IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 26 June 2024, accepted 22 August 2024, date of publication 27 August 2024, date of current version 5 September 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3450631

RESEARCH ARTICLE

Cyber-Physical Distribution Systems Resilience Against Cyberattacks via a Remediation Framework Based on Static VAR Compensators (SVCs)

EHSAN NADERI[1], (Member, IEEE), AND ARASH ASRARI[2], (Senior Member, IEEE)
[1]Department of Electrical Engineering, College of Engineering and Computer Science, Arkansas State University, Jonesboro, AR 72401, USA
[2]Department of Electrical and Computer Engineering, Purdue University Northwest, Hammond, IN 46323, USA

Corresponding author: Ehsan Naderi (enaderi@astate.edu)

This work was supported in part by the National Science Foundation under Grant 2348420.

ABSTRACT This paper proposes a framework to optimally employ static VAR compensators (SVCs) within a customized reconfiguration of system topology, leading to remediation of voltage violations caused by false data injection (FDI) cyberattacks targeting smart distribution grids. The designed framework contains formulations associated with planning and operation phases. In the planning phase, the scrutinized system, modified by photovoltaic (PV) units, is enhanced by optimally allocating static VAR compensators (SVCs) to keep the unity power factor throughout the system. Then, distribution system operator (DSO), being in attacker's shoe, examines relevant cyberattack scenarios leading to voltage violations within the distribution system. Finally, in the operation phase, DSO takes advantage of the optimally planned SVCs to identify proper vectors (i.e., remedial actions) to cope with such potential scenarios of cyberattacks. These (to be recognized) vectors are associated with the *variable shunt susceptance* of the mentioned SVCs, which will be identified by solving a customized distribution feeder reconfiguration (DFR) problem in the operation phase. The main objective of the customized DFR is to maximize the contributions of SVCs through enhancing the voltage profile of the targeted system. This will enable DSO to mitigate the negative impacts of the FDI attacks and recover the voltage profile of the smart distribution network. The effectiveness of the proposed RAS is validated on three different smart test systems (i.e., 33-bus, 95-bus, and 136-bus systems), which are modified to contain SVC components and renewable-based distributed generation (DG) units.

INDEX TERMS Distribution feeder reconfiguration (DFR), false data injection (FDI), overvoltage, remedial action scheme (RAS), smart distribution grid, undervoltage, static VAR compensator (SVC), voltage violation.

I. INTRODUCTION

A. BACKGROUND, DEFINITIONS, AND MOTIVATION

Remedial action schemes (RASs) have recently been in the spotlight as an effective approach to mitigate cyberattacks targeting smart power grids [1], [2], [3]. Power networks are frequently targeted by devastating cyberattacks, posing a variety of challenges for system operators to manage in real-time [4]. As an illustration, in 2015, a large-scale cyber-attack that targeted the Ukrainian power grid caused up to six hours of power outages for almost a quarter million end users [5]. To add to that, the U.S. power grid was targeted by attackers in 2018 for the purpose of collecting sensitive data about the operation of its power plants. According to the U.S. Department of Homeland Security, such complex cyber-attacks can be repeated in the future on larger-scale power systems [6]. Despite the fact that smart power grids allow for the operation and control of systems via computerized

The associate editor coordinating the review of this manuscript and approving it for publication was Agostino Forestiero.

platforms, they provide a significant attack surface for adversaries to inject false data into their cyber layer, which can lead to power outages, voltage instability, and other challenges in system operation. In this paper, we focus on *voltage violation*. In normal conditions and during transients, voltage violation may result in voltage collapse, which is caused by the grid's inability to keep an acceptable voltage magnitude across all buses. In other words, power system operators are responsible for maintaining acceptable voltage magnitudes on the system buses under a variety of disturbances. If the voltage profile experiences a progressive alteration (e.g., drop or rise) in the first couple of minutes following a disturbance, the entire power grid will be jeopardized since the power flow will be affected in branches. According to [7] and [8], a majority of widespread blackouts have been the consequences of voltage instabilities. Therefore, there is a critical need to 1) study the voltage profile of smart distribution grids targeted by false data injection (FDI) attacks and 2) provide feasible RASs for system operators to mitigate the voltage violations caused by such attacks.

B. LITERATURE REVIEW

1) SVC IMPLEMENTATION

Static VAR compensators (SVCs) are widely used for providing rapid regulation of reactive power and voltage profile [9]. Moreover, the firing angle of the embedded thyristors empowers the SVC component to instantaneously respond to the voltage deviation, bringing the voltage level back to normal [9]. Further, optimal placement of SVCs in a typical power system can enhance voltage stability and improve voltage profile across the entire system [10]. Toward this end, this paper 1) focuses on the described unique capability of the distributed SVCs and 2) introduces a framework based on which optimally allocated SVCs are utilized to alleviate/mitigate the voltage violations caused by FDI attacks targeting smart distribution systems. The existing literature contains research implementing SVC devices to improve the overall performance of power grids. This section briefly reviews a selection of relevant papers. For instance, Liu et al. in [11] developed a model for SVC accompanied with phase-switching to alleviate the unbalances caused by distributed PV arrays throughout a low-voltage grid. Babu et al. proposed an algorithm, recognizing the vulnerable buses to voltage instability, to optimally allocate SVC devices for voltage profile enhancement [12]. Utilizing probabilistic AC-DC power flow, Gupta introduced an optimal reactive power planning taking into account the uncertainties for renewable energy resources (i.e., solar and wind units), loads, and electric vehicle charging [13]. The developed approach in [13] implemented voltage collapse index to obtain the optimal ratings of SVCs and capacitor banks. Interested readers are referred to [14], [15], and [16] for more examples of research efforts on SVCs to improve the performance of power grids.

2) FDI TARGETING POWER GRIDS

The aim of this section is to provide a concise review of the current state-of-the-art FDI models, targeting different parts of smart power systems. For examples, changing power grid's status and modifying the parameters of the network, Liu et al. introduced a network parameter coordinated FDI cyberattack to diminish the number of measurements to be manipulated [17]. A dynamic FDI model, taking into account local network information, was proposed by Wang et al. in [18] in order to feature the typical data injection attack integrated with dynamic behavior of the attacker. Li et al. presented 1) a cyber-physical model to defend the system against cyber attackers considering ideal measurements in FDI attacks and 2) a generative adversarial network-based model to recognize the deviations from ideal measurements [19]. A secure hybrid dynamic state estimation approach, comprising a dynamic model for the attack vector, was proposed by Kazemi et al. in [20], where a Kalman filter was utilized to estimate the attack vector and the system states. Scrutinizing the impact of various levels of FDI cyberattacks on the performance of energy market-based distribution system, Jhala et al. proposed an attack model based on which an adversary was able to manipulate the smart meters by injecting false data [21]. Lakshminarayana et al. developed an algorithm to construct data driven FDIs considering limited number of measurements to bypass bad data detection via random matrix theory [22].

3) RAS AGAINST FDI ATTACKS

Several studies have been conducted on remedial action schemes (RASs) to mitigate the negative impacts of FDI cyberattacks and improve the overall performance of targeted systems. Herein, a brief discussion of the selected relevant frameworks presented recently is included. As an illustration, improving the resilience of a power grid to operate in standalone mode as a consequence of FDI attack, Ajao et al. proposed a RAS to enhance the transient stability index of the system [23]. Khan et al. in [24] proposed a RAS to determine the most critical aggregators targeted by FDI cyberattacks leading to congestion as well as increasing the consumers' electricity bill. Naderi and Asrari introduced a RAS oriented toward a secondary electricity market to react against potential cyber threats causing market power in favor of a set of sellers [25]. Huang et al. proposed a RAS considering resilience-based optimal power flow to identify critical generators in responding to cyberattacks [26]. Developing a framework to support online RAS, Hossain-McKenzie et al. confirmed that offline RASs can fail when FDI attacks are highly dynamic and unforeseeable [27]. Tan et al. presented a complete RAS capable of protecting a failed power grid against cyberattacks targeting automatic generation control via disconnecting the generation units and load centers [28]. Furthermore, Aysheh et al. in [29] proposed an active power grid layer approach using ''perturb and observe'' technique

TABLE 1. Taxonomy table summarizing focus of the proposed framework and the reviewed [23], [24], [25], [26], [27], [28], [29], [30], [31], [32], [33], presenting different RASs against FDI cyberattacks targeting smart power systems.

