This article has been accepted for publication in IEEE Transactions on Power Systems. 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/TPWRS.2022.3215128

Cyber-Impact Analysis for ISO Revenue Adequacy Considering FDIA in Real-time Market Operations

Qiwei Zhang, *Student Member, IEEE,* Fangxing Li, *Fellow, IEEE,* Xiaofei Wang, *Student Member*

***Abstract*—The consensus on the potential of market-targeting cyberattacks to cause catastrophic damage has driven recent research on electricity market cybersecurity analysis. This paper identifies two missing components in current literature. First, ISO revenue adequacy has not been analyzed under the context of cyberattacks. The false data injection attacks (FDIAs) could disturb the market settlement impacting revenue adequacy for ISOs. The lack of such analysis prevents ISOs from comprehensively assessing the financial consequences of market cyberattacks. Second, market attackers need to anticipate the market-clearing results to maximize their attack objectives. Thus, current literature focuses on formulating the attacker model and the market-clearing model as a bilevel problem. However, the coupling between the attack decision, the dispatch at ex-ante, and the price calculation at ex-post have not been explored. To fill those two research gaps, this paper first analytically explores the impact of FDIAs on real-time market operations on ISO revenue adequacy. Then, cyber-impact analysis is proposed to numerically analyze the revenue adequacy. The attacker model, ex-ante dispatch model, and ex-post incremental model are formulated as a trilevel problem to provide a reliable cyber-impact analysis on revenue adequacy. The proposed analysis and platform are demonstrated with the New-England 39-bus system.**

***Index Term*— cyberattacks, cyber-impact analysis, false data injection attacks (FDIAs), revenue adequacy, financial transmission rights, real-time market operations.**

NOMENCLATURE

Superscript:

DA, RT	Indicating the variable/parameter in the real-time (RT) and day-ahead (DA) models.
expost, exante	Indicating the variable/parameter in ex-ante and ex-post models.
att	Indicating the variable/parameter is compromised by attacks.

Sets

N_g, N_d, N_b, N_l,	Set of generators, loads, buses, and lines in the system.
N_l^{+cog}, N_l^{-cog}	Set of positive and negative congested lines.

Parameters:

P_i^{min}, P_i^{max}	The lower and upper generation capacity for the i^{th} unit.
ΔP^{min}, ΔP^{max}	The lower and upper generation capacity for the hypothetical incremental unit.
Fl^{min}, Fl^{max}	The lower and upper transmission line rating for the l^{th} line.
c_i	Generation bidding price of the i^{th} unit.
$GSF_{l\text{-}i}$	Generation shift factors of bus i to line l
D_i	Load at the i^{th} bus.
ΔD_i	Real-time deviation for load at the i^{th} bus.
ΔP_{di}	Hypothetical incremental load
d_i	Bidding price of dispatchable loads
$f_{i,j}$	Bidding price for FTR from bus i to bus j.
$q_{i,j}^{max}$, $q_{i,j}^{min}$	Upper and lower bound of FTR transactions.
o_l^r, o_i^d, o_l^p, o_i^c	Penetration level for attacks on line ratings, loads, capacities, and bidding prices
S	Value of attack degrees

Variables:

P_i	Generation dispatch for the i^{th} unit.
$q_{i,j}$	FTR transaction from bus i to bus j.
q_i	Net FTR injection at bus i.
λ	Lagrangian multiplier for power balance constraint.
γ_i^+, γ_i^-	Lagrangian multipliers for i^{th} upper and lower generation limits.
μ_l^+, μ_l^-	Lagrangian multipliers for l^{th} upper and lower transmission limits.
$\Delta\mu_l^{+att}$, $\Delta\mu_l^{-att}$	The impact of attacks on μ_l^+ and μ_l^-.
ΔP_i^{att}	The impact of attacks on the i^{th} dispatch.
δ_l^r, δ_i^d, δ_l^p, δ_i^c	Attack decisions on line ratings, loads, capacities, and bidding prices.
δ_l^+, δ_l^-	Attack decisions for the l^{th} congestion pattern.
p_i	Attack value for i^{th} generation capacity
r_l	Attack value for l^{th} line ratings.
Δc_i	Attack value for i^{th} unit's bidding.
ΔD_i^{att}	Attack value for loads at bus i.
ΔP_i	The impact of RT load deviation on the i^{th} dispatch.
ΔD_i	Load deviations in real-time at bus i
LMP_i	Locational marginal price at bus i.
N	Net revenue/shortfall of market operations.
Pay^{FTR}	Payments to FTR holders.
R^{DA}, R^{RT}	Revenue surplus from DA and RT markets.
ΔLF_l	RT line flow deviation from DA line flow at the l^{th} line.
ΔLF_l^{att}	The impact of attacks on ΔLF_l.
LF_l^{FTR}	Hypothetical FTR flow at l^{th} line.
ω	Internal variables representing the multiplication of δ_l^+, δ_l^-, μ_l^+, and μ_l^-.
φ_l^-, φ_l^+	Slack variables for negative/positive transmission constraint limits.

This work was supported in part by the US Department of Energy (DOE) CEDS Project "Watching Grid Infrastructure Stealthily Through Proxies (WISP)" under Award DE-OE0000899.

Q. Zhang, F. Li, and X. Wang are with the Min H. Kao Department of Electrical Engineering and Computer Science, The University of Tennessee, Knoxville, TN 37996 USA (e-mail: fli6@utk.edu).

I. INTRODUCTION

A. Background

THE COVID-19 pandemic has forced many companies and business to operate through remote platforms, which have made everyday life and everyone more digitally connected than ever before. The cybersecurity has become a high priority in all aspects of life.

Although more than six years have passed since the devastating cyberattack in Ukraine disabled thirty power substations, the power grid has only become more vulnerable to cyber intrusions. Due to increasing digitalization and smart applications, the number of connections and sensors placed throughout the power grid is growing rapidly, widening the potential for data breaches and cyber intrusions. In March 2019, operators at control centers in the western U.S. lost communications with multiple generators for minutes because the internet-facing firewall was compromised and had to reboot [1]. In October 2019, a malware for illegal data extractions was identified in an Indian nuclear power plant network [2]. In May 2020, a supply chain attack was launched to breach the IT networks of German energy and power companies [3]. The continuous occurrence of cyber events calls for immediate intervention today to prevent future cyberattacks on critical assets.

B. Literature Review

The deregulation of the electricity market has introduced competition and encouraged energy efficiency [4]. The electricity market in the U.S. clears hundreds of GW loads every day providing economic and reliable operation. However, the increasing grid digitalization has opened the electricity market to profit-oriented cyberattacks [5]. Since the initial discussion of market cyberattacks in [6], further research has been conducted on the aspects of electricity market cybersecurity.

The existing research works on electricity market cybersecurity can be broadly divided into three major categories: (1) developing undetectable attack paths or strategies for gaining profit; (2) analyzing sensitivities, vulnerabilities, and attackers with limited abilities; (3) developing detection or defense strategies.

The first category includes congestion pattern attacks, topology attacks, line rating attacks, and various other attack strategies. In [7], electricity market critical parameters were identified to perform profitable attacks with undetectable false data injections. In [8], a profit maximization strategy was developed through false data injection in meter measurements. In [9], a cyber topology attack was formulated to mislead customers into paying higher bills by causing small price deviations. Research work [10] developed a new set of topology attacks including a line-addition attack, a line -removal attack, and a line switching attack. In [11], a transmission line rating attack was designed to manipulate the nodal price. In [12], the short-term load forecast was compromised to mislead the dispatch, which brings financial advantages to certain players. Summarizing this first category literature, most if not all parameters in the market-clearing model have been shown to be attackable and profitable.

The second category focuses on analyzing the characteristics of market-targeting cyberattacks. In [13], the sensitivity of a corrupted sensor on locational marginal prices (LMPs) was analyzed, and the most sensitive bus and sensor were identified. Ref. [14] discussed the impact from bad topology data and bad meter data on LMP, and concluded that the compromised topology data was more detrimental than compromised meter data. In [1], a cyber-vulnerability analysis was provided to analyze vulnerability in the parameters of a market-clearing model. In [16], the vulnerability of compromising generation shift factors to impact the financial transmission rights (FTR) was analyzed. Research work [17] identified that the topology information was too extensive to be known by attackers, and developed a robust attack strategy for attackers with partial topology information. In [18], the impact of limited attacks on electricity market operations was analyzed. In [19], an independent component analysis was conducted for attackers to infer the system topology.

