Premium Calculation for Insurance Businesses Based on Cyber Risks in IP-Based Power Substations

ZHIYUAN YANG\textsuperscript{1}, (Member, IEEE), YUN LIU\textsuperscript{2}, MEGHAN CAMPBELL\textsuperscript{3}, CHEE-WOOI TEN\textsuperscript{4}, (Senior Member, IEEE), YEONWOO RHO\textsuperscript{5}, LINGFENG WANG\textsuperscript{6}, (Senior Member, IEEE), AND WEI WEI\textsuperscript{7}

\textsuperscript{1}Guangdong Electric Power Design Institute Company, Guangzhou 510663, China
\textsuperscript{2}Quicken Loans, Detroit, MI 48226, USA
\textsuperscript{3}Mercer, Minneapolis, MN 55402, USA
\textsuperscript{4}Electrical and Computer Engineering Department, Michigan Tech, Houghton, MI 49931, USA
\textsuperscript{5}Mathematical Sciences Department, Michigan Tech, Houghton, MI 49931, USA
\textsuperscript{6}Electrical Engineering Department, University of Wisconsin–Milwaukee, Milwaukee, WI 53211, USA
\textsuperscript{7}Mathematical Sciences Department, University of Wisconsin–Milwaukee, Milwaukee, WI 53211, USA

Corresponding author: Chee-Wooi Ten (ten@mtu.edu)

This work was supported by the U.S. National Science Foundation (NSF) Cyber-Physical Systems (CPS) entitled CPS: Medium: Collaborative Research: An Actuarial Framework of Cyber Risk Management for Power Grids under Award 1739422 and Award 1739485.

ABSTRACT

Insurance is a promising risk transfer tool against switching cyberattacks on power grids that can disrupt operation and potentially lead to widespread outages. This paper emphasizes on a framework of premium calculation for cyber insurance businesses by modeling potential electronic intrusion with steady-state simulation results and its direct hypothesized impacts. The proposed actuarial framework models the operational monetary losses with the hypothesized power outages based on the cyber-reliability assessment and its expected mean time to restore power (MTTRP). The ruin probability is employed as the fundamental formula to determine the feasible insurance premium pool. Hypothesized spatial correlation studies on multiple substation contingencies associated with switching attacks have shown estimated operational losses and expected duration of power restoration, which is translated into the calculation of insurance premium. The proposed actuarial framework is validated using generalized IEEE test cases with modified parameters on substations. The potential implications of grid’s hypothetical scenarios are discussed.

INDEX TERMS  Cyber-physical system, disruptive switching attack, enterprise risk management, insurance premium, power outages, ruin probability.

I. INTRODUCTION

The rise of cyber threats in the horizon has become a critical issue for infrastructural planning [1]. The North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) compliance has now published more clauses in order to implement necessary technologies for improving the cyber awareness of information communication security across power control networks [2]–[5]. Additionally, the observed frequent attempts of intrusions within critical infrastructure networks reveal the cyber threats that the U.S power grid confronts now and the urgent need for improving cybersecurity defense protection [6], [7].

A switching attack is disruptive because the electronic manipulation on substation’s circuit breakers and disconnectors will abruptly change the system operation. The attack is undergone through the controls of compromised substation network to pivot from a console of other remote locations. Insurance is proposed to cover the economic loss and liabilities, which would incentivize utility owners to optimize their investment spending [8]–[10]. The Department of Homeland Security (DHS) National Protection and Programs Directorate (NPPD) has included stakeholders to work on the critical topics of risk management in security [11], which would help improve the security posture in terms of: (1) promoting the adoption of preventative measures; and (2) encouraging the integration of best practice of self-protection based on their existing network architectures. Insurance frameworks,
as a tool of risk transfer for utilities, are aimed to establish avoiding large infrastructure investment. A switching attack to trip substation’s circuit breakers can incur system overload and other implications. Investing more transmission lines would be an option but it can be an over-reaction in anticipating a low-probability, high-impact event. There are other alternatives to hedge the risks. Accurately modeling the consequence-based attacks can be an attractive option based on presumed switching attack and technology-investing strategies to thwart electronic intrusion from the outside network. However, this requires more understanding in the context of actuarial science and power engineering knowledge to work on the synergies of cyber-physical systems (CPS) security [12], [13].

A. UNIFYING ACTUARIAL FRAMEWORK
A unifying framework in modeling cyber insurance has been established recently to address the niche area of the CPS risks and infrastructural interdependencies [14]. It is suggested that an internal failure of information system can be modeled in a general insurance market with residual risk classification associated with security [14], [15]. From the perspective of network security, stochastic processes have been employed to model the pricing based on security risks of information and communication technology (ICT) using the network topology [13]. However, security at the user level should be also incorporated as an integral part of the overall security modeling [16], [17]. By integrating the physical impacts and mitigation strategies for a power grid with the cyber aspects, pricing for insurance premium can be estimated [18].

B. GRID SECURITY COMPLIANCE
The grid balancing authority works closely with utilities to oversee the NERC CIP compliance and establish strategies to follow those guidelines and execute plans. The audit is often done every other years and pending issues will be followed up. Spot check on any utility is randomly chosen and each utility shall establish a strategic plan to work closely in implementing the plan. Penalties may impose to non-compliant utilities after a grace period. NERC CIP does not provide standardized performance metrics to quantify residual risks associated with electronic intrusion to control network.

Most asset owners have their own way to secure their control networks [19]. The implementation of an enterprise risk management (ERM) varies, depending on organizational leadership with set priorities and allocated resources each year. The approach is to address and ensure pressing issues on the compliance list be rectified, such as password policy of their critical cyber assets and how they manage their remote access control to contractors or their temporary employees. If insurance companies can harness the digital evidence from the ERM cyber systems and hypothetically enumerate some nightmare scenarios to replay the cascading outcomes, the consequence-based assessment would help to mature this emerging market. The risk theory can provide the quintessential basis to most insurance models and problems [20]. Estimating risks can be calculated using the ruin probability from the direct calculation method, which is known to be the basic risk model [20]–[23]. Assessment of risk and its profiles and its assessment on operational performance on computerized management system are proposed to address the SCADA aspect of feeder automation in distribution networks [24]. Such risk profile could take into account of electronic and physical perimeters where the critical cyber assets are deployed.

