An Extreme Value Theory Based Catastrophe Bond Design for Cyber Risk Management of Power Systems

Zhaoxi Liu, *Member, IEEE,* Wei Wei, and Lingfeng Wang, *Senior Member, IEEE*

***Abstract*—Cybersecurity is emerging as one of the most critical issues for the power system operation in recent years. The most recent studies have shown that cyber-insurance can be an effective solution for the cyber risk management of power grids. In these early attempts, actuarial frameworks and premium schemes were designed for the insurance companies to cope with the risks on power system cybersecurity. However, due to the potentially catastrophic consequences of malicious cyberattacks on power grids, the tail risk events may expose the insurance companies to undue financial risks even if applicable premiums have been designed and collected, which will demotivate the insurance companies from entering the market and providing insurance to the power system stakeholders. In this paper, a Catastrophe (CAT) bond scheme is proposed for insurance companies to address the tail risk of power system cybersecurity by seeking protection from the capital market. The CAT bonds are designed based on the extreme value theory (EVT) to quantify the underlying risk of tail cybersecurity events in power systems. A stochastic model is developed and used in this paper to evaluate the potential losses of power system stakeholders due to malicious cyberattacks on the grids. An example on the IEEE Reliability Test System (RTS-96) was conducted and analyzed to demonstrate the validity and performance of the proposed EVT based CAT bond scheme. The results of the example show that the proposed CAT bond design can effectively manage the insolvency risk of insurers when providing cyber insurance to various stakeholders in power systems.**

***Index Terms*—Actuarial analysis, catastrophe bond, cybersecurity, cyber insurance, extreme value theory, risk management.**

I. Introduction

ALONG with the widespread deployment of information and communication technologies (ICT) in power systems over recent decades, cybersecurity threats to the power grids are growing at the same time [1]–[3]. Real-world cases have revealed the substantial risks of malicious cyberattacks on the modern power systems. For instance, in December 2015, the Ukrainian power system was struck by a vicious cyberattack, which led to large-scale power outage and disconnection of substations in the grid [4], [5]. Thus, cybersecurity has become a critical issue for the electric power industry and will be increasingly important in the roadmap towards the future smart grid, in which more advanced ICT and digital devices will be applied to enable more intelligent and efficient operations of the grids [6].

Due to the fundamental importance of power systems to the modern society, great efforts have been devoted to the researches on the enhancement of power system security and resiliency against malicious cyberattacks in recent years. Cyber vulnerability assessment models, anomaly detection algorithms, robust state estimation methods, resilient operation and planning methods have been proposed in literature to harden the system against cyberattacks [7], [8]. However, while it is important to improve the system cybersecurity itself, power system stakeholders are in urgent need of effective methods to hedge the residual risk of potential cyberattacks against the grids as successful cyberattacks on power systems can lead to enormous consequences. Insurance, as a powerful risk management tool, can be a promising and socially beneficial solution to this great challenge. Cyber insurance can smooth the financial impact of cyber risks while incentivizing relevant stakeholders to enhance the cybersecurity to reduce the premium. Meanwhile, cyber insurance can also improve the overall social welfare and benefit the entire society by encouraging cybersecurity investments, indicating the quality of cyber protection, and provoking replacement of obsolete standards for cybersecurity [9]. Hence, cyber insurance holds great potential and merits substantial research and development toward future applications.

Although relatively new, cyber insurance is growing rapidly with the worldwide anxiety over increasing cybersecurity risks [10], [11]. It is an attractive and promising option for cyber risk management in addition to preventive and remedial actions, and will directly influence the cybersecurity landscape of different departments and industries. Thus, cyber insurance is gaining much attention and emerging as an important cybersecurity research topic in recent years. Initial efforts have been primarily devoted to the analysis on feasibility, peculiarities, and framework design of cyber insurance [12]–[18]. The researches analyze both the general cyber insurance scenarios [12]–[14] and specific cases of computer networks [15], Internet of Things (IoT) systems [16], cloud computing [17], and cellular networks [18], among others. Meanwhile, governments and relevant authorities start to realize the great potential of using insurance tools to manage cyber risks for critical infrastructure protection. The possibility of applying cyber insurance in critical infrastructure sectors has been suggested by the U.S. Department of Homeland Security (DHS) and Department of Energy (DOE), and serious research is urged to provide necessary insights for practical applications [19], [20]. A few studies have been initiated which analyze the relation between the cyber protection investment and cyber insurance coverage for infrastructures [21], [22], and identify the needs for building cyber risk models and accelerating the research to support new and more robust cyber insurance products that meet the evolving needs and demands of infrastructure systems [23], [24].

This work was supported in part by US National Science Foundation (NSF) under award 1739485.

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).

Cybersecurity is a very important research area in power systems with the transition toward the smart grid. A significant research effort has been made to identify the vulnerabilities and assess the risks of power systems against potential cyber threats. A cybersecurity risk assessment method is proposed in [25], [26] for the IEC 61850-based power control systems, e.g., substation automation systems, based on asset analysis. The vulnerabilities of the supervisory control and data acquisition (SCADA) systems are assessed in [27], [28] from a cyber-security perspective, and the impacts of the cyberattacks on the SCADA systems and power system reliability are studied. The risk of switching attacks in power grids is measured in [29] with a cyber-net model based on the cybersecurity technologies in substations. Reference [30] proposes a cyber-physical vulnerability assessment method for power grids by calculating the graph based security indices to measure the security level of the underlying cyber-physical setting. Reference [31] proposes a risk assessment method on the expected load curtailment for power systems under cyberattacks considering the impacts of the bus and transmission line protection systems. The vulnerability and consequence analysis of false data injection (FDI) attacks on power system state estimation is studied in [32], [33]. Meanwhile, the risk of combined data attacks to the system operation is evaluated in [34] based on the vulnerability assessment and impact analysis on the power system state estimation. A cyber risk analysis framework is proposed in [35] to evaluate the risk of increased exposure of the smart grid to cyberattacks and quantify the benefit of cybersecurity investment based on a Bayes-adaptive network security model. Risk assessment methods have also been proposed for the distribution systems and microgrids. Reference [36] proposes two types of cyberattacks on the remote terminal units (RTUs) in active distribution systems (ADSs), and develops a risk assessment index to quantify the risk of the attacks to ADSs. A risk assessment method is proposed in [37] to study the impacts of FDI attacks on the microgrids with solar photovoltaic (PV) and energy storage systems (ESSs).

Another major research focus is the detection, protection and remedial methods for risk mitigation of power systems against potential cyberattacks. Various detection methods have been developed and proposed against the cyberattacks on different systems and applications in power grids [38]–[43]. Meanwhile, a wide range of defense and protection strategies have been proposed for the security resource allocation [44], [45], robust control [40], [46], operation and planning [47], [48] of the power systems. A few remedial action strategies have also been analyzed and proposed for the power grids to reduce and limit the damage of malicious cyberattacks after they are successfully launched on the systems [49], [50].

Compared with the active research on the vulnerability and risk assessment and mitigation methods for power systems, the study on residual cyber risk management through insurance is very limited at present and has just been kicked off by a few pioneering studies recently. The establishment of insurance policy for the risk of switching attacks in power grids has been suggested and briefly discussed in [29]. Reference [51] proposes an actuarial analysis framework for the risk management of power systems against potential cyberattacks. In the study, a series of detailed premium principles tailored for the power system cyber insurance are proposed for the insurance providers considering the risk correlation. A semi-Markov process (SMP) based model is developed to analyze the interdependent risks of power grid cybersecurity. A cyber insurance premium calculation framework is developed in [52] using the ruin theory with hypothesized power outages based on the cyber-reliability assessment of the substations. The premium is calculated based on the expected value principle with the safe premium loading identified in the ruin probability calculation. In [53], a cyber insurance model is proposed based on the power system reliability evaluation considering the cyberattacks and optimal defense resource allocation of the grid. The strategic allocation of defense resources of the grid against cyberattacks is formulated by a Stackelberg security game model. The impacts of the defense resource allocation on the cyber insurance premiums are analyzed. By applying a threat likelihood model, an insurance premium discount model is proposed in [54] to incentivize the cybersecurity investment in power industry. Besides, in [55] and [56], cyber insurance is introduced and proposed to manage the cyber risks in the vehicle-to-grid (V2G) systems for plug-in electric vehicles (PEVs).

Although recent efforts have been devoted to the topic, the research on cyber insurance for bulk power system risk management remains in the fledgling stage. The existing researches in literature on the topic mainly focus on the premium principle design for the cyber insurance of power systems, and discuss the impacts of the insurance models on the system cybersecurity strategies and investments. Further, although cyber risk models and analysis have been proposed in the existing literature, the correlated cyber risks of different entities in power systems have not been studied to meet the special need of the cyber insurance model design, which is highly important to the actuarial analysis for electric power grids. One of the most critical concerns for the insurance companies in providing cyber insurance for power systems lies in the high tail risk of extreme cybersecurity events in power grids, which must be addressed before the practical applications of power system cyber insurance and yet has never been covered by the existing works. The inherent nature of the power system cybersecurity incidents as typical high-impact low-frequency events [57] will place great pressure on the cyber insurance providers, and the correlated cyber risks of different insureds in power grids will further increase the financial stress of the cyber insurance providers with high insolvency risk. Such tail risk characteristics of the power system cybersecurity will demotivate the insurance companies and raise the barrier of the cyber insurance market entry if a general insurance model is directly applied. Thus, the correlated cyber risks of the insureds in power grids must be analyzed and quantified, and specific cyber insurance models and risk transfer methods should be tailored and developed for the cyber risk management of power systems.

In financial and actuarial context, tail risk refers to the risk that a potential loss distribution has a "heavy" tail, meaning that the survival function, the probability that the random variable exceeds a given level, decays to zero relatively slow. Intuitively, a random variable with a heavy tail distribution has a relatively large probability to take large values. For example, a normal distribution is a typical light tail distribution, because the survival function as well as the density function converges to zero very fast, at an exponential rate. As a result, almost all (more than 99%) of data points fall within three times the standard deviation of the mean and very little (almost 0%) fall outside that range (known as the 3-sigma rule). On the contrary, a Pareto distribution has a heavy tail because the survival function is a power function and thus converges to zero at a slower rate compared to normal distribution.

Intuitively, that means the random variables has a relatively large probability to take large values.