The third category focuses on developing defense schemes. Since the attack path on electricity market operations is generally via state estimation, most defense schemes are targeting state estimation. In [21], a statistic consistency check method was proposed to detect attacks in state estimation. In [22], an online detection algorithm was developed to detect false data injection in state estimation. Additionally, in [23], a market-level defense scheme against cyberattacks was developed based on electricity price signals.

Following the existing research works, this paper identifies two unexplored topics. The detailed motivations and contributions are presented in the next subsection.

C. Motivations and Contributions

Although research works have started to investigate power market cyberattacks, as presented in the above subsection, this paper identifies two missing components.

Firstly, revenue adequacy, a vital financial consideration for ISOs, has not been investigated under the context of cyber intrusions. Specifically, a false data injection attack (FDIA) may disturb the market settlement and impact the revenue adequacy of ISOs under attack. The lack of such analysis prevents ISOs from comprehensively assessing the financial consequences of market cyberattacks.

Secondly, the prevailing attack model commonly contains a nested real-time (RT) market-clearing model to formulate a bilevel optimization problem because the attacker needs to anticipate RT market-clearing results to maximize the attack objective. The ex-ante and ex-post schemes are two primary approaches used to settle the RT market by ISOs. For instance, the ex-ante scheme is adopted by NYISO, where the dispatch and pricing are both determined by the ex-ante model [24]. Various ex-post models are adopted at a number of ISOs, such as PJM, MISO, and ISONE [24], in which the dispatch is done by the ex-ante model while the market settlement is done by ex-post incremental model. Previous research works, such as [1], [11], and [12], employ bilevel models where either an ex-ante model or an ex-post model is used at the lower level. These bilevel models either assume ex-ante schemes or consider that attacks happen only at ex-ante dispatch or at ex-post pricing, and thus, the consideration of the other is unnecessary. There is a lack of an electricity market cybersecurity model under ex-

post scheme considering the coupling between attack decisions, the ex-ante dispatch, and the price calculation at ex-post.

Therefore, this paper aims to address these two missing components. The detailed contributions are as follows:

- This paper is the first attempt to investigate ISO revenue adequacy under the context of cyber intrusions. The revenue adequacy problem is formulated under the existence of cyberattacks. Sufficient conditions for cyberattacks causing revenue shortfalls are developed and analyzed. Four remarks on the impact of cyberattacks on revenue adequacy are presented in detail. The formulated conditions and remarks provide ISOs with a theoretical analysis foundation on the impact of cyberattacks on revenue adequacy.
- The proposed cyber-impact analysis is the first attempt to model the coupling between attack decisions, ex-ante dispatches, and ex-post pricing, which provides ISOs a more reliable analysis platform to comprehensively evaluate potential financial consequences of cyberattacks. The proposed platform is applied to the New England 39-bus system to demonstrate the severity of the potential revenue shortfall.

D.Paper Organization

The rest of this paper is organized as follows. Section II analyzes the impact of cyber intrusions on ISO revenue adequacy, and four remarks on the revenue adequacy are discussed in detail. In Section III, the cyber-impact analysis model is proposed and formulated. Each level is described in detail. Section IV presents reformulations and algorithms to solve the proposed model. Section V demonstrates the proposed platform on the New England 39-bus system. Finally, Section VI discusses conclusions and directions for future studies.

II. Impact of Cyber-intrusions on Revenue Adequacy

The prevailing two-settlement market-clearing process uses LMPs to settle electricity purchases and sales, which reflects the price of electricity generation, transmission loss, and cost of transmission congestions. As the name suggests, the LMP is calculated by the location where power is received or delivered. The generation bus and load bus are usually settled by different prices, which leaves a revenue surplus due to congestions. Thus, FTR is proposed to entitle transmission holders to receive revenue surplus.

In general, a system is revenue adequate if the revenues collected from the two-settlement market-clearing process in the form of congestion payments are sufficient to fully fund payments for the FTRs. In this section, we first briefly discuss the two-settlement market-clearing scheme and FTR auction model. Then, revenue adequacy is analyzed under the context of cyber intrusions. Sufficient conditions for cyberattacks causing revenue shortfalls are developed, and four remarks are discussed in detail on the impact of cyberattacks on ISO revenue adequacy.

A. Market-clearing Scheme and FTR Auction Model

Two-settlement market-clearing contains a day-ahead (DA) market and an RT market [25]. The DA market is cleared a day ahead, and the RT market offers adjustments for real time deviations. The ex-post pricing scheme has been widely applied in ISOs, such as ISO-NE, PJM, and MISO, for RT market-clearing, where the dispatch is determined by the ex-ante model, while the LMP is calculated after the cycle of spot market by an ex-post incremental model.

The DA market-clearing model and RT ex-ante market-clearing model have similar formulations as shown in (1)-(4) [5], and the difference lies in the forecast intervals. The LMPs are obtained by the dual variables of the single-interval economic dispatch model (1)-(4). The values of Fl^{min} and Fl^{max} are collectively determined by various limits such as thermal limits, transient stability limits, and voltage stability limits. The details of identifying such limits are not covered here since they are beyond the scope of this paper.

$$\min \sum_{i}^{N_g} c_i \times P_i \tag{1}$$

$$\sum_{i}^{N_g} P_i = \sum_{i}^{N_d} D_i \tag{2}$$

$$P_i^{\min} \le P_i \le P_i^{\max} \tag{3}$$

$$F_l^{\min} \le \sum_{i=1}^{N_b} GSF_{l-i}(P_i - D_i) \le F_l^{\max},\ \forall l \in N_l \tag{4}$$

The formulation of LMP is shown in (5).

$$LMP_i = \lambda + \sum_{l}^{N_l} GSF_{l-i}(\mu_l^- - \mu_l^+) \tag{5}$$

The ex-post incremental model is shown in (6)-(10) [24].

$$\min \sum_{i}^{N_g} c_i \times P_i^{expost} - \sum_{j}^{N_d} \mathrm{d}_j \times \Delta \mathrm{P}_{dj} \tag{6}$$

$$\sum_{i}^{N_g} P_i^{expost} = \sum_{j}^{N_d} \Delta \mathrm{P}_{dj} \tag{7}$$

$$\Delta P_i^{\min} \le P_i^{expost} \le \Delta P_i^{\max} \tag{8}$$

$$\sum_{i=1}^{N_b} GSF_{l-i}(P_i^{expost} - \Delta P_{di}) \le 0,\ \forall l \in N_l^{+cog} \tag{9}$$

$$\sum_{i=1}^{N_b} GSF_{l-i}(P_i^{expost} - \Delta P_{di}) \ge 0,\ \forall l \in N_l^{-cog} \tag{10}$$

The portion of FTR that can be awarded is required to be within limits when all FTRs are presented simultaneously in the system. The FTR auction model is shown in (11)-(14) [26]. The amount of FTR transactions is restricted by $q_{i,j}^{max}$ and $q_{i,j}^{min}$. The FTR auction participants are mostly hedgers who purchase FTRs to hedge the congestion charges of their energy transactions. Those participants are not motivated for an unlimited amount of FTRs. Thus, it is natural to assume that the aggregate bid quantity of the FTR is bounded by a maximum value [26].

$$\max \sum_{i}^{N_b} \sum_{j \ne i}^{N_b} f_{i,j} \times q_{i,j} \tag{11}$$

$$q_i = \sum_{j \neq i}^{N_b} q_{i,j} - \sum_{k \neq i}^{N_b} q_{k,i}, \ \forall i \in N_b \tag{12}$$

$$\mathrm{F}_l^{\min} \leq \sum_{i=1}^{N_b} GSF_{l-i} q_i \leq \mathrm{F}_l^{\max}, \ \forall l \in N_l \tag{13}$$

$$q_{i,j}^{\min} \leq q_{i,j} \leq q_{i,j}^{\max}, \ \forall \{i,j\} \in N_b, \ i \neq j \tag{14}$$

The above models are presented briefly as background, and the model details can be found in [5], [24], and [26].