Ref.	Focus	FACTS Utilization
[23]	Transient stability	No
[24]	Congestion management	No
[25]	Market power	No
[26]	Critical components	No
[27]	System dynamism	No
[28]	Automatic generation control	No
[29]	Voltage deviation	No
[30]	Power outage	D-FACTS
[31]	Grid vulnerability	No
[32]	Protective relays coordination	No
[33]	System congestions	TCSC
Proposed framework in this paper	Voltage violation in both forms of overvoltage and undervoltage	SVC

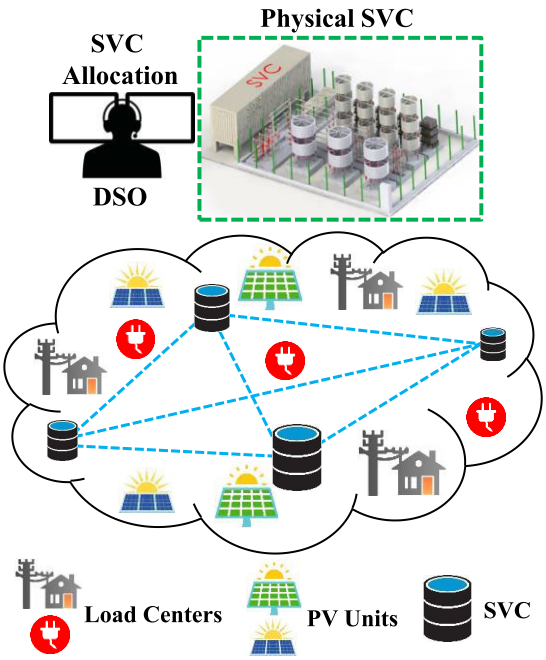

FIGURE 1. Planning phase of the proposed framework to enhance the distribution system by installing SVC components.

in order to detect and protect the distribution grid targeted by FDI attacks leading to voltage deviation. Interested readers are directed to [30], [31], [32], and [33] for more examples about the remedial action frameworks against FDI cyberattacks targeting smart power systems. To sum up, TABLE 1 presents a summary of the key features and results of the review [23], [24], [25], [26], [27], [28], [29], [30], [31], [32], [33]. From TABLE 1, it can be perceived that despite significant RASs against different types of cyberattacks, current literature needs to be enhanced via new findings associated with the effectiveness of SVC components against FDI attacks targeting voltage profiles. This stems from the fact that SVCs are extensively utilized to provide very fast voltage regulation via firing angle control of the thyristors, embedded in the body of SVCs, which enable them to have almost instantaneous speed of response [9].

C. KNOWLEDGE GAP AND CONTRIBUTION

Although there have been valuable research works on remedial actions against cyberattacks targeting smart grids (e.g., [23], [24], [25], [26], [27], [28], [29], [30], [31], [32], [33]), the following research question has yet to be addressed: *How to take advantage of SVC components as a RAS to tackle FDI attacks designed to result in voltage violation in smart distribution systems*? In other words, there is no work in the existing literature to scrutinize the effectiveness of SVCs as a remediation framework against cyberattacks targeting smart distribution systems. To precisely approach the indicated research gap, this paper proposes a unified framework, the highlighting features of which are as follows.

I) Identifying *optimal* location, size, and number of SVC components to be installed in the distribution system to improve its voltage profile (planning phase from the *system operator's perspective*, as shown in Fig. 1),

II) Targeting the system enhanced by the SVCs via different forms of FDI cyberattacks bypassing state estimation process and resulting in voltage violation (the system operator being in "*attacker's shoes*", as illustrated in Fig. 2 (a)), and

III) Utilizing RASs (i.e., solving a customized version of distribution feeder reconfiguration (DFR) integrated with SVC components) to mitigate the negative impacts of the FDI attacks and restore the voltage profile of the smart distribution system to its normal state (operation phase from the *system operator's point of view*, as displayed in Fig. 2 (b)). In other words, the main contribution of this paper is to interlink the planning and operation phases to effectively take advantage of optimally allocated SVCs in a remedial action framework via network reconfiguration, leading to remediation of voltage violations caused by FDI cyberattacks bypassing the detection stage.

D. ORGANIZATION OF THE PAPER

The rest of the paper is organized as follows: Section II presents the developed framework and the corresponding problem formulations, which can be divided into three parts including planning phase, attack phase, and remediation. Illustrative cases studies (i.e., IEEE 33-bus, 95-bus, and 136-bus test distribution systems) are introduced in Section III, where the simulation results and analyses are also provided. Finally, Section IV concludes the paper.

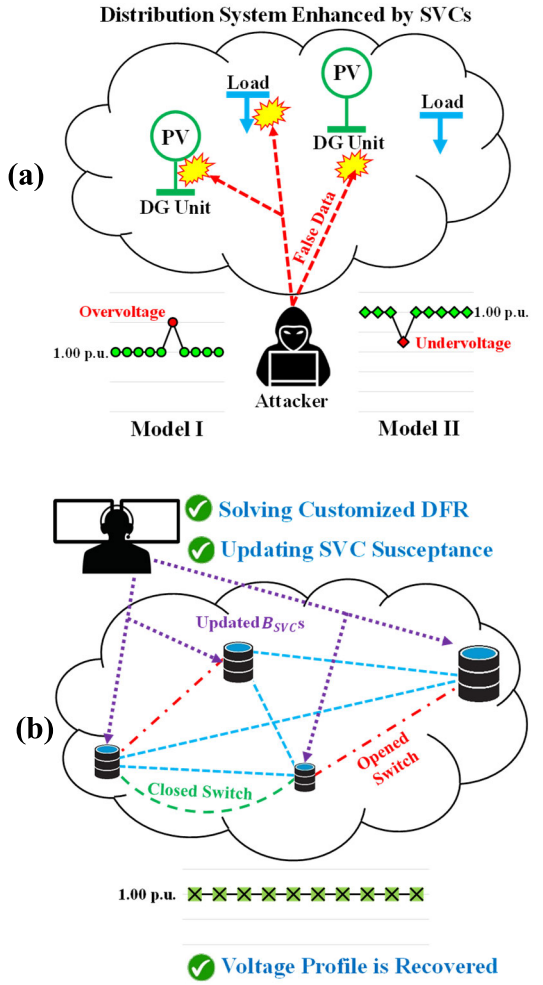

FIGURE 2. Operation phase of the proposed framework (a) FDI attacks targeting load centers and renewable-based generation units to result in overvoltages and undervoltages and (b) the proposed remedial action scheme (RAS) against FDI cyberattacks causing voltage violations.

II. PROPOSED FRAMEWORK AND PROBLEM FORMULATION

In the first phase of the proposed framework (i.e., planning phase), distribution system operator (DSO) optimally allocates SVC components in the distribution grid (see Fig. 1). This phase is a prerequisite for the operation phase to ensure that the number, location, and size of SVCs are optimally obtained to maximize the system's loadability. Otherwise, DSO will not be able to effectively perform the remedial actions. In the second phase, as demonstrated in Fig. 2 (a), DSO tries to be in the attacker's shoe to examine the scenario of system being targeted by two types of FDI attacks, one resulting in overvoltage (Model I) and one causing undervoltage (Model II). In the third phase, DSO takes advantage of the analyzed SVC devices in the first phase, which have optimally been allocated, to recover voltage profile of the targeted grid via a customized network reconfiguration approach (see Fig. 2 (b)). Detailed information about each phase is provided in the following subsections.

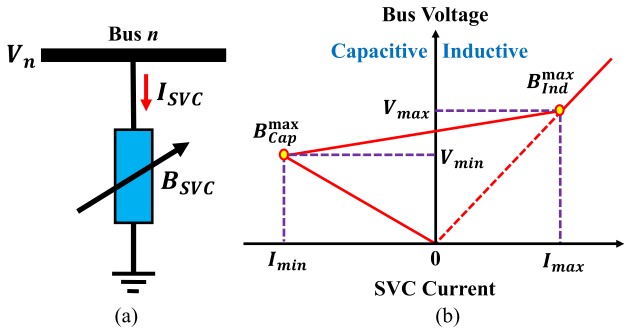

FIGURE 3. SVC component (a) model for power flow analysis and (b) Voltage-current characteristic of the SVC in voltage regulating mode.

