An Actuarial Framework for Power System Reliability Considering Cybersecurity Threats

Zhaoxi Liu, *Member, IEEE,* Wei Wei, Lingfeng Wang, *Senior Member, IEEE,* Chee-Wooi Ten, *Senior Member, IEEE,* and Yeonwoo Rho

***Abstract*—Cybersecurity has become an emerging issue for the secure operation of power systems. Besides hardening the power system to improve its cybersecurity, cyber insurance is emerging as a promising tool in cyber risk management. In this paper, an actuarial framework is established to capture and reduce the riskiness raised by interdependence among cyber risks, with the aim to enhance cyber insurance market for power systems. Absorbing semi-Markov process (SMP) is proposed to model the cyberattacks on the power grid. Also a stochastic model is developed to reflect the correlation of cyber risks across the power system. A sequential Monte Carlo simulations (MCS) framework is developed to evaluate the interruptions of the power system considering both the physical failures of the components and malicious cyberattacks. Then, the detailed insurance schemes are designed to manage the risks of the power system considering the financial consequences of cybersecurity threats. Case studies are conducted on a test system based on the IEEE Reliability Test System (RTS-79) to illustrate the application of the proposed insurance pricing schemes.**

***Index Terms*—Actuarial theory, cyber-insurance, cybersecurity, interdependent risks, power system reliability, premium principle.**

I. Introduction

In the past two decades, cybersecurity is emerging as one of the most important issues for the secure operation of power systems. Due to the extensive deployment of information and communication technologies (ICT) across all levels of power systems, the efficiency of the system operation has been greatly improved. However, as a direct consequence, vulnerabilities and risks of cyberattacks are introduced to the power systems at the same time [1], [2]. The cybersecurity threats to the power systems are increasing and becoming more serious over time [3]. A recent example of cybersecurity risks in power systems is the two consecutive malicious cyberattacks against the Ukrainian power grid in 2015 and 2016 [4]. Significant damage was caused by the attacks. Merely in the first attack in December 2015, over 130 MW of loads were lost and more than 50 substations were affected [5]. Thus, how to handle the risks of cybersecurity in power systems has become a pressing topic for both the academia and power industry.

Besides improving the cybersecurity of power systems itself, it is very important for the stakeholders to hedge the residual risk of potential cyberattacks against the electric power grids. As a primary tool for risk management, insurance (namely cyber insurance in this context) is among the most direct and effective solutions to the challenge. Cyber insurance can transfer the cyber risks and mitigate the impacts of successful cyberattacks on organizations. The overall benefit of cyber insurance pertains to the interactions among the power system stakeholders and insurance providers. First, cyber insurance smooths the financial impact of the cyber risks on the stakeholders. Meanwhile, insurance premium is calculated to reflect the self-protection strength of the stakeholders. This way, the stakeholders would be incentivized to strengthen the cybersecurity of the power system to reduce the premium and thus lower the total cost from both parties and reduce the impacts of the cyber threats on the grid. Further, cyber insurance can also benefit all the entities in the entire society in a few different ways [6]. First, cyber insurance encourages the stakeholders to increase the investments on cybersecurity so that the insurance premium is reduced. As a result, the overall social welfare is improved due to the enhancement of the cyber protection. Secondly, the premium of cyber insurance can indicate the quality of the cyber protection. Moreover, cyber insurance will provoke the replacement of obsolete standards with more timely and advanced standards for cybersecurity. Therefore, cyber insurance is a promising and socially beneficial approach to dealing with the emerging cyber risks.

Due to the aforementioned advantages, cyber insurance has been considered for cyber risk management in some existing research. Reference [7] describes a generic framework for using insurance to manage the information security risks which includes a four-step insurance decision plan for cyber risks. The work in [8] concerns a framework incorporating the operating principles of the insurance industry to provide quantitative estimates of cyber risks. The proposed framework uses optimization techniques to recommend the best levels of investment in cybersecurity and insurance coverage. Reference [9] proposes a synergistic insurance framework where organizations collaboratively insure a common platform instead of combating against the risks of cyberattacks alone. Meanwhile, the impacts of interdependent cybersecurity risks on the organizations' decisions to invest in security technologies and buy insurance coverage are investigated in [10]. The result shows that a more developed insurance market does not necessarily increase the organizations' insurance coverage but influenced by the insurance price levels. In [11], the authors extend the use of multi-state models which are commonly used to analyze the personal life or health insurance to cyber insurance. In order to classify the cyber insurance models in a unified way, a comprehensive formal framework is proposed in [12] by considering the interdependent security, correlated risk and information asymmetries. The research in [13] analyzes the insurability of the cyber risks. The results indicate that cyber risks can be insured in general while more work is needed

This work was supported by US National Science Foundation (NSF) under awards 1739485 and 1739422.

Z. Liu, and L. Wang are with the Department of Electrical Engineering and Computer Science, University of Wisconsin-Milwaukee, Milwaukee, WI 53211 USA (e-mail: zhaoxil@uwm.edu, l.f.wang@ieee.org).

W. Wei is with the Department of Mathematical Sciences, University of Wisconsin-Milwaukee, Milwaukee, WI 53211 USA (e-mail: weiw@uwm.edu).

C.-W. Ten is with the Department of Electrical and Computer Engineering, Michigan Technological University, Houghton, MI 49931, USA (e-mail:ten@mtu.edu).

Y. Rho is with the Department of Mathematical Sciences, Michigan Technological University, Houghton, MI 49931, USA (e-mail: yrho@mtu.edu).

to make the market more mature. Reference [14] investigates the self-insurance for cyber risks and analyzes how individual service providers can coordinate the investment decisions to improve the security and trustworthiness of the overall system. Reference [15] considers the adverse selection problem of cyber-insurance and proposes to separate the contracts for agents with different profiles. The moral hazard issue of the cyber-insurance scheme is studied in [16], which proposes to solve the problem with deductibles and partial coverage by the insurer.

The existing efforts mentioned above have kicked off the exploration of insurance for cyber risk management. However, the research on insurance for the risk management in power systems is very limited at the current stage. In [17], an insurance strategy is proposed to cover possible imbalance cost of the system due to the uncertainty of wind power. The concept of insurance for reliability is introduced in [18] to improve the quality of service provision in electric power distribution systems. To the best of our knowledge, the studies on the insurance schemes for power systems against the emerging cybersecurity threats have not been performed thus far. An in-depth analysis on the insurance mechanisms to manage the potential cyber risks in power systems is strongly urged.

In this paper, we proposed a new insurance model, which takes risk interdependence and small number of participants into considerations for the application of cyber insurance in power systems. The proposed premium principles and the temporal diversification-based design of the premiums are analyzed and proved to be effective in handling these two issues in the case study. Ten years ago, the North American Electric Reliability Corporation (NERC) critical infrastructure protection (CIP) compliance has been enforcing to ensure the utility's critical cyber asset of the power grid control system must be constantly audited. This ongoing effort has been critical because if a substation is under attack through manipulation of the local supervisory control and data acquisition (SCADA) system, the attack consequence can propagate to the rest of the grid. This actuarial framework focuses on the interdependence between control areas in the region of an interconnection as well as the correlation of cyber threats on different targets across the power systems. Generally, it is impossible to be 100% secure against the emerging cyber risks, and one who has control to ensure a comprehensive investment of security technologies does not guarantee attack proof because a cascading of an interconnected grid can be initiated by the cyber-related events. We have been cautious about unmanned substation automation as a combination of 9 substations (reported by the Federal Energy Regulatory Commission (FERC)) can lead to widespread catastrophe and instability [19]. Different from the conventional contingencies of power systems, the cyber risks on power systems may need a different management approach. The conventional N-1 is exhaustively enumerated for operational planning that addresses the events (e.g., storms and other weather-related events) that may trip a single or two breakers and isolate a single device. As this is an abnormal condition, the development of such a methodology to ensure the planning of the transmission grid can at least meet such conditions without further losing more components due to protective relaying. The higher order of contingencies is not exhaustively enumerated because it is hard to predict the detailed process, e.g., the trajectory of the storm. Most of such higher order contingencies are heuristic and can be a research subject. There has been an attempt to connect the storm trajectory of a hurricane to the higher order of contingencies. Since this is less likely to occur than N-1 as well as the stochastic nature of hurricane trajectories, it is not often exhaustively enumerated. In case of a cyberattack upon one substation can lead to N-10, it means 10 lines/generators are electrically connected to the substation (pivotal node of the grid). Such substation outage has been studied in [20]. As the physics of a power grid remains, such initiating events can incur massive overloading tripping in the neighborhood that can affect other control areas and weaken operational limits [21]. From the planning perspective, such rare events do not justify an investment of building new transmission lines due to the risks of potential cyberattacks upon multiple substations. Insurance would be a good hedging tool with investment of technologies. It has been shown that cyber risks are insurable and insurance can be a promising and effective tool for the management of cyber risks [6], [7], [11]. Thus, in this paper, the application of insurance for the cyber risk management in power systems is investigated. While it is important and necessary to deploy cybersecurity enhancement measures during the planning stage like the conventional contingency security enhancement practice of the power systems, there will still be residual cyber risks on the grid even if the best practice has been performed by the system operator on the ICT controls due to the rapidly evolving ICT and fast changing cybersecurity status. As it is analyzed and discussed in the existing studies on cyber-based contingency analysis, such residual cyber risks and the order of the consequential contingencies in the grid can be high, which can lead to significant damages [20]–[23]. Therefore, in addition to the cybersecurity enhancement measures, the proposed work in this paper provides the power system stakeholders with a mechanism to manage the residual cyber risks of the grid, which is missing in the existing researches. Further, the proposed actuarial model in this paper prevents free riding among the insureds and prompts them to enhance their cybersecurity against cyberattacks. The insurance tool is not proposed as an alternative option but effective addition to the cybersecurity enhancement measures for the cyber risk management of the power systems.