C. CONTRIBUTIONS TO CPS-RELATED INSURANCE
This paper proposes an actuarial framework for grid insurance with policies protecting deployed cyberinfrastructure against electronic manipulation of circuit breakers via a remote access intrusion to electrically disconnect substation off grid, known as “disruptive switching attacks,” which isolates all connected lines, local loads and generating units. This is assumed to be determined by two major aspects: (i) the probability of successful intrusion into the substation(s) which will presumably result in disruptive switching attack from the compromised substation(s) and (ii) the discrete distribution of claim size of each potential attack scenario [21]–[23]. The vulnerability and the steady-state probability of potential electronic intrusion to each power substation have been studied in the papers [25], [26], which are derived from the firewall and password models using Markov chain. The steady-state probabilities [25], [27] are further updated introducing protective intelligent electronic devices (IED) models and honeynet models, and utilized as an effective tool to generate the discrete distribution of the hypothesized scenario. The proposed claim size of power utilities is assumed to be equal to the estimated economic loss that is directly related to substation outages. To address the impact of the hypothesized cyberattacks, following assumptions are included in the proposed framework:

- The risk index studies [28]–[31], using the extended combination method and reverse pyramid model (RPM), generate the risk-based “bottleneck list.” The “critical” combinations would lead to the potential uncertainty with identified unstable cases of the power system in steady-state analysis. The definition of “unstable” refers to power flow diverged solutions for the combinations of multiple substation outages using the RPM models [31].
- The surveys on the operational loss [32]–[34] and the electricity prices [35], [36] are included in the paper to conduct a comparative study of the economic loss of the hypothesized power outages. It is assumed that the operational loss discussed in the paper only covers the direct loss that has been studied in [32]–[34].
- The studies on the mean time to restore power (MTTRP) [37]–[39] of the hypothesized power system outages are also performed, which estimate the expected restoring time of a system after a presumed switching cyberattack. Deriving from the previous model [29]–[31], the hypothesized substation outages have been incorporated with
overload implications of transmission lines. The extended enumerations on the substation outage contingencies by hypothesized switching attacks would electrically disconnect associated transmission lines, generators, and transformers. The permanent damage induced by cyberattacks are not covered in this work. This proposed insurance-based solution would help to formulate an actuarial framework to transfer the cyber risk of potential substation compromise. 

The paper is organized as follows. Section II illustrates the probability and the distribution of the cyber insurance model using the developed cyber and physical components. Section III provides the calculation details of the ruin probability based on the risk model. Section IV demonstrates the numerical results. Section V summarizes and concludes with future research opportunities.

II. PROBABILITY DISTRIBUTION BASED ON CYBER-RELIABILITY ASSESSMENT MODEL

A. PROBABILITY MASS DISTRIBUTION OF THE HYPOTHESIZED SCENARIO

The vulnerability of the control networks has been evaluated by modeling intrusions and consequences of a cyberattack on control networks [25], [26]. Assuming that the system contains $S$ substations and the substations set is denoted as $S_{\text{sub}} = \{1, 2, \ldots, S\}$. Let $T$ be the substations collection of all non-empty elements with the index of $t$, where each element in the collection $T$ is a tuple, denoted as $T$, which satisfies $T \subseteq S_{\text{sub}}$. Let’s assume substation collection $T$ consists of all $k$-combinations of $S$ with $k = 1, 2, \ldots, S$. The probability of the $t$-th substation combination $p(t, x_t)$ is defined as:

$$
\tilde{p}(t, x_t) = \left( \prod_{i \in T} \rho_i \right) \left[ \prod_{j \in S_{\text{sub}}, j \notin T} (1 - \rho_j) \right] 
$$

(1)

where $i$ and $j$ in (1) denote the indices of substations, and $\rho_i$ denotes the intrusion probability to substation $i$ that additionally denotes the claim size of the $t$-th substation combination. The cardinality $|T|$ of set $T$ is equal to $2^S - 1$, and the sum of the probability $\tilde{p}(t, x_t)$ calculated in (1) may not necessarily be equal to 1. As a consequence, the probability mass function of the discrete substation combination can be normalized that will be summed up to 1.0:

$$
p(t, x_t) = \frac{\tilde{p}(t, x_t)}{\sum_{i=1}^{\text{|T|}} \tilde{p}(t, x_t)}
$$

(2)

Equation (2) formulates the basic discrete probability distribution of hypothesized substation outages. The $p(t, x_t)$ is the function of $t$ in which it cannot be directly applied to the premium calculations because the different substation outages could claim the same size of economic loss. The following section would further illustrate the formulation of the claim size and the necessary modifications to (2).

B. THE CLAIM SIZE OF THE HYPOTHESIZED SUBSTATION OUTAGES

Determining the claim size due to the hypothesized substation outage is important for insurance companies to implement their insurance policy because of the direct effect on their own business strategy. In the following formulation, the data is obtained from the previous cyber-based contingency analysis in the steady-state studies [28]–[31] and the claim size $x$ is assumed to be equal to the direct loss due to the hypothesized power outages, which is determined by three variables:

1) the power loss $PL$ (MW) due to the substation outages in steady-state evaluation [28]–[31],
2) the expected mean time to restore power $H$ (hour) from the abnormal status to normal steady-state conditions [37]–[39], and
3) the direct costs $\gamma$ ($/MWh$) during the power outages [32]–[34].

Thus, the claim size $x_t$ ($) for the $t$-th substation combination is defined as:

$$
x_t = PL_t \cdot H_t \cdot \gamma
$$

(3)

Figure 1 depicts the flowchart of an enumerative algorithm for calculating the claim size based on (3). The “critical” lists $C$ is generated using the extended enumeration model in [31]. The “critical” combination of substation(s) recorded in $C$ may cause system unstable in the steady-state analysis,
which is considered as the blackout situation in this formulation. The critical list $C$ is applied here to identify the size of blackouts of the substations combination set $T \in T$. The MTTRP simulation is conducted based on the concept of generic restoration milestones (GRMs) [37]. The italicised MTTRP represents the vector that records the restoration time of each substation and $L$ is the total restoration time initiated from the black start units. It should be noted that the claim size in the premium calculations in this paper are based on mean claim sizes for a given combination of substation outages. This leads that different combination sets $t_1$ and $t_2$ that may have the different $p(t_1, x_{t_1})$ and $p(t_2, x_{t_2})$ but share the same claim size; that is, $x_{t_1} = x_{t_2}$. In order to create the probability mass function of the claim size $x_i$, which the cyber insurance company focuses on, the probability distribution function determined in the (2) needs to be modified by aggregating all $p(t_i, x_i)$ that have the same claim size:

$$p(x) = \sum_{t_i \in T \mid x_i = x} p(t_i, x_i)$$ (4)

Equation (4) formulates the PMF of the diverse claim sizes $x_i$ and the variable $t$ has been canceled out. Compared with (2), (4) is more clear and convenient to be applied in the ruin probability calculations to determine the insurance premium.