A. PLANNING PHASE

1) STATIC VAR COMPENSATOR (SVC) MODEL

Operating in two different modalities (i.e., voltage regulation and VAR control), SVC is one of the shunt compensators from flexible AC transmission systems (FACTS) family. In addition, due to its *rapid* and *smooth* response in regulating the voltage, SVC has been utilized in both transmission and distribution levels [34], [35]. Different models of SVC (e.g., generator behind an inductive reactance [36]) for power flow analyses have been proposed in the existing literature. Interested readers are directed to [37] for more information about SVC models. This paper presents the *shunt connected variable susceptance* model for a typical SVC, which is demonstrated in Fig. 3 (a) [9]. Based on this figure, the reactive current and reactive power related to the SVC component can be written in (1)-(2), where B_{SVC} denotes variable susceptance of SVC; V_n is the voltage of bus n; and I_{SVC} and Q_{SVC} are, respectively, the reactive current and power either injected or absorbed by the SVC device in order to regulate the voltage of bus n. It is noted that, in this model, Q_{SVC} is considered as a *state variable* in the power flow calculations. Thus, the main constraint on the application of the SVC model is presented in (3), where $B_{SVC}^{\min}$ and $B_{SVC}^{\max}$ are, respectively, the minimum and maximum limits related to SVC's admittance.

$$I_{SVC} = j\,(B_{SVC} \times V_n) \tag{1}$$

$$Q_{SVC} = -V_n^2 \times B_{SVC} \tag{2}$$

$$B_{SVC}^{\min} \le B_{SVC} \le B_{SVC}^{\max} \tag{3}$$

In this case, if the SVC is operated in voltage regulation mode, it functions based on the voltage-current characteristic illustrated in Fig. 3 (b). From this figure, it can be inferred that when the voltage magnitude of the modified bus is low, the SVC generates reactive power (i.e., capacitive role). However, when the voltage magnitude is high, it absorbs reactive power (i.e., inductive role). To obtain a better perspective, according to (4), as long as B_{SVC} remains between its upper and lower limits, the voltage magnitude will be regulated at the reference value (i.e., V_{ref}). These limits are related to reactive powers of capacitor banks (i.e., $B_{Cap}^{\max}$) and reactor

banks (i.e., $B_{Ind}^{\max}$).

$$V_n^{comp} = \begin{cases} \left(X_{Slope} \times I_{SVC}\right) + V_{ref} & \text{if } B_{SVC} \text{ is in acceptable range} \\ \dfrac{1}{B_{Ind}^{\max}} & \text{if SVC is totally inductive} \\ -\dfrac{1}{B_{Cap}^{\max}} & \text{if SVC is totally capacitive} \end{cases} \tag{4}$$

where V_{ref} is the reference value of voltage (i.e., 1.00 p.u.); Xs is the slope/droop reactance (see Fig. 3 (b)); $B_{Ind}^{\max}$ and $B_{Ind}^{\max}$ are, respectively, maximum inductive and capacitive susceptance; and V_n^{comp} is the compensated voltage magnitude for bus n.

2) OPTIMAL ALLOCATION AND SIZING OF SVCs

This step is a prerequisite for the proposed RAS against cyberattacks. This is because, if SVCs are not *optimally* allocated throughout the system, DSO cannot use them to mitigate voltage violations, caused by FDI attacks.

a: SVC COST

SVC components are installed at a cost, which needs to be minimized considering maximization of system's loadability. Hence, cost function for a typical SVC device is presented in (5), where A, B, and C are cost coefficients; s indicates the operation range of the SVC in terms of MVAR; and C_{SVC} is the SVC's cost function to be minimized ($/kVAR) [38].

$$C_{SVC} = A \times s^2 + B \times s + C \tag{5}$$

b: TOTAL ACTIVE POWER LOSS

Equations (6)-(8) denote total real power loss associated with a distribution system in which the first term (i.e., P_L^{Branch}) reflects the power loss related to the branches and the second term (i.e., P_L^{Trans}) indicates the power loss associated with transformers since different transformer loadings can affect copper loss.

$$P_{Loss} = P_L^{Branch} + P_L^{Trans} \tag{6}$$

$$P_L^{Branch} = \sum_{l=1}^{N_{line}} R_l \times \left|I_l^{Branch}\right|^2 \tag{7}$$

$$P_L^{Trans} = \sum_{t=1}^{N_{Trans}} R_t \times \left|I_t^{Trans}\right|^2 \tag{8}$$

where R_l and I_l^{Branch} are, respectively, resistance and current for lth branch; R_t and I_t^{Trans} are resistance and current for tth transformer; and P_{Loss} is the power loss to be minimized (kW).

c: VOLTAGE DEVIATION INDEX

In a distribution system, voltage deviation occurs when the voltage level of the buses deviates from its normal range, resulting in voltage violation in extreme cases. Accordingly, voltage deviation index (VDI) is calculated as the sum of all deviations from the reference value, as presented in (9) [39], which is one of the metrics to evaluate the effectiveness of the proposed remediation framework (see Section II-C).

$$VDI = \sum_{n=1}^{N_{Bus}} \left|V_{ref} - V_n\right| \tag{9}$$

where N_{Bus} is the number of buses in the distribution system; and VDI is the voltage deviation index (p.u.) to be minimized.

d: OBJECTIVE FUNCTION OF PLANNING PHASE

Equation (10), which is the main objective function related to the planning phase (i.e., enhancing the performance of the system by optimally installing SVC components), presents the summation of (5)-(9), where ω_1 and ω_2 are the relevant weighting factors to be selected by DSO. Detailed information about selecting the weighting factors can be found in [40].

$$\min \left\{ \begin{array}{l} \sum_{i=1}^{N_{SVC}} A \times s_i^2 + B \times s_i + C \\ +\omega_1 \times \left(\sum_{l=1}^{N_{line}} R_l \times \left|I_l^{Branch}\right|^2 + \sum_{t=1}^{N_{Trans}} R_t \times \left|I_t^{Trans}\right|^2 \right) \\ +\omega_2 \times \sum_{n=1}^{N_{Bus}} \left|V_{ref} - V_n\right| \end{array} \right\} \tag{10}$$

Objective function (10) is minimized subject to satisfying a set of technical constraints, which are presented in (11)-(16). It is noted that constraints (11)-(12), respectively, are the active and reactive power equilibrium in the system. Constraint (13) signifies the limits over voltage magnitude of the buses. Constraint (14) denotes the PV penetration level providing a relationship between the amounts of power injected into the grid by the PV plants and total system's demand. Constraint (15) specifies the boundaries over reactive power (either injected or absorbed) of SVC. Finally, constraint (16) retains the apparent power associated with lth branch within its acceptable range.

$$P_G^{SS} + \sum_{k=1}^{N_{PV}} P_k^{PV} - \sum_{n=1}^{N_{Bus}} P_n^{Demand} - \sum_{l}^{B_{line}} P_l^{Loss} = 0 \tag{11}$$

$$Q_G^{SS} - \sum_{n=1}^{N_{Bus}} Q_n^{Demand} - \sum_{l}^{B_{line}} Q_l^{Loss} = 0 \tag{12}$$

$$V_n^{\min} \le V_n \le V_n^{\max} \tag{13}$$

$$\sum_{k=1}^{N_{PV}} P_k^{PV} \le \xi \sum_{n=1}^{N_{Bus}} P_n^{Demand} \tag{14}$$

$$Q_{SVC}^{\min} \le Q_{SVC} \le Q_{SVC}^{\max} \tag{15}$$

$$S_l \le S_l^{\max}, \quad l \in N_{line} \tag{16}$$

where P_G^{SS} and Q_G^{SS} are, respectively, the active and reactive power delivered from the substation to the distribution

system; P_k^{PV} is the active power related to kth PV plant; P_n^{Demand} and Q_n^{Demand} are, respectively, active and reactive power demands at bus n; P_l^{Loss} and Q_l^{Loss} indicate the active and reactive power losses for lth branch, respectively; V_n is the voltage magnitude at bus n; $V_n^{\min}$ and $V_n^{\max}$ are the minimum and maximum limits of voltage magnitude at bus n, respectively; ξ is a coefficient confining the level of PV penetration with respect to the total demand of the system, which can be altered from zero (i.e., 0% collaboration in supplying the system's demand) to one (i.e., fully serving the load); $Q_{SVC}^{\min}$ and $Q_{SVC}^{\max}$ are, respectively, the minimum and maximum limits corresponding to reactive power (either absorbed or injected) of the SVC; finally, S_l and $S_l^{\max}$ are the apparent power and its maximum limit associated with lth branch, respectively.