The aim of this paper is to develop appropriate insurance schemes for the power systems to manage the risks of potential malicious cyberattacks on the grid. The potential loss of the power systems considering the cyberattacks is modeled and appropriate insurance premium principles are designed. The main contributions of this paper are summarized as follows:

- Absorbing semi-Markov process (SMP) is deployed to model the cyberattacks against the grid, with which the stochastic characteristics of the SCADA systems in cybersecurity can be captured.
- A correlation model is developed for the cyber risks across the power system, with which the common cyber risks among the entities in the system can be modeled quantitatively in the analysis. Accordingly, the correlation between the losses of different entities in the power system considering potential cybersecurity threats can be evaluated.
- A sequential Monte Carlo simulations (MCS) framework is built to evaluate the interruptions of the power system considering both physical failures and malicious cyberattacks on the grid. The potential monetary loss of power outages based on the system interruption metrics considering the consequences of the cyberattacks is estimated by the proposed sequential MCS framework.

- Several insurance premium principles are proposed to capture the riskiness raised by interdependence. Using the proposed premium principles, the insurer's insolvency risk is substantially reduced. Furthermore, a temporal diversification scheme is developed to lower individual premiums. By reducing insurer's risk and insured's premium, the participation rate in cyber insurance is anticipated to be enhanced. Meanwhile, the proposed premium principles encourage the self-protection of participants by properly allocating the premium across the grid, which prevents free-riding among the cyber insurance participants.

The rest of the paper is organized as follows. The idea of using cyber insurance to manage the cyber risks for critical infrastructure protection is introduced in Section II. The loss modeling of the power systems considering the cyberattacks is introduced in Section III. In Section IV, a set of premium principles is proposed to calculate premiums for cyber risks. In Section V, the case study is implemented to illustrate the application of the proposed premium principles and the effect of temporal diversification in reducing premium. Finally, Section VI concludes the paper.

II. Cyber-Insurance for Critical Infrastructure Protection

Critical infrastructures are of great importance to the security and life quality of the entire society. Improving the cybersecurity of critical infrastructures is always an essential task of the national security. The growing interest of using cyber insurance to manage the potential cyber risks of the critical infrastructure loss has been noticed by the U.S. Department of Homeland Security (DHS) [24]. Workshops and discussions have been organized by the DHS to develop insights into cyber insurance for critical infrastructures. The ability of insurance carriers to offer relevant cyber risk coverage at reasonable prices in return for an insured's adoption of cyber risk management controls and procedures that improve its cyber risk posture is examined. Research has also been proposed to identify the relation between the cyber protection investment and cyber insurance coverage for the critical infrastructure owners and operators by building investment optimization models and cyber insurance premium discount models [8]. Further, cyber insurance has been suggested by recent studies as an effective way to accelerate the process of critical infrastructure protection [25]. However, in practice, the lack of actuarial data and the unknowable nature of potential cybersecurity threats limit the cyber insurance offers. Therefore, cyber incident information sharing, data repository, and consequence analysis would be beneficial to enabling the progress of cyber insurance coverage for the critical infrastructure protection.

Particularly, in the energy sector, the potential of using the insurance tool to manage the cyber-related risks is already under the spotlight. The U.S. Department of Energy (DOE) examines the key risks of the critical energy infrastructure including cybersecurity and suggests how the insurance industry can help manage these risks, including how it identifies, assesses, and manages them and their potential impacts in [26]. However, developing insurance mechanisms for protecting critical infrastructure from these emerging risks is a significant challenge due to a number of factors, which include the lack of historical data on the frequency and severity of the cyberattacks, the rapidly changing nature of technologies that is impacted by them, as well as the inherent uncertainties posed by cyber risks. Thus, the investigation on the cyber insurance mechanisms for the critical infrastructure protection against the emerging cyber-related risks is still in the infant stage at present.

The power system is one of the 16 critical infrastructures identified by the U.S. government, while hundreds of millions of consumers in North America depend on the bulk power system for a reliable, secure and resilient supply of electricity. The security of the electric grid has far reaching ramifications for nearly every industry. As one of the most important sectors in the modern society, power systems should be covered by the consideration of the cyber insurance schemes in order to better mitigate the potential cyber risks. In this paper, we aim to develop viable cyber insurance schemes for power systems to manage the emerging risks of cybersecurity.

III. Loss Modeling of Power Systems Considering Cybersecurity Threats

When successful cyberattacks against the power system occur, the most direct and damaging consequence is the system interruptions which may lead to serious load curtailments and even blackouts. In this study, the damage of successful cyberattacks is evaluated from the power system reliability perspective. The loss of the system is modeled by the interruptions of the grid considering malicious cyberattacks on the power system. In this paper, the physical reliability and cybersecurity of the power system are considered and simulated in different ways. For the physical reliability of the grid, the outages of the components in the grid are modeled by exponential random variables conventionally. However, for the cybersecurity of the grid, the cyberattacks are assumed to have intentional targets. The SMP model is used to formulate the dynamics between the attackers and the response of the system during the attacks. Using stochastic models to formulate the processes and impacts of cyberattacks on cyber-physical systems is a well-accepted approach [27]–[33]. Following these works, a SMP model is built to analyze the processes and influences of the cyberattacks on the grid in this paper. When an attack is successful, the intended targets of the attack instead of random components in the grid will be compromised, the corresponding consequences of the attack will be simulated and the impacts on the grid will be analyzed accordingly.

A. Modeling of Cyberattacks against Power Systems

In order to estimate the potential loss of the power system considering cybersecurity threats, cyberattacks against the substation SCADA systems in the grids are considered in this study. Due to the integration of ICT in power systems, the SCADA systems in the grid become vulnerable, and malicious attackers may attempt to intrude the SCADA systems of the substations to interfere the normal operation of the grid. Thus, in this paper, the cyberattack against the SCADA systems of the substations in the power system is considered. The attack aims to disturb the normal operation of the power system by intruding into the substation SCADA system and disconnecting the targeted substation from the grid, which will lead to immediate and serious consequences on the grid. It is assumed that all the circuit breakers in the targeted substation will be tripped maliciously by the attacker if the attack successfully compromises the SCADA system of the substation. In other words, all the generation units, transmission branches and loads connected to the targeted substation will be forced to disconnect from the grid if the attack succeeds.

During the attack, the attacker needs to intrude into the SCADA system of the substation on the targeted node. The process of the cyberattack against the substation SCADA system can be formulated with the semi-Markov process (SMP) models [33], [34]. In this study, we focus on the cyberattack aiming to jeopardize the normal operation of the power system. Successful attacks will lead to unwanted tripping and contingencies in the grid, and may consequently result in direct loss of the system. Considering the response of the cyber systems and operational control systems of the grid in the face of the attacks, an absorbing SMP model $\{J(t) : t \geqslant 0\}$ with a discrete state space is developed and used to describe the process of the cyberattack. The absorbing SMP model is illustrated in Fig. 1.

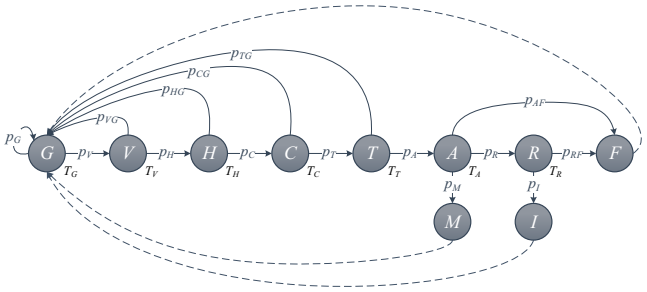


Fig. 1. Absorbing SMP Model of Cyberattack Against SCADA Systems in Power Systems.

The process of the cyberattack starts from the good state G, which represents a secure status of the SCADA system. The second stage is the intrusion process to the SCADA system which contains a series of intermediate states, each of which represents one phase of the attack. By proceeding on the attack actions step by step, the SMP transits along the intermediate states, and a greater privilege of the SCADA system is obtained by the attacker. When vulnerabilities exist in the cyber system of the SCADA system, the SMP is shifted from the good state G to the vulnerable state V. Then, the SMP is brought to the host state H if the vulnerability is exploited by the malicious attacker and used to gain one or several hosts' privilege in the SCADA network. After that, the SMP transits to the connection state C when necessary connections of the SCADA network are compromised by the attacker. Next, the targeted state T is reached if the attacker obtains the necessary privileges of the targeted servers. Subsequently, the SMP comes to the active attack state A when the destination devices are exploited and the attacker is able to launch the attack. During the penetration process of the attack from state G to A, the SMP will be brought back to the good state G if the intrusion is detected and isolated by the system protection mechanisms. However, when the active attack actions are performed, there are three possible outcomes. In the most optimistic case, the protection mechanisms manages to mask the impacts of the attack. The SMP will reach the mask compromised state M and be brought back to the good state G eventually. Generally, the system will return to the secure state immediately when the attack is masked. In contrast, the worst possibility is when the system protection mechanisms fail to recognize the attack. In this case, the SMP reaches the failure state F, in which a complete failure of the system occurs. Corresponding contingencies in the grid will arise until the system is restored. If the protection mechanisms of the SCADA system manage to recognize the attack actions while the attack cannot be masked, the SMP comes to the triage state R. The error recovery and fault treatment mechanisms of the system will be triggered in order to hedge the damage of the attack. The SMP will transit to the interrupted state I if the defensive strategies of the system are able to track and identify the route of the attack. Although the contingencies in the grid still occur, the SCADA system can be restored in a short time to eliminate the contingencies and the damage is reduced. Otherwise, the SMP will reach the failure state F, in which a longer time will be required to restore the control of the compromised devices and greater damage will be caused.

