A Cybersecurity Insurance Model for Power System Reliability Considering Optimal Defense Resource Allocation

Pikkin Lau, *Student Member, IEEE*, Wei Wei, Lingfeng Wang, *Senior Member, IEEE*, Zhaoxi Liu, *Member, IEEE,* and Chee-Wooi Ten, *Senior Member, IEEE*

***Abstract*—With the increasing application of Information and Communication Technologies (ICTs), cyberattacks have become more prevalent against Cyber-Physical Systems (CPSs) such as the modern power grids. Various methods have been proposed to model the cybersecurity threats, but so far limited studies have been focused on the defensive strategies subject to the limited security budget. In this paper, the power supply reliability is evaluated considering the strategic allocation of defense resources. Specifically, the optimal mixed strategies are formulated by the Stackelberg Security Game (SSG) to allocate the defense resources on multiple targets subject to cyberattacks. The cyberattacks against the intrusion-tolerant Supervisory Control and Data Acquisition (SCADA) system are mathematically modeled by Semi-Markov Process (SMP) kernel. The intrusion tolerance capability of the SCADA system provides buffered residence time before the substation failure to enhance the network robustness against cyberattacks. Case studies of the cyberattack scenarios are carried out to demonstrate the intrusion tolerance capability. Depending on the defense resource allocation scheme, the intrusion-tolerant SCADA system possesses varying degrees of self-healing capability to restore to the good state and prevent the substations from failure. If more defense resources are invested on the substations, the intrusion tolerant capability can be further enhanced for protecting the substations. Finally, the actuarial insurance principle is designed to estimate transmission companies' individual premiums considering correlated cybersecurity risks. The proposed insurance premium principle is designed to provide incentive for investments on enhancing the intrusion tolerance capability, which is verified by the results of case studies.**

***Index Terms*—Cybersecurity, cyber-insurance, cyber risk management, power system reliability, game theory.**

Manuscript received November 17, 2019; revised February 7, 2020 and March 22, 2020; accepted April 16, 2020. Date of publication May 6, 2020; date of current version August 21, 2020. This work was supported by the U.S. National Science Foundation under Award ECCS1739485 and Award ECCS1739422. Paper no. TSG-01738-2019. *(Corresponding author: Lingfeng Wang.)*

Pikkin Lau, Lingfeng Wang, and Zhaoxi Liu are with the Department of Electrical Engineering and Computer Science, University of Wisconsin–Milwaukee, Milwaukee, WI 53211 USA (e-mail: l.f.wang@ieee.org).

Wei Wei is with the Department of Mathematical Sciences, University of Wisconsin–Milwaukee, Milwaukee, WI 53211 USA.

Chee-Wooi Ten is with the Department of Electrical and Computer Engineering, Michigan Technological University, Houghton, MI 49931 USA.

Color versions of one or more of the figures in this article are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TSG.2020.2992782

I. Introduction

THREATS of cyberattacks had come to the public's attention in the past decade. A ransomware incident occurred in 2018 at Atlanta, which affected the core city services and might cost $44.5 million for recovery [1]. A "cyber event" on the U.S. power grid was reported in 2019. A Denial-of-Service (DoS) attack disabled the security devices in Utah, Wyoming and California without inducing actual power outage. As a result, Supervisory Control and Data Acquisition (SCADA) systems of electric utilities temporarily lost partial visibility [2]. Nevertheless, successful cyberattacks could lead to serious consequences. The first known cyber event anywhere in the world causing blackout can be traced back to the cyberattack on Ukrainian power grid in 2015. During the cyberattack, the hackers infiltrated through Virtual Private Network (VPN) and successfully disabled the power supply to the customers of three distribution companies for several hours [3]. According to an annual report from North American Electric Reliability Corporation (NERC), the focus of financially motivated cyberattacks has been shifted to cryptojacking as of 2018. Prolonged cryptojacking may result in negative impacts that may trigger a DoS condition on the system such as component burnout and exhaustion of the processing power [4].

Cybersecurity can be enhanced by more sophisticated defense systems to enable an improved resilience against potential cyberattacks. Attack-resilient Wide-Area Monitoring, Protection, And Control (WAMPAC) is a security framework constituted by an entire security life cycle from assessing risk to detecting and mitigating attacks to attack resilience [5]. For attack detection, Tang *et al.* [6], [7] work on the anomaly localization and fraud detection of smart meters in the distribution network based on the graph theory-based approaches. Anomalies in power system applications such as Automatic Generation Control (AGC) can be identified via the real-time load forecasts. In [8], an offline control is proposed as attack mitigation synthesized by the simulated real-time load and its forecast, successfully maintaining the system frequency during attack at around the nominal frequency. Different from the existing literature, our study reported in this paper focuses on the risk assessment on cybersecurity threats and system vulnerability for the actuarial study.

Vulnerability is the system weakness that can be exploited by malicious attackers. Various algorithms and tools have been developed to reduce the system vulnerability against cyber-attacks. The impacts of cyberattacks can be evaluated by carrying out the transient vulnerability assessment on bulk power systems [9]. Risk management tools like insurance, by quantifying the possibility of loss or damage, are applicable to address the residual cyber risk. Insurance transfers the risk from an insured (policyholder) to an insurance carrier (insurer). The cyber-insurance comes into play to protect and maintain financial health of the electric utilities suffering from cyberattacks. The insured utility regularly pays a cyber premium to the insurer to guarantee coverage on the losses induced by cyber risks. In the U.S. alone, the size of the market for cyber-insurance in terms of premiums was 2.0 billion in 2014, with a yearly growth rate at 10∼25% [10]. Through client contract discrimination, a cyber-insurer may improve efficiency of a cyber-insurance market and security of the network [11].

In [12], a two-stage Stackelberg game model is developed to address the security pricing by allocating the equilibrium in cyber-insurance market. A coalitional cyber-insurance is proposed as an alternative to a third-party insurance where organizations are involved as both insurers and insureds in distributing the risk [13].

This study incorporates Stackelberg Security Game (SSG) for planning the defense resource allocation. The intrusion tolerant capability of the respective Transmission Companies (TransCos) is distributed by SSG based on the amount of available defense resources. A Sequential Monte Carlo (SMC) simulation is performed for the reliability analysis on the losses induced by potential cyberattack intrusions. A cyber-insurance principle is devised to estimate the individual premium of each TransCo based on the loss distributions. The chief contributions of this paper are summarized as threefold:

- A comprehensive quantitative risk assessment approach that integrates probabilistic and game-theoretic modeling to evaluate the cyberattack impact on the reliability is developed.
- An SSG model is proposed as the optimal stochastic distribution mechanism to allocate defense resources across the target substations in each TransCo. A Semi-Markov Process (SMP) model is developed to model the intrusion tolerant capability of the SCADA system. The existent defense resource allocation strategies fall short in exploring the long-term impact of system compromise on the reliability due to cyberattacks [14], [15]. Thus, the proposed defensive strategy is devised to properly address the relationship between security investment and savings in insurance premium.
- A cyber-insurance framework is established for the TransCos to estimate the cyber risk and the corresponding premiums for long-term planning. An actuarial insurance principle for a third-party insurer is proposed to estimate the actuarial implication of potential power supply interruptions caused by cybersecurity threats, integrating vulnerability metrics into long-term reliability assessment. The proposed insurance principle effectively addresses the dependence issue of the losses from different TransCos by allocating premiums according to TransCos' individual responsibilities to the riskiness of the insurance portfolio.

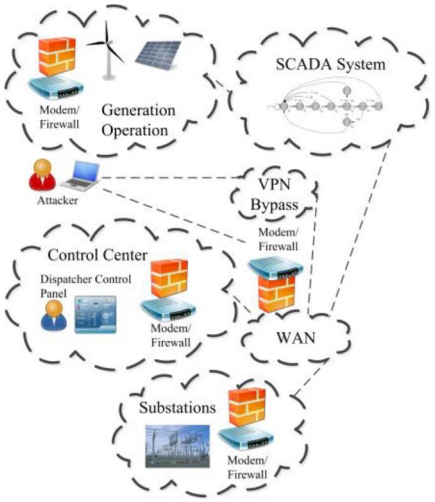


Fig. 1. ICT Network including SCADA Infrastructure, Substations, Control Center, and Generation Operation System.

The rest of this paper is organized as follows. A cyber-reliability assessment model is proposed in Section II. Section III proposes a new premium principle for the cyber-insurance. In Section IV, the proposed game-theoretic cyber-insurance model is introduced. Case studies are carried out with results discussed in Section V. The concluding remarks of this paper are given in Section VI.

II. Cyber-Reliability Assessment Model

A. SMP Intrusion Tolerant Model

Fig. 1 illustrates the ICT network of the power systems. There are three major parts connected through the Wide Area Network (WAN): generation operation, control center, and substations, each of which uses a Local Area Network (LAN) to coordinate the intelligent electronic devices. The substations are installed with the SCADA systems for monitoring the substations subject to potential cyberattacks. The cyberattack mechanism is described as follows. In the attacks, the attacker aims to infiltrate the firewalls or bypass the VPN to obtain access to the SCADA servers of the substations. After gaining the root privilege of the SCADA servers, the attacker may maliciously manipulate the voltage and current measurements or send false commands to trip the breakers in the substations. As a result, cyberattacks could disconnect generation units and transmission lines from the grid, leading to significant load curtailment and monetary losses of the TransCos.