e: OPTIMAL NUMBER OF SVC

The number of SVC components to be installed in a typical distribution system should be *optimally* recognized to be cost-effective. This is due to the fact that only after installing a *specific number* of SVC devices, the loading parameter (i.e., η in this paper) increases from the initial value (e.g., 1.00); thus, after the saturation point, installing more SVCs will no longer enhance the system's loadability [41]. In this paper, the optimal number of SVCs is identified via assessing bus loading, modifying the active and reactive power of each bus (see (17)-(18)). In (17)-(18), P_n and Q_n are, respectively, the active and reactive power of load at bus n; P_n^{Base} and Q_n^{Base} are, respectively, the active and reactive power at initial operating point associated with bus n; κ_1 and κ_2 denote the control parameters to increase bus loading level (i.e., active and reactive); and η is the loadability to be assessed to identify the optimal number of SVCs.

$$P_n = (1 + \kappa_1 \eta) \times P_n^{Base} \tag{17}$$

$$Q_n = (1 + \kappa_2 \eta) \times Q_n^{Base} \tag{18}$$

B. FDI CYBERATTACKS LEADING TO VOLTAGE VIOLATION (DSO IN ATTACKER'S SHOES)

Referring to Fig. 2 (a), an attacker attempts to compromise a smart distribution system, which has already been upgraded with SVC components during the planning phase (refer to Fig. 1). The intention of the launched FDI cyberattacks is to intentionally violate voltage (i.e., causing different rates of overvoltage and/or undervoltage). By bypassing security systems, the cyberattacker manipulates data associated with load centers and PV plants. It is noted that a noticeable alteration in the normal voltage profile of the distribution system should be taken into account as a *warning sign*, which needs to be further investigated. If the system is operated normally, that alteration in the magnitude of voltage will be the consequence of either physical or cyber incidents (e.g., short circuit faults or a software bug), which can be detected by bad data detection (BDD) algorithms embedded in state estimation. In smart distribution systems, a typical BDD mechanism calculates the Euclidian norm of the measurement residual vectors to recognize any errors in the measurements (see (19)). However, as long as attackers keep the residual vector of the norm of measurement sets below the threshold (e.g., Φ), a systematic malicious data injection into the distribution grid cannot be detected. Hence, such well-designed FDI attacks can lead to operational issues (e.g., *voltage violation* in this paper). Interested readers are directed to [17] for more information about the conditions based on which attackers can bypass AC state estimation in distribution systems.

$$\|M - h(x)\| \geq \Phi \tag{19}$$

where M is the set of measurements; Φ is the threshold of BDD; x is the vector of estimated values; and h is a nonlinear function relating measurements to the state variables.

In a distribution system modified by solar panels, the real and imaginary parts associated with voltage in bus n are, respectively, presented in (20)-(21), where P_n and Q_n are, respectively, the active and reactive power injections for nth bus; V_{PCC} denotes the voltage at the point of common coupling; and R_n^{eq} and X_n^{eq} are the equivalent resistance and reactance seen from bus n, respectively. It is noted that, in a typical distribution system, the imaginary part of voltage can be neglected since it is substantially less than the corresponding real part [42].

$$Re\{v_n\} = \frac{\left(P_n \times R_n^{eq}\right) + \left(Q_n \times X_n^{eq}\right)}{V_{PCC}} + V_{PCC} \tag{20}$$

$$Im\{v_n\} = \frac{\left(P_n \times X_n^{eq}\right) - \left(Q_n \times X_n^{eq}\right)}{V_{PCC}} \tag{21}$$

Based on (20)-(21), one can infer that the magnitude of voltage at bus n can change after any manipulations in the active and reactive powers (i.e., P_n and Q_n). As an illustration, any positive values of active and reactive powers (e.g., $+\Delta P_n$ and $+\Delta Q_n$) result in a *rise* in the magnitude of voltage at bus n (i.e., Model I FDI attack, as depicted in Fig. 2 (a)). On the other hand, the magnitude of voltage will drop if attackers inject any negative values of active and reactive powers (i.e., Model II, as shown in Fig. 2 (a)). As a result, the magnitude of voltage at the targeted bus n (i.e., $\hat{V}_n$) can be written in (22)-(24), where $\hat{P}_n$ and $\hat{Q}_n$ are, respectively the manipulated active and reactive powers; and R_n^{Th} and X_n^{Th} are elements of Thevenin equivalent circuit. It is noted that the data manipulations in both FDI models (i.e., Model I and Model II) needs to be minimized, as presented in (25), which is the main objective function of the FDI attacks causing voltage violation.

$$\hat{V}_n = \frac{\left(\hat{P}_n \times R_n^{Th}\right) + \left(\hat{Q}_n \times X_n^{Th}\right)}{V_{PCC}} + V_{PCC} \tag{22}$$

$$\hat{P}_n = P_n + \Delta P_n \tag{23}$$

$$\hat{Q}_n = Q_n + \Delta Q_n \tag{24}$$

It is noted that (25) should be minimized subject to a set of constraints, which bypass the AC state estimation (refer to (19)), to keep the attack undetectable. For the sake of

brevity, interested readers are directed to the earlier step of this research for detailed information about the mentioned process [42].

$$\min \left\{ \sum_{c\in\Omega} \left(\Delta P_c^{Demand} + \Delta Q_c^{Demand} \right) + \sum_{g\in\Xi} \left(\Delta P_g^{Gen} + \Delta Q_g^{Gen} \right) \right\} \quad (25)$$

where Ω and Ξ, respectively, indicate the set of buses that encompass load center and generating unit; ΔP_c^{Demand} and ΔQ_c^{Demand} are, respectively, the attack vectors (i.e., active and reactive) of false data associated with cth load center; and ΔP_g^{Gen} and ΔQ_g^{Gen} are the attack vectors for gth unit.

C. PROPOSED RAS AGAINST FDI LEADING TO VOLTAGE VIOLATION

The expected outcome of the second phase is a manipulated voltage profile by the FDI cyberattacks leading to system undervoltages and overvoltages. This is the time for DSO to react to targeted voltage profile, necessitating the application of the optimally pre-installed SVC components capable of instantaneously responding to the voltage violations. To this end, DSO solves an optimization problem, which is a customized version of distribution feeder reconfiguration (DFR), that is aligned with optimal updating of the SVCs' susceptance. With this upgrade, the voltage stability of the targeted system will be enhanced, and the voltage profile will be improved (refer to Fig. 2 (b)). As mentioned before, it is intended that the FDI attacks bypass the BDD mechanism (refer to (19)), which is the reason for highlighting the significance of the proposed RAS. In other words, if the system operator detects the FDI attacks, they could be prevented [17]. However, FDI attacks will result in voltage violations if attackers are able to circumvent the security systems stealthily. Thus, by solving the customized DFR problem (i.e., (26)-(41)), DSO mitigates the voltage violation issue caused by the FDI cyberattacks. Within this framework, after solving the customized DFR problem, the susceptance of preinstalled SVCs will be updated to new values since B_{SVC}s are included in the vector of decision variables (see (26)). This will modify the reactive power flow associated with SVCs, regulating the voltage magnitude of system's buses. It is also noted that the FDI attacks affect the grid's parameters, shown by circumflex.