In the SMP model of the cyberattack process, the good state G and other intermediate states of the attack are transient states while the rest states are absorbing states [35]. Thus, the transient state space of the SMP model is defined as $\mathcal{S}_T = \{G, V, H, C, T, A, R\}$, and the absorbing state space is defined as $\mathcal{S}_A = \{M, I, F\}$. Accordingly, the Markov kernel of the absorbing SMP model which is denoted by Q_T in this study can be expressed as follows.

$$Q_T = \begin{bmatrix} p_G & p_V & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ p_{VG} & 0 & p_H & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ p_{HG} & 0 & 0 & p_C & 0 & 0 & 0 & 0 & 0 & 0 \\ p_{CG} & 0 & 0 & 0 & p_T & 0 & 0 & 0 & 0 & 0 \\ p_{TG} & 0 & 0 & 0 & 0 & p_A & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & p_R & p_M & 0 & p_{AF} \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & p_I & p_{RF} \end{bmatrix} \tag{1}$$

where p_{ij} $(i \in \mathcal{S}_T, j \in \mathcal{S}_T \cup \mathcal{S}_A)$ is the transition probability between the states in the absorbing SMP model with the following relation:

$$\sum_{j \in \mathcal{S}_T \cup \mathcal{S}_A} p_{ij} = 1, \quad \forall i \in \mathcal{S}_T \tag{2}$$

Then, the average number of times that transient state j is visited before any of the absorbing states is reached in the SMP model is denoted by υ_j and calculated as follows:

$$\upsilon_j = p_j + \sum_{i \in \mathcal{S}_T} \upsilon_i p_{ij}, \quad \forall j \in \mathcal{S}_T \tag{3}$$

where p_{ij} is the element of Q_T, and p_j is the probability that the SMP starts at state j. The attack process is assumed to always start from the good state, hence

$$p_j = \begin{cases} 1, & \text{if } j = G \\ 0, & \text{otherwise} \end{cases} \tag{4}$$

With (1)-(4), it can be derived that the number of times that the transient states in $\mathcal{S}_T$ are visited before the system fails can be calculated as follows.

$$\begin{aligned} &\upsilon_G = \frac{1}{p_V p_H p_C p_T p_A (1-p_M)},\ \upsilon_V = \frac{1}{p_H p_C p_T p_A (1-p_M)}, \\ &\upsilon_H = \frac{1}{p_C p_T p_A (1-p_M)},\ \upsilon_C = \frac{1}{p_T p_A (1-p_M)}, \\ &\upsilon_T = \frac{1}{p_A (1-p_M)},\ \upsilon_A = \frac{1}{1-p_M},\ \upsilon_R = \frac{p_R}{1-p_M} \end{aligned} \tag{5}$$

We denote the time for the system to reach state F or I by $\mathcal{T}$, which is the time for the system to be compromised. The mean value of $\mathcal{T}$ is known as the mean time-to-compromise (MTTC), which is a critical indicator and commonly used for

assessing the cybersecurity of a system [33]. The MTTC of successful cyberattacks can be calculated as follows.

$$MTTC = \overline{\mathcal{T}} = \sum_{j \in \mathcal{S}_T} \upsilon_j T_j = \frac{1}{1-p_M}\left[\frac{T_G}{p_V p_H p_C p_T p_A} + \frac{T_V}{p_H p_C p_T p_A} + \frac{T_H}{p_C p_T p_A} + \frac{T_C}{p_T p_A} + \frac{T_T}{p_A} + T_A + p_R T_R\right] \tag{6}$$

where T_j is the mean sojourn time of transient state j. It can be easily seen from (6) that the MTTC of the system increases with the increase of the sojourn time of the transient states, transition probabilities p_M and p_R, as well as the decrease of transition probabilities p_V to p_A. The stochastic characteristics of the cyberattacks and the reliability of the system under attacks are described and determined by the Markov kernel and sojourn time of the transient states in the absorbing SMP model. With the SMP model, the process of the cyberattacks against the power systems can be simulated efficiently.

B. Correlation Modeling of Cybersecurity Threats

Generally, the potential losses of the power systems due to cybersecurity threats are not independent. On the one hand, for the physically connected power grids, it is evident that the effect of the cyberattack on one power grid could be propagated to the connected power grids. Usually the neighboring connected power grids would sustain the largest impacts. On the other hand, even for power grids which are not physically connected with each other, they face the common (or interdependent) cyber risks. For example, a common vulnerability of the SCADA systems in the power grids may be discovered and exploited simultaneously due to the standardized software design, communication protocols and even antivirus solutions. Therefore, the cyber risks of the power systems are correlated. Investigating the correlation of the potential cyber risks is critical which is a major challenge in the actuarial study of cyber risk management. The correlation due to the physical connection of the grids can be investigated by the power system simulation. However, the correlation due to the common cyber risks cannot be captured merely by the power system analysis. To this end, a stochastic model is proposed to analyze the correlation due to the common cyber risks.

As a kind of widely deployed industrial control systems (ICS) that are highly integrated with the information systems and usually built to international standards [36], the SCADA systems in the grids face not only independent cyber risks but also common cyber risks [37] as mentioned above. Statistically, a SCADA system performs diversely in cybersecurity in the face of different risks. It has been illustrated in the previous subsection that the Markov kernel Q_T and the sojourn time T_j in the absorbing SMP model reflect the characteristics of the SCADA systems in cybersecurity under attacks. In order to generate a proper stochastic model for the performance of the SCADA systems considering both independent and common cyber risks, the Markov kernel and mean sojourn time in the absorbing SMP model are not set as constants but modeled by stochastic variables in this study. Consider the instance of the absorbing SMP model for the SCADA systems of an individual entity $\mathcal{N}$ (e.g., a transmission company (TRANSCO)) in the power system in a certain interval. The transition probabilities in the Markov kernel and the mean sojourn time of the transient states (denoted by $p_{ij}^{\mathcal{N}}$ and $T_i^{\mathcal{N}}$ respectively) are modeled as follows.

$$p_{ij}^{\mathcal{N}} = \hat{p}_{ij}^{\mathcal{N}} u + \hat{p}_{ij}\left(1-u\right),\ \forall i \in \mathcal{S}_T, \forall j \in \mathcal{S}_T \cup \mathcal{S}_A \tag{7}$$

$$T_i^{\mathcal{N}} = \hat{T}_i^{\mathcal{N}} u + \hat{T}_i\left(1-u\right),\ \forall i \in \mathcal{S}_T \tag{8}$$

where $\hat{p}_{ij}^{\mathcal{N}}$ and $\hat{p}_{ij}$ are stochastic variables which represent the transition probabilities in the Markov kernel of the absorbing SMP model under the independent and common cyber risks respectively; and $\hat{T}_i^{\mathcal{N}}$ and $\hat{T}_i$ are stochastic variables which represent the mean sojourn time of transient state i in the absorbing SMP model under the independent and common cyber risks, respectively.

Considering the stochastic variables for the transition probabilities in the Markov kernel of the SMP model, each instance of them must fall in the interval $[0, 1]$. In this study, it is assumed that $\hat{p}_{ij}^{\mathcal{N}}$ and $\hat{p}_{ij}$ follow the Beta distributions. Meanwhile, $\hat{T}_i^{\mathcal{N}}$ and $\hat{T}_i$ are assumed to follow the truncated Gaussian distributions. Negative instances are filtered to avoid unrealistic time span although such cases are rare. Further, constraint (2) should apply for each instance of the stochastic variables for the transition probabilities in the Markov kernel. In order to guarantee the satisfaction of such constraint for every instance of the proposed model, an exponential random variable approach based sampling process is applied. The sampling process is as follows. For simplicity, we denote the instances of both $\hat{p}_{ij}^{\mathcal{N}}$ and $\hat{p}_{ij}$ by p_{ij}. Suppose the expected value

$$\mathbb{E}\left[p_{ij}\right] = \frac{k_j}{K_i},\ \forall i \in \mathcal{S}_T, \forall j \in \mathcal{S}_T \cup \mathcal{S}_A \tag{9}$$

where k_j are positive integers and

$$K_i = \sum_{j \in \mathcal{S}_T \cup \mathcal{S}_A} k_j, \quad \forall i \in \mathcal{S}_T \tag{10}$$

In each sampling process of p_{ij}, K_i i.i.d. exponential distributed random variables with mean 1 are simulated. The i.i.d. exponential random variables are denoted by $y_1, \cdots, y_{K_i}$. Then p_{ij} can be sampled as follows.

$$p_{ij} = \frac{\sum_{\kappa=k_1+\cdots+k_{j-1}+1}^{k_1+\cdots+k_{j-1}+k_j} y_\kappa}{\sum_{\kappa=1}^{K_i} y_\kappa},\ \forall i \in \mathcal{S}_T, \forall j \in \mathcal{S}_T \cup \mathcal{S}_A \tag{11}$$

With the sampling process, stochastic variable p_{ij} follows the Beta distribution with the defined mean value as (9), while constraint (2) is satisfied. In (7) and (8), u is also a stochastic variable which follows a Bernoulli distribution, i.e., $u \sim \text{Bernoulli}(\varsigma)$, where ς is the mean value of the Bernoulli distribution which indicates the degree of cyber correlation in the model. If $\varsigma = 1$, it represents the case when the entities across the power system share no common cyber risks, and the absorbing SMP models are only affected by the independent cyber risks, which means a fully independent case of the cyber risks across the entire system. In contrast, when $\varsigma = 0$, it represents the case when the common cyber risks always exist across the grids, which means the strongest dependence of the cyber risks in the power system. When $\varsigma \in (0, 1)$, it represents an intermediate strength of dependence.

C. Loss Modeling of Power Systems with Cyberattacks

Based on the absorbing SMP and cyber correlation models described in the previous subsections, a sequential Monte Carlo simulation (MCS) framework is developed to study the

load curtailments and interruption cost of the grids considering the cybersecurity threats to the power system. The detailed procedure of the MCS is presented by the following steps.