Widespread applications of the ICTs introduce higher risks on cybersecurity in the power systems. SMP model is applicable to evaluate the cyberattack on the SCADA system at each substation [16], [17]. An intrusion tolerant model of the SCADA system is formulated by SMP in this study. Referring to Fig. 2, the stochastic process of the cyberattack is composed of a set of states $S_n = \{G, V, H, C, A, T, R, M, F\}$, briefly described in Table I. The states can be classified into

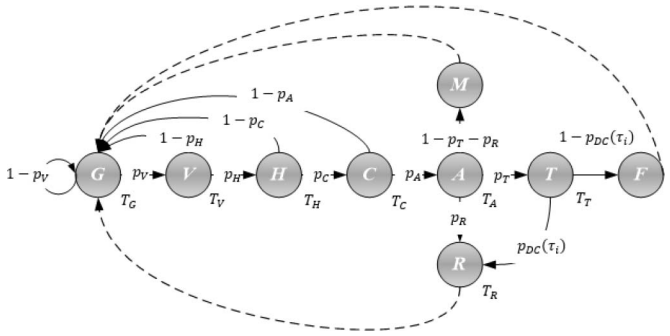


Fig. 2. Semi-Markov process model of the intrusion tolerant SCADA system at power system substations.

TABLE I
STATE DESCRIPTION IN THE SMP MODEL

State	Description
G	Good state. The system has no exposure to cybersecurity risks.
V	Vulnerability state. The cybersecurity countermeasure fails.
H	Host state. The attacker successfully gains the privilege of the targeted server.
C	Network connection state. The attacker obtains the privilege of the connection servers.
A	Attack state. The state where an active attack is successfully launched.
T	Triage state. The attack is identified during network exploitation.
R	Restoration state. Additional defense resources/security mechanisms are invested to the system to survive the attack.
M	Masked compromise state. The system has redundancy to offer normal services under the active attack.
F	Failure state. The state where damage occurs in the system.

two types: transient states and absorbing states. The transient states map the process of the attack on the SCADA system from the good state to the failure state. Restoration of the system to a good state takes place with a given probability determined by SSG. Absorbing states map the restoration process from the failure state to the good state except for state R which represents restoration. In brief, transient states $\{G, V, H, C, A, T, R\} \in S_t$ and absorbing states $\{M, F\} \in S_a$.

The details of the states in the proposed SMP are described as follows:

Step 1) The SMP starts from the good state G where the system has no exposure to cybersecurity risks. Once the strategies for cybersecurity fail, the SCADA system is transitioned from the good state G to the vulnerability state V.

Step 2) When the attacker successfully gains the privilege of the targeted server, the SCADA system proceeds to the host state H.

Step 3) After the attacker infiltrates from the targeted server to obtain the privileges of the connection servers in the whole network, the network connection state C is reached.

Step 4) During state C, the attacker embeds backdoor programs in the servers to increase vulnerabilities of the SCADA system. The system enters the attack state A if an active attack is successfully launched.

Step 5) In the intrusion states $\{G, V, H, C, A\}$, if the attack process is exposed by the detection strategies of the SCADA system, the attack process is interrupted, and the system returns to the good state G.

Step 6) If the SCADA system has redundancy to offer normal services under the active attack, the masked compromise state M occurs.

Step 7) When the attack is detected during network exploitation, the triage state T is reached. In this state, various defense approaches are considered in response to the attack. If the defense resources are invested to sustain the attack, the restoration state R occurs. Otherwise, the system enters the failure state F and results in damage [18]. The cyberattack process is completed.

B. Cyberattack Modeling

The transient states of the SMP model capture the dynamics of the attack from the good state to the failure state, which is characterized by the Mean-Time-To-Compromise (MTTC). In practice, the MTTC is modeled based on the data of vulnerabilities and exploits. Herein, the SMP model is applied to evaluate the MTTC of target substations. In contrast, Mean-Time-To-Repair (MTTR) describes the mean time for the SCADA system to recover from the failure state to the good state.

Denote the transition probability for the $(j, i)^{th}$-entry in the Markov kernel as p_{ji}, whose empirical values can be obtained by fitting the vulnerability occurrence data; and the Markov transition matrix representing the SMP model of the cyberattack can be expressed as follows:

$$P_n = \begin{array}{c} \\ G \\ V \\ H \\ C \\ A \\ T \\ R \\ M \\ F \end{array} \begin{array}{c} \begin{array}{ccccccccc} G & V & H & C & A & T & R & M & F \end{array} \\ \begin{bmatrix} \tilde{p}_V & p_V & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \tilde{p}_H & \cdot & p_H & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \tilde{p}_C & \cdot & \cdot & p_C & \cdot & \cdot & \cdot & \cdot & \cdot \\ \tilde{p}_A & \cdot & \cdot & \cdot & p_A & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & p_T & p_R & \tilde{p}_{TR} & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & p_{DC} & \cdot & \tilde{p}_{DC} \\ 1 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 1 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 1 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \end{bmatrix} \end{array} \tag{1}$$

subject to

$$\sum_{i \in S_n} p_{ji} = 1, \ \forall j \in S_n \tag{2}$$

where $\tilde{p}_i = 1 - p_i$, $\tilde{p}_{TR} = 1 - p_T - p_R$ and $\tilde{p}_{DC} = 1 - p_{DC}$.

The visit counter V_i is defined by the average number of visits on transient state i. Combining the transition probabilities and mean sojourn times, MTTC can be calculated analytically, with the visit counter as an intermediate step. Individual visit counter holds a relation as follows:

$$V_i = 1_{\{i=G\}} + \sum_j V_j p_{ji}, \ i, j \in S_t \tag{3}$$

By matrix partitioning, submatrix P_t consisting of the transient states S_t is extracted from P_n. P_t includes the information

needed to calculate V_i.

$$P_t = \begin{array}{c} \\ G \\ V \\ H \\ C \\ A \\ T \\ R \end{array} \begin{bmatrix} \tilde{p}_V & p_V & \cdot & \cdot & \cdot & \cdot & \cdot \\ \tilde{p}_H & \cdot & p_H & \cdot & \cdot & \cdot & \cdot \\ \tilde{p}_C & \cdot & \cdot & p_C & \cdot & \cdot & \cdot \\ \tilde{p}_A & \cdot & \cdot & \cdot & p_A & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & p_T & p_R \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & p_{DC} \\ 1 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \end{bmatrix} \tag{4}$$

Substituting the elements in P_t into (3), a linear system is constructed, and a unique solution for V_i is guaranteed since the system determinant is always non-zero. The analytical form of V_i is listed as follows:

$$\begin{cases} V_G = 1 + \sum_{i\in\{G,V,H,C\}} (1-p_i)V_i + V_R \\ V_V = p_V V_G \\ V_H = p_H V_V \\ V_C = p_C V_H \\ V_A = p_A V_C \\ V_T = p_T V_A \\ V_R = p_R V_A + p_{DC} V_T \end{cases} \tag{5}$$

$$V_G = \frac{1}{p_V p_H p_C p_A (1 - p_R - p_{DC} p_T)},$$
$$V_C = \frac{1}{p_A (1 - p_R - p_{DC} p_T)}$$
$$V_V = \frac{1}{p_H p_C p_A (1 - p_R - p_{DC} p_T)}, \quad V_A = \frac{1}{1 - p_R - p_{DC} p_T}$$
$$V_H = \frac{1}{p_C p_A (1 - p_R - p_{DC} p_T)}, \quad V_T = \frac{p_T}{1 - p_R - p_{DC} p_T}$$
$$V_R = \frac{p_R + p_{DC} p_T}{1 - p_R - p_{DC} p_T} \tag{6}$$

An alternative way to obtain the sequence $\{V_i\}$ numerically is to extract the first column of the transpose of the matrix inverse of $I_t - P_t$:

$$\begin{aligned} \{V_i\} &= V_1^{"} \\ \text{s.t. } V^{"} &= (I_t - P_t)^{-1} = \begin{bmatrix} V_1^{"} & \dots & V_j^{"} \end{bmatrix}^T \end{aligned} \tag{7}$$

where I_t is the identity matrix with the same size as P_t. The randomness of the cyberattack, on the other hand, is modeled by the transition probabilities and mean sojourn times estimated by the random variables:

$$\begin{cases} p_i^U = b_1 \hat{p}_i^T + b_2 \hat{p}_i^N, \ i \in S_t \\ T_i^U = b_1 \hat{T}_i^T + b_2 \hat{T}_i^N, \ i \in S_t \end{cases} \tag{8}$$

where $\hat{p}_i^T$ and $\hat{p}_i^N$ are the tangent and normal transition probabilities in the SMC model of the intrusion tolerant system, respectively; $\hat{T}_i^T$ and $\hat{T}_i^N$ are the tangent and normal mean sojourn times in the SMC model of the intrusion tolerant system, respectively; and b_1 and b_2 are the weighting coefficients. MTTC $\bar{\lambda}$ is expressed as follows by definition:

$$MTTC = \bar{\lambda} = \sum_{i\in S_t} V_i T_i \tag{9}$$

The transition probabilities, $\hat{p}_i^T$ and $\hat{p}_i^N$, which follow a Gamma distribution, must lie in [0,1]. The mean sojourn times, $\hat{T}_i^T$ and $\hat{T}_i^N$, follow an exponential distribution. The weighting coefficients b_1 and b_2 follow a Bernoulli distribution, i.e., $b_1 = 1 - b_2$, $b_2 \sim Bern(\zeta)$, where ζ is the mean value of the Bernoulli distribution. A Bernoulli distribution is a single-trial special case of the Binomial distribution. For observing the correlation of the cyber risk across the TransCos, the tangent components $\hat{p}_i^T$, $\hat{T}_i^T$ represent individual cyber risks, while the normal components $\hat{p}_i^N$, $\hat{T}_i^N$ represent common cyber risks. In this model, $\zeta \in [0, 1]$ is the strength of interdependence. $\zeta = 0$ indicates no interdependence of the cyber risks across the TransCos. $\zeta = 1$ indicates complete interdependence of the cyber risks. Otherwise, it is a case with partial interdependence of the cyber risks.

