecturer in Electrical Power Systems with the Department of Electronic, Electrical, and Systems Engineering (EESE), University of Birmingham. He is also a Chartered Engineer in U.K., a Chartered Professional Engineer in Australia, and a Fellow at Engineers, Australia. He has wide experiences in energy industry, research, and teaching. He has authored a significant number of research articles in scientific journals, conference proceedings, and as book chapters in the fields of power system security, reliability, active distribution network operation, smart grids, smart asset management, micro grids, and risks in power systems. He is also an Editor of IEEE TRANSACTIONS ON POWER SYSTEMS and POWER ENGINEERING LETTERS.