1) DECISION VARIABLES OF THE PROBLEM

Decision variables of the DFR problem (i.e., the proposed RAS) from the DSO's standpoint are provided in (26)-(30).

$$\hat{X} = [TS, SW, \hat{B}_{SVC}] \quad (26)$$

$$[TS] = [TS_1, TS_2, \ldots, TS_r, \ldots, TS_{N_{TS}}]_{1\times N_{TS}} \quad (27)$$

$$[SW] = [SW_1, SW_2, \ldots, SW_s, \ldots, SW_{N_{SW}}]_{1\times N_{SW}} \quad (28)$$

$$[\hat{B}_{SVC}] = [\hat{B}_{SVC_1}, \hat{B}_{SVC_2}, \ldots, \hat{B}_{SVC_i}, \ldots, \hat{B}_{SVC_{N_{SVC}}}]_{1\times N_{SVC}} \quad (29)$$

$$D = N_{TS} + N_{SW} + N_{SVC} \quad (30)$$

where $\hat{X}$ is the vector of decision variables after the FDI attack; TS_r is the status of rth tie-switch (zero shows the open status and one is related to the closed status); SW_s indicates the sth sectionalizing switch; $\hat{B}_{SVC_i}$ is the susceptance for ith SVC after the FDI attack; N_{TS} and N_{SW} are, respectively, the number of tie-switches and sectionalizing switches; and D is the dimension of the problem (i.e., the proposed RAS) or the number of decision variables.

2) OBJECTIVE FUNCTION (VOLTAGE STABILITY)

Reducing the short circuit capacity (SCC), distributed energy sources jeopardize the stability of distribution systems, which is due to the design and operation of such systems. Further, the SCC level (i.e., the current level) is proportional to the voltage of substation [43]. Hence, the main objective of the RAS (i.e., (31)-(36)) is to enhance the voltage stability index (VSI) of the targeted smart distribution system, which considers 1) advantage of the pre-installed SVC components and 2) the security challenges of PV arrays based on the SCC limit.

$$\max \left\{ \left(\frac{1}{N_B} \times \sum_{n=1}^{N_B} \hat{\Gamma}_n \right) + \Psi \right\} \quad (31)$$

$$\hat{\Gamma}_n = \frac{\min \hat{\Upsilon}_n}{\hat{\Upsilon}_n} \quad (32)$$

$$\min \hat{\Upsilon}_n = \left(\frac{2 \times \sqrt{\hat{P}_n^2 + \hat{Q}_n^2}}{\hat{V}_n^{Th}} \right) \times \left(1 - \sin\hat{\alpha}\right) \quad (33)$$

$$\hat{\Upsilon}_n = \frac{\hat{V}_n^{Th}}{\sqrt{\left(\hat{R}_n^{Th}\right)^2 + \left(\hat{X}_n^{Th}\right)^2}} \quad (34)$$

$$\hat{P}_n = \frac{\hat{V}_n^{Th}\hat{V}_n \left(\hat{R}_n^{Th}\cos\hat{\Phi} - \hat{X}_n^{Th}\sin\hat{\Phi}\right) - \hat{R}_n^{Th}\hat{V}_n^2}{\left(\hat{R}_n^{Th}\right)^2 + \left(\hat{X}_n^{Th}\right)^2} \quad (35)$$

$$\hat{Q}_n = \frac{\hat{V}_n^{Th}\hat{V}_n \left(\hat{R}_n^{Th}\sin\hat{\Phi} + \hat{X}_n^{Th}\cos\hat{\Phi}\right) - \hat{X}_n^{Th}\hat{V}_n^2}{\left(\hat{R}_n^{Th}\right)^2 + \left(\hat{X}_n^{Th}\right)^2} \quad (36)$$

where $\hat{\Upsilon}_n$ indicates the voltage stability index for bus n affected by cyberattack; Ψ is a penalty factor excluding the unstable decision variables (i.e., Ψ is equal to 0 if $VSI_n \geq 0$; otherwise it equals ∞); $min\ \hat{\Upsilon}_n$ denotes the lower level of SCC to guarantee voltage stability at targeted bus n; $\hat{\alpha}$ is power factor angle after the cyberattack; $\hat{V}_n^{Th}$, $\hat{R}_n^{Th}$, and $\hat{X}_n^{Th}$ are elements of Thevenin equivalent circuit for the targeted distribution system seen from the substation [43], [44]; and $\hat{P}_n$ and $\hat{Q}_n$ are, respectively, the manipulated active and reactive power of load at bus n after launching the cyberattack.

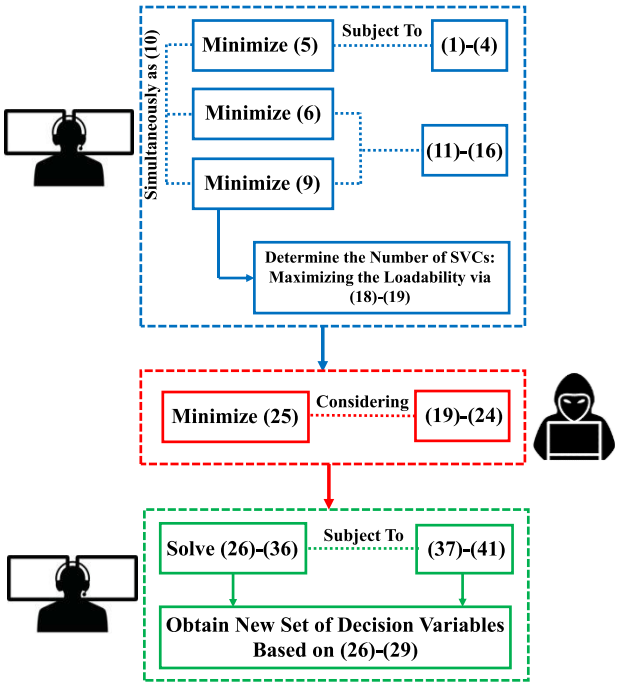

FIGURE 4. The flowchart of mathematical equations for the proposed framework solved via optimization toolboxes of MATLAB.

3) RELEVANT CONSTRAINTS

The proposed optimization problem presented in (31)-(36) is solved subject to satisfying a set of constraints provided in (37)-(41), where N_{sub} is the number of substations; $\hat{I}_t^{Trans}$ and $I_{t,\max}^{Trans}$ are, respectively, tth transformer's current after attack and its upper limit; $\hat{I}_x^{Feeder}$ and $I_{x,\max}^{Feeder}$ are, respectively, the current magnitude after attack and its upper boundary for xth feeder; and $\hat{S}_l$ is the apparent power for lth branch after attack.

$$N_{line} = N_B - N_{sub} \tag{37}$$

$$\hat{I}_t^{Trans} \leq I_{t,\max}^{Trans} \tag{38}$$

$$\hat{I}_x^{Feeder} \leq I_{x,\max}^{Feeder} \tag{39}$$

$$V_n^{\min} \leq \hat{V}_n \leq V_n^{\max} \tag{40}$$

$$\hat{S}_l \leq S_l^{\max}, \quad l \in N_{line} \tag{41}$$

Fig. 4 clearly illustrates implementation of the presented problem formulation (i.e., (1)-(41)) within the proposed framework including three separate phases of planning phase (i.e., the top box depicted in Fig. 4), cyberattack phase (i.e., the middle box shown in Fig. 4), and the remediation phase (i.e., the bottom box displayed in Fig. 4), all described in detail in Section II. It is necessary to note that the associated optimization problems have been solved via optimization toolboxes of MATLAB such as fsolve.

III. ILLUSTRATIVE CASE STUDIES AND OBTAINED RESULTS

The proposed framework was coded in MATLAB. In addition, MATPOWER package, which is a powerful tool for electric power system simulation and optimization, was used to accomplish the power flow calculations [45]. The cost coefficients of SVC components were assumed to be 0.0003, -0.305, and 127.38, which are adopted from [38].

TABLE 2. Obtained results of the planning phase (i.e., optimal SVC allocation, sizing, and number) on test system I.