The cyber-related loss is generally considered to have a tail risk because the total loss of the insureds is more likely (compared to the traditional insurance business) to take large values due to the potential dependence among cyberattacks. To see this point, we can make a comparison to traditional insurance where individual losses are independent. Because individual losses are independent, the central limit theorem implies that the total loss approximately follows a normal distribution, which is a light tail distribution. When dependence comes into play, the central limit theorem fails, the losses are more likely to occur simultaneously and result in large realization of total loss, which causes tail risk.

In the context of cyber-physical power systems, the potential losses of insureds due to cyberattacks in a certain period are not deterministic but follow a certain probability distribution. Such cyber risks can cause intense financial pressure on the compromised entities of successful cyberattacks in power grids. As an effective and mature risk management tool, insurance is an attractive option to handle the cyber risks in power industry. Thus, cyber insurance is suggested and proposed for the entities in power systems to transfer and hedge the risks for the stochastic losses due to cyberattacks. The cyber insurance is expected to mitigate the financial impacts of cyberattacks on the insureds in power systems and encourage cybersecurity investment of the entities in the power industry. Among other critical infrastructures, the research and investigation on cyber insurance schemes for electric power grids are encouraged by the governments and industries to support the cyber risk management in power energy sector. Therefore, the cyber insurance for electric power grids deserves careful study and research. As discussed above, the cybersecurity risk is expected to have a tail risk since the cyber risks between different insureds are correlated, and the potential impacts of successful cyberattacks on power systems can be extreme. Thus, the concept of tail risk is used in this paper to analyze the insolvency risk of cyber insurance providers for power systems.

Many insurers hesitate to enter the cyber insurance market due to the unknown nature of cyber risks. One of their biggest concerns is that cyber risks are potentially dependent and can cause extreme losses when cyber risks occur simultaneously across different locations and thus impose significant insolvency risk to insurers. Reference [51] proposes a set of premium principles to mitigate the insolvency risk, at the cost of resulting in relatively high premiums. In this paper, the authors aim to mitigate the insolvency risk from a different perspective: transferring the extreme losses to the capital market via catastrophe (CAT) bonds. CAT bonds have been proven successful in mitigating traditional insurance catastrophe risks, such as flood, hurricanes, and earthquakes. By issuing CAT bonds, insurers are able to transfer the extreme tail risks to the capital market and thus control their insolvency risk at an acceptable level. In this paper, the idea of CAT bonds will be adapted and tailored to mitigate and manage the cyber risks in power systems.

The design of CAT bonds calls for detailed study on the extreme losses, which naturally brings up the extreme value theory (EVT). According to EVT, the extreme loss data are fitted into the generalized Pareto distribution, and then CAT bond is designed based on the estimated parameters in this paper. The challenge lies in the design of the CAT bond. The majority of the literature of CAT bonds focuses on developing pricing techniques. Meanwhile, the CAT bonds are assumed to follow a conventional structure. What have been missing in the literature are justification of this conventional design, the choice of parameters, and more fundamentally proper criteria to evaluate the CAT bonds. In this paper, we introduce the criterion of insolvency risk to demonstrate how to evaluate the efficiency of CAT bonds in mitigating tail risk. It has to be admitted that the study presented in this paper is exploratory. More in-depth studies are subject to future work from a theoretical actuarial perspective.

Although some exiting methods are applied in designing and pricing CAT bonds in this paper, however, the novel contribution of the proposed work is beyond these straightforward applications. Specifically, the criterion of insolvency probability is introduced in this paper to demonstrate how issuing CAT bonds helps mitigate tail risk and thus promote the insurer's participation rate. Moreover, the introduction of the criterion of insolvency probability naturally formulates an optimization problem, which has the potential to answer some fundamental questions in the design of CAT bonds, such as, what is the rationale to take the ratchet payoff structure; how to set up appropriate trigger points for payoff functions. The current literature of CAT bond design mainly focuses on pricing techniques and has left these questions open.

Meanwhile, in the existing literature, the correlated loss model of different insureds in power systems due to the cyber risks has not been analyzed quantitatively yet. In this paper, the loss of the transmission company (TRANSCO) is correlated with the losses of other TRANSCOs as well as the generation companies (GENCOs) and distribution companies (DISCOs), and vice versa. With the proposed loss models of different insureds in power systems, the critical impact of both the heavy-tail and correlation characteristics of cyber risk of the insurance policy holders can be formulated and quantified simultaneously to meet the need of cyber insurance analysis when various types of insureds exist in the cyber insurance scheme. As such, the potential insolvency risk of the cyber insurance provider can be evaluated more comprehensively and accurately. Further, the proposed model in this paper integrates the EVT based cyber risk modeling in the CAT bond design, which has not been covered in the existing literature.

The main contributions of this paper are summarized as follows:

- A CAT bond scheme is designed for the cyber insurance provider to transfer tail risks to the capital market. The CAT bond is priced using the EVT.
- The ingredient of insolvency risk is incorporated to the traditional CAT bond pricing model. Under the augmented model, insolvency risk analysis is conducted to demonstrate the efficiency of CAT bond in mitigating the tail risk. Moreover, the interplay between premium charge and CAT bond design is investigated to form a comprehensive risk management strategy.
- A stochastic model is built to evaluate the consequences of the power system interruptions due to potential malicious cyberattacks on the grids. The consequences of cyberattacks on the power system stakeholders including the GENCOs, TRANSCOs or regional transmission organizations (RTOs), and DISCOs are evaluated by the coordinated optimal operation model.

The rest of the paper is organized as follows. The proposed CAT bond scheme and the EVT based CAT bond design are presented in Section II. The stochastic model for evaluating the cyber risks of entities in power systems is introduced in

Section III. In Section IV, the proposed CAT bond scheme is demonstrated with an example on the IEEE Reliability Test System (RTS-96), and the results are analyzed and discussed. Finally, Section V concludes the paper.

II. The Mechanism of Catastrophe Bonds

In a bond transaction, an investor pays premium to the bond issuer at the issuance and receives cash at the maturity date. For a regular bond, the amount that the investor receives is fixed, and equal to the principal amount. For a CAT bond, the principal amount will be divided between the bond issuer (the insurer) and the investor. In order to determine the amount of indemnity to the insurer, a trigger needs to be specified. In general, there are two categories of triggers: indemnity triggers and non-indemnity triggers. See [58] for more discussions. In this paper, the trigger is set to be the total loss, which is an indemnity trigger. Denoting the total loss by X, the amount of indemnity to the insurer is specified by

$$I(X) = K \sum_{k=1}^{n} \alpha_k \mathbb{I}\left\{X \in (y_k, y_{k+1}]\right\}, \tag{1}$$

where K is the principal amount of the bond, $\{\alpha_k, k = 1, \ldots, n\} \subset [0, 1]$ is an increasing sequence representing payoff ratios on different layers, and $\{y_k, k = 1, \ldots, n\}$ is the sequence of trigger points to determine the payoff layers. Intuitively, the payoff to the insurer is triggered when the actual loss exceeds y_1. If the actual loss falls into interval $(y_k, y_{k+1}]$, the payoff ratio to the insurer is α_k. The more severe the loss is, the more indemnity the insurer receives.

Due to the randomness of the final payoff, pricing a CAT bond is more complicated than a regular bond. Different approaches have been established for the CAT bond pricing in the literature [59]. In this paper, the approach of probability transformation will be used. Under this approach, the price is calculated by the expected discount value of the final payoff, with the probability measure adjusted to reflect risk award to investors. Assume X has distribution F under probability measure $\mathbb{P}$. The price of the CAT bond is calculated by

$$\begin{aligned} B &= \mathbb{E}\left[e^{-rT}\left(K - I(X)\right)\right] \\ &= Ke^{-rT}\Big(1 - \sum_{k=1}^{n}(\alpha_k - \alpha_{k-1})\mathbb{Q}[X > y_k]\Big), \end{aligned} \tag{2}$$

where r is the risk free interest rate, T is the term of the bond, $\alpha_0 = 0$, and $\mathbb{Q}$ is a probability measure specified by

$$\mathbb{Q}[X \le y] = \Phi\left[\Phi^{-1}\left(\mathbb{P}[X \le y]\right) - \Phi^{-1}(\kappa)\right]. \tag{3}$$

Probability measure $\mathbb{Q}$ is referred to as Wang's transform [60] of probability measure $\mathbb{P}$. These two probability measures represent perceptions of the risk from the perspectives of the insurer and the investor. Probability measure $\mathbb{Q}$ is typically more conservative than $\mathbb{P}$ to allow a risk award to the investor, the amount of which can be controlled by the parameter κ.

Since a CAT bond is designed to cover high layers of loss, its pricing requires only the information of tail distribution of X, which naturally calls for the utilization of the EVT [61]. Generally, EVT provides a platform to study different types of tail risks. It concludes that the conditional distribution of the exceedance loss above a certain level always follow a generalized Pareto distribution, regardless of the original distribution of the loss. Specifically, the conditional distribution of $X - y_1 | X > y_1$ has an asymptotic generalized Pareto distribution (GPD). Such a parametric model enables us to derive explicit formulas for insolvency probability and conduct comparative analysis. The distribution function of the GPD for the conditional distribution of $X - y_1 | X > y_1$ can be expressed as follows.

$$G(x) = 1 - \left(1 + \xi \frac{x}{\beta}\right)^{-1/\xi}. \tag{4}$$

The parameters β and ξ are to be estimated from data.

The detailed application and pricing process of the proposed EVT based CAT bond scheme for the power system cyber insurance will be demonstrated later in Section IV.

III. Loss Modeling of Power Systems With Cybersecurity Threats

In this study, the direct impacts of successful cyberattacks on different entities in the power systems are analyzed. The investigated entities in this paper include the DISCOs, GENCOs and TRANSCOs (or RTOs).

A. Losses of Entities in Power Systems due to Cyberattacks

For the cyberattacks on DISCOs, it is assumed that the distribution substation will be disconnected from the grid if it is compromised by the cyberattack. In this case, the load connected to the DISCO's substation will be lost until the cyberattack is isolated and the control of the compromised distribution substation is restored. The annual monetary losses of the DISCO due to successful cyberattacks are evaluated as

$$X_{\varphi}^{\mathbf{D}} = \sum_{k=1}^{K_{\varphi}} \sum_{i \in \mathcal{N}_{\varphi}} d_{i,k} \mathcal{V}_{\varphi}\left(\tau_k\right) = \sum_{k=1}^{K_{\varphi}} \sum_{i \in \mathcal{N}_{\varphi}} d_{i,k} \eta_{\varphi} \tau_k, \tag{5}$$

where $X_{\varphi}^{\mathbf{D}}$ is a stochastic variable of the losses due to potential cyberattacks on DISCO φ; $d_{i,k}$ and τ_k are the load loss of the DISCO at bus i and the duration of load loss event k due to cyberattacks, respectively; $\mathcal{N}_{\varphi}$ denotes the set of distribution substations of DISCO φ; η_{φ} is the cost coefficient of DISCO φ for the load loss due to successful cyberattacks; K_{φ} is the total number of successful cyberattacks on the DISCO throughout a year.