B. Impact of Cyber-Intrusions on Revenue Adequacy

Periodical FTR auctions are held monthly and yearly, and it decides the financial right allocation of transmission capacities. FTR auctions entitle the holder to receive a stream of revenues based on the hourly congestion price in the DA market. This paper considers the point-to-point type of transmission right. The FTR holder receives payments, which are equal to the FTR quantity multiplied by the price difference between the injection bus and withdrawn bus. The total payment to FTR holders under a DA market-clearing result is shown in (15).

$$Pay^{FTR} = \sum_{i}^{N_b} \sum_{j \neq i}^{N_b} q_{i,j} \times (LMP_j^{DA} - LMP_i^{DA}) \tag{15}$$

By replacing the LMP with equation (5), the equation (15) can be reformulated as (16). The payment to FTR holders is equal to the congestion price multiplied by the FTR quantity at all lines.

$$\begin{aligned} Pay^{FTR} &= \sum_{i}^{N_b} \sum_{j \neq i}^{N_b} q_{i,j} \times \Big(\sum_{l} GSF_{l-i} - GSF_{l-j}\Big) \times \left(\mu_l^{+DA} - \mu_l^{-DA}\right) \\ &= \sum_{l}^{N_l} LF_l^{FTR} \times \left(\mu_l^{+DA} - \mu_l^{-DA}\right) \end{aligned} \tag{16}$$

The ISO collects payments from load aggregators and pays generation companies [27]. The net revenue in the DA market is formulated in (17). Equation (17) can be reformulated as (18) by (5), which means the net revenue is also equal to the congestion price multiplied by the transmission capacity at all lines.

$$R^{DA} = \sum_{i}^{N_b} (D_i - P_{gi}) \times LMP_i^{DA} \tag{17}$$

$$R^{DA} = \sum_{l}^{N_l} F_l^{\max} \times \mu_l^{+DA} - F_l^{\min} \times \mu_l^{-DA} \tag{18}$$

It should be noted that Fl^{max} is always higher than LF_l^{FTR}, and the Fl^{min} is always lower than LF_l^{FTR} because the FTR flow is constrained to be smaller than the line rating as in (13). Therefore, R^{DA} is always greater than Pay^{FTR} because the Lagrangian duals for line flow constraints are always positive. As such, the FTR auction model ensures revenue adequacy at the DA market ($R^{DA} > Pay^{FTR}$) under normal operations, which is also referred to as a simultaneous feasibility test [28].

In the same vein, the net revenue for RT operation is shown in (19), which means the net revenue is equal to the deviation of RT line flow from the DA line flow multiplied by the RT congestion price. Under normal operations, R^{RT} is non-negative because ΔLF is positive for nonzero μ^+ and negative for nonzero μ^-. Thus, revenue adequacy is always ensured, and it is independent of the dispatch results. The net revenue of ISOs is shown in (20).

$$R^{RT} = \sum_{l} \Delta LF_l \times (\mu_l^{+RT} - \mu_l^{-RT}) \tag{19}$$

$$N = R^{DA} + R^{RT} - Pay^{FTR} \tag{20}$$

As presented in the literature review, cyberattacks can alter RT market-clearing results through various attack paths. Cyberattacks targeting DA market have not been fully explored and justified in the literature, and thus, they are not discussed in this paper. However, the discussion of DA market cyberattacks will be similar to RT market cyberattacks. RT cyberattacks can inject false data on bids, line rating, demand response, etc., which impacts both the ΔLF and the congestion price μ for RT operations. Then, (19) can be reformulated as in (21), which represents RT revenue under cyberattacks.

$$R^{RT,att} = \sum_{l} \Delta LF_l^{att} \times \left[(\mu_l^{+RT} + \Delta\mu_l^{+att}) - (\mu_l^{-RT} + \Delta\mu_l^{-att}) \right] \tag{21}$$

Assuming the cyberattack is the only unexpected event when μ^{DA} and μ^{RT} are the same, the revenue adequacy (20) can be reformulated as in (22).

$$\begin{aligned} N = \sum_{l} & (F_l^{\max} - LF_l^{FTR} + \Delta LF_l^{att}) \times \mu_l^{+DA} \\ & - (F_l^{\min} - LF_l^{FTR} + \Delta LF_l^{att}) \times \mu_l^{-DA} \\ & + \Delta LF_l^{att} \times (\Delta\mu_l^{+att} - \Delta\mu_l^{-att}) \end{aligned} \tag{22}$$

Therefore, if the value of N is negative, the cyberattack leads to revenue shortfalls. The sufficient conditions (but not necessary) can be developed as the following conditions A.1) and A.2) to make the value of N negative.

A.1) For a positively congested line:

$$\Delta LF_l^{att} \leq LF_l^{FTR} - F_l^{\max}, \quad l \in N_l^{+cog} \tag{23}$$

$$\Delta\mu_l^{+att} \geq 0, \quad l \in N_l^{+cog} \tag{24}$$

A.2) For a negatively congested line:

$$\Delta LF_l^{att} \geq LF_l^{FTR} - F_l^{\min}, \quad l \in N_l^{-cog} \tag{25}$$

$$\Delta\mu_l^{-att} \leq 0, \quad l \in N_l^{-cog} \tag{26}$$

If an attacker can inject false data making ΔLF and μ satisfy A.1) and A.2), it is sufficient for the attack, causing an ISO revenue shortfall. The positively congested lines and negatively congested lines represent lines where the line flow values are equal to the upper limits and lower limits, respectively.

Four remarks are discussed in detail on the impact of a cyberattack on revenue adequacy by the proposed sufficient conditions. The four remarks are also demonstrated in Section V on the New England 39-bus system by the proposed model in Section IV.

Remark 1. Considering an important scenario when all transmission rights have been auctioned as shown in (27), the total payment to FTR holders Pay^{FTR} is equal to the revenue from DA operation R^{DA}. Then, revenue adequacy purely depends on RT operations, which is an easier goal for attacks to achieve.

$$LF_l^{FTR} = F_l^{\max} \ or \ F_l^{\min}, \ \ \forall l \in N_l \tag{27}$$

With (27), the sufficient conditions A.1) and A.2) can be relaxed as (28)-(31), which ensure the negative revenue from RT operations. Equations (28) and (30) ensure ΔLF_l at a

positive congestion line is negative and ΔLF_l at a negative congestion line is positive. Equations (29) and (31) satisfy (24) and (26) with the help of line rating attack r_l. Equations (28)-(31) are sufficient conditions for cyberattacks causing negative RT revenue, and they are sufficient conditions for cyberattacks causing revenue shortfall when all of the transmission rights have been auctioned.

$$\Delta LF_l^{att} \le 0, \quad \forall l \in N_l^{+cog} \tag{28}$$

$$F_l^{\max} - r_l = \Delta LF_l^{att}, \ \forall l \in N_l^{+cog} \tag{29}$$

$$\Delta LF_l^{att} \ge 0, \ \forall l \in N_l^{-cog} \tag{30}$$

$$F_l^{\min} + r_l = \Delta LF_l^{att}, \ \forall l \in N_l^{-cog} \tag{31}$$

Remark 2. Generally, RT demands slightly deviate from the DA forecast. When load forecast error is considered, (28)-(31) can be reformulated as (32)-(35). It is worth noting that when load forecast errors contribute to relieving congestion (negative or positive), it helps the cyberattack cause revenue shortfalls because (32) and (34) can be satisfied by particular load forecast errors, instead of cyberattacks. It is also worth mentioning that load deviations do not necessarily worsen/relieve the shortfall created by an attack but that deviations do increase/decrease the value of necessary false data being injected.

$$\Delta LF_l^{att} + \Delta LF \le 0, \quad \forall l \in N_l^{+cog} \tag{32}$$

$$F_l^{\max} - r_l = \Delta LF_l^{att} + \Delta LF, \ \forall l \in N_l^{+cog} \tag{33}$$

$$\Delta LF_l^{att} + \Delta LF \ge 0, \ \forall l \in N_l^{-cog} \tag{34}$$

$$F_l^{\min} + r_l = \Delta LF_l^{att} + \Delta LF, \ \forall l \in N_l^{-cog} \tag{35}$$

The incremental change in the line flow caused by load forecast error is shown in (36). The impact of an attack on the value of line flow is shown as in (37). Therefore, the sufficient conditions (32)-(35) can be reformulated as (38)-(41), which relates the sufficient conditions with market parameters (attack paths).

$$\Delta LF_l = \sum_i (\Delta D_i - \Delta P_i) \times GSF_{l-i} \tag{36}$$

$$\Delta LF_l^{att} = \sum_i (\Delta D_i^{att} - \Delta P_i^{att}) \times GSF_{l-i} \tag{37}$$

$$\sum_i (\Delta D_i^{att} + \Delta D_i - \Delta P_i^{att}) \times GSF_{l-i} \le 0, \ \forall l \in N_l^{+cog} \tag{38}$$

$$F^{\max} - r_l = \sum_i (\Delta D_i^{att} + \Delta D_i - \Delta P_i^{att}) \times GSF_{l-i}, \ \forall l \in N_l^{+cog} \tag{39}$$

$$\sum_i (\Delta D_i^{att} + \Delta D_i - \Delta P_i^{att}) \times GSF_{l-i} \ge 0, \ \forall l \in N_l^{-cog} \tag{40}$$

$$F^{\min} + r_l = \sum_i (\Delta D_i^{att} + \Delta D_i - \Delta P_i^{att}) \times GSF_{l-i}, \ \forall l \in N_l^{-cog} \tag{41}$$

Remark 3. Injecting false data on demand, bidding, and unit capacity does not affect revenue adequacy if not combined with transmission line rating attacks. From the necessary conditions, although the above three types of attack can manipulate the value of congestion price, meaning that (24) and (26) can be ensured, conditions (23) and (25) cannot be satisfied unless combined with the transmission line rating attack. However, the transmission line rating attack alone can theoretically satisfy the sufficient conditions A.1) and A.2). From this observation, the transmission line rating attack ensures the feasibility of causing a shortfall and the other types of attacks enhance the severity of the resulting shortfall.