The mathematical modeling of these variates is explained below. The exponential variate for each mean sojourn time component is generated through a simple logarithmic operation on the uniform variate. Given the specified mean value $T_j > 0$, $j \in S_t$, the random variable for the tangent mean sojourn time $\hat{T}_i^T$ that follows an exponential distribution is expressed as:

$$f\left(\hat{T}_i^T\right) = \frac{1}{T_j} \exp\left(-\frac{x}{T_j}\right) \tag{10}$$

By the inverse transform method, the sampled tangent mean sojourn time $\hat{T}_i^T$ is obtained:

$$\hat{T}_i^T = F^{-1}(U) = -T_j \ln(1 - U) \tag{11}$$

where U is a uniform variate between (0, 1). The normal mean sojourn time $\hat{T}_i^N$ is computed in a similar manner.

The components of the transition probabilities $\hat{p}_i^T$ and $\hat{p}_i^N$ are Gamma variates. Set $\hat{p}_i = \{\hat{p}_i^T, \hat{p}_i^N\}$. Since the inverse transform of the Gamma distribution is quite complicated, the variates of $\hat{p}_i$ are instead obtained from summing i.i.d. exponential variates. Denote each exponential variate as Z_i s.t. $E[Z_i] = \bar{z}_i$, then:

$$\hat{p}_i = Z_1 + Z_2 + \cdots + Z_n = \sum_{i=1}^{n} Z_i, \ E\left[\hat{p}_i\right] = n\bar{z}_i. \tag{12}$$

Remark 1: Using the moment generating function method, it can be shown that if $Z_i \sim Exp(\bar{z}_i)$, $\hat{p}_i \sim Gamma(n, \bar{z}_i)$ [19].

The randomness of cyberattacks is modeled by a time sequence generated by a given variate. Weibull distribution, a distribution function typically used in failure analysis, is the selected type of variate. Time-To-Compromise (TTC) λ following a Weibull distribution has the following probability density function:

$$g(\lambda) = \frac{k}{\breve{\lambda}} \lambda^{k-1} \exp\left[-\left(\frac{\lambda}{\breve{\lambda}}\right)^k\right] \tag{13}$$

where $\lambda \geq 0, k > 0$, with the mean value $\breve{\lambda}\Gamma(1+\frac{1}{k}) = \bar{\lambda}$. Take indefinite integral, the cumulative density function is obtained:

$$U = G(\lambda) = \int_0^{\lambda} g(\mathcal{T}) d\mathcal{T} = 1 - \exp\left[-\left(\frac{\lambda}{\breve{\lambda}}\right)^k\right] \tag{14}$$

The state duration sampling is implemented using the following relation:

$$\lambda = G^{-1}(U) = \breve{\lambda}[-\ln(1 - U)]^{1/k}. \tag{15}$$

C. Loss Modeling

The power system reliability worth evaluated in this study is the monetary loss. Expected Interruption Cost (EIC) is computed as [20]:

$$EIC = \sum_{i\in\Omega} C_i W(D_i) = \sum_{i\in\Omega} C_i \mu D_i \ (\$/yr) \tag{16}$$

where Ω is the set of load loss events; for the load loss event $i \in \Omega$, C_i is the load curtailment, D_i is the duration, and $W(D_i)$ is the unit interruption cost. In this study, we assume $W(D_i)$ to be proportional to D_i with a fractional coefficient μ.

III. Insurance Premium Principle

The design goals of the cyber-insurance principle are as follows: (1) the premiums should sufficiently cover the claims of the potential losses; and (2) the premiums should be affordable for the TransCos. In this section, the losses mentioned are referred to the reliability worth, i.e., the monetary losses induced by load interruption.

A fundamental and widely used insurance principle is the expected value premium. Given a potential loss X, the expected value premium is calculated as follows:

$$\pi(X) = (1+\rho)E[X] \tag{17}$$

where ρ is the Risk Loading Coefficient (RLC). RLC is set positive to cushion against uncertainty, administration cost, as well as to provide some profit margin. On the other hand, RLC is usually relatively low to guarantee the affordability of the insurance product. Fortunately, even with a low RLC, the law of large number guarantees that the total premium collected by the insurer is sufficient to cover the total potential losses, as long as the insurance pool is large enough. It should be stressed that this law works well only in traditional insurance practice where individual risks are independent. However, due to the nature of cybersecurity threats, cyber-related losses from different TransCos are likely to be dependent. Therefore, more advanced premium principles are needed to price and manage these potentially dependent risks.

Definition 1 (Total Premium via VaR): Denote the potential losses in different TransCos as $X_1, X_2, \ldots, X_n$. Given the total loss $TL = \sum_{i=1}^{n} X_i$, a total premium via Value at Risk (VaR) is calculated as:

$$TP_1 = VaR_\alpha(TL) = VaR_\alpha\left(\sum_{i=1}^{n} X_i\right) \tag{18}$$

where $VaR_\alpha(Y) = \inf\{y : P(Y > y) \le \alpha\}$, $\alpha \in (0,1)$. The premium is defined to control the confidence level α that the total loss TL exceeds the total premium TP_1, i.e., $P(TL > TP_1) = \alpha$.

Definition 2 (Total Premium via TVaR): To ensure the premium better covers the potential loss, a more conservative option for the insurer is a total premium via Tail Value at Risk (TVaR):

$$TP_2 = TVaR_\alpha(TL) = \frac{1}{\alpha}\int_0^\alpha VaR_p(TL)dp \tag{19}$$

Mathematically, the probability that the total loss TL exceeds the total premium TP_2 is bounded by the confidence level α, i.e., $P(TL > TP_2) < \alpha$. In this sense, the TVaR premium is more conservative than the VaR premium.

The determined total premium is then allocated to individual TransCos. To do so, new premium designs are necessary. Denote the centralized version of the i^{th} potential loss X_i as $X_i' = X_i - E[X_i]$, and the centralized total loss as $TL' = \sum_{i=1}^{n}(X_i - E[X_i])$.

Definition 3 (VaR and TVaR-Derived Premiums): The individual premiums via VaR (π_1) and TVaR (π_2) can be respectively calculated by:

$$\pi_1(X_i) = E[X_i] + \frac{VaR_\alpha(X_i')}{\sum_{i=1}^{n} VaR_\alpha(X_i')} VaR_\alpha(TL') \tag{20}$$

$$\pi_2(X_i) = E[X_i] + \frac{TVaR_\alpha(X_i')}{\sum_{i=1}^{n} TVaR_\alpha(X_i')} TVaR_\alpha(TL') \tag{21}$$

The allocated individual premiums are straightforward for the total premiums $TP_1$and TP_2 in the sense that:

$$\sum_{i=1}^{n} \pi_1(X_i) = VaR_\alpha(TL) = TP_1 \tag{22}$$

$$\sum_{i=1}^{n} \pi_2(X_i) = TVaR_\alpha(TL) = TP_2 \tag{23}$$

A simpler premium design (π_3) to allocate TP_2 based on individual contributions to the total TVaR is defined as below:

$$\pi_3(X_i) = E[X_i | TL > VaR_\alpha(TL)] \tag{24}$$

It can be easily shown that $\sum_{i=1}^{n} \pi_3(X_i) = TVaR_\alpha(TL) = TP_2$.

The premium allocation is analogous to the capital allocation problem, which has been well studied in the financial literature [21]. Therefore, the premium designs proposed above share certain commonalities with some capital allocation principles. However, a necessary emphasis is that the proposed insurance premium principle is an innovative attempt for insurance pricing application. The major difference between the proposed premium designs and traditional ones lies in the consideration of potential dependence among risks. Traditional premium designs price risks based on marginal characteristics without considering dependence. In the context of cyber-insurance, this could result in serious insolvency situation for the insurer. The proposed premium designs determine the premiums based on the total losses and thus substantially mitigate the insolvency risk.

IV. Proposed Game-Theoretic Cyber-Insurance Framework

Game theory has been applied to decentralize the power system control to reduce the risk of failures in the communication infrastructures. By avoiding the need of a top-down design, decentralized multiplayer games can model the power system dynamics as component players in a game. In addition, the nature of the general-sum games also enables the possibility of cooperation or bargaining [22], [23]. Stackelberg game is a class of hierarchical games. The leading agent commits to a strategy before the following agent in a typical Stackelberg game. The agent can be a player or a coordinated group. In a two-player Stackelberg Security Game (SSG),

the defender is the leader, and the attacker is the follower. Specifically, the attacker chooses its best strategy given the action of the defender. SSG is widely used in practical applications such as scheduling patrols, traffic checkpoints, airport transportation protection in areas of heavy terrorist activities [24]–[28]. Interested readers are referred to [29] for more details of the applications and corresponding challenges of the SSG. The compact-form algorithms for multi-target SSGs can significantly accelerate the computation compared to the normal-form approaches [30]–[32].