In this study, the cyberattacks on DISCOs are assumed to be launched on the distribution substations. The compromised distribution substations are assumed to be disconnected from the grid, and the loads connected to the compromised substations of the DISCOs are assumed to be lost. The case with distributed generation (DG) to support all or part of the loads in the distribution networks in the presence of successful cyberattacks on the DISCOs is not considered in the simulation. However, if a DISCO can support all or part of the loads in the distribution network with DG when the compromised substations are disconnected from the grid due to successful cyberattacks, the loss modeling of the DISCO can be modified in the proposed model. The lost load $d_{i,k}$ in (5) should be adjusted and determined based on the ability of the DISCO in maintaining the electricity supply to demands with the DG in its distribution network. In this case, the loss of the DISCO will be reduced, and the premium of the DISCO will also be reduced accordingly. The other parts of the proposed method will remain the same, as the compromised distribution stations are disconnected from the grid similar to the case when DG in the distribution systems is not available.

If a power plant of a GENCO in the grid is compromised by the cyberattack, it is assumed that the capacity of the generation units in the power plant will be lost until the attack is isolated. Then losses of the GENCOs in the grid due to cyberattacks are calculated by the lost power output which has been scheduled by the economic dispatch at each bus of the grid without the cyberattacks. The economic dispatch of the grid can be formulated by the optimization problem as follows.

$$p_g^* = \arg\min \sum_{g\in\mathcal{G}} \left(\alpha_g p_g^2 + \beta_g p_g + \gamma_g\right) \tag{6}$$

Subject to

$$-M s_{i,j} \leqslant p_{i,j} - \frac{\vartheta_i - \vartheta_j}{x_{i,j}} \leqslant M s_{i,j}, \quad \forall (i,j) \in \mathcal{E} \tag{7}$$

$$\sum_{(i,j)\in\mathcal{E}} p_{i,j} - \sum_{g\in\mathcal{G}_i} p_g + l_i = 0, \quad \forall i \in \mathcal{N} \tag{8}$$

$$-p_{i,j}^{\max}(1 - s_{i,j}) \leqslant p_{i,j} \leqslant p_{i,j}^{\max}(1 - s_{i,j}), \forall (i,j) \in \mathcal{E} \tag{9}$$

$$0 \leqslant p_g \leqslant p_g^{\max} s_g, \quad \forall g \in \mathcal{G} \tag{10}$$

$$0 \leqslant \delta_i \leqslant l_i, \quad \forall i \in \mathcal{N} \tag{11}$$

where α_g, β_g and γ_g are the generation cost coefficients of generation unit g; p_g is the active power output of the generation unit; $p_{i,j}$ is the power flow of the transmission branch between buses i and j; ϑ_i is the phase angle of bus i; $p_{i,j}^{\max}$ is the capacity limit of the transmission branch between buses i and j; $p_g^{\max}$ is the active power output limit of generation unit g; l_i is the demand at bus i; M is a large enough positive constant. $s_{i,j}$ is the physical status of the transmission branch between buses i and j. $s_{i,j} = 1$ if the transmission branch between buses i and j is out of service physically. Otherwise, $s_{i,j} = 0$. Meanwhile, s_g represents the physical status of generation unit g. $s_g = 0$ if generation unit g is out of service physically. Otherwise, $s_g = 1$. Constraint (7) is the power flow model considering the transmission branch status $s_{i,j}$. Expression (8) is the power balance constraint of each bus in the grid. Expression (9) is the transmission capacity constraint considering the transmission branch status $s_{i,j}$, and (10) is the generation output limit considering the generation status s_g. Meanwhile, constraint (11) is the load shedding limit at each bus. Then the annual monetary losses of the GENCO due to successful cyberattacks are evaluated as

$$X_\upsilon^{\mathbf{G}} = \sum_{k=1}^{K_\upsilon} \sum_{g\in\widetilde{\mathcal{G}}_{\upsilon,k}} p_{g,k}^* \mathcal{V}_\upsilon(\tau_k) = \sum_{k=1}^{K_\upsilon} \sum_{g\in\widetilde{\mathcal{G}}_{\upsilon,k}} p_{g,k}^* \eta_\upsilon \tau_k, \tag{12}$$

where $X_\upsilon^{\mathbf{G}}$ is a stochastic variable of the losses due to potential cyberattacks on GENCO υ; $g_{g,k}^*$ and τ_k are the scheduled output of generation unit g and the duration of interruption event k due to cyberattacks, respectively; $\widetilde{\mathcal{G}}_{\upsilon,k}$ is the set of generation units of GENCO υ that have been compromised by the cyberattack in interruption event k; η_υ is the cost coefficient of the GENCO for the interruptions due to successful cyberattacks; K_υ is the total number of successful cyberattacks on the GENCO throughout a year.

It should be noted that the shutdown of generation units in the grid due to cyberattacks may lead to increased operational cost of the grid. However, for the system operator or other cyber insurance policy holders in the grid, the shutdown of the generation units of a GENCO due to cyberattacks is not different from that due to other reasons, e.g., physical failures. The compromised GENCO is supposed to be penalized for the undelivered power which is included in the losses of the compromised GENCO. The compromised GENCO may get compensated by the claims to the insurance provider. The system operator or other cyber insurance policy holders in the grid are not supposed to claim the coverage for the increased operational cost. Thus, in the proposed cyber insurance model of the paper, the damage claims of the insureds are constrained to the losses due to direct cyberattacks on the insureds. The increased operational cost of the grid is not included in the losses of the insureds in the paper. Nevertheless, if an insurance provider agrees a specific insurance policy with an insured on the risk of extra operational cost of the grid due to successful cyberattacks on the GENCOs or any other entities in the network, a higher loss correlation is expected. In this case, the insurance provider needs to evaluate the insolvency risk considering such insurance policyholders together with the original insureds. The insurance provider can estimate the loss distribution by calculating the increased operational cost using the results of the optimal redispatch model of the TRANSCOs.

When a transmission substation of the TRANSCOs (or RTOs) is compromised by successful cyberattacks, it is assumed that all the transmission branches as well as the generation units and loads connected to the targeted substation will be tripped and forced to disconnect from the grid until the attack is cleared and the normal control of the substation is restored. When successful cyberattacks on the TRANSCOs are launched, the interconnected TRANSCOs may coordinate their operations to minimize the load losses in the grid under the faults at the compromised substations due to the attacks. However, for each TRANSCO, the coordinated operations should not result in a higher load loss than the result of the self dispatch within its network. In other words, the interest of each TRANSCO should be protected but not compromised by the coordinated operations. In this paper, an alternating direction method of multipliers (ADMM) based model is used to formulate the coordinated operations of interconnected TRANSCOs with the cyberattacks. The original coordinated operation model of the interconnected TRANSCOs can be represented as follows.

$$\min \sum_{i\in\mathcal{N}} \delta_i \tag{13}$$

Subject to

$$-M(z_{i,j} + s_{i,j}) \leqslant p_{i,j} - \frac{\vartheta_i - \vartheta_j}{x_{i,j}} \leqslant M(z_{i,j} + s_{i,j}), \quad \forall (i,j) \in \mathcal{E} \tag{14}$$

$$\sum_{(i,j)\in\mathcal{E}} p_{i,j} - \sum_{g\in\mathcal{G}_i} p_g + (l_i - d_i - \delta_i) = 0, \quad \forall i \in \mathcal{N} \tag{15}$$

$$-p_{i,j}^{\max}(1 - z_{i,j}) \leqslant p_{i,j} \leqslant p_{i,j}^{\max}(1 - z_{i,j}), \forall (i,j) \in \mathcal{E} \tag{16}$$

$$-p_{i,j}^{\max}(1 - s_{i,j}) \leqslant p_{i,j} \leqslant p_{i,j}^{\max}(1 - s_{i,j}), \forall (i,j) \in \mathcal{E} \tag{17}$$

$$0 \leqslant p_g \leqslant p_g^{\max} s_g z_g, \quad \forall g \in \mathcal{G} \tag{18}$$

$$0 \leqslant \delta_i \leqslant l_i - d_i, \quad \forall i \in \mathcal{N} \tag{19}$$

$$\sum_{i\in\mathcal{N}_\psi} \delta_i \leqslant \Lambda_\psi^*, \quad \forall \psi \in \Psi \tag{20}$$

where

$$\Lambda_{\psi}^{*} = \arg\min \sum_{i \in \mathcal{N}_{\psi}} \tilde{\delta}_i \tag{21}$$