III. DETERMINATION OF CYBER INSURANCE PREMIUM USING RUIN THEORY

A. RUIN PROBABILITY CALCULATION

Ruin theory has been widely implemented since the beginning of last century and has demonstrated its effectiveness in evaluating the long-run viability of insurance portfolios [21]–[23]. In actuarial context, ruin refers to the event that the surplus of a business unit goes below zero. Ruin probability is thus used to measure the riskiness of a business line. In this section, this concept shall be applied to study the insurer’s financial position and appropriate the amount of premium so as to control the insurer’s ruin probability at a low level.

The mathematical model is formulated as follows. Suppose an insurer covers all the cyber-related losses from an accident and receives claims according to a Poisson process $N(t)$ with arrival intensity $\lambda$. Assume the claim sizes $\{Y_1, Y_2, \ldots\}$ are independent and have a common distribution as $Y$, whose distribution is specified by formula (4). Furthermore, the insurance premium is charged with a safe loading coefficient of $\theta$. That is, the premium charged over a time period of length $t$ equals the expected value of the total claim over the period plus a safe loading, or mathematically $(1 + \theta)\lambda \mu t$, where $\mu = E[Y]$. With an initial reserve of $u$, the insurer’s surplus at time $t$ is represented as

$$U_t = u + (1 + \theta)\lambda \mu t - \sum_{i=1}^{N(t)} Y_i.$$ (5)

The ruin probability, depending on $u$, is defined to be $\psi(u) = P(\inf_{t \geq 0} U_t < 0)$. Readers are referred to [40] for a comprehensive review of ruin theory. Generally, ruin probability may be difficult to obtain. With a compound Poisson setup as specified in the above model, the calculation of ruin probability can be related to the calculation of a compound geometric aggregate loss model, as seen in [21].

Following [21], consider the independent and identically distributed (i.i.d.) ladder heights $L_1, L_2, \ldots$ of Model (5), that is, the sizes of drops of $U_t$. When these drops aggregate to exceed the initial reserve $u$, ruin occurs. In this sense, the ruin probability can be expressed as $\psi(u) = P(M > u)$, where the maximum aggregate loss $M$ is defined as

$$M = L_1 + L_2 + \cdots + L_N,$$

where $N$ is the number of drops, following a geometric distribution with parameter $q = \psi(0) = 1/(1 + \theta)$. Furthermore, the probability density function of the common drop size $L$ can be obtained based on the distributional information of $Y$ as follows:

$$f_L(x) = \frac{1 - F_Y(x)}{\mu}$$ (6)

Note that the distribution of $L$ is continuous. In order to derive a recursive formula to compute the ruin probability, the distribution of $L$ has to be discretized. The discretization can be realized in different ways. Here, we follow the moment matching approach provided by [21]. Specifically, set a step size $h$ such that $u/h$ is an integer and assume a distribution on $[0, h, 2h, \ldots]$ with probabilities $\{f_x : x = 0, 1, 2, \ldots\}$ to be solved from the following system so as to match the range probabilities and the first two moments to the original distribution of $L$:

$$\begin{bmatrix}
1 & 1 & 1 & f_k \\
kh & (k+1)h & (k+2)h & f_{k+1} \\
k^2h^2 & (k+1)^2h^2 & (k+2)^2h^2 & f_{k+2}
\end{bmatrix}
+ \begin{bmatrix}
f_kh \\
f_kh \\
f_kh
\end{bmatrix}
\begin{bmatrix}
f_{xL}(x)dx \\
f_{xL}(x)dx \\
x^2f_{xL}(x)dx
\end{bmatrix}.$$ (7)

Based on the above discretization, [21] provides a recursive formula to compute the ruin probability $\psi(u) = P(M > u)$:

$$\psi(u) = 1 - \frac{\sum_{k=1}^{u/h} f_k}{1 + \theta - f_0} - \frac{1}{1 + \theta - f_0} \sum_{y=1}^{u/h} f_y \cdot \psi(u - y).$$ (8)

B. PREMIUM CALCULATION USING RUIN THEORY

Based on the details of ruin probability calculation in previous section, the premium amount, $I$, is defined [40]:

$$I = (1 + \theta f)\lambda \mu$$ (10)

where $\theta_f$ is the feasible premium loading that can be identified in the ruin probability calculation. The lambda $\lambda$ denotes the expected number of claims of the process and can be obtained by using (1). Compared with the traditional insurance policy, the frequency of claims for the cyber insurance
on the power system outage may be much less because of its low occurrence in the historical data. The mean $\mu$ is the mean of the successive claims that can be derived through (2) and (6). Additionally, $\theta_l$ may not be unique if the insurance company provides an acceptable range of ruin probabilities, which would affect the range of $\theta$ and the feasible premium amount. In Section IV, we provide a list of the feasible ruin probabilities with different choices of $\theta$'s and different settings of initial reserve $u$.

C. SPATIAL CORRELATION VERIFICATION
The proposed model incorporates the assumption of spatial correlation with two layers:

1) at the attack stage, which is at the cyber level,
2) at the enumeration stage, which is at the physical level and it is based on its presumed resulting impacts.

The second level of spatial correlation has been addressed in the steady-state enumeration model, which identifies the “critical” substation combination outages and assume it as diverged case with the highest claim size. In the actuarial framework, the variable of severity losses have been incorporated into the mean of claim sizes $\mu$ in (10). It is noticed that the variable $\mu$ includes a high correlation ratio for diverged cases. For example, let the substation $s$, where $s \in S_{sub}$, has been identified pivotal substation in steady-state analysis. From (3), the claim size $x$ of all events of substation outages that contain $s$ would be diverged and aligned with the same highest claim size, which would be reflected in the mean of claims sizes $\mu$. For this reason, the highly dependent correlation among those diverged events have been verified in terms of claim sizes.