1) Modeling of physical failures of components in the grids: The time-to-failure and time-to-repair of all the components including generation units and transmission lines are generated by sampling the probability distributions of the state residence time [38]. In this study, both the residence time of the components to stay in the fault and healthy states are assumed to be exponentially distributed. Thus, the residence time of any state j is simulated using a random variable τ with the exponential probability density function as follows:

$$f_{\tau_j}(t) = \lambda_j e^{-\lambda_j t} \tag{12}$$

where $1/\lambda_j$ is the mean residence time of state j. Accordingly, the random variable τ can be sampled as follows based on the inverse transform method.

$$\tau_j = -\frac{1}{\lambda_j}\ln(1-U) \tag{13}$$

where U is a uniformly distributed random variable in the interval $(0,1)$. Accordingly, the states of all the components in the grids considering the physical failures can be determined along the time throughout the simulation horizon.

2) Modeling of cyberattacks to the grids: Considering the correlation model of the cybersecurity threats in the power system, the corresponding parameters in the absorbing SMP model for the cyberattacks are simulated in this study. For every certain period, stochastic variable $u \sim \text{Bernoulli}(\varsigma)$ is simulated to model the possibility that the power system is under a common cyber risk and all the absorbing SMP models are affected. When the parameters of the absorbing SMP model for each node of the power system are determined, the states of the system can be simulated with the absorbing SMP model described in the previous subsection. We denote the instance of the Markov kernel of the absorbing SMP model for node n in the power system by Q_T^n and the transition probabilities in the kernel by p_{ij}^n $(i \in \mathcal{S}_T, j \in \mathcal{S}_T \cup \mathcal{S}_A)$. If the current state of the SCADA system is i, the probability that the next state of the system is j can be determined as follows:

$$p\{J_{\xi+1}^n = j \mid J_\xi^n = i\} = p_{ij}^n, \quad \forall i \in \mathcal{S}_T,\, j \in \mathcal{S}_T \cup \mathcal{S}_A \tag{14}$$

where J_ξ^n and $J_{\xi+1}^n$ are the states of the absorbing SMP model in the ξ^{th} and following steps, respectively. If the absorbing SMP model of any node in the system reaches the interrupted state I or the failure state F, corresponding contingencies will occur in the grid. In this study, it is assumed that all the breakers in the substation of the targeted node will be tripped if the attack is successful. The duration of the contingencies is then simulated according to the parameters of the time to restore the SCADA system, and the states of the system will be updated accordingly.

3) Modeling of system operations with states of components over time: With the simulated sequences of both the physical failures and successful cyberattacks, the states of all the components in the grids in every interval along the sampling time sequences are determined and updated. If any contingencies occur according to the updated states of the components, an optimal power flow (OPF) analysis is performed to evaluate the load curtailments during the contingencies by minimizing the load curtailment with the network constraints. The major steps of the proposed sequential MCS for the power system reliability evaluation considering the cyberattacks are illustrated by the flow diagram in Fig. 2.

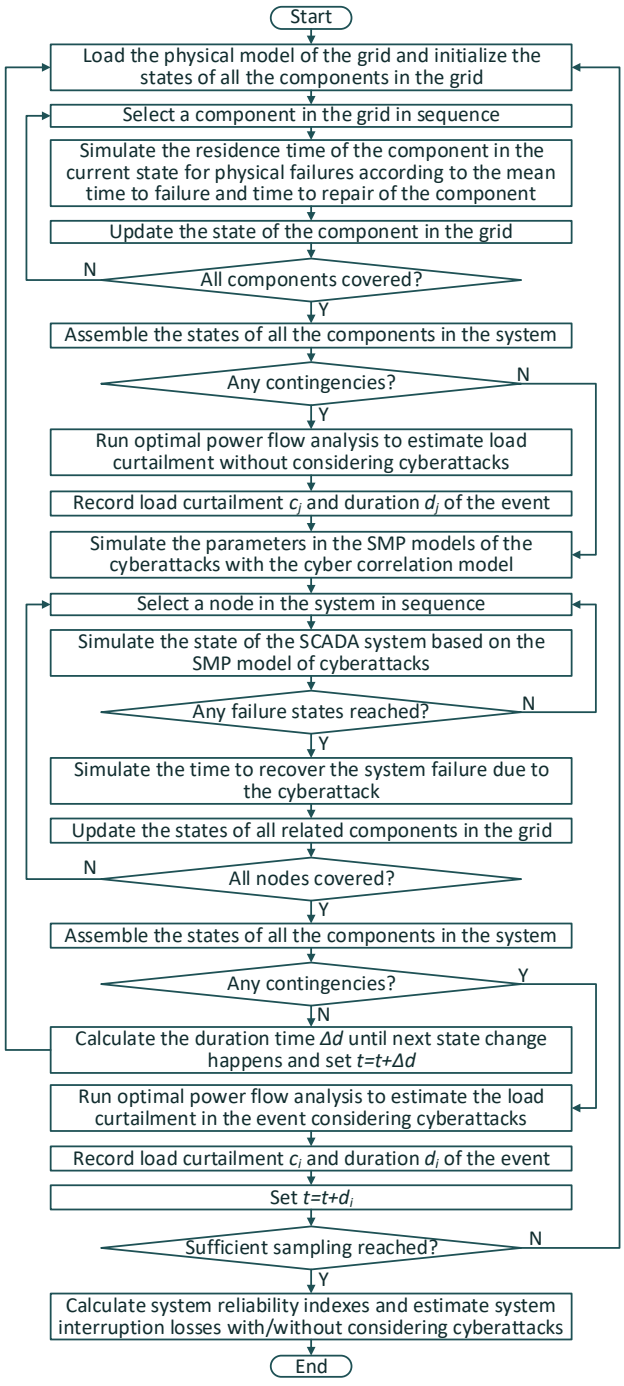


Fig. 2. Power Reliability Analysis Considering Cyberattacks and Cybersecurity Threat Correlation.

D. Monetary Loss Evaluation

Based on the results of the sequential MCS presented in the previous subsection, the load curtailment and duration of the load loss events considering the cyberattacks on the power system are obtained. Then, the monetary loss of the power system due to the cyberattacks is estimated by the annual interruption cost (AIC) in this study [38]. In order to estimate the

loss of the grid due to the cyberattacks precisely, the AIC of the grid only considering the interruptions due to the physical failures is subtracted from the AIC of the grid considering both the physical failures and potential cyberattacks. The loss of the grid due to the cyberattacks is denoted by X, and can be calculated as follows.

$$X = \sum_{i=1}^{N} c_i W(d_i) - \sum_{j=1}^{M} c_j W(d_j) \tag{15}$$

where X is a stochastic variable of the loss due to potential cyberattacks on the power system; c_i and d_i are the load curtailment and duration of load loss event i considering cyberattacks respectively; c_j and d_j are the load curtailment and duration of load loss event j without considering cyberattacks respectively; N and M are the total numbers of load loss events in the grid throughout a year with and without considering cyberattacks respectively. The stochastic characteristics of X can be studied through the proposed sequential MCS model to assess the risk of the power system considering the cybersecurity threats.

In this paper, the proposed insurance scheme focuses on the potential loss of the power system due to the cyberattacks on the substation SCADA systems in the grids, which will be presented in detail in the following section. Meanwhile, the proposed insurance scheme succeeds in avoiding free riding among the insureds and prompting them to enhance their self-protection against the cyberattacks, which will be shown by the results of the case study in Section V. The other impacts of the cyberattacks on power systems are not considered and discussed in this paper.

IV. Insurance Premium Principles

In traditional insurance practice, the expected value premium principle is commonly used. That is, the premium for a risk X is calculated as $\pi(X) = (1+\rho)E[X]$, where $\rho > 0$ is called safe loading coefficient. With appropriate choice of safe loading coefficient, the total premium collected by the insurer is guaranteed to be sufficient to cover the potential losses with high probability when the insurance pool is large.

It is worth noting that the rationale of expected value premium principle, as well as many other existing premium principles, is built upon the underlying assumption of independence between individual risks. This assumption, however, is violated in the context of cyber insurance, as cyber risks tend to be interdependent. Therefore, it is necessary to establish a new premium principle that takes interdependence into consideration.

Let $X_1, \ldots, X_n$ denote the potential losses from different TRANSCOs in an insurance portfolio. Denote the total loss by $TL = \sum_{i=1}^{n} X_i$. From the perspective of the insurer, the total premium needs to be sufficient to cover the potential claims with high probability. In order to meet this goal, the total premium can be set to be

$$TP_1 = VaR_\alpha(TL) = VaR_\alpha\left(\sum_{i=1}^{n} X_i\right) \tag{16}$$

where $VaR_\alpha(Y) = \inf\{y : P(Y > y) \leq \alpha\}$ is called *Value at Risk* (VaR) with $\alpha \in (0,1)$. With such a premium, the probability that the total loss TL would exceed the total premium TP is controlled at the level of α (which is usually set to be a small value), or mathematically $P(TL > TP_1) = \alpha$.

A more conservative choice is to calculate the total premium via *Tail Value at Risk* (TVaR), as defined below

$$TP_2 = TVaR_\alpha(TL) = \frac{1}{\alpha}\int_{1-\alpha}^{1} VaR_p(TL)\mathrm{d}p \tag{17}$$

This premium principle is more conservative in the sense that it is greater than the premium calculated by (16) at the same confidence level, and thus $P(TL > TP_2) < \alpha$.

Value at Risk and *Tail Value at Risk* are two risk measures commonly used in insurance and finance. Readers are referred to [39] for more detailed discussions on these risk measures.