Remark 4. Unexpected line derating and outage may also lead to a revenue shortfall [29]. As shown in (32)-(35), when unexpected line derating happens with a particular load forecast error, high revenue shortfalls could happen without a cyberattack. However, compared with unexpected contingency events, the threat from cyberattacks is much more severe because it not only strategically selects the most effective lines to de-rate, but is also able to inject false data at other parameters to enhance the revenue shortfall. Furthermore, a conventional procedure for allocating revenue shortfall is that an ISO prorates the shortfall to all FTR settlements. However, allocating the shortfall caused by attacks could make some FTRs lose the ability to hedge against congestion rents for bilateral transactions due to the significant number of shortfalls.

In summary, this section analytically discusses the impact of cyberattacks on revenue adequacy and sufficient conditions for revenue shortfalls. The next section will formulate an impact analysis platform to numerically investigate revenue adequacy under the context of a cyberattack.

III. Cyber-Impact Analysis Platform for ISO Revenue Adequacy

In Section II, the impacts of cyberattacks on revenue adequacy have been analytically investigated. This section presents a cyber-impact analysis platform to numerically evaluate the impact of cyberattacks on revenue adequacy.

The proposed cyber-impact platform places an attacker model at the upper-level, an ex-ante model at the middle-level, and an ex-post model at the lower-level. The ex-post scheme is shown in Section II.A, where the dispatch is determined by ex-ante model, while the market is cleared after the cycle of the spot market using an ex-post incremental model. This paper proposes a trilevel model to consider the coupling between attacks, ex-ante dispatches, and ex-post pricing. Prior bilevel models, such as [1], ignore such coupling, which makes them less desirable under the context of this paper. The proposed trilevel model is a more proper way to estimate the impact of cyberattacks under ex-post scheme. The detailed mathematical model and descriptions are provided in the following subsections.

A. Assumptions

Several assumptions and notes related to the proposed model are listed as follows:

- The proposed model is a cyber-impact analysis model for ISOs. Therefore, the upper-level model considers as many attack paths as possible. Although some parameters may not be easily compromised unless the cyber threats are from insiders, the proposed model considers comprehensive scenarios for market operators to analyze revenue adequacy. The proposed analysis model can be simplified by removing specific attack paths if decision makers consider these parameters to be perfectly secure or unpractical.
- The potential attack targets are the parameters in the market-clearing database. As discussed in the literature review, most if not all parameters of the RT market-clearing model have been justified as attackable and profitable. This paper

considers the following false data injection based on previous literature: demand [12], line rating [11], unit capacity [30], bidding [31], and congestion pattern [6]. Other FDIAs can be easily integrated, but it is worth noting that the proposed analysis model does not apply to FDIAs that assume operators are insiders. The reason is that if the operator is the insider and does not care about the revenue adequacy, the proposed analysis model will not be applicable.

- The proposed model uses penetration levels and attack degrees to model the success and ability of attacks. The attack degree indicates the number of parameters that the attacker can perturb. For a wide range of attack targets, the attack ability restricts the attacker to select limited targets, which means that attacks are successful on a limited number of the parameters and will not be successful on the other parameters. The penetration level restricts the maximum percentage of parameters that the attack can manipulate without alerting the operator. If the operator believes that some attacks are not likely to happen, the penetration level can be set to 0. The modeled attack is assumed to know the system topology. The clearing results of FTR and DA markets are generally public on ISOs' websites.
- Cyberattacks could lead to ISO revenue shortfall, as shown in the above remarks. Multiple types of attackers may be interested in launching such attacks, like malicious agents whose goal is to disrupt power system operations. The revenue shortfall would severely impact on the FTR transactions and market settlements leading to a chain of damages in power system operations. The revenue shortfall could also be a side-effect of attacks whose goal is not the revenue shortfall. For example, profit-oriented cyberattacks inevitably alter the power market-clearing result, potentially leading to revenue shortfall. Although the side effect is generally not a concern for the attacker, this paper provides the revenue adequacy analysis for market operators to comprehensively analyze the impact of cyberattacks on market operations.

B. Upper-level Model (Attacker Model)

To investigate the impact of a cyberattack on revenue adequacy, the objective of the attacker model is set to maximize the revenue shortfall (22), as shown in (42).

$$\max \quad -N \tag{42}$$

The data sources, i.e., demand, line rating, unit capacity, bidding, and congestion pattern mentioned in the second bullet of subsection III-A, are assumed to be susceptible to attacks in the proposed platform, as shown in (43)-(47). The attack values on the parameters are constrained by the penetration level o, the attack decision δ, and their original value. The attack decisions δ are binary variables indicating if the corresponding parameter is attacked. The penetration level o is a parameter indicating the maximum percentage of the parameter that the attack can manipulate. Equation (47) shows that the congestion pattern attack for a line is either for positive congestion or for negative congestion. The details of congestion pattern attacks are discussed in the lower-level model.

$$-\delta_i^d \times D_i \times o_i^d \le \Delta D_i^{att} \le \delta_i^d \times D_i \times o_i^d \tag{43}$$

$$\delta_l^r \times F_l^{\min} \times o_l^r \le r_l \le \delta_l^r \times F_l^{\max} \times o_l^r \tag{44}$$

$$-\delta_i^p \times P_i^{\max} \times o_i^p \le p_i \le \delta_i^p \times P_i^{\max} \times o_i^p \tag{45}$$

$$\delta_i^c \times c_i \times o_i^c \le \Delta c_i \le \delta_i^c \times c_i \times o_i^c \tag{46}$$

$$\delta_l^+ + \delta_l^- \le 1 \tag{47}$$

The attacker is assumed to have limited attack abilities. The attack degree S restricts the number of parameters that the attacker can perturb, as in (48).

$$\sum_i \sum_l \delta_l^r + \delta_i^p + (1-\delta_l^+) + (1-\delta_l^-) + \delta_i^c + \delta_i^d \le S \tag{48}$$

In summary, the upper level models an envisaged attacker who aims to create a revenue shortfall with limited abilities.

C. Middle-level Model (Ex-ante Dispatch Model)

The injected false data impacts the RT economic dispatch obtained by the ex-ante model (1)-(5) because some parameters are compromised. The upper-level decision variables impact the bid at the objective (1), unit capacity at (3), line rating at (4), and load in (2) and (4). Therefore, the ex-ante model (1)-(5) can be reformulated as in (49)-(54) considering cyberattacks. The false data injected by attackers deviate dispatch decisions, which are sent to generators. The compromised dispatch, in turn, impacts the goal of the attacker.

$$\min \sum_i^{N_g} (c_i + \Delta c_i) \times P_i^{exante} \tag{49}$$

$$\sum_i^{N_g} P_i^{exante} = \sum_i^{N_d} D_i^{exante} \tag{50}$$

$$D_i^{exante} = D_i + \Delta D_i + \Delta D_i^{att}, \forall i \in N_b \tag{51}$$

$$P_i^{\min} \le P_i^{exante} \le P_i^{\max} + p_i \tag{52}$$

$$\sum_{i=1}^{N_b} GSF_{l-i} \times (P_i^{exante} - D_i^{exante}) \le F_l^{\max} + r_l, \forall l \in N_l \tag{53}$$

$$\sum_{i=1}^{N_b} GSF_{l-i} \times (P_i^{exante} - D_i^{exante}) \ge F_l^{\min} + r_l, \forall l \in N_l \tag{54}$$