With the increasing penetration of Wide Area Network (WAN), protecting the CPSs from potential risks becomes of the utmost importance. Since the resources for defending the CPS are usually scarce, the strategy for effectively distributing the defense resources determines the strength of the targets to resist the adversaries. The defense resources are referred to a weight assignment system that quantifies the available security budget. The defense resources reflect the relative cost and effort required to construct the security countermeasure, including authentication, authorization, encryption, firewalls, antivirus software, intrusion detection systems, etc. To ensure the cybersecurity of substations, defense resources can be invested on necessary defense mechanisms against the cyberattacks. For example, the firewalls of SCADA servers can be equipped with advanced security tools such as network analyzers, scanners, and forensic software to monitor and control the incoming and outgoing network traffic.

Optimizing Resources In GAmes using Maximal Indifference (ORIGAMI) is an algorithm designed for a two-player general-sum game. Here ORIGAMI is intended to identify the vulnerability of each target considering the security budget available for each TransCo in a two-player general-sum SSG [30]. The algorithm serves as a risk evaluation method on the defender's end, envisioning potential cybersecurity threats in the system. Distributed ORIGAMI is deployed by each TransCo to allocate the defense resources on the associated substations. In other words, the investment of defense resources protects the targets from potential cyberattacks. In this paper, the ORIGAMI algorithm is integrated into power system reliability analysis subject to cybersecurity threats considering the optimal defense resource allocation scheme. ORIGAMI transforms the original NP-hard problem to a more efficient iteration form. The detailed procedure of ORIGAMI is depicted in Algorithm 1.

Remark 2: In ORIGAMI, the compact two-player SSG model is represented by the payoff functions of the attacker α and the defender β on the target set $\tau = \{\tau_1, \tau_2, \ldots, \tau_n\}$ given the defense coverage sequence $\mathcal{C} = \{p_{DC}(\tau_i)\}$. Each target τ_i is assumed to start from a good state. For both the attacker and defender, two scenarios are considered: a target is either covered c or uncovered u by the defender. The payoff functions are calculated as follows:

$$U_\alpha(\mathcal{C}, \tau_i) = p_{DC}(\tau_i)U^c_{\alpha,\tau_i} + (1 - p_{DC}(\tau_i))U^u_{\alpha,\tau_i} \quad (25)$$

$$U_\beta(\mathcal{C}, \tau_i) = p_{DC}(\tau_i)U^c_{\beta,\tau_i} + (1 - p_{DC}(\tau_i))U^u_{\beta,\tau_i} \quad (26)$$

Algorithm 1 Substation Protection Coverage Considering Optimal Defense Resource Allocation

1: Inputs: target set $\tau = \{\tau_1, \tau_2, \ldots, \tau_n\}$, defense resources m
2: Generate $\{U^u_{\alpha,\tau_i}\}$, $\{U^c_{\alpha,\tau_i}\}$ by a set of random variables.
3: Sort the targets by uncovered attacker's payoff $\{U^u_{\alpha,\tau_i}\}$
4: Initialize $left \leftarrow m, next \leftarrow 1, \mathcal{C} \leftarrow \mathbf{0}$, $\{\Delta p_{DC}(\tau_i)\} \leftarrow \mathbf{0}$
$Cvg_{Bnd} \leftarrow -inf$
5: Repeat Until $next == n$
6: FOR $i = 1$: $next$ do
7: Compute $\Delta p_{DC}(\tau_i) \leftarrow \frac{U^u_\alpha(next) - U^u_\alpha(\tau_i)}{U^c_\alpha(\tau_i) - U^u_\alpha(\tau_i)}$
8: IF $p_{DC}(\tau_i) + \Delta p_{DC}(\tau_i) \geq 1$
9: $Cvg_{Bnd} \leftarrow \max(Cvg_{Bnd}, \quad U^c_{\alpha,\tau_i})$
10: Compute $sum(\Delta p_{DC}(\tau_i))$
11: IF $Cvg_{Bnd} \geq -inf$ OR $\Delta p_{DC}(\tau_i) \leq left$
12: BREAK
13: $\mathcal{C}(\tau) \leftarrow \mathcal{C}(\tau) + \Delta p_{DC}(\tau)$
14: $left \leftarrow left - sum(\Delta p_{DC}(\tau_i))$
15: $next++$
16: Compute $ratio(i) \leftarrow 1/(U^u_{\alpha,\tau_i} - U^c_{\alpha,\tau_i})$, $i = 1$: $next$
17: Compute $sum(ratio(i))$
18: FOR $i = 1$: $next$ do
19: $p_{DC}(\tau_i) \leftarrow p_{DC}(\tau_i) + ratio(\tau_i) * \frac{left}{sum(ratio(i))}$
20: IF $Cvg(\tau_i) \geq 1$
21: $Cvg_{Bnd} \leftarrow \max(Cvg_{Bnd}, \quad U^c_{\alpha,\tau_i})$
22: IF $Cvg_{Bnd} > -Inf$
23: $p_{DC}(\tau_i) \leftarrow \frac{Cvg_{Bnd} - U^u_\alpha(\tau_i)}{U^c_\alpha(\tau_i) - U^u_\alpha(\tau_i)}$, $i = 1$: $next$
24: Output $\mathcal{C} = \{p_{DC}(\tau_i)\}$

where $p_{DC}(\tau_i) \in [0, 1]$; the attacker's payoff for a covered attack is denoted by U^c_{α,τ_i}, and an uncovered attack is denoted by U^u_{α,τ_i}. Likewise, U^c_{β,τ_i} and U^u_{β,τ_i} for the defender. With the binary attack sequence $\mathcal{A} = \{a(\tau_i)\}$, the defender's payoff is:

$$U_\beta(\mathcal{C}, \mathcal{A}) = \sum_\tau a_\tau U_\beta(\mathcal{C}, \tau_i) \quad (27)$$

subject to $a(\tau_i) \in \{0, 1\}$.

Remark 3: A solution of Strong Stackelberg Equilibrium (SSE) is always guaranteed in SSG, which occurs when the defender chooses an optimal mixed strategy to maximize the defender's payoff. In a typical two-player SSG, the SSE does not coincide with the Nash equilibrium unless the game is zero-sum.

ORIGAMI computes the attacker/defender's payoff with randomized covered/uncovered initial payoffs on each target to accelerate the defense resource allocation. The optimal mixed strategy of the defender in this setting can be computed in polynomial time [33]. Randomly distributing the initial payoffs facilitates the encryption against the attack. ORIGAMI features iterative search for the attacker's minimal payoff whose defense coverage roughly coincides with the defender's maximal payoff.

In this study, ORIGAMI allocates the defense resources based on the attack/defense payoff of each target according to the TransCo ownership of the load buses. In Algorithm 1, the defense resources m are either assigned to individual targets or not at all, generating the defense coverage sequence $\mathcal{C} = \{p_{DC}(\tau_i)\}$. The effect of the target correlation is mostly induced by the SMP model, with slight variation caused by

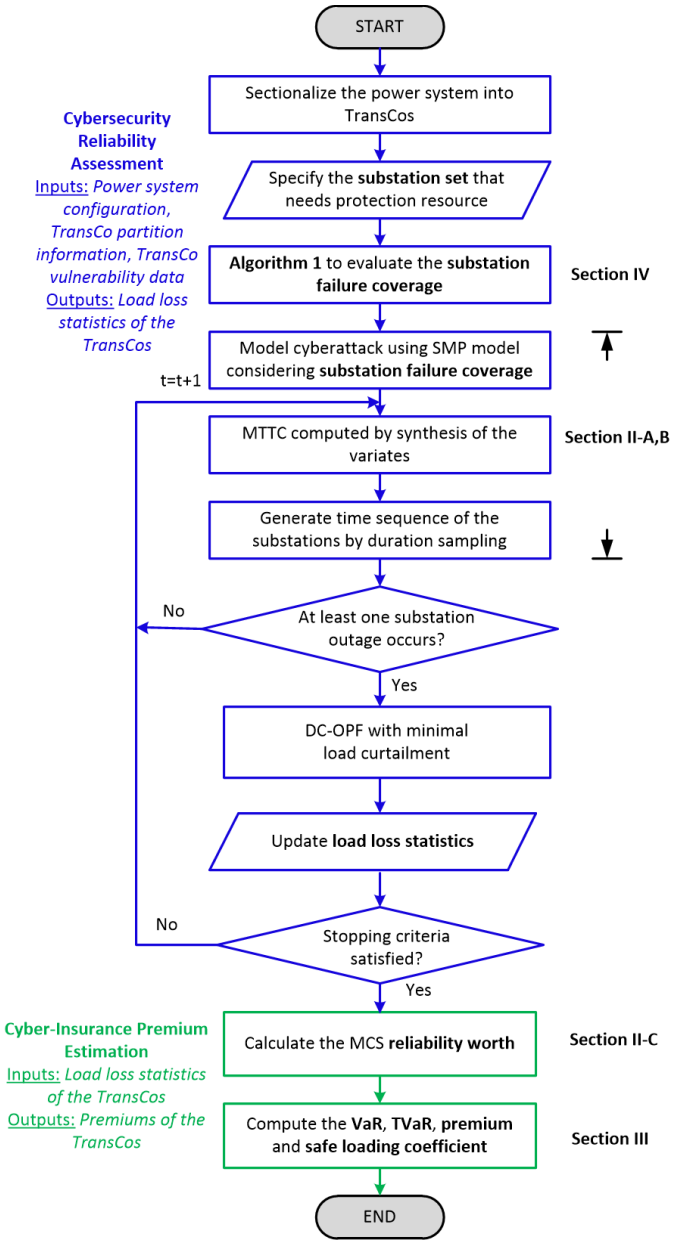


Fig. 3. Procedure of the proposed cyber-insurance framework considering integrated cybersecurity-reliability assessment.