After the total premium is determined, it is to be allocated across individual risks according to the individual riskiness. Below, two principles are proposed for the allocation of the total premium calculated by (16) and (17) respectively.

$$\pi_1(X_i) = E[X_i] + \frac{VaR_\alpha(X_i')}{\sum_{i=1}^{n} VaR_\alpha(X_i')} VaR_\alpha(TL') \tag{18}$$

$$\pi_2(X_i) = E[X_i] + \frac{TVaR_\alpha(X_i')}{\sum_{i=1}^{n} TVaR_\alpha(X_i')} TVaR_\alpha(TL') \tag{19}$$

where $X_i' = X_i - E[X_i]$ is the centralized version (with respect to the expected value) of risk X_i for all $i = 1, 2, \ldots, n$, and $TL' = \sum_{i=1}^{n}(X_i - E[X_i])$ represents the centralized total loss. The centralization of risks separates the impacts of location and variability on the individual premium and thus makes these two factors more tractable. It is easy to verify that

$$\sum_{i=1}^{n} \pi_1(X_i) = VaR_\alpha(TL) = TP_1 \tag{20}$$

$$\sum_{i=1}^{n} \pi_2(X_i) = TVaR_\alpha(TL) = TP_2 \tag{21}$$

This confirms that individual premium principles π_1 and π_2 are indeed allocations of the total premiums TP_1 and TP_2 respectively.

The key difference between the existing insurance programs and the proposed scheme in this paper lies in the consideration of interdependence among losses from different TRANSCOs. Most existing insurance programs charge premiums based on marginal characteristics of the individual TRANSCO but fail to consider the interdependence among losses from different TRANSCOs. This way, the insurance provider is exposed to insolvency risks. For example, due to the correlated cyber risks, the total premiums collected according to the traditional models would not be sufficient to pay the total claims for the interruptions in the grids. As a consequence, insurance providers would pose major limitations on losses to be covered or even quit this market. Either way, the well-being of the cyber insurance market will be jeopardized. The insurance model proposed in this paper factors independence into premium determination and thus reduces the insolvency risk for insurance providers. Consequently, more insurance providers would be willing to participate in this market, which further promotes the development of the cyber insurance market.

In practice, it is impossible for the insurer to examine all the possible cyberattack methods, and there are always particular cyberattack scenarios that are unknown to the insurer. In the real-world practice, the contracts between the insurer and insured may specify the characteristics of the cyberattack scenarios to determine the insurance coverage and claim scenarios, which is a common practice in the insurance industry.

Generally, the insurer is more interested in the cyber-attacks that induce losses/claims rather than all possible cyberattacks. The insureds are highly motivated to report such attacks to indemnify their losses. In this sense, the collection of data on the loss-inducing cyber-attacks is generally consistent with the purpose of insurance pricing. Even if there are undetected or unreported loss-inducing cyberattacks, the insurance algorithm allows self-correction over the long term. Further, the proposed actuarial design in this paper provides a robust solution against the insurer's insolvency risk. The proposed VaR and TVaR based design limits the risks of underestimation on the losses due to cyberattacks with the actuarial model. Meanwhile, in order to further reduce the risk due to unknown cyberattack scenarios, a safety margin can be applied on the parameters in the proposed model to guarantee that the losses due to successful cyberattacks can be covered even if there is a more serious cybersecurity condition in reality.

V. Case Study and Discussion

A. Test System Model and Power System Simulation

In order to illustrate the proposed insurance framework for the power systems to handle the risk of cyberattacks, a case study is performed based on a test system which consists of two independent IEEE Reliability Test Systems (RTS-79) [40]. The single line diagram of the test system in the case study is shown in Fig. 3.

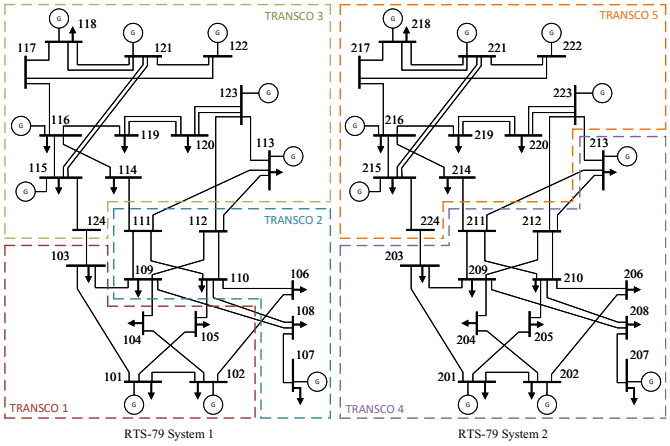


Fig. 3. Test System with Two Independent IEEE (RTS-79) Reliability Test Systems.

In the case study, five individual TRANSCOs are assumed in the grids. TRANSCOs 1-3 are located in the first IEEE RTS-79 system, and TRANSCOs 4 and 5 are located in the second IEEE RTS-79 system. The two systems are not physically interconnected. The load points at the nodes of the five TRANSCOs are listed in Table I.

TABLE I
Load Buses of TRANSCOs

	TRANSCO No.	Load Bus No.
RTS-79 System 1:	TRANSCO 1	101,102,103,104,105
	TRANSCO 2	106,107,108,109,110
	TRANSCO 3	113,114,115,116,118,119,120
RTS-79 System 2:	TRANSCO 4	201-210, 213
	TRANSCO 5	214,215,216,218,219,220

In the case study, a typical ICT configuration of the substation SCADA systems is considered as demonstrated in Fig. 4. The local area network (LAN) in the substation SCADA system is built based on the Ethernet protocol. The substation SCADA system connects to the external network through the firewall and router. In the site of the substation, the intelligent electronic devices (IEDs) including the protection relays, control and measurement units are connected to the devices in the physical layer including the circuit breakers, switches, current transformers (CTs) and potential transformers (PTs) in each bay/feeder of the substation to enable the control and monitoring. All the circuit breakers in the substation are connected to and controlled by the control units through independent auxiliary relays with adequate contact capacity. The control units communicate with and receive commands from the workstations and application servers on the station level through the Ethernet in the substation. This study focuses on the malicious attacks on the substation operation with false tripping commands of the circuit breakers by the attacker, and it is assumed that the circuit breakers in the substation will be tripped if the attackers successfully compromise the control units. The attacks are not dependent on the measurements in the substation, and thus the configuration of the CTs, PTs and corresponding A/D converters to the IEDs is not specified in this study.

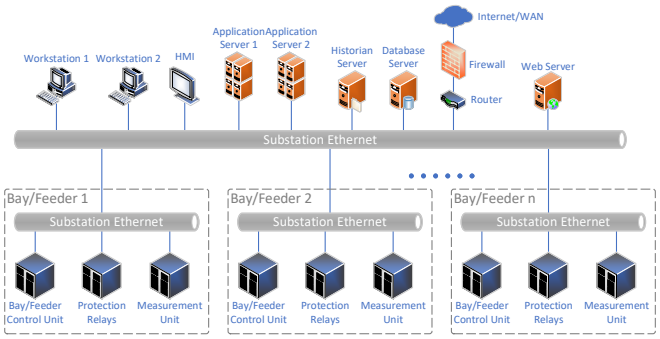


Fig. 4. ICT Configuration of Substation SCADA System.

Based on the proposed absorbing SMP based cyberattack model, the sequential MCS is performed to estimate the interruptions considering the consequences of the cyberattacks. In the case study, the customer damage function $W(d_i)$ is assumed to be fractional to the duration d_i. Hence, the losses due to the cyberattacks are calculated as follows.

$$X = \sum_{i=1}^{N} c_i W(d_i) - \sum_{j=1}^{M} c_j W(d_j) = \sum_{i=1}^{N} c_i \eta d_i - \sum_{j=1}^{M} c_j \eta d_j \tag{22}$$

where η is the fractional coefficient and assumed to be $2.5\text{k\$/MWh}$ in this case study. For the sequential MCS, an hourly time sequence of 2,000 years is sampled, and the system reliability evaluation considering the cyberattacks is performed. The mean values of the parameters in the absorbing SMP model are listed in Table II. Three cases with $\varsigma = 0, \varsigma = 0.5$ and $\varsigma = 1$ are studied, representing different strengths of dependence, with $\varsigma = 0.5$ being the base case.

The expected values, standard deviations and coefficients of variation (CoV) of the annual loss of the TRANSCOs in different cases are listed in Table III. Table III shows that the marginal loss for each TRANSCO under the three different dependence scenarios are similar, as confirmed by Fig. 5. This is expected from the design of the model, because what varies

TABLE II
PARAMETERS OF ABSORBING SMP MODEL

Par.	Val.	Par.	Val.	Par.	Val.	Par.	Val.
p_V	1	p_A	0.5	p_{AF}	0.2	T_H	1 day
p_H	0.5	p_R	0.5	p_{RF}	0.6	T_C	1 day
p_C	0.5	p_M	0.3	T_G	20 days	T_T, T_A	1 day
p_T	0.5	p_I	0.4	T_V	1 day	T_R	1 hour

across the three cases is the dependence strength, while there is little change to marginal characteristics. The intent of the model is to demonstrate that dependence structure can impose significant impact on insurance premiums without changing marginal settings. The coefficients of variation measure the relative variability and the riskiness of marginal losses from the five TRANSCOs. These coefficients all fall into the interval $(1, 1.5)$, which are typical values in traditional insurance practice.