D. Lower-level Model (Ex-post Pricing Model)

The ex-post pricing model is an incremental model based on the results of state estimations. A remote transmission unit collects various measurements, such as generation and line flow, and sends them to the state estimator. The resulting data, such as generations and congestion patterns, are used for calculating market settlements. The random errors are filtered by bad data detection, and thus, the injected false data is assumed to be the only source of bad data. Similar to (49)-(54), with the consideration of the compromised parameters, the original ex-post model (6)-(10) can be reformulated as (55)-(59). The ex-ante model determines the dispatch, and state estimation outputs the congestion pattern, which provides the transmission binding constraints in the ex-post model as in (58) and (59). The congestion pattern attack can compromise state estimation

results to manipulate transmission binding constraint sets N_l^{+cog} and N_l^{-cog} in (58) and (59).

$$\min \sum_{i}^{N_g} (c_i + \Delta c_i) \times \Delta P_i^{expost} \tag{55}$$

$$\sum_{i}^{N_g} \Delta P_i^{expost} = 0 \tag{56}$$

$$\Delta P_i^{\min} \le \Delta P_i^{expost} \le \Delta P_i^{\max} \tag{57}$$

$$\sum_{i=1}^{N_b} GSF_{l-i} \times \Delta P_i^{expost} \le 0, \forall l \in N_l^{+cog,m} \tag{58}$$

$$\sum_{k=1}^{N_b} GSF_{l-i} \times \Delta P_i^{expost} \ge 0, \forall l \in N_l^{-cog,m} \tag{59}$$

The ex-post model determines the LMP at each bus to clear the market, which impacts the value of the attack objective. The reformulations and solution algorithms for the proposed model are presented in the next section.

IV. Solution Method

The structure of the proposed trilevel problem is different from conventional trilevel models where each level interacts with each other. The middle-level ex-ante model only passes the congestion status to the lower-level ex-post model, and the lower-level ex-post model does not impact the solution of middle-level problem. This characteristic will be exploited in the proposed solution algorithm to make it efficient, which is specifically discussed in subsection IV-C. The detailed solution of the proposed trilevel problem is presented in the following subsections.

A. Modeling the Transmission Binding Constraint Set

The first step of solving the trilevel problem is to explicitly model the set $N_l^{+cog,m}$ and $N_l^{-cog,m}$ in the lower-level ex-post problem. Here, $N_l^{+cog,m}$ and $N_l^{-cog,m}$ indicate the set of positively and negatively congested lines, which may have been compromised by attackers. The formulation of $N_l^{+cog,m}$ and $N_l^{-cog,m}$ depends on the attack decision on the congestion pattern and the market-clearing results at the ex-ante model in the second level. The line flow constraints in (53) and (54) can be reformulated to (60) and (61) with a slack variable φ. When φ^+ or φ^- for the l^{th} line is 0, the l^{th} line is positively or negatively congested; otherwise, the l^{th} line flow constraint is not binding. Then, the line flow constraints (58) and (59) in the ex-post model can be reformulated as in (62) and (63). When φ_l^+ or φ_l^- for the l^{th} line is 0 in the ex-ante model, the l^{th} line constraint is binding in the ex-post model. When φ_l^+ or φ_l^- for the l^{th} line is not 0 in the ex-ante model, the l^{th} line constraint is not binding in the ex-post model. Further, the binary variable δ_l^+ and δ_l^- for the congestion pattern attack decides the number of transmission binding constraints at the ex-post pricing model. When δ_l^+ or δ_l^- is 0 (i.e., congestion pattern attack happens at the l^{th} line), the constraint (62) or (63) is removed. When δ_l^+ or δ_l^- is 1 (i.e., no attack), the constraint (62) or (63) stays. Thus, equations (62) and (63) are equivalent to (58) and (59).

The congestion pattern attack in this model only considers relieving a congested line because relieving a congested line is generally more feasible than congesting a line. For example, if a line is originally congested at its upper limit 200 MW, then the attack only needs to make a slight change to un-congest the line flow (e.g., changing it by 1 MW to 199 MW). As such, the attack vector only contains small values in order to remain undetectable.

$$\sum_{i=1}^{N_b} GSF_{l-i} \times (P_{gi}^{exante} - D_i^{exante}) + \psi_l^+ = F_l^{\max} + r_l, l \in N_l \tag{60}$$

$$\sum_{i=1}^{N_b} GSF_{l-i} \times (P_i^{exante} - D_i^{exante}) - \psi_l^- = F_l^{\min} + r_l, l \in N_l \tag{61}$$

$$\delta_l^+ \times \sum_{i=1}^{N_b} GSF_{l-i} \times P_i^{expost} \le \psi_l^+, \; l \in N_l \tag{62}$$

$$\delta_l^- \times \sum_{k=1}^{N_b} GSF_{l-i} \times P_i^{expost} \ge -\psi_l^-, \; l \in N_l \tag{63}$$

B. Converting the Lower-level Problem

Next, the lower-level problem is converted with Karush-Kuhn-Tucker (KKT) conditions [32]. The lower-level problem (55)-(59) is equivalent to (56), (57), (62), (63), and (64)-(69) because the lower-level problem is a convex model. Thus, with the value of φ_l from the ex-ante model and the attack decision from the attacker model, solving the KKT equations gives the LMP at each bus, which is the same as solving (55)-(59).

$$(56),\ (57),\ (62),\ (63)$$

$$(c_i + \Delta c_i) - \lambda^{expost} + \gamma_i^{+expost} - \gamma_i^{-expost} + \omega^{expost} = 0 \tag{64}$$

$$\omega^{expost} = \sum_{l=1}^{N_L} GSF_{l-i} \times (\delta_l^+ \times \mu_l^{+expost} - \delta_l^- \times \mu_l^{-expost}) \tag{65}$$

$$\delta_l^+ \times \mu_l^{+expost} \times (\sum_{i=1}^{N_b} (GSF_{l-i} \times P_i^{expost}) - \psi_l^+) = 0 \tag{66}$$

$$\delta_l^- \times \mu_l^{-expost} \times (-\sum_{i=1}^{N_b} (GSF_{l-i} \times P_i^{expost}) - \psi_l^-) = 0 \tag{67}$$

$$\gamma_i^{-expost} \times (\Delta P_i^{\min} - P_i^{expost}) = 0 \tag{68}$$

$$\gamma_i^{+expost} \times (P_i^{expost} - \Delta P_i^{\max}) = 0 \tag{69}$$

It is worth noting that although the variables representing a congestion pattern attack are binary variables in the lower-level model, the upper-level variables are treated as parameters in the lower-level problem. When the value of δ_l is 0, all the KKT conditions related to the l^{th} transmission constraint are removed. When the value of δ_l is 1, the KKT conditions related to the l^{th} transmission constraint are included.

C. Converting the Middle-level Problem

The structure of the proposed model is shown in Fig. 1.

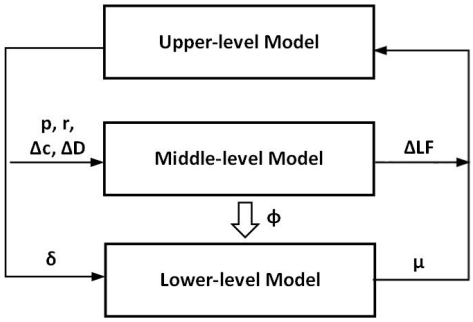

Fig. 1. Structure of the proposed model

The trilevel coupling is explained as follows. The upper-level decision variable impacts the optimal solution of the middle-level and lower-level problems. The optimal solution of the middle-level and lower-level problems also impact the optimality of the upper-level problem. Thus, the upper-level problem interacts with both the middle-level and lower-level problems.