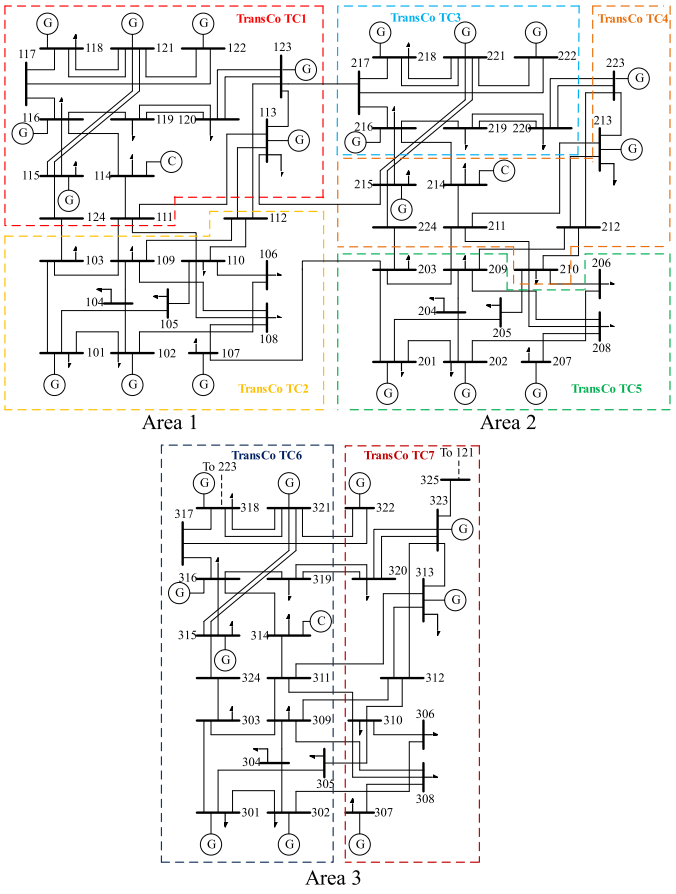


Fig. 4. IEEE Reliability Test System RTS-96 [34].

the power system configuration and the defense resource allocation. In Section V, target correlation among TransCos will be demonstrated in the case studies of reliability assessment.

The complete procedure of the proposed cyber-insurance framework is demonstrated by the flow chart in Fig. 3.

- *Cybersecurity reliability assessment:* based on the ownership boundary indicated in the TransCo partition information, the power system is sectionalized into individual TransCos. The empirical mean values in the SMC model can be obtained by fitting the vulnerability data in practice. In the SMP model, defense resource allocation is achieved by plugging in $\{p_{DC}(\tau_i)\}$ obtained from Algorithm 1. In Section II-B, incorporating the randomness in the transition probabilities and mean sojourn times, the MTTC statistics is synthesized to generate the time sequence of the cyberattacks via the sampled TTC. If at least one substation outage exists, the optimal power flow analysis is performed to minimize the load curtailment. The total load curtailment and loss of load duration are then recorded. The process is repeated until the stopping criterion is reached.
- *Cyber-insurance premium estimation:* based on the statistical records of the load loss in the Monte Carlo Simulation (MCS), the reliability worth based on the results of the MCS is calculated. The cyber-insurance premiums for the TransCos are then determined. The premium principle was presented in detail in Section III.

V. Numerical Evaluation and Analysis

A. Base Case Loss Evaluation

The single-line diagram of the IEEE Reliability Test System RTS-96 used for case studies of the proposed cyber-insurance framework is shown in Fig. 4. The IEEE RTS-96 is composed of 3 identical areas, 6 inter-area transmission lines, with details specified in [34]. The test system is assumed to be individually operated by 7 independent TransCos. The load buses of each of the TransCos TC1-TC7 are tabulated in Table II: TC1-TC2 are located at Area 1, TC3-TC5 are located at Area 2, and TC6-TC7 are located at Area 3.

In the case studies, sequential MCS is conducted using the SMP model to estimate TransCo adequacy subject to cyber-attacks. For each TransCo, the defense resource coverage is allocated in the SMP model using SSG. The sequential MCS is

TABLE II
TRANSCO OWNERSHIP ON LOAD BUSES

Area No.	TransCo	Load Bus No.	Peak Load (MW)
Area 1	TC1	113 – 120	1518
	TC2	101 – 110	1332
Area 2	TC3	216, 218, 219, 220	742
	TC4	210, 213, 214, 215	971
	TC5	201 – 209	1137
Area 3	TC6	301 - 305, 309, 314-319	1830
	TC7	306 - 308, 310, 313, 320	1020

conducted over a period of 2,000 years with hourly intervals. Coefficient μ is set to be 2.225 k$/MWh.

The following parameters are the mean values of the SMP model in case studies:

$$\begin{cases} T_G = 5\ days,\ \ T_V = 2\ day, T_H = 1\ day, T_C = 0.5\ day \\ T_A = 0.5\ day,\ \ T_T = 0.5\ day, T_R = 1\ day \end{cases}$$
$$\begin{cases} p_V = 1,\ \ p_H = 0.6, p_C = 0.5 \\ p_A = 0.4,\ \ p_T = 0.5, p_R = 0.3 \end{cases} \quad (28)$$

where $\{p_{DC}(\tau_i)\}$ is directly determined by Algorithm 1.

In addition to the parameters, the allocation of the defense resources determines the intrusion tolerant capability and thus the security level of each TransCo. Two case groups are set up to demonstrate the impact of the intrusion tolerant capability in the case studies. In the case group of Low Defense Coverage (LDC), the available defense resources only suffice for protecting 20% of the substations in each TransCo. This case group examines the effectiveness of the SSG with a tight budget of the defense resources. On the other hand, we would also like to know the loss distribution across the TransCos when abundant defense resources are accessible. In the case group of High Defense Coverage (HDC), the available defense resources are increased to cover 80% of the substations. The nominal MTTCs calculated based on the foregoing SMP mean values in (28) and $\{p_{DC}(\tau_i)\}$ are illustrated in Fig. 5, with the substations sorted in ascending order of the bus number in the individual TransCos. TransCos with high defense coverage are expected to provide protection more robust against cyberattacks. For example, TransCo TC1 has 13 buses, with high defense coverage, the defense resources are set as $m_{TC1} = 13 * 80\% \approx 10$ and allocated as follows:

$$\{p_{DC}(\tau_i)\}_{TC1} = \{0.5491, 0.5757, 0.3778, 0.8704, 0.5171, 0.6996, 1.0000, 0.4610, 0.7340, 0.8944, 0.7562, 0.8893, 0.8987\} \quad (29)$$

The defense coverage sequence has a sum limited by the defense resources. For verification, $sum(p_{DC}(\tau_i))_{TC1} \leq m_{TC1}$.

By substituting (28) and (29) into (6) and (9), the resulting nominal MTTC (days) are given as follows:

$$\{MTTC\}_{TC1} = \{154.91, 159.95, 128.79, 249.51, 149.27, 188.43, 330.67, 140.29, 198.21, 261.38, 205.08, 258.77, 263.63\} \quad (30)$$

Likewise, the nominal MTTC of other TransCos can be computed.

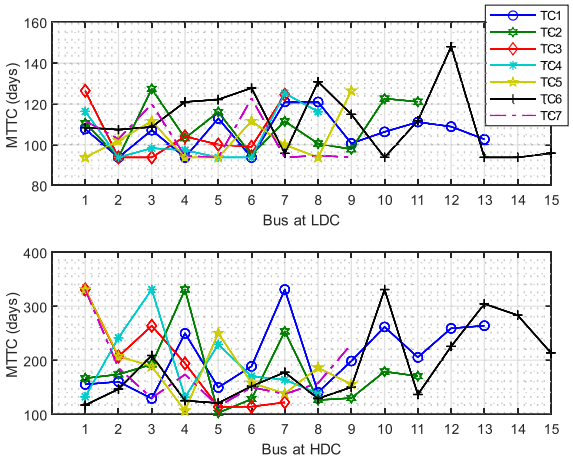


Fig. 5. Substation nominal MTTCs of the TransCos at various defense coverages.

TABLE III
EXPECTED VALUES (K$), STANDARD DEVIATIONS (K$) AND COEFFICIENTS OF VARIATION OF MONETARY LOSS IN THE TRANSCOS AT LDC

$\zeta = 0$	**TC1**	**TC2**	**TC3**	**TC4**	**TC5**	**TC6**	**TC7**
E[X]	27102	12138	7714	6252	8806	19440	10663
SD	17220	9031	5369	4704	6425	12746	7411
CoV	0.635	0.744	0.696	0.753	0.730	0.656	0.695
$\zeta = 0.7$	**TC1**	**TC2**	**TC3**	**TC4**	**TC5**	**TC6**	**TC7**
E[X]	27790	12585	7835	6685	9191	20214	10769
SD	17862	9548	5549	4910	6677	13102	7491
CoV	0.643	0.759	0.708	0.735	0.727	0.648	0.696
$\zeta = 1$	**TC1**	**TC2**	**TC3**	**TC4**	**TC5**	**TC6**	**TC7**
E[X]	28324	13215	8239	6815	9779	20465	11437
SD	18129	9852	5853	5072	7234	13522	8013
CoV	0.640	0.746	0.710	0.744	0.740	0.661	0.701

In both case groups, various strengths of interdependence are considered: $\zeta = 0$, $\zeta = 0.7$, and $\zeta = 1$. Interdependence strength is a contributing factor for high vulnerabilities of the TransCos. Cyberattacks are launched to the targets/substations. The time sequence of each substation is determined by random variables in the SMP model. Herein, we assume when a substation which enters the failure state is compromised by cyberattacks, the connected generators and transmission lines will be tripped.