TABLE III
EXPECTED VALUES, STANDARD DEVIATION AND COEFFICIENT OF VARIATION OF LOSS OF TRANSCOS

$\varsigma = 0$	**TC1**	**TC2**	**TC3**	**TC4**	**TC5**
Expected Value (k$)	3307	5037	9443	9914	7815
Standard Deviation (k$)	4137	6320	11494	11303	9590
Coefficient of Variation	1.25	1.25	1.22	1.14	1.23
$\varsigma = 0.5$	**TC1**	**TC2**	**TC3**	**TC4**	**TC5**
Expected Value (k$)	3430	5150	9352	10404	7786
Standard Deviation (k$)	4714	6711	11138	12644	10245
Coefficient of Variation	1.37	1.30	1.19	1.22	1.32
$\varsigma = 1$	**TC1**	**TC2**	**TC3**	**TC4**	**TC5**
Expected Value (k$)	3249	4947	9378	10089	7654
Standard Deviation (k$)	3874	6208	11223	14467	9384
Coefficient of Variation	1.19	1.26	1.20	1.43	1.23

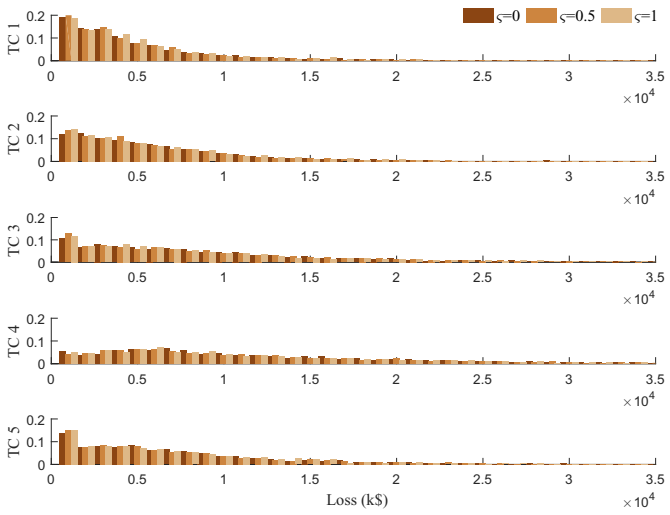


Fig. 5. Marginal Distributions of Losses of TRANSCOs.

The correlation matrices for the losses of the TRANSCOs when $\varsigma = 0$, 0.5 and 1 are summarized in Table IV respectively. Table IV clearly demonstrates that ς is an index of strength of dependence. Specifically, $\varsigma = 0$ represents the strongest dependence, and $\varsigma = 1$ represents the weakest dependence. The case when $\varsigma = 1$ corresponds to the independent case of cyber threats across the system. In this case, the correlation between all the TRANSCOs is low as expected. Generally, the results show that the proposed cyber correlation model properly reflects the dependency of the potential cyber risks across the power systems.

TABLE IV
CORRELATION MATRICES OF LOSSES OF TRANSCOS

		TC1	**TC2**	**TC3**	**TC4**	**TC5**
$\varsigma = 0$	**TC**	1.00	0.79	0.83	0.84	0.81
	TC2	0.79	1.00	0.85	0.85	0.82
	TC3	0.83	0.85	1.00	0.88	0.86
	TC4	0.84	0.85	0.88	1.00	0.85
	TC5	0.81	0.82	0.86	0.85	1.00
$\varsigma = 0.5$	**TC1**	1.00	0.40	0.47	0.49	0.42
	TC2	0.40	1.00	0.45	0.44	0.46
	TC3	0.47	0.45	1.00	0.50	0.52
	TC4	0.49	0.44	0.50	1.00	0.49
	TC5	0.42	0.46	0.52	0.49	1.00
$\varsigma = 1$	**TC1**	1.00	0.00	-0.02	-0.01	0.01
	TC2	0.00	1.00	0.03	-0.04	-0.01
	TC3	-0.02	0.03	1.00	0.00	-0.01
	TC4	-0.01	-0.04	0.00	1.00	-0.02
	TC5	0.01	-0.01	-0.01	-0.02	1.00

B. Premium Calculation and Analysis

The individual premiums for the five TRANSCOs calculated based on the VaR and TVaR principles, i.e. under formulas (18) and (19), are summarized in Table V. Throughout this section, the confidence level is set to be $\alpha = 0.1$. That means, there is only 10% chance that the total loss would exceed the total premium calculated under (16), and the chance becomes smaller than 10% if the total premium is calculated by (17). In this sense, the insurer's riskiness is controlled at a relatively low level. The individual premiums based on VaR (π_1) and TVaR (π_2) for different TRANSCOs roughly exhibit similar behaviors but the TVaR premiums are higher, simply because the TVaR premium principle is more conservative.

The risk loading coefficients are calculated by

$$\rho_i = \pi(X_i)/E[X_i] - 1 \qquad \text{for all } i = 1, 2, \ldots, n. \tag{23}$$

Intuitively, the risk loading coefficient measures by how much the individual premium exceeds the expected value of the corresponding risk. They play the same role as the safe loading coefficient in the expected value premium principle, but appear to be significantly larger than those in traditional insurance practice (which are below 50%). The large values of risk loading coefficients in the cases $\varsigma = 0$ and $\varsigma = 0.5$ are mainly caused by the high degree of interdependence among the losses from different TRANSCOs, as evidenced in Table IV. It is worth noting that, under the independence scenario ($\varsigma = 1$), the safe loading coefficients are the lowest among three dependence scenarios but still significantly higher than the desirable level. This is because the size of the pool (five) is too small for the law of large number to take effect. As the size of the pool increases, it is anticipated that the safe loading coefficients would reach the desirable level. TVaR premiums exhibit a similar behavior to VaR premiums and is only more conservative. In the following only VaR premiums will be calculated.

As presented in Table V, premiums and thus risk loading coefficients are significantly high, which may discourage TRANSCOs to participate in insurance. This is essentially due

TABLE V
INDIVIDUAL PREMIUMS BASED ON VAR AND TVAR PRINCIPLES

$\varsigma = 0$	**TC1**	**TC2**	**TC3**	**TC4**	**TC5**
VaR-premium (π_1)	7357	10524	19308	20806	16795
Risk loading	1.22	1.09	1.04	1.10	1.15
TVaR-premium (π_2)	11902	17683	32463	32961	27297
Risk loading	2.60	2.51	2.44	2.32	2.49
$\varsigma = 0.5$	**TC1**	**TC2**	**TC3**	**TC4**	**TC5**
VaR-premium (π_1)	6442	9388	17153	19025	14808
Risk loading	0.88	0.82	0.83	0.83	0.90
TVaR-premium (π_2)	10799	15703	26544	30160	23508
Risk loading	2.15	2.05	1.84	1.90	2.02
$\varsigma = 1$	**TC1**	**TC2**	**TC3**	**TC4**	**TC5**
VaR-premium (π_1)	5359	8336	15647	15765	12290
Risk loading	0.65	0.69	0.67	0.56	0.61
TVaR-premium (π_2)	7366	11363	21636	23876	17362
Risk loading	1.27	1.30	1.31	1.37	1.27

to interdependence of risks among different TRANSCOs. Such a spatial dependence is difficult to dilute because of the physical structures and cyber characteristics of the power grids. On the other hand, the losses within different time intervals are considered independent. Such temporal independence provides a solution to diversify the riskiness in the power grids across time.

In order to illustrate this temporal diversification effect, a five year period is considered and loss data for the five TRANSCOs in the case $\varsigma = 0.5$ are resampled using bootstrap method to deliver a joint distribution for the five-year losses of different TRANSCOs. Annual premiums are calculated for each TRANSCO based on the five-year data set. The results are summarized in Table VI. A comparison between Table VI and Table V demonstrates that the premiums and risk loading coefficients are reduced by considerable amounts, due to the temporal diversification effect. As a matter of fact, this diversification effect can be further amplified if a longer (than 5 years) period is considered. However, that would bring challenges in practice, as it is not common for either insurer or insured to enter into an insurance contract lasting for years. More studies need to be conducted to address this issue in the future research.

TABLE VI
ANNUAL INDIVIDUAL PREMIUMS BASED ON 5-YEAR DATA: $\varsigma = 0.5$

	TC1	**TC2**	**TC3**	**TC4**	**TC5**
VaR-premium (π_1)	4770	7782	13703	14868	12679
Risk loading	0.48	0.50	0.47	0.47	0.51

C. Impacts of System Cybersecurity Level

In order to study the impact of the system cybersecurity level on the insurance premiums, three comparative scenarios with respective to the base case $\varsigma = 0.5$ are designed and compared. The cybersecurity level of the systems under attacks are reflected by the parameters in the SMP model. In Scenario 1, it is assumed that the cybersecurity of TRANSCO 1 is weakened. In this scenario, for TRANSCO 1, T_G in the absorbing SMP model is reduced from 20 days in the base case to 15 days, and p_H, p_C, p_T and p_A are increased from 0.5 to 0.6, which means it takes shorter time for the SCADA systems of TRANSCO 1 to become vulnerable and has higher possibilities to be compromised by the attempts of malicious attacks. In Scenario 2, it is assumed that the cybersecurity of TRANSCO 1 is enhanced. In this scenario, for TRANSCO 1, T_G is increased to 25 days, and p_H, p_C, p_T and p_A are reduced to 0.4, which means it takes longer time for the SCADA systems in TRANSCO 1 to become vulnerable and has lower possibilities to be compromised by the attempts of malicious attacks. In Scenario 3, it is assumed that there is a global increase of cyber threats and the cybersecurity of all the TRANSCOs are weakened. In this scenario, T_G is reduced to 15 days, and p_H, p_C, p_T and p_A are increased to 0.6 for all the TRANSCOs.

Table VII summarizes the expected values of losses and premiums to be charged under three comparative scenarios, as well as the base case for the convenience of comparison. When the reliability of TRANSCO 1 in cybersecurity is weakened, the premium for TRANSCO 1 increases from 6,442 to 10,962, with an increment of 4,520. This amount is even larger than 3,426, the amount of increase in the total premium for all five TRANSCOs. This means that the premiums for the other four TRANSCOs are actually reduced due to the reliability degradation of TRANSCO 1. In this sense, TRANSCO 1 is penalized for its degradation not only by a marginal increase in premium but also by attracting premium burdens from other TRANSCOs who maintain their self cybersecurity levels. Such a double penalty algorithm introduced by the proposed premium principle provides a strong incentive for individual TRANSCOs to invest on self-protection in cybersecurity.

On the contrary, if TRANSCO 1 enhances its reliability, its premium drops significantly, as expected. On the other hand, the premiums for the other four TRANSCOs all experience slight increases. This implies that the enhancement of TRANSCO 1 benefits only itself. There is no free riding. Therefore, under the proposed premium principle, every TRANSCO is motivated to invest on their own self-protections.