Variables	Scenario I	Scenario II	Scenario III
	$-0.2 \leq B_{SVC} \leq 0.2$	$-0.4 \leq B_{SVC} \leq 0.4$	$-0.6 \leq B_{SVC} \leq 0.6$
# of SVCs	10	7	6
Location (Bus)	#6, #9, #12, #16, #18, #22, #25, #28, #30, and #33	#6, #12, #18, #22, #25, #30, and #33	#6, #12, #18, #22, #25, and #33
Sum Q_{SVC}	0.81 MVAR	0.83 MVAR	0.82 MVAR
Sum C_{SVC}	\$131.13/kVAR	\$132.05/kVAR	\$131.89/kVAR
P_{Loss}	98.50 kW	115.12 kW	126.34 kW
VDI	0.107 p.u.	0.672 p.u.	0.756 p.u.
Time (s)	64.3	38.5	19.1

A. TEST SYSTEM I (IEEE 33-BUS SYSTEM)

This test system is a small-scale case study with only one substation. The full data related to IEEE 33-bus distribution system can be found in [45]. For this test system, ξ is 0.3 meaning that up to 30% of the system's demand can be supplied by the PV power plants, the characteristics of which are extracted from [42]. The total active and reactive power demands on the system are, respectively, 3715 kW and 2300 kVAR. Further, initial values of total power loss (i.e., (7)) and VDI ((i.e., (10)) are, respectively, 203 kW and 1.7 p.u.

1) SVC ALLOCATION AND ITS IMPACTS ON IEEE 33-BUS SYSTEM

The main objective of SVC implementation is to decrease both P_{Loss} and VDI by installing an *optimal number* of SVC components at *optimal places* with *optimal sizes*. Considering various levels of compensation (i.e., constraint (4)), TABLE 2 presents the obtained results associated with optimal allocation, sizing, and number of SVC devices to be installed in IEEE 33-bus distribution system to improve the voltage profile throughout the system. In this regard, Fig. 5 depicts the relationship between η (i.e., system's loadability presented in (17)-(18)) and the number of SVCs. From this figure, it can be perceived that Scenario I is the best scenario in terms of improving the system's loadabolity (i.e., $\eta = 1.71$). Furthermore, Fig. 6 illustrates the voltage profile of the IEEE 33-bus test system in different situations. It can be concluded from Fig. 6 that the planning phase has been successful since the voltage profile of the system is noticeably enhanced after installing ten SVCs for Scenario I (i.e., green dash-dotted curve) with respect to the original system (i.e., black solid curve). Referring to Figs. 5-6 and also TABLE 2, one can perceive that although the amount of compensation and the total cost of SVCs as a consequence (see Q_{SVC} and C_{SVC} presented in TABLE 2) almost remain the same for all three scenarios, Scenario I signifies better loadability (see blue dashed

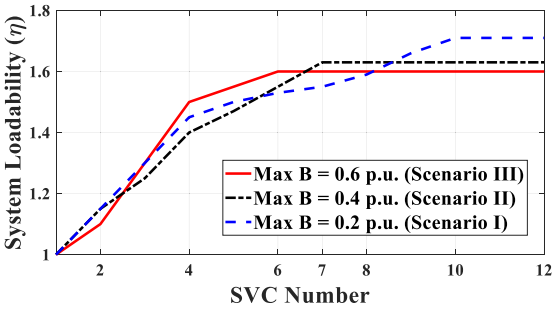

FIGURE 5. Loadability of IEEE 33-bus system for different numbers of SVCs.

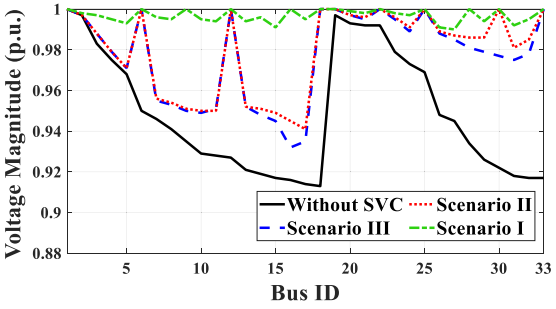

FIGURE 6. Voltage profile of IEEE 33-bus system before/after SVC installations.

curve in Fig. 5) and voltage profile (see green dash-dotted curve in Fig. 6) because more SVCs are distributed throughout the system; hence, Scenario I is considered as the enhanced distribution system for the rest of this section to be examined for the cyberattack and the relevant remedial action.

To show the effectiveness of implanting SVC components to enhance the voltage profile of IEEE 33-bus test system, TABLE 3 provides a comparison between optimally allocating SVC components in the system and taking advantage of distributed renewable energy resources (i.e., small scale PV panels and wind turbines), as presented in [46]. From this table, it can be inferred that installing SVC components in the body of the distribution system has a superior performance compared to the alternative methods with respect to the voltage deviation index.

2) ATTACKS LEADING TO VOLTAGE VIOLATION

Fig. 7 (a) displays the voltage profile of the IEEE 33-bus test system, already enhanced by SVC devices, after different types of FDI cyberattacks leading to voltage violation (see Section II.D). The corresponding FDIs are displayed in Fig. 7 (b), showing different patterns associated with the injected malicious data. Although the voltage profile of the system was noticeably improved after installing ten SVCs (see green dash-dotted curve shown in Fig. 6), it undergoes intentional changes (see Fig. 7 (a)) toward higher magnitudes of voltage as a consequence of *attack Model I* (see the red dotted curve) and also lower magnitude of voltage as

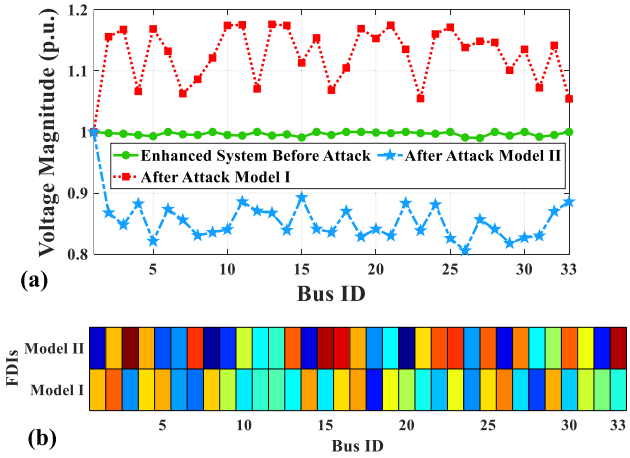

FIGURE 7. (a) Voltage profile of the improved system by 10 SVCs after FDI attacks resulting in overvoltage (i.e., attack Model I) and undervoltage (i.e., attack Model II) and (b) the obtained FDI vectors (kW).

TABLE 3. SVC vs. other remediations against voltage violation.

Technique	Original VDI (p.u.)	VDI (p.u.) After Implementing the Technique
SVC Allocation	1.7	0.107
Feeder Reconfiguration	1.7	0.421
Capacitor Banks Allocation [46]	–	0.25
Distributed Generation and Capacitor Banks Allocations [46]	–	0.29

a consequence of *attack Model II* (see the blue dash-dotted curve). Comparing Figs. 6-7, one can infer that even if a typical distribution system is streamlined by SVC components maintaining the voltage profile of the system in an acceptable range, *well-designed FDI cyberattacks* targeting load centers can push the system toward extreme voltage violations. This is where the significance of RAS (i.e., the focus of this paper) comes under the spotlight.

3) RAS TO MITIGATE THE ATTACK'S IMPACTS

Responding to the cyberattacks leading to voltage violation (see Fig. 7 (a)), DSO takes advantage of the pre-installed SVC devices and solves the described customized network reconfiguration aiming at improving the voltage stability index of the targeted system (i.e., (26)-(41)) and mitigating the impacts of the FDI cyberattacks. Table 4 provides the obtained results associated with the proposed RAS when $\hat{B}_{SVC}$ is limited to [-0.2,0.2] p.u. (i.e., Scenario I). From this table, it can be inferred that the RAS has significantly improved the voltage profile of the targeted system since the voltage magnitude of buses have come back to the normalcy (see the bold faced VDI presented in TABLE 4). Moreover, Fig. 8 illustrates the value of susceptance associated with ten SVCs installed in the system before and after the RAS applied by the DSO. From TABLE 4 and Fig. 8, one can infer that the

TABLE 4. Obtained results of the RAS related to Scenario I on test system I.