The Optimal Power Flow (OPF) is then performed in the TransCos to minimize the load curtailment subject to the deficient generation capacity and network constraints. Reliability worth, i.e., the monetary losses, is calculated based on the OPF results. Finally, the actuarial insurance principle is applied to estimate the individual TransCo premiums based on the monetary loss distribution due to cyberattacks.

In the case group of low defense coverage, the expected values (EIC), Standard Deviations (SD), and Coefficients of Variation (CoV) under various cases are listed in Table III. The expected values and standard deviations only vary slightly with the increased strength of interdependence ζ. The CoV lies in a typical range [0.64, 0.76]. The loss distribution histogram illustrated as Fig. 6 agrees with the values in Table III. For different levels of interdependence strength, the bins follow a heavy-tailed and roughly monotonic distribution. The

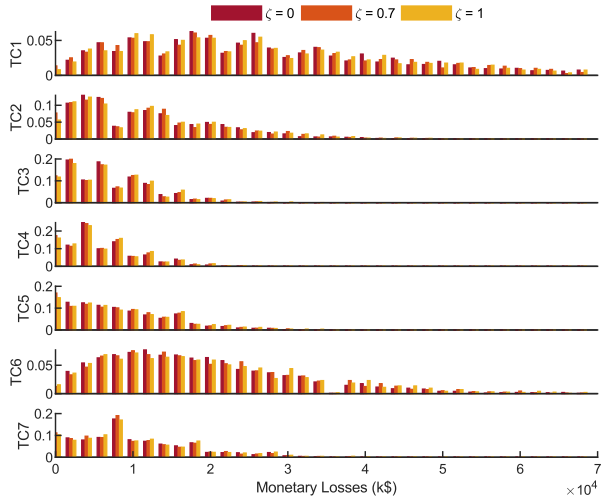


Fig. 6. Histogram of the marginal distributions of the losses in the TransCos at Low Defense Coverage.

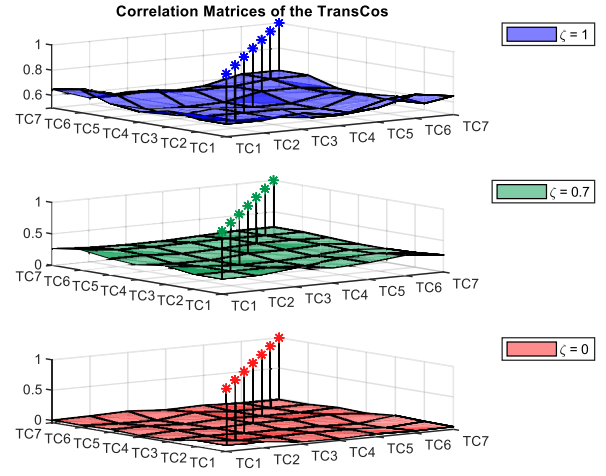


Fig. 7. Correlation matrices with various strengths of interdependence at Low Defense Coverage.

correlation matrices visualized as Fig. 7 indicate the correlation between the TransCos increases as the common cyber risk increases. Except the diagonal entries (which must be 1), the planes of the correlation remain quite flat. When $\zeta = 0$, any two of the TransCos share no interdependence as indicated by the fact that the correlations are close to zero. The correlations range between [0.20, 0.30] as ζ increases to 0.7. $\zeta = 1$ results in high correlations up to 0.69.

In the case group where high defense coverage is applied, disappearance of high losses is noticeable in Fig. 8. In the marginal distributions, it can be clearly observed that the probability mass shifts to the low loss area. Concentration of the loss distribution on the lower end also contributes to the increased CoVs lying in [0.73 0.92] as listed in Table IV. Substantial reduction on the losses can be clearly observed across the TransCos. Fig. 9 shows the strength of interdependence is decreased with high defense coverage. The case of $\zeta = 0$ reflects exact uncorrelation. $\zeta = 0.7$ induces mild correlations bounded by [0.15, 0.25]. When $\zeta = 1$, the correlations shift to [0.45, 0.60]. Both the relatively reduced losses and weaker interdependence as shown by the correlation matrices

TABLE IV
EXPECTED VALUES (K$), STANDARD DEVIATIONS (K$) AND COEFFICIENTS OF VARIATION OF MONETARY LOSS IN THE TRANSCOS AT HDC

$\zeta = 0$	TC1	TC2	TC3	TC4	TC5	TC6	TC7
E[X]	13845	6614	5035	4244	4472	11558	6169
SD	10109	5717	3788	3406	3947	8524	4845
CoV	0.730	0.864	0.752	0.802	0.883	0.738	0.785
$\zeta = 0.7$	**TC1**	**TC2**	**TC3**	**TC4**	**TC5**	**TC6**	**TC7**
E[X]	14052	6757	5052	4403	4562	12106	6424
SD	10879	6140	3937	3614	4127	9005	5065
CoV	0.774	0.909	0.779	0.821	0.905	0.744	0.789
$\zeta = 1$	**TC1**	**TC2**	**TC3**	**TC4**	**TC5**	**TC6**	**TC7**
E[X]	14745	7266	5304	4645	4865	12324	6712
SD	11394	6362	4268	3975	4452	9540	5633
CoV	0.773	0.876	0.805	0.856	0.915	0.774	0.839

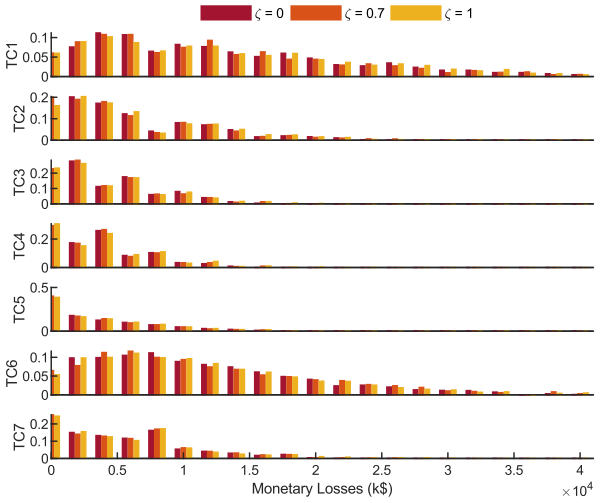


Fig. 8. Histogram of the marginal distributions of the losses in the TransCos at High Defense Coverage.

result from the high defense coverage. Correlation between any two TransCos is varied by the TransCos' interconnection and security against cyberattacks.

Given the mean values of the parameters in the SMP model, the marginal statistics of the TransCos are chiefly determined by the defense resource coverage and respective load distributions. Since the assumed cyberattacks are launched evenly to each substation, the TransCos with more evenly distributed loads would preserve higher power security.

For example, TransCo TC6 has a higher peak load but lower intrusion-induced loss than TransCo TC1.

Individual premiums of the TransCos are designed to reflect the distribution of the losses due to the cyberattacks. In the following subsection, the interdependence strength ζ which is varied in the SMC models across the TransCos would exhibit its impacts on the premiums.

B. Actuarial Premium Calculation

Using the premium principle formulae (20), (21), (24), individual premiums of all the TransCos are calculated. In this subsection, a confidence level of $\alpha = 5\%$ is set for all the premiums. From the insurer's perspective, controlling the riskiness at a relatively low level is preferable. Specifically, π_1 (Premium via VaR) is designed to ensure the total premium is greater than the total loss with a probability of $1 - \alpha$.

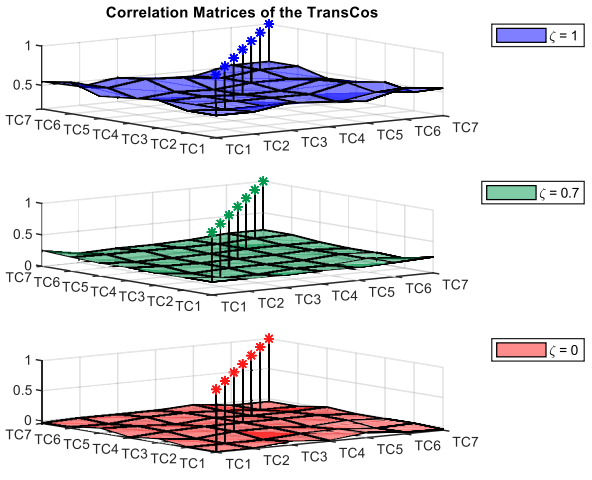


Fig. 9. Correlation matrices with various strengths of interdependence at High Defense Coverage.