An additional comparative case is analyzed here to further illustrate the impact of self-protections with the proposed insurance scheme. Suppose TRANSCO 1 invests and installs a new intrusion detection system (IDS) in the IEDs of the substations to increase the probability to detect and filter the intrusions and false commands at the IEDs from 0.5 in the base case to 0.6, which is represented by the transition probability $p_{TG} = 1 - p_A$ in the SMP model. A case study is performed with the new transition probability. In this case, the VaR premium π_1 and TVaR premium π_2 for TRANSCO 1 with the updated transition probability drop by 12% and 16% respectively compared to the base case. Both the proposed VaR and TVaR premiums manage to reflect the change of the cybersecurity level and can serve as an incentive for the TRANSCOs to enhance their self-protections.

Finally, if the reliability of all TRANSCOs considering cybersecurity is weakened, every TRANSCO experiences an increase in both the expected value of the loss and the premium. More importantly, premiums increase faster than the expected values, as seen from the increases of the loading coefficients. This implies that the increase of riskiness due to the weakening of reliability is nonlinear. The increase will accelerate if the weakening of system reliability considering cybersecurity continues. In this sense, the proposed premium principle confirms that the reliability of the power systems considering cybersecurity should be planned and managed at not only the individual TRANSCO level but also the global network level.

TABLE VII
IMPACT OF SELF PROTECTION

Base Case	**TC1**	**TC2**	**TC3**	**TC4**	**TC5**
Expected value	3430	5150	9352	10404	7786
VaR-premium (π_1)	6642	9388	17153	19025	14808
Risk loading	0.88	0.82	0.83	0.83	0.90
TC1 Weakened	**TC1**	**TC2**	**TC3**	**TC4**	**TC5**
Expected value	6075	5145	9489	10492	8052
VaR-premium (π_1)	10962	9509	16742	18559	14469
TC1 Enhanced	**TC1**	**TC2**	**TC3**	**TC4**	**TC5**
Expected value	2307	5144	9693	10315	7893
VaR-premium (π_1)	4839	9941	17893	18733	15236
All Weakened	**TC1**	**TC2**	**TC3**	**TC4**	**TC5**
Expected value	5948	8966	16980	17693	13921
VaR-premium (π_1)	11786	18471	34039	35021	28191
Risk loading	0.98	1.06	1.00	0.98	1.03

D. Sensitivity Analysis

In general, the input parameters of the proposed model need to be estimated based on the statistics of the considered cyber-attacks. However, available data from the real-world operation of the power grids is limited at present. As an alternative, such statistical data can be collected from the intrusion experiments or honeypots data. The transition probability in the SMP model represents the conditional probability of the occurrence of the system vulnerabilities or a successful step in a malicious attempt of cyberattacks under different conditions of the cyber system. Such conditional probability can be estimated and quantified through the intrusion experiments [41]. Meanwhile, these stochastic characteristics of the cyberattack processes can be mapped using the honeypot captured data statistically [42]. If empirical data is available with adequate records in the future smart grid, the stochastic characteristics of the cyberattack processes can also be evaluated based on the empirical data similarly. Further, considering the generality of the cyberattack mechanisms on the cyber systems, such statistical data can also be obtained from the general cybersecurity data sets to further broaden the data sources. Long-term databases have been built and maintained to keep track of and analyze various types of cyberattacks and cyber system vulnerabilities, e.g., the National Vulnerability Database (NVD) by the National Institute of Standards and Technology (NIST) [43], the PRC database by the Privacy Rights Clearinghouse [44], and the Zero Day Initiative (ZDI) program by the TippingPoint [45].

In order to study the impacts of the parameters on the results of the proposed model, a sensitivity analysis is performed. The sensitivity of the proposed insurance premiums to the transition probabilities in the SMP model is evaluated with the sensitivity coefficients. The normalized sensitivity coefficients are calculated by (24) and (25) as follows.

$$s_1(p_{ij}) = \frac{\partial \pi_1(p_{ij})/\partial p_{ij}}{\pi_1}, \ \forall i \in \mathcal{S}_T, \forall j \in \mathcal{S}_T \cup \mathcal{S}_A \quad (24)$$

$$s_2(p_{ij}) = \frac{\partial \pi_2(p_{ij})/\partial p_{ij}}{\pi_2}, \ \forall i \in \mathcal{S}_T, \forall j \in \mathcal{S}_T \cup \mathcal{S}_A \quad (25)$$

where s_1 and s_2 are the normalized sensitivity coefficients of the VaR- and TVaR-based premiums π_1 and π_2 to the transition probability in the absorbing SMP model, respectively. The premiums of TRANSCO 1 in the result of the sensitivity analysis are shown and discussed as an example. Fig. 6 shows the absolute values of s_1 and s_2 in the sensitivity analysis. As shown in the figure, the sensitivity coefficients of all the transition probabilities are at a moderate level without any extremely sensitive parameters. Specifically, transition probability p_T has relatively higher impact on the VaR-based premium, while p_V, p_T and p_R have greater impact on the TVaR-based premium in the absorbing SMP model. The highest values of both normalized sensitivity coefficients s_1 and s_2 are about 2, which means the VaR- and TVaR-based premiums π_1 and π_2 will change by about 2% if the value of the probability changes by 0.01. In practice, the insurance providers can set a safety margin for the relatively sensitive transition probabilities (e.g., p_T) in the SMP model to further guarantee their financial security.

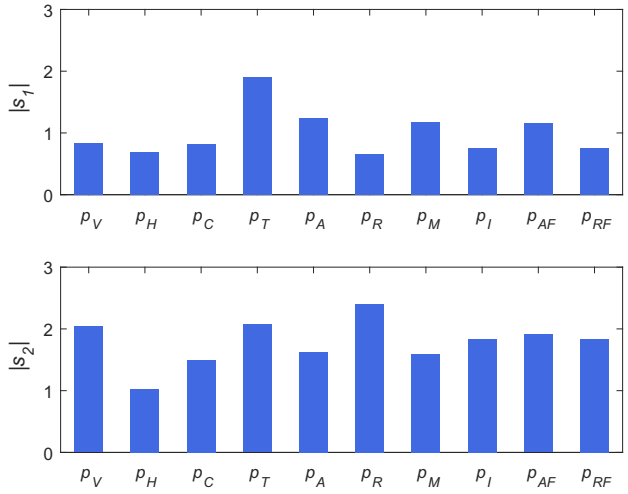


Fig. 6. Normalized Sensitivity Coefficients of Transition Probability in SMP Model.

VI. CONCLUSION

In this paper, an absorbing SMP and correlation model for cyber risks is proposed to model the cyberattacks against the power systems. Based on the cybersecurity threat model, a sequential MCS framework is developed to evaluate the loss for the system interruptions considering malicious cyberattacks on the power grids. An actuarial framework has been developed to price and manage the cyber-related risks for the power systems. Several new premium principles are introduced to take interdependence among risks into consideration and substantially control the insolvency risk from the perspective of insurance providers. Using these premium principles, individual premiums are calculated in a case study. The individual premiums turn out to be significantly high compared to the traditional insurance framework; which, on the one hand, demonstrates the riskiness raised by interdependence, and on the other hand, makes the insurance product unacceptable to the insured parties. The temporal diversification technique is further introduced to dilute the risk concentration caused by interdependence and therefore lower individual premiums. Under the proposed premium principle, the impact of self protection in cybersecurity proves to be significant, which is expected to incentivize investment in cybersecurity technologies. The presented actuarial framework is anticipated to enhance the participation rate from the perspectives of both insurers and insured parties and thus promote a healthy, sustainable cyber-insurance market for the electric power sector.

REFERENCES

[1] North American Electric Reliability Corporation (NERC), "High-Impact, Low-Frequency Event Risk to the North American Bulk Power System," NERC and U.S. Department of Energy (DOE), Atlanta, GA, Tech. Rep., June 2010.

[2] MIT Technology Review, "Industrial control systems are still vulnerable to malicious cyberattacks," January 2019. [Online]. Available: https://www.technologyreview.com/s/612829/industrial-control-systems-are-still-vulnerable-to-malicious-cyberattacks/

[3] North American Electric Reliability Corporation (NERC), "State of Reliability 2017," NERC, Atlanta, GA, Tech. Rep., June 2017.

[4] N. Kshetri and J. Voas, "Hacking Power Grids: A Current Problem," *Computer*, vol. 50, no. 12, pp. 91–95, 2017.

[5] D. E. Whitehead, K. Owens, D. Gammel, and J. Smith, "Ukraine Cyber-Induced Power Outage: Analysis and Practical Mitigation Strategies," in *Proc. 70th Annual Conference for Protective Relay Engineers (CPRE)*. College Station, TX: IEEE, 2017, pp. 1–8.

[6] A. Marotta, F. Martinelli, S. Nanni, A. Orlando, and A. Yautsiukhin, "Cyber-insurance survey," *Computer Science Review*, vol. 24, pp. 35–61, 2017.

[7] L. A. Gordon, M. P. Loeb, and T. Sohail, "A framework for using insurance for cyber-risk management," *Communications of the ACM*, vol. 46, no. 3, pp. 81–85, 2003.

[8] D. Young, J. Lopez, M. Rice, B. Ramsey, and R. McTasney, "A framework for incorporating insurance in critical infrastructure cyber risk strategies," *International Journal of Critical Infrastructure Protection*, vol. 14, pp. 43–57, 2016.

[9] I. Vakilinia and S. Sengupta, "A Coalitional Cyber-Insurance Framework for a Common Platform," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 6, pp. 1526–1538, 2018.

[10] H. Ogut, N. Menon, and S. Raghunathan, "Cyber insurance and it security investment: Impact of interdependent risk," in *Proc. Workshop on the Economics of Information Security (WEIS)*, Cambridge, MA, 2005, pp. 1–30.

[11] C. Barracchini and M. E. Addessi, "Cyber Risk and Insurance Coverage: An Actuarial Multistate Approach," *Review of Economics & Finance Submitted*, vol. 4, pp. 57–69, 2014.