Variables	Before Attack		Model I		Model II	
	Before SVC	After SVC	Attack	RAS	Attack	RAS
P_{Loss} (kW)	203	98.50	225	131	251	128
VDI (p.u.)	1.7	0.107	4.13	**0.22**	5.78	**0.24**
Reaction Time (s)	–	–	22.6		19.8	

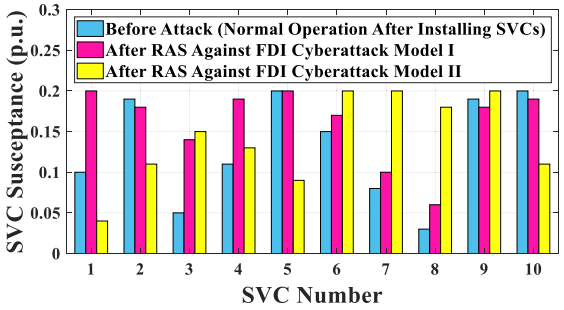

FIGURE 8. Upgrading the susceptance of SVCs in response to the FDI cyberattacks leading to voltage violation (Vertical axis: absolute value).

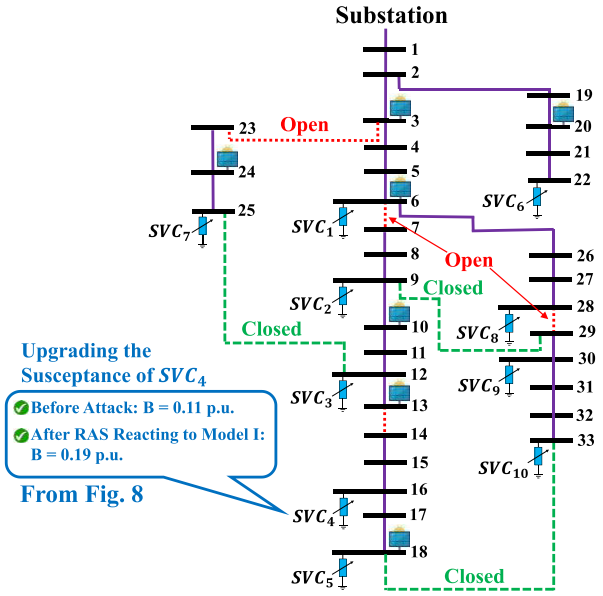

FIGURE 9. The configuration of IEEE 33-bus test system after the proposed RAS to mitigate the FDI cyberattack (Network has 32 normally closed switches, 4 of which are opened after the RAS, and 5 normally open switches, 3 of which are closed after the RAS).

DSO has been able to handle the FDI attack by solving the proposed DFR problem, which took 39.4 s obtained from a quad-core laptop machine with 1.6 MHz frequency and 4 GB of RAM. To obtain a better perspective about the new topology of switches after the RAS responding to attack Model I, Fig. 9 compares the status of switches before and after solving the proposed DFR problem enhancing the voltage stability (i.e., (10)) of the targeted system. It is noted that for the sake of cleanness of Fig. 9, we have reflected only the change in B_{SVC} for the fourth SVC component after solving the DFR problem, reacting to Model I FDI attack; however, all the ten SVCs have experienced different rates of change in their susceptance while reacting to both Model I and Model II cyberattacks, as illustrated in Fig. 8.

B. TEST SYSTEM II (IEEE 95-BUS SYSTEM)

This section validates the effectiveness of the proposed RAS on a larger distribution system (i.e., IEEE 95-bus test system with eighteen feeders) to highlight the performance of the proposed approach irrespective of the size of distribution systems. The full data associated with IEEE 95 bus distribution system can be extracted from [47] and [48]. Plus, this case study is modified by installing nine PV plants at buses #6, #10, #20, #25, #34, #41, #50, #70 and #76. All PVs have a 1.8 MW rated capacity. The main characteristics of the installed PV plants are provided in TABLE 5, where FPP is the fixed purchased price [49]. For this test system, ξ equals 0.4 meaning that only up to 40% of system's demand can be served by the PV power plants. Finally, B_{SVC} is bounded into range of [−0.2,0.2] p.u.

TABLE 5. Descriptions of the features associated with PV plants.

# of PV	Bus	P_{min} (kW)	P_{max} (kW)	Q_{min} (kVAR)	Q_{max} (kVAR)	FPP
1	6	0	200	-200	200	0.10
2	10	0	200	-200	200	0.18
3	20	0	200	-200	200	0.22
4	25	0	200	-200	200	0.16
5	34	0	200	-200	200	0.25
6	41	0	200	-200	200	0.12
7	50	0	200	-200	200	0.22
8	70	0	200	-200	200	0.25
9	76	0	200	-200	200	0.11

1) SVC ALLOCATION AND ITS IMPACTS ON IEEE 95-BUS SYSTEM

After solving (1)-(18), which is related to the planning phase, the optimal number of SVCs to be installed in IEEE 95-bus test system is obtained 25. The summation of Q_{SVC} and C_{SVC} associated with these 25 installed SVC devices are, respectively, 3.4 MVAR and \$129/kVAR. The VDI and active power losses (i.e., P_{Loss}) of IEEE 95-bus system before and after installing 25 SVC devices are presented in TABLE 6. According to this table, one can infer that the active power losses and voltage deviation index of the distribution grid reduce by approximately 82% and 93%, respectively, after installing the optimal number of 25 SVC devices compared to the original system. Although the distribution system is equipped with SVCs installed in their optimal locations to improve the voltage profile of the system, organized FDI cyberattacks can increase voltage deviations and power losses.

TABLE 6. Comparison of voltage profile and power loss on test system II.

Variables	Before Attack		Model I		Model II	
	Before SVC	After SVC	Attack	RAS	Attack	RAS
P_{Loss} (kW)	554	101	608	113	622	114
VDI (p.u.)	6.2	0.441	7.1	**0.5**	7.8	**0.51**
Reaction Time (s)	–	–	93.1		95.0	

TABLE 7. Comparison of voltage profile and power loss on test system III.

Variables	Before Attack		Model I		Model II	
	Before SVC	After SVC	Attack	RAS	Attack	RAS
P_{Loss} (kW)	668	284	792	312	814	321
VDI (p.u.)	9.1	0.665	11.1	**0.699**	11.7	**0.706**
Reaction Time (s)	–	–	144		149	

TABLE 8. The proposed RAS against FDI attack Model I with different intensities on test system III.

Variables	5%		10%		20%	
	Attack	RAS	Attack	RAS	Attack	RAS
VDI (p.u.)	9.8	**0.675**	11.1	**0.699**	13.7	**0.739**
Reaction Time (s)	144		144		151	

2) FDI CYBERATTACKS AND RAS TO MITIGATE THEM

TABLE 6 also provides the VDI and P_{Loss} of the system after the FDI cyberattacks launched by the attacker and also after the RAS (i.e., (26)-(41)) applied by the DSO in response to the FDI attacks leading to voltage violation. From this table, the following conclusions can be obtained.

i) After optimal SVC allocation, P_{Loss} and VDI decrease by 82% and 93%, respectively,

ii) Launching attack Model I results in 502% and 1510% rise in P_{Loss} and VDI, respectively; however, after applying the proposed RAS responding to this cyberattack in about 93.1 s, the power loss and voltage deviation decrease to new values, which show only a 12% increase with respect to the enhanced system by SVCs, and

iii) After launching attack Model II, P_{Loss} and VDI, respectively, skyrocket to 515% and 1670%; however, the proposed framework is able to recover the voltage profile after almost 95 s such that new values of P_{Loss} and VDI are about 12% more than the amounts associated with the enhanced system in the normal operation.