TABLE V
ACTUARIAL INSURANCE PREMIUMS OF THE TRANSCOS AT LOW DEFENSE COVERAGE

$\zeta = 0$	TC1	TC2	TC3	TC4	TC5	TC6	TC7
π_1	40159	18684	11557	10068	13744	28306	16167
ρ_1	0.482	0.539	0.498	0.611	0.561	0.456	0.516
π_2	68020	33946	20999	18252	25404	52429	28880
ρ_2	1.51	1.80	1.72	1.92	1.88	1.70	1.71
π_3	68606	34258	20902	17767	24939	52795	28665
ρ_3	1.53	1.82	1.71	1.84	1.83	1.72	1.69
$\zeta = 0.7$	TC1	TC2	TC3	TC4	TC5	TC6	TC7
π_1	48088	23619	14430	12301	17633	34663	19177
ρ_1	0.730	0.877	0.842	0.840	0.919	0.715	0.781
π_2	70266	36165	22366	19289	26918	53872	29490
ρ_2	1.53	1.87	1.85	1.89	1.93	1.67	1.74
π_3	71255	36715	21827	19164	25895	53736	29774
ρ_3	1.56	1.92	1.79	1.87	1.82	1.66	1.76
$\zeta = 1$	TC1	TC2	TC3	TC4	TC5	TC6	TC7
π_1	57069	29479	17110	14548	21075	42191	24000
ρ_1	1.01	1.23	1.08	1.13	1.16	1.06	1.10
π_2	73704	37950	23549	19922	28585	55663	31876
ρ_2	1.60	1.87	1.86	1.92	1.92	1.72	1.79
π_3	74535	38403	23336	19919	28427	54552	32073
ρ_3	1.63	1.91	1.83	1.92	1.91	1.67	1.80

π_2 (Premium via TVaR) guarantees the total premium exceeds the total loss with a probability greater than $1 - \alpha$. In this sense, π_2 can better cover the potential loss than π_1 premium although both exhibit the same trend in each TransCo. Unlike π_2, π_3 (Simplified Premium via TVaR) allocates the total premium TP_2 based on the individual contributions to the total TVaR instead of the ratios associated to marginal characteristics. In this way, π_3 better reflects individual responsibilities to the riskiness of the insurance portfolio. Individual premiums estimated using π_2 and π_3 turn out to be close. Under the proposed premium principle, the Risk Loading Coefficient (RLC) is reintroduced as a measure of affordability of the insurance premiums. Specifically, it measures the proportion by which the premium exceeds the expected value of the risk:

$$\rho_i(X_i) = \pi(X_i)/E[X_i] - 1 \tag{31}$$

Due to the common cyber risks, individual RLCs would be substantially higher than those in traditional insurance practice (usually less than 50%). As shown in Table V, relative to $\zeta = 0$, the increment of the strength of interdependence, excluding proportionality to the increment of the premiums, results in high premiums. Besides, MCS with limited sampled years produces results which are susceptible to the risk uncertainty, reflected by the high RLCs of the individual TransCos.

TABLE VI
ACTUARIAL INSURANCE PREMIUMS OF TRANSCOS AT HIGH DEFENSE COVERAGE

$\zeta = 0$	TC1	TC2	TC3	TC4	TC5	TC6	TC7
π_1	21271	10972	7926	6726	7569	17658	9515
ρ_1	0.536	0.659	0.574	0.585	0.692	0.528	0.542
π_2	38848	20469	14523	12953	14698	32307	17939
ρ_2	1.81	2.09	1.88	2.05	2.29	1.80	1.91
π_3	39286	20815	14082	12604	14111	32772	18066
ρ_3	1.84	2.15	1.80	1.97	2.16	1.84	1.93
$\zeta = 0.7$	TC1	TC2	TC3	TC4	TC5	TC6	TC7
π_1	25940	13156	9209	8632	8976	21763	12021
ρ_1	0.846	0.947	0.823	0.961	0.968	0.798	0.871
π_2	42524	22284	15010	14381	15582	34736	19827
ρ_2	2.03	2.30	1.97	2.27	2.42	1.87	2.09
π_3	43723	22938	15089	13766	15281	34415	19132
ρ_3	2.11	2.39	1.99	2.13	2.35	1.84	1.98
$\zeta = 1$	TC1	TC2	TC3	TC4	TC5	TC6	TC7
π_1	30710	16115	11908	10385	10817	25689	15613
ρ_1	1.08	1.22	1.25	1.24	1.22	1.08	1.33
π_2	44326	23709	16958	15181	16945	37800	23449
ρ_2	2.01	2.26	2.20	2.27	2.49	2.07	2.49
π_3	44881	24017	16678	15280	16941	38191	22381
ρ_3	2.04	2.31	2.14	2.29	2.48	2.10	2.33

The actuarial principle is designed to incentivize high defense coverage with reduced individual premiums. In the case group of high defense coverage, a significant reduction on the premiums can be observed in Tables VI. In both Tables V and VI, the sum of individual premiums estimated using π_3 is equal to that using π_2 with minor redistributed allocation. The RLCs increase along with the increased defense coverage, indicating that the expected losses decrease more than the premiums. The analysis shows that the individual premium is negatively correlated with the defense resource coverage and positively correlated with the strength of interdependence.

VI. DISCUSSION AND CONCLUSION

Considering the increasing cyber vulnerabilities, it is possible that purchase of cyber-insurance might become mandatory in the future for TransCos and electric utilities. Cyber-insurance could be further integrated as a part of the operation cost. The TransCos and electric utilities would be able to avoid high premiums by complying with more rigorous security standards mandated by the national Electric Reliability Organization (ERO) such as the North American Electric Reliability Corporation (NERC). Since cyberattacks are becoming more and more prevalent along with the widespread use of leading-edge ICTs, the trend of increasing cyberattacks is expected to continue. Although cyberattacks causing large-scale load losses are uncommon thus far, cyber-insurance should be developed as a promising tool for transferring the risks and combatting the consequential cybersecurity threats.

In this paper, a new actuarial insurance principle is designed for a single insurer undertaking the cyber risks transferred from the power system TransCos. In each TransCo, the cyber premium is determined according to the intrusion tolerant

capability of the SCADA system. A Stackelberg Security game model is developed to optimally allocate the stochastic defense resource coverage that is unpredictable by the attacker. Investment on the defense resource coverage to enhance the intrusion tolerance capability of the SCADA systems better protects the substations from failure. As shown in the case studies, the proposed actuarial insurance principle incentivizes the TransCos with higher intrusion tolerance capability by reduced premiums. Due to the potential consequential losses caused by cyber threats on power grids, the estimated premiums are relatively high compared to those of the traditional insurance models. Preliminary studies show that a longer insurance contract can effectively reduce the annual premium. As the proposed cybersecurity insurance model is innovative to cyber risk pricing, we do anticipate some practical issues in the implementation. To apply the proposed model, dynamic modeling is required in contrast to the static settings in this paper: the interactions between the insurer and the TransCos and their behaviors along time need to be taken into consideration. Specifically, when the insurer expands business and covers more TransCos, we require the addition of new TransCos not to increase the premiums of the existing TransCos under the given insurance principle. These issues are being analyzed through studying theoretical properties of the proposed cybersecurity insurance model. Future work can also be extended but not limited to the coalition of the insurers to distribute the cyber risks and reach more affordable insurance packages. Moreover, a platform can be established for the insurers and TransCos to negotiate the premiums based on the available information revealed by the TransCos. In the premium designs, the transparency of the operating history and cyber incidents of the TransCos should be encouraged and incentivized. To promote the cyber-insurance, premium packages may be re-designed or adjusted to be more flexible according to actual situations of the respective TransCo, with partial coverage on the potential monetary losses with stricter conditions and limitations. Furthermore, novel studies for optimally allocating the defense resources may be performed to manage cyber risks with advanced game theories. The study will also be extended to the distribution network level such that the cyber-insurance premium framework will be directly related to the electric utilities.

REFERENCES

[1] *Atlanta Officials Reveal Worsening Effects of Cyber Attack*. Accessed: Jun. 6, 2018. [Online]. Available: https://www.reuters.com/article/us-usa-cyber-atlanta-budget/atlanta-officials-reveal-worsening-effects-of-cyber-attack-idUSKCN1J231M

[2] *Experts Assess Damage After First Cyberattack on U.S. Grid*. Accessed: May 6, 2019. [Online]. Available: https://www.eenews.net/stories/1060281821

[3] *Inside the Cunning, Unprecedented Hack of Ukrain's Power Grid*. Accessed: Mar. 3, 2016. [Online]. Available: https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/

[4] *2019 State of Reliability*, North Amer. Elect. Rel. Corp., Atlanta, GA, USA, Jun. 2019. [Online]. Available: https://www.nerc.com/pa/RAPA/PA/Performance%20Analysis%20DL/NERC_SOR_2019.pdf

[5] A. Ashok, M. Govindarasu, and J. Wang, "Cyber-physical attack-resilient wide-area monitoring, protection, and control for the power grid," *Proc. IEEE*, vol. 105, no. 7, pp. 1389–1407, Jul. 2017.

[6] Y. Tang, C.-W. Ten, and K. P. Schneider, "Inference of tampered smart meters with validations from feeder-level power injections," in *Proc. IEEE Innov. Smart Grid Technol. Asia (ISGT Asia)*, Chengdu, China, May 2019, pp. 2783–2788.

[7] Y. Tang, C.-W. Ten, and L. E. Brown, "Switching reconfiguration of fraud detection within an electrical distribution network," in *Proc. Resilience Week (RWS)*, Wilmington, DE, USA, Sep. 2017, pp. 206–212.

[8] S. Sridhar and M. Govindarasu, "Model-based attack detection and mitigation for automatic generation control," *IEEE Trans. Smart Grid*, vol. 5, no. 2, pp. 580–591, Mar. 2014.

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

[10] A. Marotta, F. Martinelli, S. Nanni, A. Orlando, and A. Yautsiukhin, "Cyber-insurance survey," *Comput. Sci. Rev.*, vol. 24, pp. 35–61, May 2017.

[11] R. Pal, L. Golubchik, K. Psounis, and P. Hui, "Will cyber-insurance improve network security? A market analysis," in *Proc. IEEE INFOCOM IEEE Int. Conf. Comput. Commun.*, Toronto, ON, Canada, Apr./May 2014, pp. 235–243.