For the first layer of spatial correlation at attack level. We assume outside attacks occur from control center networks [25] and different control networks would be deployed with diverse cybersecurity technologies. Let $SN_l$ denote the set of substations that can be accessed through sub-network $l$. It is assumed $L$ sub-networks are deployed in the system. For the substations in different sub-network $SN_l$ and $SN_{l+1}$, the intrusion probability on these two sets are independent while within the sub-network, the intrusion probability would be dependent with a correlation ratio. Let’s denote binary results 1 and 0 in a Bernoulli trial be the successful and failure intrusion attempt accordingly. The expected number of claims of the process $\lambda$ without the spatial correlation assumption is defined:

$$\lambda = 1 - P(X_1 = 0, X_2 = 0, \cdots, X_S = 0)$$
$$= 1 - (1 - \rho(1))(1 - \rho(2)) \cdots (1 - \rho(S))$$

(11)

In contrast, in an extreme case with correlation ratio 1 within each sub-network, the $\lambda$ is modified as:

$$\hat{\lambda} = 1 - \left(1 - \hat{\rho}(SN_1)\right)\left(1 - \hat{\rho}(SN_2)\right) \cdots \left(1 - \hat{\rho}(SN_L)\right)$$

(12)

In (12), $\hat{\lambda}$ denotes the expected number of claims with spatial correlation assumption. The $\hat{\rho}(\cdot)$ represents the probability of intrusions on the substation in the set $SN_l$.

Since the number $L$ of sub-network would be less than the substation number $S$, it can be easily seen that $\hat{\lambda} < \lambda$, if $\hat{\rho}(\cdot) \leq \rho(\cdot)$. This means that the probability of no claims within the insurance contract period becomes smaller in the existence of strong correlations in the cyber-systems within each sub-network and of strong cyber defense systems. This iterates the importance of discarding weak cyber defense systems and placing stronger systems on more critical substations in lowering insurance premium. This implies that using a smaller number of cyber defense systems can be cost-effective, so long as those in use are the strongest possible ones.

IV. NUMERICAL ILLUSTRATION
A. TEST CASE SETUP
1) STEADY-STATE PROBABILITIES
The steady-state probabilities for substation attacks are derived according to the proposed procedure that is demonstrated in [27]. For each substation, it is assumed that 4 firewalls and 6 machines are deployed in the cyber-net, and for each firewall rule, the probability of packets passing through is randomly selected from assumed probabilities $[0.0096, 0.0049, 0.0080, 0.0014]$. The firewall execution rate is assumed to be 0.001. of “Model 1” and “Model 3” from “outside” attack in [25], denoted as $\pi_1$ and $\pi_3$, respectively. Notice that $\pi_1 \in \Pi_1$ and $\pi_3 \in \Pi_3$, where $\Pi_1$ and $\Pi_3$ are two probability sets for different models.

In order to improve the feasibility of the model, the authors also assume that the substations with generation units installed are deployed with more secure protective parameters, which would lead to a higher rate of packets rejection. For example, in the IEEE 14-bus system (10 substations), substations 1 and 2 are equipped with firewalls which are in lower probabilities of being compromised, i.e., $\pi(1) = 0.00034856$ and $\pi(2) = 0.00038848$. In the IEEE 30-bus system (24 substations), substations 1, 2, 4, 17, 18 and 22 are connected with generation unit, which would be assigned with lower probabilities. Similarly, substations 1, 2, 3, 6, 8, 9 and 12 in the IEEE 57-bus system are with lower probabilities of successful intrusion.

It is observed that substations 1 and 2 are equipped with generators which are in lower probabilities of being compromised, i.e., $\pi(1) = 0.0034856$ and $\pi(2) = 0.0038848$. In the IEEE 30-bus system (24 substations), substations 1, 2, 4, 17, 18 and 22 are connected with generation unit, which would be assigned with lower probabilities. Similarly, substations 1, 2, 3, 6, 8, 9 and 12 in the IEEE 57-bus system are with lower probabilities of successful intrusion.

2) CRITICAL LIST OF HYPOTHESIZED SUBSTATION OUTAGES
The critical list $C$ is derived using the extended RPM [31], which enumerates all the hypothesized substations and their combined, and the “worst” combinations are identified. The extended reverse pyramid model (RPM) [29] is applied to identify the critical substations and “worst-case” substation combinations. The extended RPM applies a steady-state approach to enumerate all events of hypothesized substations
FIGURE 2. The summary of intrusion probabilities and the expected mean time to restore power for IEEE test cases. Note: figures in brackets denote the number of relay settings for the corresponding relay.

outage combinations. Additionally, the overload implications of transmission lines are incorporated in the model. In the 14-bus system, 3 “critical” substations are identified, which are substation 2, 4 and 5. There are 8 substations identified be critical in the 30-bus system, which are substation 2, 4, 5, 6, 10, 17, 20 and 22. Similarly, in the 57- and the 118-bus system, 18 and 42 “critical” substations are found, which may lead the system diverged in terms of steady-state analysis.

Based on the critical list, the complete combination list $T$ would be determined to identify the hypothesized power outages. In this study, the threshold of intrusion attempts per year is assumed within the interval [8000, 10000], every single attack is assumed to be independent. Figure 2 gives the detailed settings of the successful intrusion probability for each system, highlighted in blue bar and based on the left-side axis. The generic restoration milestones (GRMs) have been applied in this paper to estimate the expected mean time to restore power (MTTRP) [37]. The GRMs introduces a practical method for construction of system restoration process by applying numerous constraints on status-assessment, optimization of generation outputs, and load pickup. The GRMs consists of six major thrusts and each process contains an objective function with different constraint settings. MTTRP simulations demonstrate that it takes 3, 6, 3 and 8 steps to restore 14-, 30-, 57-, and 118-bus systems respectively, which cost 118, 404, 373, and 414 minutes in total. In Fig. 2, the expected restoration time $H$ of each system is marked in red based on the right-side axis.