Subject to

$$-M\left(z_{i,j}+s_{i,j}\right) \leqslant \tilde{p}_{i,j} - \frac{\tilde{\vartheta}_i - \tilde{\vartheta}_j}{x_{i,j}} \leqslant M\left(z_{i,j}+s_{i,j}\right), \quad \forall (i,j) \in \mathcal{E}_{\psi} \tag{22}$$

$$\sum_{(i,j)\in\mathcal{E}_{\psi}} \tilde{p}_{i,j} - \sum_{g\in\mathcal{G}_i} \tilde{p}_g + \left(l_i - d_i - \tilde{\delta}_i\right) = 0, \quad \forall i \in \mathcal{N}_{\psi} \tag{23}$$

$$-p_{i,j}^{\max}\left(1-z_{i,j}\right) \leqslant \tilde{p}_{i,j} \leqslant p_{i,j}^{\max}\left(1-z_{i,j}\right), \quad \forall (i,j) \in \mathcal{E}_{\psi} \tag{24}$$

$$-p_{i,j}^{\max}\left(1-s_{i,j}\right) \leqslant \tilde{p}_{i,j} \leqslant p_{i,j}^{\max}\left(1-s_{i,j}\right), \quad \forall (i,j) \in \mathcal{E}_{\psi} \tag{25}$$

$$0 \leqslant \tilde{p}_g \leqslant p_g^{\max} s_g z_g, \quad \forall g \in \mathcal{G}_{\psi} \tag{26}$$

$$0 \leqslant \tilde{\delta}_i \leqslant l_i - d_i, \quad \forall i \in \mathcal{N}_{\psi} \tag{27}$$

where d_i is the load loss of the DISCOs due to the cyberattacks on the distribution substations connected to bus i; $z_{i,j}$ is the status of the transmission branch between buses i and j. $z_{i,j} = 1$ if the transmission branch between buses i and j is out of service due to the cyberattacks on the TRANSCOs. Otherwise, $z_{i,j} = 0$. Meanwhile, z_g represents the status of generation unit g. $z_g = 0$ if generation unit g is out of service or disconnected from the grid due to the cyberattacks. Otherwise, $z_g = 1$. Constraint (14) is the power flow model considering the transmission branch status $s_{i,j}$ and $z_{i,j}$. Expression (15) is the power balance constraint of each bus in the grid. Expressions (16) and (17) formulate the transmission capacity constraint considering the transmission branch status $s_{i,j}$ and $z_{i,j}$. Expression (18) is the generation output limit considering the generation status s_g and z_g. Expression (19) is the load shedding limit at each bus. Constraint (20) guarantees that the coordinated operations of the TRANSCOs does not violate the interest of each individual TRANSCO. As shown in the optimization model above, for each TRANSCO ψ, the load loss with the coordinated operations must be lower than the minimum load loss in the cyberattacks Λ_{ψ}^{*} when only self dispatch is considered as (21)-(27). Thus, the interest of each TRANSCO is protected in the coordinated operations. Then the coordination between the interconnected TRANSCOs can be formulated and realized by the ADMM based decentralized optimal operation model as follows.

$$\{\delta_{\psi,i}^{\kappa+1},\, \vartheta_{\psi,i}^{\kappa+1}\} = \arg\min \left[\sum_{i\in\mathcal{N}_{\psi}} \delta_i + \sum_{i\in\widehat{\mathcal{N}}_{\psi}} \left(y_{\psi,i}^{\kappa}\vartheta_i + \frac{\rho}{2}\left(\vartheta_i - z_i^{\kappa}\right)^2\right)\right], \tag{28}$$

$$\{z_i^{\kappa+1}\} = \arg\min \sum_{i\in\widehat{\mathcal{N}}_{\psi}} \left[\frac{\rho}{2}\left(z_i - \vartheta_i^{\kappa+1}\right)^2 - y_{\psi,i}^{\kappa} z_i\right], \tag{29}$$

$$y_{\psi,i}^{\kappa+1} = y_{\psi,i}^{\kappa} + \rho\left(\vartheta_{\psi,i}^{\kappa+1} - z_i^{\kappa+1}\right), \tag{30}$$

where $\widehat{\mathcal{N}}_{\psi}$ is the set of buses connected to the transmission tie lines of TRANSCO ψ to the external networks. The ADMM based decentralized optimal operation model can then be realized by **Algorithm 1** presented below.

Algorithm 1: ADMM Based Coordinated Operations of TRANSCOs

1. Set iteration index $\kappa = 0$, and initialize parameters $y_{\psi,i}^{\kappa}$ and z_i^{κ}, $\forall\psi \in \Psi$, $\forall i \in \mathcal{N}$.
2. For each TRANSCO $\psi \in \Psi$, calculate the load loss and voltage phase angle at each bus by solving (28).
3. Update parameters z_i^{κ} and $y_{\psi,i}^{\kappa}$ according to (29) and (30).
4. If $\left|\boldsymbol{\vartheta}^{\kappa+1} - \mathbf{z}^{\kappa+1}\right| \leqslant \epsilon$, then return $\delta_{\psi,i}^{\kappa+1}$, $\forall\psi \in \Psi$, $\forall i \in \mathcal{N}$ as the solution. Otherwise, go to Step 2.

Due to the convexity of the coordinated optimal operation model, it is easy to examine and proof that the ADMM based model can converge to the optimal solution of the coordinated dispatch of the TRANSCOs to minimize the load losses. Then the annual monetary losses of the TRANSCO due to successful cyberattacks are evaluated as

$$X_{\psi}^{\mathbf{T}} = \sum_{k=1}^{K_{\psi}} \sum_{i\in\mathcal{N}_{\psi}} \delta_{i,k}\mathcal{V}_{\psi}\left(\tau_k\right) = \sum_{k=1}^{K_{\psi}} \sum_{i\in\mathcal{N}_{\psi}} \delta_{i,k}\eta_{\psi}\tau_k, \tag{31}$$

where $X_{\psi}^{\mathbf{T}}$ is a stochastic variable of the losses due to potential cyberattacks on TRANSCO ψ; $\delta_{i,k}$ and τ_k are the load loss at bus i and the duration of interruption event k due to cyberattacks, respectively; η_{ψ} is the cost coefficient of the TRANSCO for the interruptions due to successful cyberattacks; K_{υ} is the total number of successful cyberattacks on the TRANSCO throughout a year.

When the control systems of the substations are compromised by the cyberattacks, the attackers are assumed to be able to send false commands to force the tripping of the circuit breakers in the substations. In this case, the transmission branches connected to the compromised substations will be forced to be disconnected until the attacks are isolated. This assumption has been applied in the existing cybersecurity research [28] and validated by the real-world successful cyberattack on the Ukrainian power grid [62]. Thus, the assumption is applied in this study.

In the proposed model, an optimal redispatch is performed by the TRANSCOs to reduce the losses due to the successful cyberattacks. Optimal redispatch is a well-accepted and practical assumption in cybersecurity analysis of power systems in mitigating the damage of malicious cyberattacks [47], and thus is also applied in this study. Nevertheless, it is believed that a reconfiguration strategy can be able to further reduce the loss of the TRANSCOs against the cyberattacks due to increased flexibility of the operation. However, the reconfiguration method will considerably increase the computational burden due to its inherent nature as an integer-programming problem. A highly computational efficient algorithm for the reconfiguration problem needs to be developed if a reconfiguration-based mitigation strategy is supposed to be applied by the TRANSCO when it is compromised by malicious cyberattacks in the loss modeling. Optimal reconfiguration and network topology optimization methods can be good strategies for the TRANSCOs to mitigate the damage of the cyberattacks. More in-depth analysis on the optimal reconfiguration and network topology optimization methods in the risk management of power systems against cyberattacks will be carried out in the future work.

B. Modeling of Cyberattacks on Power Systems

In the study, the statuses of the distribution substations, generation units and transmission branches are affected by the

This article has been accepted for publication in IEEE Transactions on Smart Grid. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TSG.2021.3131468

cyberattacks on power systems. In the cyberattacks on power systems, the attackers are assumed to intrude into the SCADA systems to interrupt the normal operation of the substations and power plants in the grid. An absorbing Semi-Markov Process (SMP) model as shown in Fig. 1 [51] is applied in this study to formulate the cyberattacks on the SCADA systems of the substations and power plants. The SMP model is briefly introduced here.

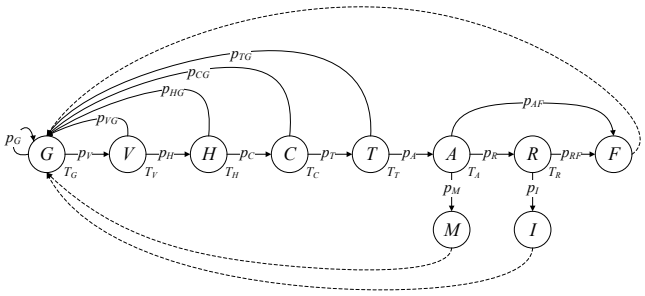

Fig. 1. Absorbing SMP Model of Cyberattacks on SCADA Systems in Power Systems.

The absorbing SMP model of the cyberattacks $\{J(t) : t \geqslant 0\}$ starts from the good state G, which represents the secure situation of the SCADA system. Then a series of intermediate states follow, each of which represents one phase of the attack. The SMP transits along the intermediate states as the attacker proceeds with the attack actions step by step and gains a greater privilege of the SCADA system. If the malicious intrusion is detected and isolated by the system protection mechanisms during the penetration process, the system will be brought back to the good state G as shown in Fig. 1. If the attacker manages to exploit the targeted components in the SCADA system to launch the attack, three different cases may occur. If the protection mechanisms of the control system manage to mask the impacts of the attack adequately, the normal operation of the system is maintained and the SMP will be brought back to the good state G. In contrast, if the protection mechanisms fail to recognize and isolate the attack, a complete failure of the control system occurs. Corresponding contingencies in the grid will arise until the control system is restored. In the third case, the protection mechanisms of the SCADA system manage to recognize the attack actions while the attack cannot be masked. The error recovery and fault treatment mechanisms of the system will be initiated to hedge the damage of the attack. The SMP transits to the interrupted state I if the error recovery and fault treatment mechanisms are able to track and identify the route of the attack promptly. 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 of the attack is reduced. Otherwise, the SMP reaches the failure state F, in which a longer time will be required to restore the system and greater damage of the attack will be caused. The meaning of each transient state in the SMP model is introduced as follows:

- G: The SCADA system is in a good and healthy state.
- V: Vulnerabilities exist in the SCADA system.
- H: The vulnerability is exploited by attacker and used to gain one or more hosts' privilege in the SCADA network.
- C: Necessary connections in the SCADA network are compromised by the attacker.
- T: Necessary privileges of the targeted servers are obtained by the attacker.
- A: Destination devices are exploited by the attacker.
- R: Error recovery and fault treatment mechanisms are triggered to hedge the damage of the attack.

Accordingly, the Markov kernel of the absorbing SMP model Q_T can be expressed as follows.

$$Q_T = \begin{bmatrix} p_G & p_V & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ p_{VG} & 0 & p_H & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ p_{HG} & 0 & 0 & p_C & 0 & 0 & 0 & 0 & 0 & 0 \\ p_{CG} & 0 & 0 & 0 & p_T & 0 & 0 & 0 & 0 & 0 \\ p_{TG} & 0 & 0 & 0 & 0 & p_A & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & p_R & p_M & 0 & p_{AF} \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & p_I & p_{RF} \end{bmatrix}, \tag{32}$$

where $\mathcal{S}_T = \{G, V, H, C, T, A, R\}$ is the transient state space, $\mathcal{S}_A = \{M, I, F\}$ is the absorbing state space, and 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:

$$\sum_{j \in \mathcal{S}_T \cup \mathcal{S}_A} p_{ij} = 1, \quad \forall i \in \mathcal{S}_T. \tag{33}$$

The Markov kernel and sojourn time of the transient states in the absorbing SMP model describe the stochastic characteristics of the cyberattacks and the cybersecurity performance of the SCADA system under attacks. The success probability of cyberattack attempts is formulated implicitly in the proposed SMP model. The transition probabilities of the transient states to the next state in the SMP model represent the success probability of each step in the process of the cyberattacks to compromise the SCADA systems of the power plants and substations. In contrast, the transition probabilities from the transient states to the good state represent the probabilities of the defense mechanisms in detecting and blocking the malicious attempts. As such, the probability of each cyberattack attempt on the entities in the grid is modeled and determined by the proposed SMP model.