However, different from conventional trilevel problems, the middle-level and lower-level problems in the proposed model exhibit a one-way relationship. The middle-level problem only needs to pass the value of φ_l to the lower-level and does not need to anticipate the solution of the lower-level problem for its own optimization. Thus, the middle-level problem can also be converted by KKT conditions based on this unique one-way relationship. Eventually, the model is converted into the upper-level problem with two sets of KKT conditions. The middle-level problem (49)-(54) can be converted to KKT conditions as in (50)-(52), (60), (61), and (70)-(75). Then, the optimization problem (42)-(59) is equivalent to solving (42)-(54), (56), (57), (60)-(63), and (64)-(75).

$$(49)-(54),\ (60),\ (61)$$

$$c_i + \Delta c_i - \lambda^{exante} + \gamma_i^{+exante} - \gamma_i^{-exante} + \omega^{exante} = 0 \quad (70)$$

$$\omega^{exante} = \sum_{l=1}^{N_L} GSF_{l-i} \times (\mu_l^{+exante} - \mu_l^{-exante}) \quad (71)$$

$$\mu_l^{+exante}(\sum_{i=1}^{N_b} GSF_{l-i} \times (P_i^{exante} - D_i^{exante}) - \psi_l^{+}) = 0 \quad (72)$$

$$\mu_i^{-exante} \times \sum_{i=1}^{N_b}(-GSF_{l-i} \times (P_i^{exante} - D_i^{exante}) + \psi_l^{-}) = 0 \quad (73)$$

$$\gamma_i^{-exante} \times (P_{gi}^{\min} - P_{gi}^{exante}) = 0 \quad (74)$$

$$\gamma_i^{+exante} \times (P_i^{exante} - P_i^{\max} - p_i) = 0 \quad (75)$$

In summary, Sections III presents the trilevel cyber-impact analysis model formulation, and Section IV develops the solution techniques of the trilevel model based on the model characteristics. The unique interaction between the lower-level model and the middle-level model, as discussed in the opening paragraph and subsection IV-C, is utilized to make the solution algorithm efficient.

V. Case Study

In this section, the impact of cyberattacks on ISO revenue adequacy is analyzed on the New England 39-bus system using the proposed platform. The detailed system parameters can be found in [33] and [34], and the system topology is sketched in Fig. 2 using CURENT Large-scale Test Bed (LTB) [35]. The simulation studies were performed with MATLAB 2018 on a PC with Intel i7-8650U processor and 8GB RAM.

Four case studies are conducted to show the impact of cyberattacks on revenue shortfall in detail. The four case studies discuss and analyze the four remarks in subsection II-B accordingly.

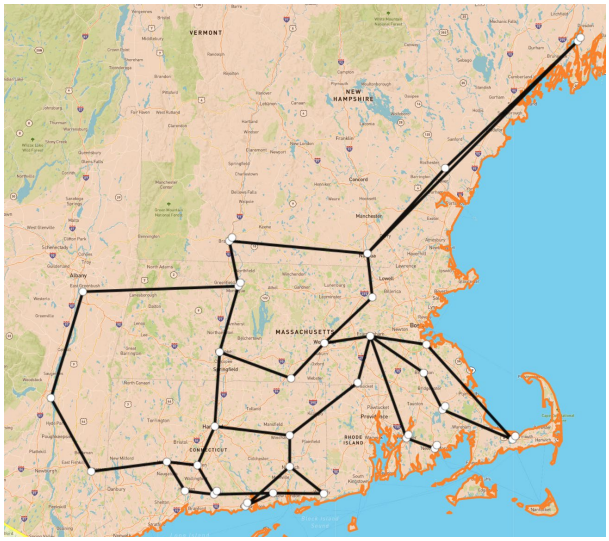

Fig. 2. One-line diagram of the New England 39-bus system (for illustration only)

A. Case Study 1: Margin of the Revenue Shortfall

As shown in Remark 1, cyberattacks can more easily cause revenue shortfall when all transmission rights are auctioned. If only a part of the transmission capacity is auctioned, the unauctioned capacity leaves ISOs revenue surplus (margin), which can be used to recover shortfalls.

As shown in Table I, the revenue margin decreases proportionally with the transmission capacities margin. When all of the capacities are auctioned, the revenue margin goes to 0. An attack scenario is performed on the proposed analysis platform to analyze the revenue shortfall. The attack is assumed to have three attack degrees and a 20% penetration level. The resulting shortfall by the attack is shown in the third column of Table I.

Table I. Margin of The Revenue Shortfall

Capacity Margin	Revenue Margin	Shortfall by attack
0%	$0	$145,026
25%	$76,801	$68,225
50%	$153,602	N/A (-$8577<0)
75%	$230,403	N/A (-$185,378<0)

When all the transmission capacities are auctioned (i.e., the margin is 0), the attack can cause a shortfall of $145,025. However, the attack cannot cause shortfalls when the capacity margin is high. For example, when the margin is 75%, a shortfall is not achievable. Furthermore, 47.2% is the critical point for the capacity margin, below which the cyberattack can cause a revenue shortfall.

This article has been accepted for publication in IEEE Transactions on Power Systems. 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/TPWRS.2022.3215128

It is worth mentioning that a conservative revenue margin may lead to inefficient FTR auctions and market operations, although the revenue margin can recover part of the revenue shortfall led by the attacks. Furthermore, the capacity margin does not impact the selection of attack decisions although it diminishes the effectiveness of cyberattacks.

B. Case Study 2: Importance of Real-time Load Deviations

As shown in Remark 2, RT load deviations can increase/decrease the amount of false data needed to be injected. The following example is considered to demonstrate this phenomenon. If the attacker wants to induce a shortfall greater than \$20,000, a negative 90MW line rating attack at line 2-30 can be combined with an attack at bus 25 that increases the demand by 150MW. Similarly, if the RT deviation at bus 25 is more than 150MW, the same shortfall can be achieved without applying the demand attack.

Furthermore, based on the proposed cyber-impact analysis model, RT load deviations impact the effectiveness of cyberattacks on revenue shortfall. Some load deviations may reduce the shortfall caused by attacks, and some load deviations may increase the shortfall caused by attacks. The cyber-impact analysis platform is performed iteratively considering load deviation at each bus from negative 60% to positive 60%. Fig. 3 shows a heat map describing the impact of load deviation at each bus on revenue shortfall. The brighter/darker color means that the load deviation decreases/increases the effectiveness of cyberattacks. From the heat map, the load deviations at bus 4, bus 9, bus 16, bus 21, and bus 29 decrease the shortfall. The load deviation at bus 39 can increase the shortfall. Load deviations at other buses have no impact.

This phenomenon aligns with Remark 2 that load deviations can help the false data injection but do not necessarily impact the value of shortfalls. The reason is that some load deviations cause a step change at shadow prices, while other deviations do not cause step changes. Thus, load deviation is a vital consideration for designing cyberattacks causing shortfalls. It is worth mentioning that the heat map only shows single bus load deviations for illustrative purposes, and that load deviation may have more impact if combined at different buses.

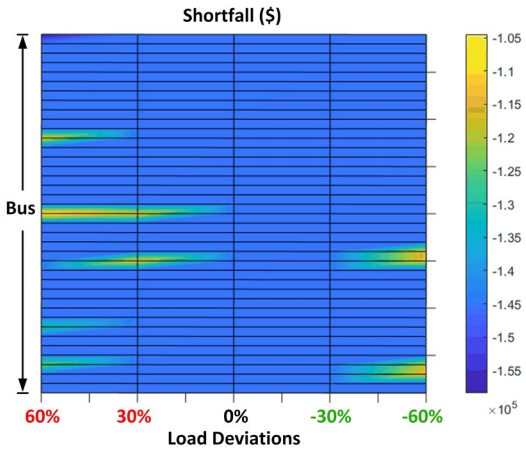

Fig. 3. Impact of load deviation at each bus on revenue shortfall

C. Case Study 3: Importance of Different Types of Attacks.

Different types of false data may contribute differently to the revenue shortfall. As shown in Remark 3, cyberattacks on demands, bids, and unit capacities do not affect revenue adequacy if the attack is not combined with transmission line rating attacks. Thus, the cyber-impact analysis is first performed on the above three types of attack individually, and these three attacks cannot cause shortfalls, as shown in the first row of Table II. Any penetration level (i.e., the amount of injected false data) cannot induce shortfalls when r_l is 0. The attack on the congestion pattern is not applicable to this case study because the congestion status is a binary variable that does not have a penetration level.

Table II. Effectiveness of different types of attacks

Penetration level	Shortfall by load attack (\$ $\times 10^4$)	Shortfall by bid attack (\$ $\times 10^4$)	Shortfall by unit attack (\$ $\times 10^4$)
$r_l = 0$	0	0	0
0%	6.96	6.96	6.96
5%	6.96	7.52	6.96
10%	6.96	8.07	6.96
15%	7.86	8.62	7.86
20%	7.86	9.18	7.86

The rest of Table II shows the effectiveness of load attack, bid attack, and unit capacity attack with respect to penetration levels when a line rating attack is fixed to a 20% penetration level (i.e., r_l is 20%). The shortfall experiences step changes with load attack and unit capacity attack, which means the shortfall stays the same until the penetration level increases to a certain value. For example, the shortfall changes from \$6.96×10^4 to \$7.86×10^4 when the penetration level increases from 10% to 15%. The reason is that load attack and unit capacity attack induce a step change for shadow prices when the penetration level increases from 10% to 15%. The shortfall changes linearly with the penetration level of the bid attack because the value of the bid attack at the marginal unit directly impacts the value of the shadow prices. Table III shows the shortfall induced by the line rating attack. Similarly, the higher the penetration level, the larger the shortfall will be. The second row of Table II, where attacks on load, bid, unit capacity are at 0% penetration and the attack on line rating are at 20% penetration, has the same shortfall as the last column in Table III. If Table II is compared with Table III, the line rating attack provides a base value for the shortfall, and the other attacks further increase the shortfalls. This phenomenon aligns with Remark 3 that line rating attacks serve as a base for causing a shortfall, and the other attacks further enhance the severity of the shortfall.