B. NUMERICAL RESULTS OF RUIN PROBABILITY AND PREMIUM AMOUNT

In this simulation part, the direct operational costs $\gamma$ ($/MWh) incurred by the hypothesized substation outage are extracted from four different studies: 1) the studies on value of loss load (VOLL) [33], [34]; 2) the surveys on the estimated direct costs (DC) in the previous power outage [32]; 3) the statistical studies of the average retail electricity price (AREP) [35]; and 4) the basic local marginal price (LMP) from the optimal power flow (OPF) solution [41]. Based on the results of the contingency analysis $C$ and the MTTRP simulations, the operational loss of substations, denoted as $\gamma_1-4$ and with four colors shown in Fig. 3.

By combining (6), (7) and (9), the results of ruin probability and the corresponding feasible premium amounts are summarized in Table 1. In the table, $\theta$ is selected from 0 to 1 with the increment of 0.2. The initial reserve $u$ are selected among 0, 10 and 100, which, refer to (7), would determine the recursive level for calculating the ruin probability $\psi$. It is observed that, when $u$ is 0, (7) could be written as $\psi(0) = (1 - f_0)/(1 + \theta - f_0)$, which only involves the first iteration. In the row of “System constants,” parameter $\lambda$ denotes the
frequency of the claim that have been formulated through \( (1) \), which is 0.019537, 0.080008, 0.062407, and 0.094434 in the 14-, 30-, 57-, and 118-bus systems, respectively. It is observed that in \( (7) \), variable \( h \) denotes the general increment for each global moment, here the authors consider the formulation of the proposed problem as a two-moment process which would optimally cover the whole interval of the claim size. It indicates that each interval would cover half of the claim size. To distinguish the general increment \( h \), \( h' \) is introduced as the proportion of the coverage.

From Table 1, among all the test systems, \( \psi(0) \) is always larger than 0.75. It might be “too risky” and may not be an acceptable probability. Additionally, it is found that the ruin probability \( \psi(u) \) in each case would be decreasing with \( \theta \)
increased, which coincides with (7). Consider \( \psi(0)' \) with a larger \( \theta' \) and \( \psi(0)'' \) with a smaller \( \theta'' \), it can be calculated that for the first ruin probability, it holds: \( \psi(0)' < \psi(0)'' \). Since the \( \psi(u) \) is calculated recursively based on the first item \( \psi(0) \), then the probability of \( \psi(u)' \) with a larger \( \theta \) would be eventually smaller than \( \psi(u)'' \). Therefore, \( \psi(u) \) is a decreasing function as \( \theta \) increases. For this reason, the authors are able to give a reasonable guess of certain ruin probability even without a determined value of \( \theta \). Take the calculation results of IEEE 30-bus system as an example, even though the ruin probability \( \psi(10) \) under the condition of \( \theta = 0.9 \) is not provided, it is reasonable to conclude that the probability \( \psi(10) \) would locate the interval \([4.175 \times 10^{-3}, 1.790 \times 10^{-3}]\), which are the lower and upper bounds of the probability detailed in the table when \( \theta = 0.8 \) and 1.0.

According to (10), Table 1 also provides estimated premium amounts for each IEEE test system with different settings of \( \gamma \), where \( \theta_f \) is assumed to be 0.8. In a more general case, for example, if the insurance company would be able to accept the ruin probability that less than \( 5.0 \times 10^{-3} \) for the 57-bus system, with the initial reserve settings of 10 and cost settings of \( \gamma_i \), the feasible set of \( \theta \) can be determined from the table: [0.6, 1.0]. Based on (10), the feasible premium interval \([I', I'']\) could be determined as \([$1,740,518, $2,175,648]\), where \( I' \) and \( I'' \) denote the lower and upper bound of the premium \( I \) accordingly. From (7), \( \psi(0) = \theta/(1 + \theta) \) is determined as survival probability [40]. It is observed that the survival probability would increase as the premium loading \( \theta \) increases. In other words, the insurance company sells more expensive policies to utilities, as premium loading increased, which would accordingly increase their survival probability.

### C. Sensitivity Analysis and Spatial Correlation Study

According to (3) and (4), the premium amount is calculated from two fundamental variables, the probability and the claim size of each event. For this reason, a comparison study is conducted in this section by allowing only one of the variable changes with a ratio and keep another variable constant. Figure 4 represents changes of premium amount, mean MTTRP, and maximum insurance claims corresponding to diverse system settings of generator ramping capacity, bus loads, and steady-state probability using the IEEE 30-bus system. The setting of economic cost \( \gamma \) is selected as VOLL. With the reference of initial power flow solution, the coefficient ratio is within the interval of [50%, 200%], which is assumed to be an acceptable threshold for the key parameters such as probability, ramping rate, and load. It is observed that in the sub-figure (a), premium amounts of all three conditions are the same if the coefficient is set with 1.0. It can be observed that raising the ramping rate would decrease the premium by reducing MTTRP, which directly decreases the claims size for each case. The premium amount increases most rapidly on the condition of the changes of the steady-state probability, which can be estimated from the (10) that the premium changes linearly with the expected number of claims \( \lambda \). Increasing the steady-state probability would directly increase \( \lambda \), which raises the premium level as shown in the sub-figure (a).

Sub-figure (b) gives a rough estimation by describing the relationship between the mean MTTRP and claim sizes under different coefficient conditions. The black coordinate axis at the left side denotes the mean of MTTRP and the right side color in blue represents the maximum insurance claims. As revealed from the sub-figure (b), in both conditions such as changes of ramping capacity and bus load, the claim size and MTTRP are highly correlated, which corresponds to the (3). As depicted in the sub-figure (a), the premium decreases as the loading condition increase from 120% to 150% which can be extrapolated from sub-figure (b), where the claim size decreases as the MTTRP decreases from this change. Specifically, it is observed that the GRMs simulation model takes a few steps and less time to recover the system at the 150% loading condition compared with the restoration time at the condition of 120%. Although the system load increases from condition of 120% to 150%, the MTTRP has decreased, which would balance the claim size and premium in general.