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 $\mathcal{N}$ 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.

$$p_{ij}^{\mathcal{N}} = \hat{p}_{ij}^{\mathcal{N}} u + \hat{p}_{ij} \left(1 - u\right), \ \forall i \in \mathcal{S}_T, \forall j \in \mathcal{S}_T \cup \mathcal{S}_A, \tag{34}$$

$$T_i^{\mathcal{N}} = \hat{T}_i^{\mathcal{N}} u + \hat{T}_i \left(1 - u\right), \ \forall i \in \mathcal{S}_T, \tag{35}$$

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. u is a stochastic variable following a Bernoulli distribution. With the SMP model, the process of the cyberattacks against the power grids can be simulated efficiently.

This article has been accepted for publication in IEEE Transactions on Smart Grid. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TSG.2021.3131468

C. Modeling of Physical Failures in Power Grids

Meanwhile, the physical statuses of the generation units and transmission branches in the grids are determined by a sequential Monte Carlo method with the time-to-failure and time-to-repair for the physical outages of generation units and transmission branches [63]. In this study, both the time-to-failure and time-to-repair for the physical outages of the generation units and transmission branches are assumed to be exponentially distributed. Therefore, the residence time of any state j (i.e., out-of-service or in-service) can be simulated by a random variable τ with the exponential probability density function as follows:

$$f_{\tau_j}(t) = \lambda_j e^{-\lambda_j t}, \tag{36}$$

where $1/\lambda_j$ is the mean residence time of state j.

At each interval, with the statues of the system components according to the physical failures and successful cyberattacks in the grid, the losses of the DISCOs, GENCOs and TRANSCOs due to the cyberattacks can be determined. Then, the distributions of the annual losses due to successful cyberattacks of the DISCOs, GENCOs and TRANSCOs can be simulated with a sequential Monte Carlo approach.

The relation between the DISCOs, GENCOs and TRANSCOs in the proposed loss modeling approach is illustrated by the framework shown in Fig. 2. In the proposed model, the SMP based cyberattack event sampling is performed to determine the cyber status of the generation units of each GENCO, the distribution substations of each DISCO, and the transmission substations of each TRANSCO. For the GENCO model, a physical status sampling is performed to obtain the physical status of each generation unit s_g. Then the economic dispatch without cyberattacks is performed to identify the scheduled outputs of the generation units. Then the losses of the GENCOs are determined based on the scheduled outputs and sampled cyber status of the generation units. For the DISCO model, the loss is determined by the sampled cyber status of the distribution substations and the loads connected to the compromised substations at the interval. For the TRANSCO model, a physical status sampling is performed to determine the physical status of the transmission branches. The cyber status of the transmission substations is determined by the output of the SMP based cyberattack event sampling, and the connectivity of the generation units and transmission branches at each substation is determined. The physical status and cyber status of the generation units is obtained from the GENCO model, the load at each bus is obtained from the DISCO model. With these inputs, the coordinated redispatch model of the TRANSCOs is performed to determine the losses of the TRANSCOs.

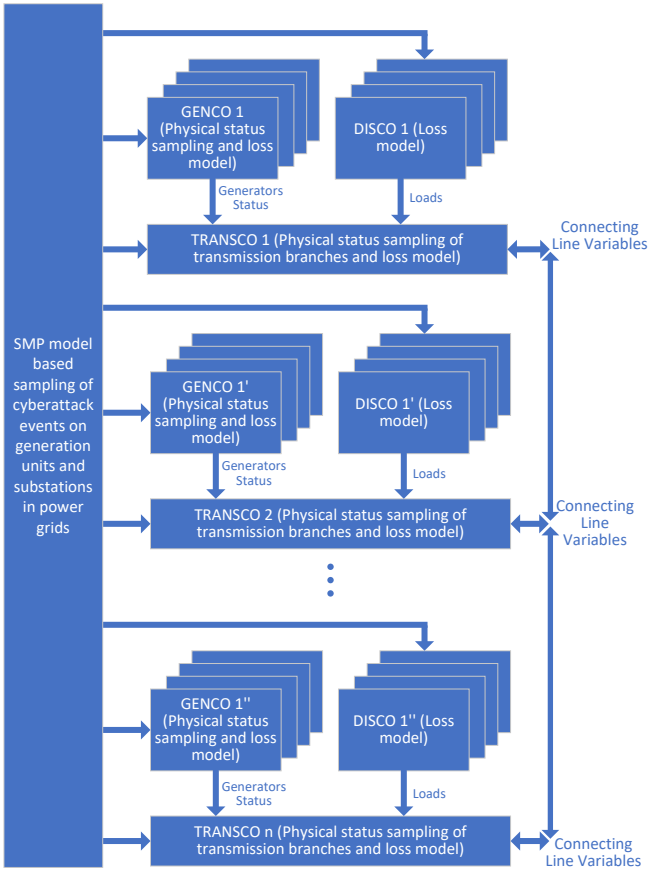

Fig. 2. Loss Modeling Framework of DISCOs, GENCOs and TRANSCOs.

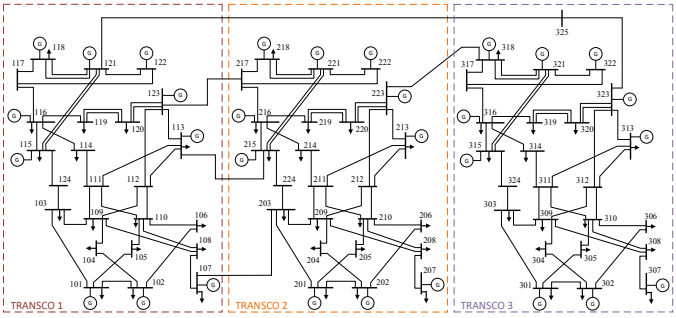

Fig. 3. Test System with IEEE (RTS-96) Reliability Test System.

IV. CAT Bond Model Demonstration and Discussions

A. Test System Model and Power System Simulation

In order to demonstrate and validate the proposed CAT bond scheme for the insurance companies in handling the tail risk of cyberattacks on power systems, an example on the IEEE Reliability Test System (RTS-96) [64] is conducted and discussed in this section. The single line diagram of the test system used in the example is shown in Fig. 3.

In the test system, it is assumed that three individual TRANSCOs with 12 GENCOs and 21 DISCOs serve the loads of the grid. TRANSCO 1 covers Buses 101-124, TRANSCO 2 covers Buses 201-224 and TRANSCO 3 covers Buses 301-325 in the IEEE RTS-96 system as shown in Fig. 3. The configurations of the DISCOs and GENCOs in the test system are listed in Table I and II, respectively.

In the sequential Monte Carlo approach to evaluate the losses of the power grid, an hourly time sequence of 80,000 years is sampled. The mean values of the parameters in the absorbing SMP model are listed in Table III. It should be noted that the simulation of the proposed model in the case study does not rule out the scenarios with relatively fast state transition when highly skilled and resourceful attackers appear. The sojourn time of the transient states in the case study follows the normal distributions with the mean values shown in Table III. There is a possibility that the sojourn time is transient for the cyberattacks in the proposed SMP based model.

The proposed model in the case study is solved using

This article has been accepted for publication in IEEE Transactions on Smart Grid. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TSG.2021.3131468

TABLE I
LOAD BUSES OF DISCOS

DISCOs	Load Buses	DISCOs	Load Buses
DISCO 1	101, 103, 104, 105	DISCO 12	214, 215, 216
DISCO 2	102, 106, 107, 108	DISCO 13	218
DISCO 3	109, 110	DISCO 14	219, 220
DISCO 4	113	DISCO 15	301, 303, 304, 305
DISCO 5	114, 115, 116	DISCO 16	302, 306, 307, 308
DISCO 6	118	DISCO 17	309, 310
DISCO 7	119, 120	DISCO 18	313
DISCO 8	201, 203, 204, 205	DISCO 19	314, 315, 316
DISCO 9	202, 206, 207, 208	DISCO 20	318
DISCO 10	209, 210	DISCO 21	319, 320
DISCO 11	213		

TABLE II
BUSES WITH GENERATION UNITS OF GENCOS

GENCOs	Buses	No. of Units	Total Gen. Cap.
GENCO 1	101,102,107,113,115	21	1490 MW
GENCO 2	116,118	2	555 MW
GENCO 3	121,122	7	700 MW
GENCO 4	123	3	660 MW
GENCO 5	201,202,207,213,215	21	1490 MW
GENCO 6	216,218	2	555 MW
GENCO 7	221,222	7	700 MW
GENCO 8	223	3	660 MW
GENCO 9	301,302,307,313,315	21	1490 MW
GENCO 10	316,318	2	555 MW
GENCO 11	321,322	7	700 MW
GENCO 12	323	3	660 MW

TABLE III
PARAMETERS IN THE ABSORBING SMP MODEL

Par.	Val.	Par.	Val.	Par.	Val.	Par.	Val.
p_V	1	p_A	0.5	p_{AF}	0.2	T_H	10 days
p_H	0.5	p_R	0.5	p_{RF}	0.6	T_C	10 days
p_C	0.5	p_M	0.3	T_G	200 days	T_T, T_A	10 days
p_T	0.5	p_I	0.4	T_V	10 days	T_R	10 hours

CPLEX on a laptop with Intel Core i5 quadcore CPU (1.60-3.90GHz) and 12GB RAM. The computation time of the ADMM based distributed optimization model is less than 2 seconds for the scenario of each interval with cyberattack events.