[12] R. Böhme and G. Schwartz, "Modeling Cyber-Insurance : Towards A Unifying Framework," in *Proc. Workshop on the Economics of Information Security (WEIS)*, Cambridge, MA, 2010, pp. 1–36.

[13] C. Biener, M. Eling, and J. H. Wirfs, "Insurability of cyber risk," *Newsletter on Insurance and Finance*, vol. 14, pp. 1–4, 2014.

[14] J. Grossklags, S. Radosavac, A. A. Cardenas, and J. Chuang, "Nudge: Intermediaries role in interdependent network security," in *Proc. 3rd International Conference on Trust and Trustworthy Computing*, 2010, pp. 323–336.

[15] S. Radosavac, J. Kempf, and U. C. Kozat, "Using insurance to increase internet security," in *Proc. 3rd International Workshop on Economics of Networked Systems*. ACM, 2008, pp. 43–48.

[16] L. M. D. Baileya, "Mitigating Moral Hazard in Cyber-Risk Insurance," *Journal of Law & Cyber Warfare*, vol. 3, no. 1, pp. 1–42, 2014.

[17] H. Yang, J. Qiu, K. Meng, J. Zhao, Z. Dong, and M. Lai, "Insurance strategy for mitigating power system operational risk introduced by wind power forecasting uncertainty," *Renewable Energy*, vol. 89, pp. 606–615, 2016.

[18] E. Fumagalli, J. W. Black, I. Vogelsang, and M. Ilic, "Quality of service provision in electric power distribution systems through reliability insurance," *IEEE Transactions on Power Systems*, vol. 19, no. 3, pp. 1286–1293, 2004.

[19] R. Smith, "U.S. Risks National Blackout From Small-Scale Attack," Mar. 2014. [Online]. Available: http://online.wsj.com/news/articles/SB10001424052702304020104579433670284061220/

[20] C. W. Ten, A. Ginter, and R. Bulbul, "Cyber-Based Contingency Analysis," *IEEE Transactions on Power Systems*, vol. 31, no. 4, pp. 3040–3050, 2016.

[21] C. W. Ten, K. Yamashita, Z. Yang, A. V. Vasilakos, and A. Ginter, "Impact Assessment of Hypothesized Cyberattacks on Interconnected Bulk Power Systems," *IEEE Transactions on Smart Grid*, vol. 9, no. 5, pp. 4405–4425, 2018.

[22] Z. Yang, C. W. Ten, and A. Ginter, "Extended Enumeration of Hypothesized Substations Outages Incorporating Overload Implication," *IEEE Transactions on Smart Grid*, vol. 9, no. 6, pp. 6929–6938, 2018.

[23] L. Che, X. Liu, T. Ding, and Z. Li, "Revealing Impacts of Cyber Attacks on Power Grids Vulnerability to Cascading Failures," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 66, no. 6, pp. 1058–1062, 2019.

[24] National Protection and Programs Directorate (NPPD), "Insurance for cyber-related critical infrastructure loss: Key issues," Department of Homeland Security (DHS), Washington, DC, Tech. Rep., July 2014.

[25] G. Gluschke and M. H. Caşin, *Cyber Security Policies and Critical Infrastructure Protection*, M. Macori, Ed. Potsdam, Germany: Institute for Security and Safety (ISS) Press, 2018.

[26] P. Hoffman and W. Bryan, "Insurance as a Risk Management Instrument for Energy Infrastructure Security and Resilience," U.S. Department of Energy (DOE), Washington, DC, Tech. Rep., March 2013.

[27] D. Shi, R. J. Elliott, and T. Chen, "On Finite-State Stochastic Modeling and Secure Estimation of Cyber-Physical Systems," *IEEE Transactions on Automatic Control*, vol. 62, no. 1, pp. 65–80, 2017.

[28] A. Ramos, M. Lazar, R. H. Filho, and J. J. P. C. Rodrigues, "Model-Based Quantitative Network Security Metrics: A Survey," *IEEE Communications Surveys and Tutorials*, vol. 19, no. 4, pp. 2704–2734, 2017.

[29] R. Gore, J. Padilla, and S. Diallo, "Markov Chain Modeling of Cyber Threats," *Journal of Defense Modeling and Simulation*, vol. 14, no. 3, pp. 233–244, 2017.

[30] J. Almasizadeh and M. A. Azgomi, "A stochastic model of attack process for the evaluation of security metrics," *Computer Networks*, vol. 57, no. 10, pp. 2159–2180, 2013.

[31] X. Li, T. P. Parker, and S. Xu, "A Stochastic Model for Quantitative Security Analyses of Networked Systems," *IEEE Transactions on Dependable and Secure Computing*, vol. 8, no. 1, pp. 28–43, 2011.

[32] R. E. Carlson, M. A. Turnquist, and L. K. Nozick, "Expected Losses, Insurability, and Benefits from Reducing Vulnerability to Attacks," Sandia National Laboratories and Cornell University, Albuquerque, NM, Tech. Rep., 2004.

[33] 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," *Performance Evaluation*, vol. 56, no. 1-4, pp. 167–186, 2004.

[34] Y. Zhang, L. Wang, Y. Xiang, and C. Ten, "Inclusion of SCADA Cyber Vulnerability in Power System Reliability Assessment Considering Optimal Resources Allocation," *IEEE Transactions on Power Systems*, vol. 31, no. 6, pp. 4379–4394, 2016.

[35] K. S. Trivedi, *Probability and Statistics with Reliability, Queuing, and Computer Science Applications*. Hoboken, NJ: WILEY, 2001.

[36] K. Stouffer, V. Pillitteri, S. Lightman, M. Abrams, and A. Hahn, "Guide to Industrial Control Systems (ICS) Security," *NIST Special Publication 800-82*, pp. 1–68, 2015.

[37] W. Shim, "Interdependent risk and cyber security: An analysis of security investment and cyber insurance," Ph.D. Dissertation, Michigan State University, East Lansing, MI, 2010.

[38] R. Billinton and R. N. Allan, *Reliability Evaluation of Power Systems*. New York, NY: Plenum Press, 1996.

[39] S. A. Klugman, H. H. Panjer, and G. E. Willmot, *Loss Models: From Data to Decisions*. John Wiley & Sons, 2012.

[40] Probability Methods Subcommittee, "IEEE Reliability Test System," *IEEE Transactions on Power Apparatus and Systems*, vol. PAS-98, no. 6, pp. 2047–2054, 1979.

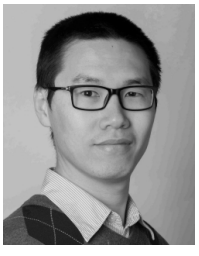
[41] M. Sahinoglu, "An Input–Output Measurable Design for the Security Meter Model to Quantify and Manage Software Security Risk," *IEEE Transactions on Instrumentation and Measurement*, vol. 57, no. 6, pp. 1251–1260, 2008.

[42] Z. Zhan, M. Xu, and S. Xu, "Characterizing Honeypot-Captured Cyber Attacks: Statistical Framework and Case Study," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 11, pp. 1775–1789, 2013.

[43] Information Technology Laboratory, National Institute of Standards and Technology (NIST), "National vulnerability database," 2020. [Online]. Available: https://nvd.nist.gov/

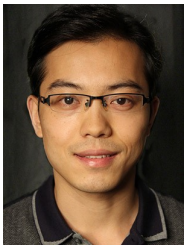
[44] M. Xu, K. M. Schweitzer, R. M. Bateman, and S. Xu, "Modeling and Predicting Cyber Hacking Breaches," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 11, pp. 2856–2871, 2018.

[45] TippingPoint, "Zero day initiative," 2020. [Online]. Available: https://www.zerodayinitiative.com/



Zhaoxi Liu (M'17) 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 operation, integration of distributed energy resources in power systems, power system security and resiliency.

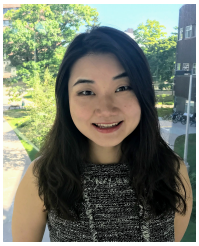


Wei Wei is an associate professor in Actuarial Science at the University of Wisconsin-Milwaukee. He joined UWM in 2013 after receiving his Ph.D. in Actuarial Science at the University of Waterloo (Canada). His research interests mainly lie in the areas of actuarial science and quantitative risk management, 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 (S'02-M'09-SM'18) 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.

Dr. Wang is an Editor of the IEEE TRANSACTIONS ON SMART GRID, IEEE TRANSACTIONS ON POWER SYSTEMS, and IEEE POWER ENGINEERING LETTERS, and served on the Steering Committee of the IEEE TRANSACTIONS ON CLOUD COMPUTING. He is a recipient of the Outstanding Faculty Research Award of College of Engineering and Applied Science at UWM in 2018.

Chee-Wooi Ten (SM'11) is an Associate Professor of Electrical and Computer Engineering at Michigan Technological University. He received the B.S.E.E. and M.S.E.E. degrees from Iowa State University, Ames, in 1999 and 2001, respectively. He received the Ph.D. degree in 2009 from University College Dublin (UCD), National University of Ireland prior joining Michigan Tech in 2010. Dr. Ten was a Power Application Engineer working in project development for EMS/DMS with Siemens Energy Management and Information System (SEMIS) in 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. Dr. Ten is currently serving as an Editor for IEEE TRANSACTIONS ON SMART GRID and ELSEVIER JOURNAL SUSTAINABLE ENERGY, GRIDS, AND NETWORKS (SEGAN).



Yeonwoo Rho received her B.S. degree in Mathematics and B.A. degree in Economics from Seoul National University, Korea, in 2006. She later received the M.S. degree in Statistics from Seoul National University in 2009, and the Ph.D degree in Statistics from University of Illinois at Urbana-Champaign in 2014. She is currently an Associate Professor of Statistics in the Department of Mathematical Sciences at Michigan Technological University. Her primary research interest is in time series analysis and forecasting, econometrics, spatial-temporal dependence modeling, bootstrap and resampling methods, and mixed frequency data.