The spatial correlation study is summarized in the Table 2. It is assumed that four different sub-networks are deployed in the control center of the IEEE 30-bus system with detailed correlation ratio given in each network. The joint probability

![Figure 4](image-url)
The matrix can be user-defined and would generate different other 6 diagonal elements would be set as 1. The correlation diagonal elements in the correlation matrix would be 0.05 and dimension of the correlation matrix is 6 by 6 and all 30 off-
and premium are. As demonstrated in (12), the probability of interesting that the stronger the correlation is, the smaller with corresponding premium, as summarized in the table. It is determined by the size of
are zero. The dimension of the correlation matrix would be 30-bus system.

| Correlation settings of different control networks | \( \lambda \) | Premium |
|---------------------------------------------------|-------------|---------|
| \( SN_1\) | \( SN_3\) | \( SN_3\) | \( SN_4\) | | |
| 0.05 | 0.05 | 0.05 | 0.05 | 0.0756 | $797,289 |
| 0.05 | 0.05 | 0.10 | 0.10 | 0.0729 | $796,158 |
| 0.10 | 0.10 | 0.10 | 0.10 | 0.0704 | $777,717 |
| 0.10 | 0.20 | 0.10 | 0.20 | 0.0666 | $755,972 |
| 0.10 | 0.10 | 0.30 | 0.30 | 0.0592 | $690,916 |
| 0.10 | 0.10 | 0.30 | 0.40 | 0.0585 | $653,571 |
| 0.10 | 0.10 | 0.40 | 0.40 | 0.0574 | $662,082 |
| 0.15 | 0.15 | 0.30 | 0.40 | 0.0560 | $634,538 |
| 0.15 | 0.15 | 0.40 | 0.40 | 0.0559 | $658,564 |
| 0.20 | 0.20 | 0.40 | 0.40 | 0.0543 | $666,747 |
| 0.30 | 0.30 | 0.40 | 0.40 | 0.0513 | $645,904 |
| 0.30 | 0.40 | 0.30 | 0.60 | 0.0488 | $645,904 |
| 0.40 | 0.40 | 0.60 | 0.60 | 0.0480 | $632,767 |
| 0.40 | 0.50 | 0.60 | 0.80 | 0.0462 | $517,443 |

with dependent Bernoulli trials\(^1\) are generated through the Monte Carlo method with 10,000 trials [42], [43]. The spatial correlation for each sub-network is introduced as the off-

diagonal elements of its correlation matrix. In contrast, in the case of independent Bernoulli trials, all off-diagonal elements are zero. The dimension of the correlation matrix would be determined by the size of \( SN_1 \). For example, in the first row, the \( SN_1 \) represents the substation 1 to substation 6, thus the dimension of the correlation matrix is 6 by 6 and all 30 off-
diagonal elements in the correlation matrix would be 0.05 and other 6 diagonal elements would be set as 1. The correlation matrix can be user-defined and would generate different \( \lambda \) with corresponding premium, as summarized in the table. It is interesting that the stronger the correlation is, the smaller \( \lambda \) and premium are. As demonstrated in (12), the probability of zero claims, \( 1 - \hat{\lambda} \), would also increase.

V. CONCLUDING REMARKS
The preliminary establishment on cyber insurance premium using IEEE test cases has demonstrated the promise of actuary and correlation of problematic combinations of disruptive switching cyberattacks. The studies provide the simulation results of steady-state probability and its distribution function, the expected MTTRP for each substation, and the diverse settings of estimated operation loss. All factors provided here are the necessary setups to calculate the ruin probability. With detailed and numerous cases provided in the studies, the insurance companies can formulate the feasible premium amounts based on their owner-defined conditions and their base cases. Future work includes detailing the consequential events and their stochasticity, and how they may lead to brownout and/or blackout as well as establishing new models for security technologies. The results shown in the case study are based on the proposed model, the detailed sensitivity analysis can incorporate specified settings with regulatory issues can be elaborated in future research. This includes extensive analysis between probability and the claim size that can be further enhanced to incorporate other electrical settings, such as, ramping rates of generating units and variation of loading level.

ACKNOWLEDGMENT
The authors would like to thank Prof. Yunhe Hou of The University of Hong Kong to provide the GRM model in order to complete the study of the proposed premium model and Mr. Koji Yamashita for the insightful discussions on practical deployment of microprocessor-based protective relaying in IP-based substations.

REFERENCES

[1] Idaho National Laboratory. (Aug. 2016). Mission Support Center Analysis Report: Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector. [Online]. Available: https://www.energy.gov/sites/prod/files/2017/01/f34/Cyber%20Threat%20and%20Vulnerability%20Analysis%20of%20the%20U.S.%20Electric%20Sector.pdf

[2] Office of the Press Secretary and T. W. House. Executive Order—Commission on Enhancing National Cybersecurity. Accessed: Feb. 9, 2016. [Online]. Available: https://www.whitehouse.gov/the-press-office/2016/02/09/executive-order-commission-enhancing-national-cybersecurity

[3] NERC Board of Trustees. (May 2012). Cyber Attack Task Force: Final Report. [Online]. Available: http://www.nerc.com/docs/cip/catf/12-CATF_Final_Report_BOT_clean_Mar_26%202012-Board%20Accepted%200525.pdf

[4] NERC Board of Trustees. (May 2017). Reliability Standards for the Bulk Electric Systems of North America. [Online]. Available: http://www.nerc.com/pa/Stand/ReliabilityStandardsCompleteSet/RSCompleteSet.pdf

[5] NERC. Reliability Concepts. Accessed: Dec. 19, 2007. [Online]. Available: https://www.nerc.com/files/concepts_v1.0.2.pdf

[6] N. Archives, “Executive order 13636: Improving critical infrastructure cybersecurity,” Federal Register, vol. 78, no. 33, pp. 1–8, Feb. 19, 2013.

[7] National Institute of Standards and Technology. (Jun. 21, 2005). Cybersecurity Framework. [Online]. Available: https://www.nist.gov/sites/default/files/documents/8t/preliminary-cybersecurity-framework.pdf

[8] W. S. Baer and A. Parkinson, “Cyberinsurance in IT security management,” IEEE Secur. Priv. Mag., vol. 5, no. 3, pp. 50–56, May 2007.