[12] S. Feng, Z. Xiong, D. Niyato, and P. Wang, "Competitive security pricing in cyber-insurance market: A game-theoretic analysis," in *Proc. IEEE 88th Veh. Technol. Conf. (VTC Fall)*, Chicago, IL, USA, Aug. 2018, pp. 1–5.

[13] I. Vakilinia and S. Sengupta, "A coalitional cyber-insurance framework for a common platform," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 6, pp. 1526–1538, Jun. 2019.

[14] L. Changchen, X. Jiangwen, and L. Yunfeng, "An analysis on defense procurement entry right allocation mechanism," in *Proc. Int. Conf. E Bus. E Government*, Guangzhou, China, May 2010, pp. 432–435.

[15] M. Wang, B. Liu, and H. Xu, "Resource allocation for threat defense in cyber-security IoT system," in *Proc. 28th Wireless Opt. Commun. Conf. (WOCC)*, Beijing, China, May 2019, pp. 1–3.

[16] Y. Zhang, L. Wang, Y. Xiang, and C.-W. Ten, "Power system reliability evaluation with SCADA cybersecurity considerations," *IEEE Trans. Smart Grid*, vol. 6, no. 4, pp. 1707–1721, Jul. 2015.

[17] 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.

[18] B. B. Madan, K. Goševa-Popstojanova, K. Vaidyanathan, and K. S. Trivedi, "A method for modeling and quantifying the security attributes of intrusion tolerant systems," *Perform. Eval.*, vol. 56, nos. 1–4, pp. 167–186, Mar. 2004.

[19] A. Rakhshan and H. Pishro-Nik, *Introduction to Probability, Statistics, and Random Processes: Statistics and Random Processes*, Kappa Research, LLC, Blue Bell, PA, USA, 2014, Ch. 12, pp. 703–723.

[20] R. Billinton and W. Li, *Reliability Assessment of Electric Power Systems Using Monte Carlo Methods*. New York, NY, USA: Springer, 1994.

[21] J. Dhaene, A. Tsanakas, E. A. Valdez, and S. Vanduffel, "Optimal capital allocation principles," *J. Risk Insurance*, vol. 79, no. 1, pp. 1–28, 2012.

[22] W. W. Weaver and P. T. Krein, "Game-theoretic control of small-scale power systems," *IEEE Trans. Power Del.*, vol. 24, no. 3, pp. 1560–1567, Jul. 2009.

[23] D. Korzhyk, Z. Yin, C. Kiekintveld, V. Conitzer, and M. Tambe, "Stackelberg vs. Nash in security games: An extended investigation of interchangeability, equivalence, and uniqueness," *J. Artif. Intell. Res.*, vol. 41, pp. 297–327, May 2011.

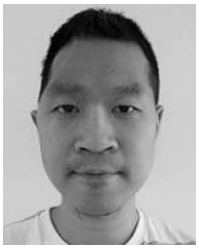
[24] P. Paruchuri, J. P. Pearce, J. Marecki, M. Tambe, F. Ordonez, and S. Kraus, "Efficient algorithms to solve Bayesian Stackelberg games for security applications," in *Proc. 23rd Assoc. Adv. Artif. Intell. (AAAI) Conf. Artif. Intell.*, Chicago, IL, USA, Jul. 2008, pp. 1559–1562.

[25] J. Pita *et al.*, "Deployed ARMOR protection: The application of a game theoretic model for security at the Los Angeles international airport," in *Proc. 7th Int. Conf. Auton. Agents Multiagent Syst. (AAMAS)*, Estoril, Portugal, May 2008, pp. 125–132.

[26] J. Pita, M. Tambe, C. Kiekintveld, S. Cullen, and E. Steigerwald, "GUARDS: Game theoretic security allocation on a national scale," in *Proc. 10th Int. Conf. Auton. Agents Multiagent Syst. (AAMAS)*, vol. 1. Taipei, Taiwan, May 2011, pp. 37–44.

[27] J. Tsai, Z. Yin, J. Kwak, D. Kempe, C. Kiekintveld, and M. Tambe, "Urban security: Game-theoretic resource allocation in networked domains," in *Proc. 24th Assoc. Adv. Artif. Intell. (AAAI) Conf. Artif. Intell.*, Atlanta, GA, USA, Jul. 2010, pp. 881–886.

[28] E. Shieh *et al.*, "Protect: A deployed game theoretic system to protect the ports of the United States," in *Proc. 11th Int. Conf. Auton. Agents Multiagent Syst. (AAMAS)*, vol. 1, Valencia, Spain, Jun. 2012, pp. 13–20.
[29] B. An, J. Pita, E. Shieh, M. Tambe, C. Kiekintveld, and J. Marecki, "GUARDS and PROTECT: Next generation applications of security games," in *Proc. ACM Special Interest Group Econ. Comput. (SIGecom) Exchanges*, 2011, pp. 31–34.
[30] C. Kiekintveld, M. Jain, J. Tsai, J. Pita, F. Ordóñez, and M. Tambe, "Computing optimal randomized resource allocations for massive security games," in *Proc. 8th Int. Conf. Auton. Agents Multiagent Syst. (AAMAS)*, Budapest, Hungary, May 2009, pp. 689–696.
[31] M. Jain *et al.*, "Software assistants for randomized patrol planning for the LAX airport police and the federal air marshal service," *Inst. Oper. Res. Manag. Sci. J. Appl. Anal.*, vol. 40, no. 4, pp. 267–290, 2010.
[32] J. Tsai, S. Rathi, C. Kiekintveld, F. Ordóñez, and M. Tambe. "IRIS—A tool for strategic security allocation in transportation networks," in *Proc. 8th Int. Conf. Auton. Agents Multiagent Syst. (AAMAS)*, Budapest, Hungary, May 2009, pp. 37–44.
[33] D. Korzhyk, V. Conitzer, and R. Parr, "Complexity of computing optimal stackelberg strategies in security resource allocation games," in *Proc. 24th Assoc. Adv. Artif. Intell. (AAAI) Conf. Artif. Intell.*, Atlanta, GA, USA, Jul. 2010, pp. 805–810.
[34] C. Grigg *et al.*, "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.

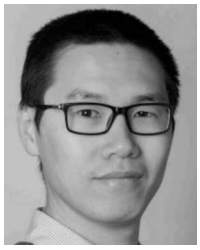


Pikkin Lau (Student Member, IEEE) received the M.S. degree in electrical engineering from Washington State University, Pullman, WA, USA, in 2017. He is currently pursuing the Ph.D. degree in electrical engineering with the University of Wisconsin–Milwaukee, Milwaukee, WI, USA. He is an Engineer in training certified by the state of Washington. His research interests include reliability analysis, dynamic state estimation, cybersecurity assessment, and model validation for power systems.

Wei Wei received the Ph.D. degree in actuarial science from the University of Waterloo, Canada. In 2013, he joined the University of Wisconsin–Milwaukee as an Associate Professor of actuarial science. His research interests mainly lie in the areas of actuarial science and quantitative risk management, as well as applied probability and operations research. Specifically, he works on the topics of optimal insurance design, dependence modeling, stochastic ordering, cyber risk management, optimal scheduling, and ruin theory.

Lingfeng Wang (Senior Member, IEEE) received the B.E. degree in measurement and instrumentation from Zhejiang University, Hangzhou, China, in 1997, the M.S. degree in electrical and computer engineering from the National University of Singapore, Singapore, in 2002, and the Ph.D. degree from the Electrical and Computer Engineering Department, Texas A&M University, College Station, TX, USA, in 2008.

He is currently a Professor with the Department of Electrical Engineering and Computer Science, University of Wisconsin–Milwaukee (UWM), Milwaukee, WI, USA. His major research interests include power system reliability, security, and resiliency. He is a recipient of the Outstanding Faculty Research Award of College of Engineering and Applied Science at UWM in 2018. He is an Editor of the IEEE TRANSACTIONS ON SMART GRID, the IEEE TRANSACTIONS ON POWER SYSTEMS, and IEEE POWER ENGINEERING LETTERS, and served on the Steering Committee of the IEEE TRANSACTIONS ON CLOUD COMPUTING.



Zhaoxi Liu (Member, IEEE) received the B.S. and M.S. degrees in electrical engineering from Tsinghua University, Beijing, China, in 2006 and 2008, respectively, and the Ph.D. degree in electrical engineering from the Technical University of Denmark, Kgs. Lyngby, Denmark, in 2016.

He is currently a Research Associate with the Department of Electrical Engineering and Computer Science, University of Wisconsin–Milwaukee, Milwaukee, WI, USA. His research interests include power system operations, integration of distributed energy resources in power systems, and power system cybersecurity.

Chee-Wooi Ten (Senior Member, IEEE) received the B.S.E.E. and M.S.E.E. degrees from Iowa State University, Ames, in 1999 and 2001, respectively, and the Ph.D. degree from University College Dublin, in 2009. In 2010, he joined Michigan Technological University as an Associate Professor of electrical and computer engineering. He was a Power Application Engineer working in project development for EMS/DMS with Siemens Energy Management and Information System, Singapore, from 2002 to 2006. His primary research interests are modeling for interdependent critical cyberinfrastructures and SCADA automation applications for a power grid. He is an Active Reviewer for IEEE PES Transactions Journals and was a member of IEEE PES computer and analytical method for cybersecurity task force. He is currently serving as an Editor for the IEEE TRANSACTIONS ON SMART GRID and *Elsevier Journal Sustainable Energy, Grids, and Networks*.