Table III. Effectiveness of line rating attack

Penetration level	5%	10%	15%	20%
Shortfall by line rating attack (\$ $\times 10^4$)	1.08	2.74	4.11	6.96

D. Case Study 4: Severity of Revenue Shortfall Caused by Cyberattacks

As indicated in Remark 4, cyberattacks are able to cause a much more significant impact on revenue shortfall than other unexpected contingency events. This case study compares

unexpected contingency events and cyberattacks using the proposed cyber-impact analysis model.

In a DA market-clearing scenario, three lines are congested: line 2-3, line 2-30, and line 6-11. Thus, to induce a revenue shortfall, three unexpected contingency events are considered to be 10% line-derating at each of the lines. To show the severity of the revenue shortfall caused by a cyberattack fairly, the penetration level of the line rating attack is also considered to be 10%, and the line rating attack can only perform at one line. Fig. 4 compares the revenue shortfall caused by cyberattacks with unexpected contingency events under different attack degrees (i.e., from 1 to 10). Higher attack degrees mean more attacks are successful in manipulating parameters. When the attack degree is higher than 7, the resulting revenue shortfall stays the same, which means that the attacker can achieve the most desirable result if 7 of the attacks on parameters are successful. Under such scenarios, cyberattacks can lead up to shortfalls which are 141%, 903%, and 180% of that caused by contingency event 1, event 2, and event 3, respectively. It is worth noting that some attacks could be easily detected, and the capability of the attacker could be limited. Therefore, the attacker may not always achieve an attack degree as high as 7. As shown in the curve of Fig. 4, a lower attack degree makes a lower revenue shortfall. However, the revenue shortfall caused by attacks is still significant compared with contingency events, even when the attack degree is low. For example, when the attack degree is as low as 2, the cyberattack can lead to shortfalls which are 115%, 481%, and 148% of that caused by contingency event 1, event 2, and event 3, respectively. Therefore, the threat from cyberattacks is much more severe than unexpected contingency events.

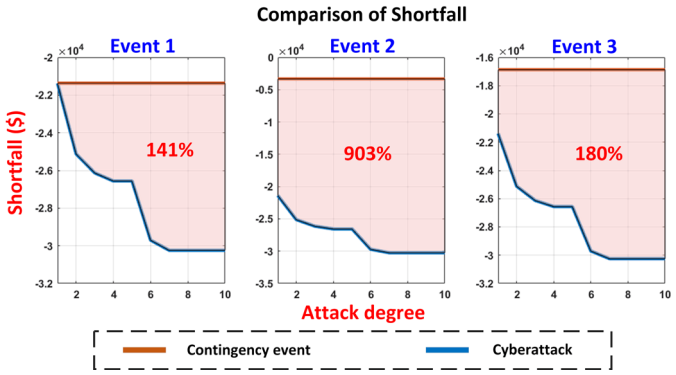

Fig. 4. Comparison of shortfall between contingency events and cyberattacks

Further, the significant amount of shortfall impacts bilateral transactions. Conventional solutions to cover the revenue shortfall are prorating the settlements to all FTRs, which makes the FTR lose the ability to create a perfect hedge for bilateral contracts when the shortfall is high. The allocation procedure in [36] is an example. Considering a FTR transaction between node 3 and node 2, the revenue loss due to the shortfall allocation under contingency events and cyberattacks is shown in Table IV. The attack can induce up to an 89.4% revenue loss for this FTR, which basically makes the FTR lose its ability to hedge the congestion charge for bilateral transactions.

Table IV. Revenue loss for FTR 3-2 due to allocation

	Event 1	Event 2	Event 3	Attack
Revenue lost (%)	48.4	32.3	36.8	Up to 89.4

Figure 4 and Table IV show that the cyberattack could severe a revenue shortfall and damage FTR transactions. It is worth noting that the revenue shortfall could be intentionally induced by malicious agents through cyberattacks to disrupt the FTR transactions and market settlements. The revenue shortfall could also be a side-effect, even if the revenue shortfall is not the main target. For example, the leftmost subplot of Figure 4 shows that a cyberattack at line 2-3 would lead to a $21,956 revenue shortfall. It is possible that the attack at line 2-3 aims to create congestions for higher LMPs. However, the $21,956 revenue shortfall is inevitably induced by such attacks.

VI. Conclusion

In conclusion, this paper identifies two missing components in current electricity market cybersecurity research: (1) the lack of impact analysis of cyberattacks on ISO revenue adequacy, which prevents ISOs from comprehensively understanding the financial consequences of cyberattacks; and (2) the lack of investigations into the trilevel coupling between attack decisions, ex-ante dispatches, and ex-post pricing because previous research focuses only on the bilevel modeling of the attack and RT market-clearing.

Therefore, this paper first provides a theoretical analysis of the impact of cyberattacks on revenue adequacy by formulating sufficient conditions and summarizing four remarks. Next, a cyber-impact analysis platform for revenue adequacy analysis with an attacker model on the upper-level, an ex-ante model at the middle-level, and an ex-post model at the lower-level is proposed to numerically investigate the impact of cyberattacks on revenue adequacy. In the end, the New England 39-bus system is applied to discuss the theoretical analysis remarks on impact of cyberattacks on revenue adequacy with the proposed numerical analysis platform.

Our future works will focus on combining the proposed cyber-impact platform with artificial intelligence techniques providing a more efficient and accurate analysis platform, where the analytical sensitivity analysis is provided for each falsely injected data type.

VII. Reference

[1] Q. Zhang and F. Li, "Cyber-Vulnerability Analysis for Real-Time Power Market Operation," *IEEE Transactions on Smart Grid*, vol. 12, no. 4, pp. 3527-3537, July 2021.

[2] CSIS, “Significant Cyber Incidents Since 2006,” Washington, DC, Dec. 2020, [Online]. Available: https://csis-website-prod.s3.amazonaws.com/s3fs-public/200626_Cyber_Events.pdf.

[3] S. Lyngaas, “German intelligence agencies warn of Russian hacking threats to critical infrastructure,” cyberscoop.com. https://www.cyberscoop.com/german-intelligence-memo-berserk-bear-critical-infrastructure/ (accessed Mar. 2021)

[4] G. Liang, J. Zhao, F. Luo, S. R. Weller, and Z. Y. Dong, “A review of false data injection attacks against modern power systems,” *IEEE Trans. Smart Grid*, vol. 8, no. 4, pp. 1630–1638, Jul. 2017.

[5] Q. Zhang, F. Li, Q. Shi, K. Tomsovic, J. Sun and L. Ren, "Profit-Oriented False Data Injection on Electricity Market: Reviews, Analyses, and Insights," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 9, pp. 5876-5886, Sept. 2021.

[6] L. Xie, Y. Mo, and B. Sinopoli, ‘‘Integrity data attacks in power market operations, *IEEE Trans. Smart Grid*, 2(4), pp. 659–666, Dec. 2011.

[7] H. Xu, Y. Lin, X. Zhang and F. Wang, "Power System Parameter Attack for Financial Profits in Electricity Markets," *IEEE Transactions on Smart Grid*, vol. 11, no. 4, pp. 3438-3446, July 2020.

[8] S. Tan, W.-Z. Song, M. Stewart, J. Yang, and L. Tong, "Online data integrity attacks against real-time electrical market in smart grid," *IEEE Trans. Smart Grid*, vol. 9, no. 1, pp. 313–322, Jan. 2018.

[9] G. Liang, S. R. Weller, F. Luo, J. Zhao, and Z. Y. Dong, "Generalized FDIA-based cyber topology attack with application to the Australian electricity market trading mechanism," *IEEE Trans. Smart Grid*, vol. 9, no. 4, pp. 3820–3829, Jul. 2017.