[9] U.S. Department of Energy and the Critical Infrastructure Protection Program of George Mason University School of Law. (Jun. 21, 2005). Insurance and the Nation’s Electrical Infrastructure: Mutual Understanding and Maturing Relationships. George Mason University School of Law, Arlington, VA, USA. [Online]. Available: https://cip.gmu.edu/wp-content/uploads/2016/06/CIPHS_Insurance-and-the-Nations-Electrical-Infrastructure_White-Paper.pdf

[10] E. Network and I. S. Agency. Incentives and Barriers of the Cyber Insurance Market in Europe. Accessed: Jun. 28, 2012. [Online]. Available: http://www.biztosiaszemsze.hu/files/201207/cyber_insurance_market.pdf

[11] U.S. Department of Homeland Security. Cybersecurity Insurance. [Online]. Available: https://www.dhs.gov/cybersecurity-insurance

[12] P. H. Meland, I. A. Tondel, and B. Solhaug, “Mitigating risk with cyberinsurance,” IEEE Secur. Privacy, vol. 13, no. 6, pp. 38–43, Nov. 2015.

[13] M. Xu and L. Hua. Cybersecurity Insurance: Modeling and Pricing. Accessed: Mar. 2017. [Online]. Available: https://www.soa.org/Files/Research/Projects/cybersecurity-insurance-report.pdf

[14] R. Böhme and G. Schwartz, “Modeling cyberinsurance: Towards a unifying framework,” in Proc. Workshop Econ. Inf. Secur. (WEIS). Cambridge, MA, USA: Harvard Univ., Jun. 2010, pp. 1–36.

[15] R. Böhme and G. Kataria, “Models and measures for correlation in cyberinsurance,” in Proc. Workshop Econ. Inf. Secur. (WEIS). Cambridge, MA, USA: Univ. of Cambridge, Jun. 2006, pp. 1–26.

\(^1\)These trials are based on probability theory in statistics where a randomized generator with two binary outcomes, i.e., either it is “success” state or “failure,” which shows the probability of success is the same as every randomly generated sample.
[16] N. Shetty, G. Schwartz, M. Felegyhazi, and J. Walrand, “Competitive cyber-insurance and Internet security,” in Proc. Econ. Inf. Secur. Privacy, T. Moore, D. Pym, and C. Ioannidis, Eds. Boston, MA, USA: Springer, 2010, pp. 229–247.

[17] G. Schwartz, N. Shetty, and J. Walrand, “Cyber-insurance: Missing market driven by user heterogeneity,” in Proc. Workshop Econ. Inf. Secur. (WEIS), Cambridge, MA, USA: Harvard Univ., Jun. 2010, pp. 1–17.

[18] D. O. Energy, Electric Grid Security and Resilience: Establishing a Baseline for Adversarial Threats. Accessed: Jun. 2016. [Online]. Available: https://www.energy.gov/sites/prod/files/2017/01/f14/Electric%20Grid%20Security%20and%20Resilience-Establishing%20Baseline%20for%20Adversarial%20Threats.pdf

[19] U.S. Department of Homeland Security. (2014). Insurance for Cyber-Related Critical Infrastructure Loss: Key Issues. Insurance Industry Working Session Readout Report. [Online]. Available: https://www.dhs.gov/sites/default/files/publications/July%202014%20In%20%20Industry%20Working%20Session%201.pdf

[20] P. Embrechts, C. Klüppelberg, and T. Mikosch, Risk Theory. Berlin, Germany: Springer, 1997, pp. 21–57, doi: 10.1007/978-3-642-33483-2_2.

[21] H. H. Panjer, “Direct calculation of ruin probabilities,” J. Risk Insurance, vol. 53, no. 3, pp. 521–529, Sept. 1986.

[22] T. Pentikainen, “The theory of risk and some applications,” J. Risk Insurance, vol. 47, no. 1, pp. 16–43, Mar. 1989.

[23] F. Dufresne and H. U. Gerber, “Three methods to calculate the probability of ruin,” ASTIN Bull., vol. 19, no. 1, pp. 71–90, Apr. 1989.

[24] 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, Jul. 2019.

[25] 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, Nov. 2008.

[26] C.-W. Ten, C.-C. Liu, and M. Govindarasu, “Vulnerability assessment of cybersecurity for SCADA systems using attack trees,” in Proc. IEEE Power Eng. Soc. Gen. Meeting, Jun. 2007, pp. 1–8.

[27] 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., to be published.

[28] R. Bulbul, Y. Gong, C.-W. Ten, A. Ginter, and S. Mei, “Impact quantification of hypothesized attack scenarios on bus differential relays,” in Proc. Power Syst. Comput. Conf., Wroclaw, Poland, Aug. 2014, pp. 1–7.

[29] C.-W. Ten, A. Ginter, and R. Bulbul, “Cyber-based contingency analysis,” IEEE Trans. Power Syst., vol. 31, no. 4, pp. 3040–3050, Jul. 2016.

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

[31] Z. Yang, C.-W. Ten, and A. Ginter, “Extended enumeration of hypothesized substations outages incorporating overload implication,” IEEE Trans. Smart Grid, vol. 9, no. 6, pp. 6029–6038, Nov. 2018.

[32] U.S. Congress, Office of Technology Assessment. (Jun. 1990). Physical Vulnerability of Electric System to Natural Disasters and Sabotage. OTA-E-453, Washington, DC, USA. Government Printing Office. [Online]. Available: http://ota.fas.org/reports/9034.pdf

[33] K. K. Kariuki and R. N. Allan, “Evaluation of reliability worth and value of lost load,” IEEE Proc.: Gener., Transmiss. Distrib., vol. 143, no. 2, pp. 171–180, Mar. 1996.

[34] London Economics International LLC. Estimating the Value of Lost Load. Accessed: Jun. 17, 2013. [Online]. Available: http://www.ercot.com/content/gridinfo/resource/2015/mktanalysis/ERCOT_ValueofLostLoad_LiteratureReviewandMacroeconomic.pdf

[35] Statista. (2018). Average Retail Electricity Prices in the U.S. From 1990 to 2017 (in U.S. Cents Per Kilowatt Hour). [Online]. Available: https://www.statista.com/statistics/183700/us-average-retail-electricity-price-since-1990/

[36] R. A. Ponrajah and F. D. Galiana, “Derivation and applications of optimum bus incremental costs in power system operation and planning,” IEEE Trans. Power App. Syst., vol. PAS-104, no. 12, pp. 3416–3422, Dec. 1985.