Fig. 4 shows the marginal distribution of the annual loss of TRANSCO 1 in the result as an example. It clearly shows the heavy tail risk of the cyberattacks on the grid. Fig. 5 shows the values of the correlation coefficients between the losses of the DISCOs, GENCOs and TRANSCOs in the case study. It indicates the correlation level between the DISCOs, GENCOs and TRANSCOs' losses. Each off-diagonal element shows the correlation coefficient between two different entities, which lies in the interval $[-1, 1]$. A higher correlation coefficient means a higher correlation level, a zero correlation coefficient means the two variables are independent, and a negative correlation coefficient means negative correlation. A positive correlation between the losses of the DISCOs, GENCOs and TRANSCOs is clearly shown in the figure. All the off-diagonal elements are clearly greater than zero, of which the lowest number is about 0.26, and the average number is about 0.45. As discussed in the paper, both the heavy tail characteristics and positive correlation structure of the cyber risks of the power grid will pose excessive financial tail risks on the cyber insurance providers of power systems.

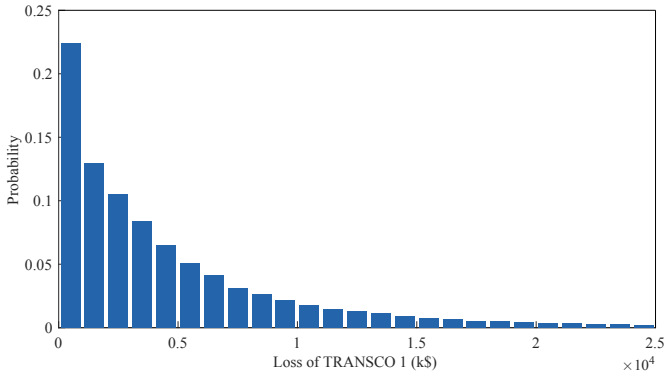

Fig. 4. Marginal Loss Distribution of TRANSCO 1.

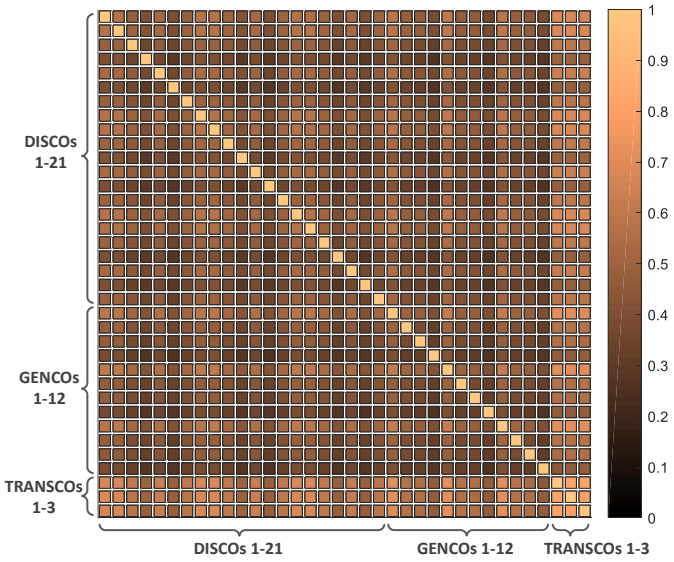

Fig. 5. Correlation Coefficients of Losses of DISCOs, GENCOs and TRANSCOs.

B. CAT Bond Design and Analysis

The simulation generates a sample of size 80,000 for the total annual loss X. Some useful characteristics are summarized as follows:

TABLE IV
USEFUL CHARACTERISTICS OF X

Expected Value	95% Percentile	99% Percentile
$\mathbb{E}[X] = 43011$	$y_1 = 138996$	$y_2 = 281209$

Design a one-year CAT bond that has a two-layer payoff structure and a principal amount of $K = 1000$. Set the two trigger points to be y_1 and y_2, and the payoff ratios to be $\alpha_1 = 0.5$ and $\alpha_2 = 1$. The indemnity to the insurer from each unit CAT bond is

$$I(X) = 0.5K \times \left(\mathbb{I}\{X > y_1\} + \mathbb{I}\{X > y_2\} \right). \quad (37)$$

According to EVT, $X - y_1 | X > y_1$ has an asymptotic generalized Pareto distribution specified by (4). Fitting data

into this model using the maximum likelihood method, the parameters ξ and β are estimated to be $\hat{\xi} = 0.324732$ and $\hat{\beta} = 69486.9$. The Q-Q plot in Fig. 6 is introduced to demonstrate the goodness of the fitting of the simulation data into the estimated GPD model based on EVT. The Q-Q plot show that the quantiles of the simulation data and GPD model match well. The fitting of the estimated GPD model is desirable.

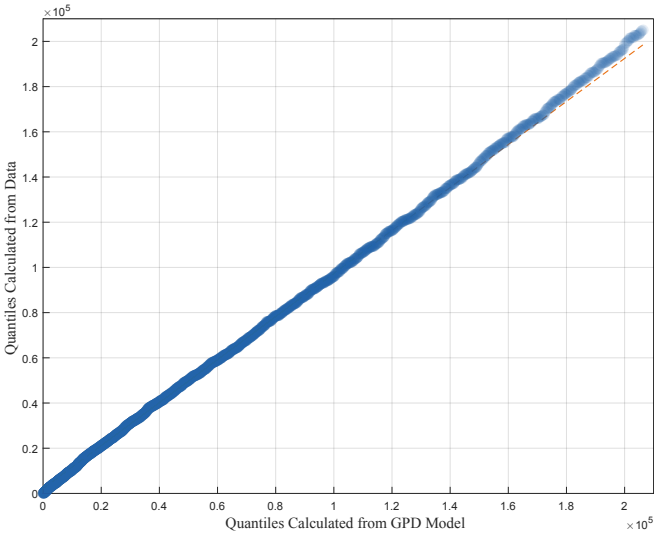

Fig. 6. Q-Q Plot for the Fitting into GPD Model.

Note that $\mathbb{P}\{X \le y_1\} = 0.95$. Following the GPD model,

$$\begin{aligned}\mathbb{P}\{X \le y_2\} &= 0.95 + 0.05 \times \mathbb{P}\{X - y_1 \le y_2 - y_1 | X > y_1\} \\ &= 0.95 + 0.05 \times \left[1 - \left(1 + \hat{\xi}\frac{y_2 - y_1}{\hat{\beta}}\right)^{-1/\hat{\xi}}\right] \\ &= 0.9896\end{aligned} \tag{38}$$

Setting $\kappa = 0.75$ in (3) yields $\mathbb{Q}\{X \le y_1\} = 0.8341$ and $\mathbb{Q}\{X \le y_2\} = 0.9492$. Assume an annual interest rate of $r = 3\%$. Following (2), the price of the CAT bond is calculated to be $B = 865.26$.

Suppose the insurer sells w units of CAT bond at the beginning of the year. The insurer's net loss is

$$L(w) = X + w(K - I(X)) - (P + wB)e^r, \tag{39}$$

where $P = (1 + \theta)\mathbb{E}[X]$ is the total premium collected from the insureds, and $(P+wB)e^r$ represents the accumulated value of the insurer's total income at the end of the year. Plugging in the expressions for $I(X)$ and B yields

$$\begin{aligned}L(w) = X - Pe^r + wK(\mathbb{Q}\{X > y_1\} - \mathbb{I}\{X > y_1\}) \\ + wK(\mathbb{Q}\{X > y_2\} - \mathbb{I}\{X > y_2\}).\end{aligned} \tag{40}$$

An insolvency event occurs if $L(w) > 0$. The insurer is particular concerned about the tail insolvency probability, that is, the conditional probability of insolvency given that the CAT bonds are triggered. It is calculated by

$$\begin{aligned}p_d &= \mathbb{P}\{L(w) > 0 | X > y_1\} \\ &= \begin{cases}\bar{G}(a(w)), & \text{if} w \le \frac{y_2 - Pe^r}{Be^r} \\ \bar{G}(b(w)), & \text{if} w \ge \frac{y_2 - Pe^r}{Be^r - 0.5K} \\ \bar{G}(a(w)) + \bar{G}(b(w)) - \bar{G}(y_2 - y_1), & \text{otherwise}\end{cases}\end{aligned} \tag{41}$$

where $\bar{G}(x) = \left(1+\xi\frac{x}{\beta}\right)^{-1/\xi}$ is the survival function of $X - y_1$ conditional on $X > y_1$, and $a(w) = Pe^r + w(Be^r - 0.5K) - y_1, b(w) = Pe^r + wBe^r - y_1$.

The tail insolvency probability p_d is a function of θ and w. Table V below presents the value of p_d with different θ and w:

TABLE V
TAIL INSOLVENCY PROBABILITY

θ \ w	0	250	500	750	1000	1250
0%	1	0.955	0.146	0.018	0.008	0.005
25%	1	0.819	0.112	0.017	0.008	0.004
50%	1	0.694	0.083	0.017	0.008	0.004
100%	1	0.493	0.040	0.015	0.007	0.004
200%	1	0.241	0.032	0.013	0.006	0.004
300%	0.602	0.097	0.026	0.011	0.006	0.003

Table V demonstrates that, in the sense of reducing the tail insolvency probability, increasing the sale of CAT bonds is substantially more efficient than elevating the safe loading coefficient. In particular, without any indemnity from CAT bonds ($w = 0$), the safe loading coefficient has to exceed 200%, which is already impractical, to merely avoid insolvency with certainty; let alone control the insolvency probability at a desirable level. The conclusion is consistent with the TVaR premium principle proposed in [51], which controls the insolvency risk well but results in a high safe loading coefficient.

It is worth pointing out that, although the insolvency probability p_d is a decreasing function of w, it is not sensible to sell CAT bonds without limitation. There is an implicit cost of issuing CAT bonds, which is hidden in the scenarios when the CAT bonds are not triggered. To demonstrate the implicit cost, consider the unconditional expected value (under probability measure $\mathbb{P}$) of the net loss:

$$E[L(w)] = X - Pe^r + wK\sum_{k=1}^{2}(\mathbb{Q}\{X > y_k\} - \mathbb{P}\{X > y_k\}). \tag{42}$$

Typically, $\mathbb{Q}\{X > y_k\} > \mathbb{P}\{X > y_k\}$, and thus $E[L(w)]$ is increasing in w. That means, increasing the sale of CAT bonds would increase the expected loss in general. The insurer would balance the cost and benefit of selling CAT bonds and obtain an optimal level of w based on its specific risk attitude.