[10] G. Liang, S. R. Weller, J. Zhao, F. Luo, and Z. Y. Dong, "A framework for cyber-topology attacks: Line-switching and new attack scenarios," *IEEE Trans. Smart Grid*, vol. 9, no. 4, pp. 3820-3829, Mar. 2017.

[11] H. Ye, Y. Ge, X. Liu and Z. Li, "Transmission Line Rating Attack in Two-Settlement Electricity Markets," *IEEE Transactions on Smart Grid*, vol. 7, no. 3, pp. 1346-1355, May 2016.

[12] C. Liu, M. Zhou, J. Wu, C. Long, and D. Kundur, "Financially motivated FDI on SCED in real-time electricity markets: Attacks and Mitigation," *IEEE Transactions on Smart Grid*, vol. 10, no. 2, pp. 1949–1959, Dec. 2017.

[13] D.-H. Choi and L. Xie, "Sensitivity analysis of real-time locational marginal price to SCADA sensor data corruption," *IEEE Trans. Power Syst*., vol. 29, no. 3, pp. 1110–1120, May 2014.

[14] L. Jia, J. Kim, R. J. Thomas, and L. Tong, "Impact of data quality on real-time locational marginal price," *IEEE Trans. Power Syst*., vol. 29, no. 2, pp. 627–636, Mar. 2014.

[15] A. Tajer, "False data injection attacks in electricity markets by limited adversaries: stochastic robustness," *IEEE Trans. Smart Grid*, vol. 9, no. 6, pp. 5710-5720, 2017.

[16] Y. Lin, A. Abur and H. Xu, "Identifying Security Vulnerabilities in Electricity Market Operations Induced by Weakly Detectable Network Parameter Errors," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 1, pp. 627-636, Jan. 2021.

[17] M. R. Mengis and A. Tajer, "Data injection attacks on electricity markets by limited adversaries: Worst-case robustness," *IEEE Transactions on Smart Grid*, vol. PP, no. 99, April 2017.

[18] S. Tan, W.-Z. Song, M. Stewart, J. Yang, and L. Tong, "Online data integrity attacks against real-time electrical market in smart grid," *IEEE Trans. Smart Grid*, vol. 9, no. 1, pp. 313–322, Jan. 2018.

[19] M. Esmalifalak, H. Nguyen, R. Zheng, L. Xie, L. Song, and Z. Han, "A stealthy attack against electricity market using independent component analysis," *IEEE Syst. J.,* vol. 12, no. 1, pp. 297–307, Mar. 2018.

[20] G. Chaojun, P. Jirutitijaroen, and M. Motani, "Detecting false data injection attacks in AC state estimation," *IEEE Trans. Smart Grid*, vol. 6, no. 5, pp. 2476–2483, Sep. 2015.

[21] J. Zhao, G. Zhang and R. A. Jabr, "Robust Detection of Cyber Attacks on State Estimators Using Phasor Measurements," *IEEE Transactions on Power Systems*, vol. 32, no. 3, pp. 2468-2470, May 2017.

[22] A. Ashok, M. Govindarasu and V. Ajjarapu, "Online Detection of Stealthy False Data Injection Attacks in Power System State Estimation," *IEEE Transactions on Smart Grid*, vol. 9, no. 3, pp. 1636-1646, May 2018.

[23] Q. Zhang, F. Li, H. Cui, R. Bo and L. Ren, "Market-Level Defense Against FDIA and a New LMP-Disguising Attack Strategy in Real-Time Market Operations," *IEEE Transactions on Power Systems*, vol. 36, no. 2, pp. 1419-1431, March 2021.

[24] F. Li, Y. Wei and S. Adhikari, "Improving an Unjustified Common Practice in Ex Post LMP Calculation," *IEEE Transactions on Power Systems*, vol. 25, no. 2, pp. 1195-1197, May 2010.

[25] Q. Zhang, F. Li, W. Feng, X. Wang, L. Bai and R. Bo, "Building Marginal Pattern Library With Unbiased Training Dataset for Enhancing Model-Free Load-ED Mapping," *IEEE Open Access Journal of Power and Energy*, vol. 9, pp. 88-98, 2022.

[26] S. Deng, S. Oren, and A.P. Meliopoulos, "The inherent inefficiency of simultaneously feasible financial transmission rights auctions," *Energy Economics*, vol. 32, no. 4, pp. 779-785, July 2010.

[27] S. Bhattacharjee, R. Sioshansi and H. Zareipour, "Energy Storage Participation in Wholesale Markets: The Impact of State-of-Energy Management," *IEEE Open Access Journal of Power and Energy*, vol. 9, pp. 173-182, 2022.

[28] W. W. Hogan, "Financial transmission rights, revenue adequacy and multi-settlement electricity markets," vol. 31813, 2013. [Online]. Available: https://sites.hks.harvard.edu/fs/whogan/Hogan_FTR_Rev_Adequacy_031813.pdf.

[29] V. Sarkar and S. A. Khaparde, "A Comprehensive Assessment of the Evolution of Financial Transmission Rights," *IEEE Transactions on Power Systems*, vol. 23, no. 4, pp. 1783-1795, Nov. 2008.

[30] N. K. Kandasamy, "An Investigation on Feasibility and Security for Cyberattacks on Generator Synchronization Process," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 9, pp. 5825-5834, Sept. 2020.

[31] K. Khanna, B. K. Panigrahi and A. Joshi, "Bid Modification Attack in Smart Grid for Monetary Benefits," *2016 IEEE International Symposium on Nanoelectronic and Information Systems (iNIS)*, 2016.

[32] J. Zhao, F. Li, S. Mukherjee and C. Sticht, "Deep Reinforcement Learning-Based Model-Free On-Line Dynamic Multi-Microgrid Formation to Enhance Resilience," *IEEE Trans. on Smart Grid*, vol. 13, no. 4, pp. 2557-2567, July 2022.

[33] R. D. Zimmerman, C. E. Murillo-Sanchez, and R. J. Thomas, "MATPOWER: Steady-State Operations, Planning and Analysis Tools for Power Systems Research and Education," *IEEE Transactions on Power Systems*, vol. 26, no. 1, pp. 12–19, Feb. 2011.

[34] A. Mehrzad, M. Darmiani, Y. Mousavi, M. Shafie-Khah and M. Aghamohammadi, "An Efficient Rapid Method for Generators Coherency Identification in Large Power Systems," *IEEE Open Access Journal of Power and Energy*, vol. 9, pp. 151-160, 2022.

[35] F. Li, K. Tomsovic, and H. Cui, "A Large-Scale Test Bed as a Virtual Power Grid - For Closed Loop Controls for Research and Testing," *IEEE Power and Energy Magazine*, vol. 18, issue 2, pp. 60-68, March-April 2020.

[36] S. S. Oren and K. W. Hedman, "Revenue adequacy, shortfall allocation and transmission performance incentives in FTR/FGR markets," *2010 IREP Symposium Bulk Power System Dynamics and Control - VIII (IREP)*, Rio de Janeiro, Brazil, 2010, pp. 1-6.

BIOGRAPHIES

Qiwei Zhang (S'17) is presently a Ph.D. student in the department of electrical engineering and computer science at The University of Tennessee, Knoxville (UTK). He received his B.S.E.E. degree from North China Electrical Power University in 2016 and M.S.E.E degree from UTK in 2018. His research interests include cybersecurity in power systems, power system optimization, and market operation.

Fangxing Li (S'98–M'01–SM'05–F'17) is also known as Fran Li. He received the B.S.E.E. and M.S.E.E. degrees from Southeast University, Nanjing, China, in 1994 and 1997, respectively, and the Ph.D. degree from Virginia Tech, Blacksburg, VA, USA, in 2001. From 2001 to 2005, he worked as a Senior and then Principal Consulting Engineer at ABB Energy Systems Consulting, Raleigh, NC. He has been a faculty member at UTK since 2005. Currently, he is the James W. McConnell Professor in electrical engineering and the UTK Campus Director of CURENT. His current research interests include resilience, artificial intelligence in power, demand response, distributed generation and microgrid, and energy markets. Prof. Li is presently serving as the Editor-In-Chief of *IEEE Open Access Journal of Power and Energy (OAJPE)*. During 2020-2021, he served as the Chair of IEEE Power System Operation, Planning and Economics committee.

Xiaofei Wang (S'20) received the B.S. degree from North China Electric Power University in 2014, and the M.S. degree from Wuhan University, China, in 2017. Presently, he is pursuing the Ph.D. degree at the University of Tennessee, Knoxville, USA. His research interests include power system optimization, demand response, and distribution market.