[37] Y. Hou, C.-C. Liu, K. Sun, P. Zhang, S. Liu, and D. Mizumura, “Computation of milestones for decision support during system restoration,” IEEE Trans. Power Syst., vol. 26, no. 3, pp. 1399–1409, Aug. 2011.

[38] Y. Hou, C. C. Liu, P. Zhang, and K. Sun, “Constructing power system restoration strategies,” in Proc. Int. Conf. Elect. Electron. Eng., Bursa, Turkey, Nov. 2009, pp. 1–6.

[39] S. Liu and R. Podmore, “System restoration navigator: A decision support tool for system restoration,” in Proc. IEEE Power Energy Soc. Gen. Meeting, San Diego, CA, USA, Jul. 2012, pp. 1–5.

[40] S. A. Klugman, H. H. Panjer, and G. E. Willmot, Loss Models: From Data to Decisions, vol. 715. Hoboken, NJ, USA: Wiley, 2012.

[41] R. D. Zimmerman, C. E. Murillo-Sanchez, and R. J. Thomas, “MAT-POWER: Steady-state operations, planning, and analysis tools for power systems research and education,” IEEE Trans. Power Syst., vol. 26, no. 1, pp. 12–19, Feb. 2011.

[42] A. J. Lee, “Generating random binary deviates having fixed marginal distributions and specified degrees of association,” Amer. Statistician, vol. 47, no. 3, pp. 219–225, Aug. 1993.

[43] B. F. Qaqish, R. C. Zink, and J. S. Preisser, “Orthogonalized residuals for estimation of marginally specified association parameters in multivariate binary data,” Scandin. J. Statist., vol. 39, no. 3, pp. 515–527, Sep. 2012.

ZHIYUAN YANG (Member, IEEE) received the B.S. degree in electrical engineering from North China Electric Power University (NCEPU), in 2015, and the Ph.D. degree in electrical engineering from Michigan Technological University, in 2018. He is currently working as a Postdoctoral Researcher with Guangdong Electric Power Design Institute Company under the China Energy Engineering Group. His research interests include operational planning in transmission systems and security framework. He was a recipient of the Michigan Tech ECE Outstanding Teaching Award for the year of 2017.

YUN LIU received the B.S. degree in applied math from Northwest Polytechnical University, China, in 2013, and the M.S. and Ph.D. degrees in statistics from Michigan Technological University, in 2019 and 2015, respectively. She is currently working as a Data Scientist with Quicken Loans. Her new routine includes dealing with mortgage-related projects and client activation tasks. Her main research interest is in mixed frequency data and forecasting.

MEGHAN CAMPBELL received the B.S. degree in mathematics from Michigan Technological University, in 2018. She concentrated her studies in actuarial science. She is currently a Government Health Consulting Analyst with Mercer, Minneapolis. Her current focus is on capitation rate development for the states of District of Columbia, North Carolina, and Washington Medicaid programs. She is currently pursuing an Associate of the Society of Actuaries credential.
CHEE-WOOI TEN (Senior Member, IEEE) received the B.S.E.E. and M.S.E.E. degrees from Iowa State University, Ames, in 1999 and 2001, respectively, and the Ph.D. degree from the University College Dublin (UCD), in 2009. From 2002 to 2006, he was a Power Application Engineer working in project development for EMS/DMS with Siemens Energy Management and Information System (SEMIS), Singapore. He was with the National University of Ireland prior joining Michigan Tech, in 2010. He is currently an Associate Professor of electrical and computer engineering with Michigan Technological University. He has recently published a textbook entitled Distribution Emergency Operation, addressing the reconfigurability (a notion of resilience) of distribution feeders and promotion of large-scale data extraction of topologies from geographic information systems (GIS) for advanced distribution engineering. His primary research interests are in modeling for interdependent critical cyberinfrastructures and SCADA automation applications for a power grid. He was a member of the IEEE PES computer and analytical method for cybersecurity task force. He is an Active Reviewer of the IEEE PES Transactions journals. He is currently serving as an Editor for the IEEE Transactions on Smart Grid and Sustainable Energy, Grids, and Networks (SEGAN) (Elsevier).

LINGFENG WANG (Senior Member, IEEE) received the B.E. degree in measurement and instrumentation from Zhejiang University, Hangzhou, China, in 1997, the M.S. degree in electrical and computer engineering from the National University of Singapore, Singapore, in 2002, and the Ph.D. degree from the Electrical and Computer Engineering Department, Texas A&M University, College Station, TX, USA, in 2008. He is currently a Professor with the Department of Electrical Engineering and Computer Science, University of Wisconsin-Milwaukee (UWM), Milwaukee, WI, USA. His major research interests include power system reliability, security, and resiliency. He was a recipient of the Outstanding Faculty Research Award of College of Engineering and Applied Science at UWM, in 2018. He served on the Steering Committee of the IEEE TRANSACTIONS ON CLOUD COMPUTING. He is an Editor of the IEEE TRANSACTIONS ON SMART GRID, the IEEE TRANSACTIONS ON POWER SYSTEMS, and the IEEE POWER ENGINEERING LETTERS. He is also an Editorial Board Member of several international journals, including the Journal of Modern Power System and Clean Energy, Sustainable Energy Technologies and Assessments, and Intelligent Industrial Systems.

YEONWOO RHO received the B.S. degree in mathematics and the B.A. degree in economics from Seoul National University, South Korea, in 2006, the M.S. degree in statistics from Seoul National University, in 2009, and the Ph.D. degree in statistics from the University of Illinois at Urbana-Champaign, in 2014. She is currently an Assistant Professor of statistics with the Department of Mathematical Sciences, Michigan Technological University. Her primary research interests are in time series analysis and forecasting, econometrics, spatial-temporal dependence modeling, bootstrap and resampling methods, and mixed frequency data.

WEI WEI received the Ph.D. degree in actuarial science from the University of Waterloo, Canada. He joined the University of Wisconsin-Milwaukee, in 2013, where he is currently an Associate Professor of actuarial science. He works on the topics of optimal insurance design, dependence modeling, stochastic ordering, cyber risk management, optimal scheduling, and applications of ruin theory. His research interests mainly include the areas of actuarial science and quantitative risk management, as well as applied probability and operations research. He is an Associate of the Society of Actuaries and the China Association of Actuaries.

* * *