To demonstrate the results of the proposed CAT bond design more clearly, a comparison with the VaR-based premium scheme proposed in [51] is conducted. The total premium of the insureds and the safe loading coefficients with the VaR-based premium scheme are listed in Table VI. As shown in the table, a high total premium and safe loading coefficients are necessary for the VaR-based premium in order to achieve a low insolvency probability. Fig. 7 shows the safe loading coefficients with the VaR-based premium and the proposed CAT bond scheme with $w = 750$. As shown in the figure, the safe loading coefficient is much lower with the proposed CAT bond scheme compared with the result of the VaR-based premium model. As such, the premiums of the insureds can be reduced and extremely high safe loading levels can be avoided while a low insolvency probability can be achieved by the cyber insurance provider with the proposed CAT bond design.

In the case study, an hourly time sequence of 80000 years was simulated. In fact, the sequence can be shorter

TABLE VI
TOTAL PREMIUM AND SAFE LOADING WITH VAR-BASED PREMIUM IN [51]

Insolvency Probability	5%	4%	3%
Total Premium	138997	156518	178467
Safe Loading	2.23	2.64	3.15
Insolvency Probability	2%	1%	0.5%
Total Premium	211140	281237	371813
Safe Loading	3.91	5.54	7.64

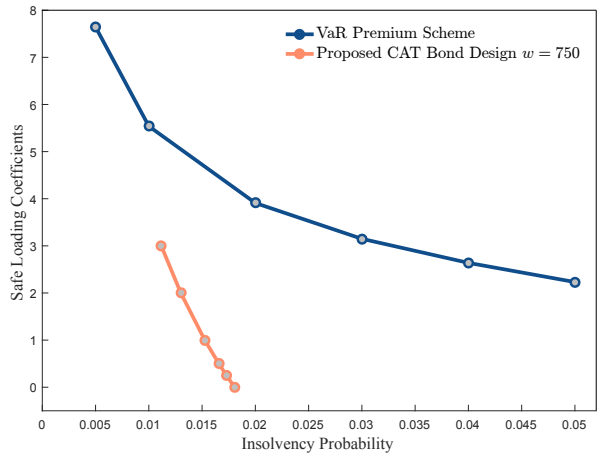

Fig. 7. Safe Loading Coefficients to Insolvency Probabilities with VaR-based Premium and CAT Bond Schemes.

in the simulation while obtaining a stable result of the loss distribution. Fig. 8 shows the relative changes of the critical statistics including the expected value, 95%-percentile and 99%-percentile of the total annual loss X to the length of the time sequence. As shown in the figure, the relative changes of all the three statistics fall below a criterion of 5e-3 when the horizon of the sample time sequence is over 27000 years. The extra length of the time sequence was sampled to further guarantee the stability of the results.

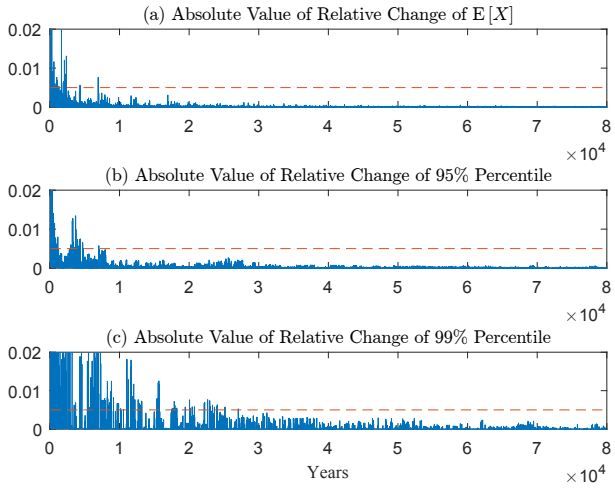

Fig. 8. Relative Changes of the Expected Value, 95% and 99% Percentiles of X to the Length of Sample Time Sequence.

In practice, the insurer gathers the risk data from the insureds in power systems and third-party investigation/survey to evaluate the tail insolvency risk with the EVT based GPD model. Then the insurer sets the insolvency probability criterion according to his/her risk attitude, and determines the price and amount of CAT bonds to sell accordingly. The indemnity of the bonds to the insurer determined by the actual total loss due to successful cyberattacks in the power system. When preset trigger points are reached, the corresponding indemnity amount is determined accordingly.

The proposed work in the paper is developed based on the concept of tail risk, and the results of the simulation also demonstrate that the cyber risks of the insureds have heavy tails in the case study. It is somehow difficult to construct a valid comparative scenario without tail risk. When the cyber risks of the insureds in power systems have not heavy tails, there will be no obvious need for the insurance providers to handle the insolvency risk in the insurance scheme, and it does not agree with current understanding and concerns on cyber risks [65], [66]. Therefore, the case without tail risk is not simulated in the case study.

V. CONCLUSION

In this paper, a CAT bond scheme is proposed for the power system cyber insurance providers to mitigate the impacts of the tail risk of power system cybersecurity. The EVT is used to model the tail and price the CAT bond. A case on the IEEE RTS-96 system is conducted to validate and demonstrate the performance of the proposed CAT bond scheme. The results demonstrate that issuing CAT bonds can efficiently reduce the tail insolvency probability even the premium is charged at a low safe loading coefficient. Generally, there is high demand for cyber insurance products. However, insurer's participation in cyber insurance market is not active, mainly due to the concern of insolvency risk. Reference [51] proposes a set of premium principles to ease this concern, but results in relatively high premiums, which would jeopardize insureds' interest in participation. In this paper, we aim to improve participation rates of both insurers and insureds by designing CAT bonds. Indeed, the case study shows that by issuing appropriate amounts of CAT bonds, the insolvency probability can be controlled at a desirable level, this benefits the insurers. Meanwhile, the premium does not have to be charged as high as revealed in [51], which benefits the insureds. It is worth noting that, although the tail insolvency probability is decreasing in the number of units of CAT bonds, the hidden cost of issuing CAT bonds prevents the insurer to issue CAT bonds without limitation. How to determine the optimal units to sell remains an open question and calls for further investigation.

REFERENCES

[1] G. N. Ericsson, "Cyber Security and Power System Communication-Essential Parts of a Smart Grid Infrastructure," *IEEE Trans. Power Deliv.*, vol. 25, no. 3, pp. 1501–1507, 2010.
[2] North American Electric Reliability Corporation (NERC), "State of Reliability 2017," NERC, Atlanta, GA, Tech. Rep., June 2017.
[3] M. M. Hossain and C. Peng, "Cyberphysical security for on-going smart grid initiatives: a survey," *IET Cyber-Physical Syst. Theory Appl.*, vol. 5, no. 3, pp. 233–244, 2020.
[4] N. Kshetri and J. Voas, "Hacking Power Grids: A Current Problem," *Computer*, vol. 50, no. 12, pp. 91–95, 2017.
[5] R. M. Lee *et al.*, "Analysis of the Cyber Attack on the Ukrainian Power Grid," E-ISAC and SANS Industrial Control Systems, Washington, DC, Tech. Rep. TLP: White, Mar. 2016.
[6] C. Glenn, D. Sterbentz, and A. Wright, "Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector," Idaho National Laboratory, Idaho Falls, ID, Tech. Rep. INL/EXT-16-40692, June 2017.

[7] C. C. Sun, A. Hahn, and C. C. Liu, "Cyber security of a power grid: State-of-the-art," *Int. J. Electr. Power Energy Syst.*, vol. 99, pp. 45–56, 2018.

[8] G. Liang, J. Zhao, F. Luo, S. R. Weller, and Z. Dong, "A Review of False Data Injection Attacks Against Modern Power Systems," *IEEE Trans. Smart Grid*, vol. 8, no. 4, pp. 1630–1638, 2017.

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

[10] N. Kshetri, "The Economics of Cyber-Insurance," *IT Prof.*, vol. 20, no. 6, pp. 9–14, 2018.

[11] P. H. Meland, I. A. Tondel, and B. Solhaug, "Mitigating Risk with Cyberinsurance," *IEEE Secur. Priv.*, vol. 13, no. 6, pp. 38–43, 2015.

[12] M. M. Khalili, P. Naghizadeh, and M. Liu, "Designing Cyber Insurance Policies: The Role of Pre-Screening and Security Interdependence," *IEEE Trans. Inf. Forensics Secur.*, vol. 13, no. 9, pp. 2226–2239, 2018.

[13] I. Vakilinia and S. Sengupta, "A Coalitional Cyber-Insurance Framework for a Common Platform," *IEEE Trans. Inf. Forensics Secur.*, vol. 14, no. 6, pp. 1526–1538, 2018.

[14] R. Pal, L. Golubchik, K. Psounis, and P. Hui, "Security Pricing as Enabler of Cyber-Insurance A First Look at Differentiated Pricing Markets," *IEEE Trans. Dependable Secur. Comput.*, vol. 16, no. 2, pp. 358–372, 2017.

[15] R. Zhang, Q. Zhu, and Y. Hayel, "A Bi-Level Game Approach to Attack-Aware Cyber Insurance of Computer Networks," *IEEE J. Sel. Areas Commun.*, vol. 35, no. 3, pp. 779–794, 2017.

[16] R. Zhang and Q. Zhu, "FlipIn: A Game-Theoretic Cyber Insurance Framework for Incentive-Compatible Cyber Risk Management of Internet of Things," *IEEE Trans. Inf. Forensics Secur.*, vol. 15, pp. 2026–2041, 2020.

[17] J. Chase, D. Niyato, P. Wang, S. Chaisiri, and R. K. L. Ko, "A Scalable Approach to Joint Cyber Insurance and Security-As-A-Service Provisioning in Cloud Computing," *IEEE Trans. Dependable Secur. Comput.*, vol. 16, no. 4, pp. 565–579, 2019.

[18] X. Lu, D. Niyato, N. Privault, H. Jiang, and P. Wang, "Managing Physical Layer Security in Wireless Cellular Networks: A Cyber Insurance Approach," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 7, pp. 1648–1661, 2018.

[19] 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.

[20] 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.

[21] D. Young, J. Lopez, M. Rice, B. Ramsey, and R. McTasney, "A framework for incorporating insurance in critical infrastructure cyber risk strategies," *Int. J. Crit. Infrastruct. Prot.*, vol. 14, pp. 43–57, 2016.

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

[23] Y. Zhang, L. Wang, Z. Liu, and W. Wei, "A Cyber-Insurance Scheme for Water Distribution Systems Considering Malicious Cyberattacks," *IEEE Trans. Inf. Forensics Secur.*, vol. 16, 2020.

[24] G. Tonn, J. P. Kesan, L. Zhang, and J. Czajkowski, "Cyber risk and insurance for transportation infrastructure," *Transp. Policy*, vol. 79, pp. 103–114, 2019.

[25] N. Liu, J. Zhang, and X. Wu, "Asset Analysis of Risk Assessment for IEC 61850-Based Power Control SystemsPart I: Methodology," *IEEE Trans. Power Deliv.*, vol. 26, no. 2, pp. 869–875, 2011.

[26] ——, "Asset Analysis of Risk Assessment for IEC 61850-Based Power Control SystemsPart II: Application in Substation," *IEEE Trans. Power Deliv.*, vol. 26, no. 2, pp. 876–881, 2011.

[27] C. W. Ten, C. C. Liu, and G. Manimaran, "Vulnerability Assessment of Cybersecurity for SCADA Systems," *IEEE Trans. Power Syst.*, vol. 23, no. 4, pp. 1836–1846, 2008.

[28] 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, 2016.

[29] K. Yamashita, C. W. Ten, Y. Rho, L. Wang, W. Wei, and A. Ginter, "Measuring Systemic Risk of Switching Attacks Based on Cybersecurity Technologies in Substations," *IEEE Trans. Power Syst.*, vol. 35, no. 6, pp. 4206–4219, 2020.

[30] C. Vellaithurai, A. Srivastava, S. Zonouz, and R. Berthier, "CPINDEX: Cyber-Physical Vulnerability Assessment for Power-Grid Infrastructures," *IEEE Trans. Smart Grid*, vol. 6, no. 2, pp. 566–575, 2015.

[31] X. Liu, M. Shahidehpour, Z. Li, X. Liu, Y. Cao, and Z. Li, "Power System Risk Assessment in Cyber Attacks Considering the Role of Protection Systems," *IEEE Trans. Smart Grid*, vol. 8, no. 2, pp. 572–580, 2017.

[32] G. Hug and J. A. Giampapa, "Vulnerability Assessment of AC State Estimation With Respect to False Data Injection Cyber-Attacks," *IEEE Trans. Smart Grid*, vol. 3, no. 3, pp. 1362–1370, 2012.

[33] J. Liang, L. Sankar, and O. Kosut, "Vulnerability Analysis and Consequences of False Data Injection Attack on Power System State Estimation," *IEEE Trans. Power Syst.*, vol. 31, no. 5, pp. 3864–3872, 2016.

[34] K. Pan, A. Teixeira, M. Cvetkovic, and P. Palensky, "Cyber Risk Analysis of Combined Data Attacks Against Power System State Estimation," *IEEE Trans. Smart Grid*, vol. 10, no. 3, pp. 3044–3056, 2019.

[35] M. D. Smith and M. E. Pate-Cornell, "Cyber Risk Analysis for a Smart Grid: How Smart is Smart Enough? A Multiarmed Bandit Approach to Cyber Security Investment," *IEEE Trans. Eng. Manag.*, vol. 65, no. 3, pp. 434–447, 2018.

[36] Q. Dai, L. Shi, and Y. Ni, "Risk Assessment for Cyberattack in Active Distribution Systems Considering the Role of Feeder Automation," *IEEE Trans. Power Syst.*, vol. 34, no. 4, pp. 3230–3240, 2019.

[37] X. Liu, M. Shahidehpour, Y. Cao, L. Wu, W. Wei, and X. Liu, "Microgrid Risk Analysis Considering the Impact of Cyber Attacks on Solar PV and ESS Control Systems," *IEEE Trans. Smart Grid*, vol. 8, no. 3, pp. 1330–1339, 2017.

[38] Y. Yang, H.-Q. Xu, L. Gao, Y.-B. Yuan, K. McLaughlin, and S. Sezer, "Multidimensional Intrusion Detection System for IEC 61850-Based SCADA Networks," *IEEE Trans. Power Deliv.*, vol. 32, no. 2, pp. 1068–1078, 2017.

[39] M. Jamei, A. Scaglione, C. Roberts, E. Stewart, S. Peisert, C. McParland, and A. McEachern, "Anomaly Detection Using Optimally Placed μPMU Sensors in Distribution Grids," *IEEE Trans. Power Syst.*, vol. 33, no. 4, pp. 3611–3623, 2018.

[40] M. Khalaf, A. Youssef, and E. El-Saadany, "Joint Detection and Mitigation of False Data Injection Attacks in AGC Systems," *IEEE Trans. Smart Grid*, vol. 10, no. 5, pp. 4985–4995, 2019.

[41] M. N. Kurt, Y. Yilmaz, and X. Wang, "Real-Time Detection of Hybrid and Stealthy Cyber-Attacks in Smart Grid," *IEEE Trans. Inf. Forensics Secur.*, vol. 14, no. 2, pp. 498–513, 2019.

[42] A. Patel and S. Purwar, "Event-triggered detection of cyberattacks on load frequency control," *IET Cyber-Physical Syst. Theory Appl.*, vol. 5, no. 3, pp. 263–273, 2020.

[43] V. K. Singh and M. Govindarasu, "A Cyber-Physical Anomaly Detection for Wide-Area Protection using Machine Learning," *IEEE Trans. Smart Grid*, vol. 12, no. 4, pp. 3514–3526, 2021.

[44] M. Touhiduzzaman, A. Hahn, and A. Srivastava, "A Diversity-based Substation Cyber Defense Strategy utilizing Coloring Games," *IEEE Trans. Smart Grid*, vol. 10, no. 5, pp. 5405–5415, 2019.

[45] Z. Zhang, S. Huang, Y. Chen, B. Li, and S. Mei, "Cyber-Physical Coordinated Risk Mitigation in Smart Grids Based on Attack-Defense Game," *IEEE Trans. Power Syst.*, Early Access, 2021.

[46] M. Chlela, D. Mascarella, G. Joos, and M. Kassouf, "Fallback Control for Isochronous Energy Storage Systems in Autonomous Microgrids Under Denial-of-Service Cyber-Attacks," *IEEE Trans. Smart Grid*, vol. 9, no. 5, pp. 4702–4711, 2018.

[47] X. Wu and A. J. Conejo, "An Efficient Tri-Level Optimization Model for Electric Grid Defense Planning," *IEEE Trans. Power Syst.*, vol. 32, no. 4, pp. 2984–2994, 2017.

[48] B. Liu and H. Wu, "Optimal Planning and Operation of Hidden Moving Target Defense for Maximal Detection Effectiveness," *IEEE Trans. Smart Grid*, vol. 12, no. 5, pp. 4447–4459, 2021.

[49] M. Bahrami, M. Fotuhi-Firuzabad, and H. Farzin, "Reliability Evaluation of Power Grids Considering Integrity Attacks Against Substation Protective IEDs," *IEEE Trans. Ind. Informatics*, vol. 16, no. 2, pp. 1035–1044, 2020.

[50] E. Naderi, S. Pazouki, and A. Asrari, "A Remedial Action Scheme Against False Data Injection Cyberattacks in Smart Transmission Systems: Application of Thyristor Controlled Series Capacitor (TCSC)," *IEEE Trans. Ind. Informatics*, Early Access, 2021.

[51] Z. Liu, W. Wei, L. Wang, C. W. Ten, and Y. Rho, "An Actuarial Framework for Power System Reliability Considering Cybersecurity Threats," *IEEE Trans. Power Syst.*, vol. 36, no. 2, pp. 851–864, 2021.

[52] Z. Yang, Y. Liu, M. Campbell, C. W. Ten, Y. Rho, L. Wang, and W. Wei, "Premium Calculation for Insurance Businesses Based on Cyber Risks in IP-Based Power Substations," *IEEE Access*, vol. 8, pp. 78 890–78 900, 2020.

[53] P. Lau, W. Wei, L. Wang, Z. Liu, and C. W. Ten, "A Cybersecurity Insurance Model for Power System Reliability Considering Optimal Defense Resource Allocation," *IEEE Trans. Smart Grid*, vol. 11, no. 5, pp. 4403–4414, 2020.

[54] J. Rosson, M. Rice, J. Lopez, and D. Fass, "Incentivizing Cyber Security Investment in the Power Sector Using An Extended Cyber Insurance Framework," *Homeland Security Affairs*, vol. 15, pp. 1–24, 2019.

[55] D. Niyato, D. T. Hoang, P. Wang, and Z. Han, "Cyber Insurance for Plug-In Electric Vehicle Charging in Vehicle-To-Grid Systems," *IEEE Netw.*, vol. 31, no. 2, pp. 38–46, 2017.

[56] D. T. Hoang, P. Wang, D. Niyato, and E. Hossain, "Charging and Discharging of Plug-In Electric Vehicles (PEVs) in Vehicle-to-Grid (V2G) Systems: A Cyber Insurance-Based Model," *IEEE Access*, vol. 5, pp. 732–754, 2017.

[57] 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.
[58] D. J. Cummins, "CAT Bonds and Other Risk-linked Securities: State of the Market and Recent Developments," *Risk Management and Insurance Review*, vol. 11, no. 1, pp. 23–47, 2008.
[59] Q. Tang and Z. Yuan, "CAT Bond Pricing under a Product Probability Measure with POT Risk Characterization," *ASTIN Bulletin*, vol. 49, no. 2, pp. 457–490, 2019.
[60] S. Wang, "Premium Calculation by Transforming the Layer Premium Density," *ASTIN Bulletin*, vol. 26, no. 1, pp. 71–92, 1996.
[61] L. De Haan and A. Ferreira, *Extreme Value Theory: An Introduction*. Berlin, Germany: Springer Science & Business Media, 2007.
[62] 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.
[63] R. Billinton and R. N. Allan, *Reliability Evaluation of Power Systems*. New York, NY: Plenum Press, 1996.
[64] Reliability Test System Task Force of the Application of Probability Methods Subcommittee, "The IEEE Reliability Test System - 1996," *IEEE Trans. Power Syst.*, vol. 14, no. 3, pp. 1010–1020, Aug. 1999.
[65] R. Böhme and G. Schwartz, "Modeling Cyber-Insurance: Towards A Unifying Framework," in *Proc. 2010 Workshop on the Economics of Information Security (WEIS)*, Cambridge, MA, 2010, pp. 1–36.
[66] T. Maillart and D. Sornette, "Heavy-tailed distribution of cyber-risks," *European Physical Journal B*, vol. 75, no. 3, pp. 357–364, 2010.