C. TEST SYSTEM III (136-BUS UNBALANCED DISTRIBUTION SYSTEM)

This section performs the validation of the proposed RAS on a well-known 136-bus distribution system [50], which is modified to be an unbalanced three-phase system to mimic the nature of realistic distribution grids. Interested readers are directed to [25] for more information about the taken steps to change the original system into an unbalanced three-phase system. Through solving (1)-(18) in the planning phase, the optimal number of SVCs to be installed in the modified 136-bus test system is obtained to be 32. The summation of Q_{SVC} and C_{SVC} associated with these SVCs are, respectively, 4.2 MVAR and \$131/kVAR. The VDI and active power losses of 136-bus system before and after installing 32 SVC components are presented in TABLE 7. According to this table, it can be inferred that although the 136-bus test system is vulnerable to voltage violation, the negative impacts of the undervoltage attack (i.e., Model II) can be more severe. However, the proposed RAS was able to alleviate the impacts of both FDI cyberattacks causing overvoltage and undervoltage (see the bold-faced numbers shown in TABLE 7).

To demonstrate the robustness of the proposed RAS against FDI attacks having different intensities, load centers are manipulated by injecting malicious data (i.e., ΔP_n and ΔQ_n), as provided in (23)-(24), to 5%, 10%, and 20% of the rating of each targeted bus. The obtained results are presented in TABLE 8, which confirms that the proposed RAS is effective to recover the targeted power system regardless of the scale of the system and the intensities of the FDI cyberattacks.

To obtain a better understanding about how changes in system parameters affect the performance of the proposed RAS against FDI cyberattacks targeting voltage profile, two different configurations of 136-bus distribution system are considered as follows:

- The original version of the system without any kind of distributed generation units, and
- The modified version of the system including distributed renewable and diesel engine units including 11 PV modules, 13 wind turbines, and 15 diesel engines. Specifications and technical information about these units, which includes location, size, etc. are extracted from the previous step of this research [25].

These two variants of 136-bus distribution system are targeted via both Model I and Model II FDI attacks, respectively, causing overvoltage and undervoltage. The threshold of manipulating the load data is set to 10% of the rated power of each bus for both FDI cyberattacks to obtain a fair comparison. Fig. 10 presents the results obtained from these two scenarios on 136-bus test system. According to this figure, it can be concluded that although system parameters are different in the aforementioned situations, the proposed RAS was able to reduce the VDI of the targeted system to an acceptable level.

D. DISCUSSION

Integration of SVC components into the current power and energy infrastructures poses several implementation issues. The technical compatibility of SVCs with the current grid infrastructure presents a huge barrier, as handling the new technology may necessitate significant changes to existing equipment and supervisory and control systems.

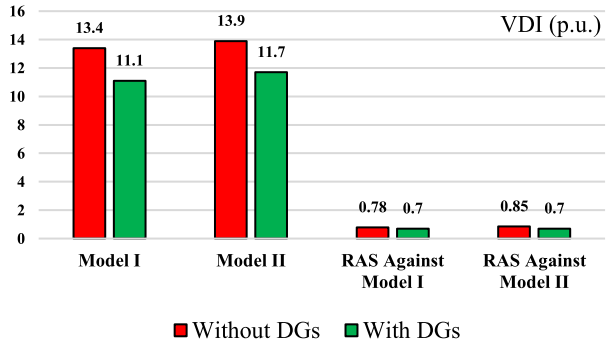

FIGURE 10. VDIs in terms of p.u. for 136-bus system after FDI cyberattack and after applying the proposed RAS considering significant alterations in the system parameters.

Furthermore, there are significant financial ramifications because installing SVCs necessitates paying for system modifications, installation labor, continuing maintenance, and compensators themselves. Many utility companies, particularly those with limited resources, may find these expenses prohibitive. Moreover, the integration of SVCs calls for modifications to the way that current operational procedures are carried out, such as the requirement that system operators receive enhanced training and the new protocols be developed to manage the dynamic behavior of the reactive power that SVCs provide as a response to voltage violations. These operational adjustments are necessary to guarantee that power system's reliability and resilience are maintained while still realizing the full benefits of SVCs, such as increased voltage stability and power quality. Hence, careful planning and strategic investment are necessary to overcome these obstacles and achieve successful SVC integration, as highlighted in [51] and [52].

IV. CONCLUSION

Given that the main application of static VAR compensator (SVC) is voltage regulation via reactive power compensation, this article scrutinized a *secondary* application of SVC to be implemented as a remedial action scheme (RAS) to mitigate the voltage violation caused by FDI cyberattacks in 33-bus, 95-bus, and 136-bus distribution systems. In order to validate the effectiveness of the proposed SVC-based RAS, the distribution systems were initially enhanced by installing an optimal number of SVC components in their optimal locations to maximize the loadability of the distribution grids. Then, the distribution system operator (DSO) was modeled to be in attacker's shoe to approach the modified distribution systems via simulating two different methods of FDI cyberattacks leading to overvoltage and undervoltage. In the next step, when the cyberattacks were confirmed by authorities, the DSO took advantage of the pre-installed SVC components via *a*) solving a customized distribution feeder reconfiguration (DFR) with the objective function of voltage stability index and *b*) identifying a new optimal set of decision variables including the susceptance of SVCs to maximize the voltage stability of the targeted systems.

Simulation results verify that installing more SVC devices with smaller capacities in all three test systems can lead to a more flexible RAS against different models of FDI attacks. For example, in the IEEE 33-bus distribution network, 10 SVC components with the capacity of 0.81 MVAR were optimally allocated in the system. The distributed SVCs reduced the voltage deviation indices (VDIs) from 4.13 p.u. and 5.78 p.u. after the FDI attacks Model I and Model II, respectively, to 0.22 p.u. and 0.24 p.u. after applying the RAS (i.e., solving the customized DFR problem to improve the voltage stability index). In the IEEE 95-bus test system, 25 SVC devices were optimally allocated in the system, which significantly reduced the VDIs from 7.1 p.u. and 7.8 p.u. after the FDI attacks to 0.5 p.u. after applying the presented RAS.

In this paper, we proposed a RAS to remediate overvoltages and undervoltages to maintain the voltage profile against the analyzed FDI attacks. However, cyberattacks leading to voltage collapse were not examined in this paper. Therefore, in the next step of this research, we will investigate an intelligent remedial action framework coping with the FDI cyberattacks designed to result in voltage collapse in smart distribution systems.

REFERENCES

[1] P. Nespoli, F. G. Mármol, and J. M. Vidal, "A bio-inspired reaction against cyberattacks: AIS-powered optimal countermeasures selection," *IEEE Access*, vol. 9, pp. 60971–60996, 2021.

[2] A. Panda, A. Baird, S. Pinisetty, and P. Roop, "Incremental security enforcement for cyber-physical systems," *IEEE Access*, vol. 11, pp. 18475–18498, 2023.

[3] J. Jithish, B. Alangot, N. Mahalingam, and K. S. Yeo, "Distributed anomaly detection in smart grids: A federated learning-based approach," *IEEE Access*, vol. 11, pp. 7157–7179, 2023.

[4] H. Kumar, Oscar. A. Alvarez, and S. Kumar, "Experimental evaluation of smart electric meters' resilience under cyber security attacks," *IEEE Access*, vol. 11, pp. 55349–55360, 2023.

[5] G. Liang, S. R. Weller, J. Zhao, F. Luo, and Z. Y. Dong, "The 2015 Ukraine blackout: Implications for false data injection attacks," *IEEE Trans. Power Syst.*, vol. 32, no. 4, pp. 3317–3318, Jul. 2017.

[6] The President's National Infrastructure Advisory Council (NIAC). *Surviving a Catastrophic Power Outage*. Accessed: Jun. 20, 2024. [Online]. Available: https://www.cisa.gov/sites/default/files/publications/NIAC%20Catastrophic%20Power%20Outage%20Study_FINAL.pdf

[7] M. Jonsson and J. E. Daalder, "An adaptive scheme to prevent undesirable distance protection operation during voltage instability," *IEEE Trans. Power Del.*, vol. 18, no. 4, pp. 1174–1180, Oct. 2003.

[8] M. A. M. Ariff and B. C. Pal, "Adaptive protection and control in the power system for wide-area blackout prevention," *IEEE Trans. Power Del.*, vol. 31, no. 4, pp. 1815–1825, Aug. 2016.

[9] E. Acha, C. R. Fuerte-Esquivel, H. Ambriz-Perez, and C. Angeles-Camacho, *FACTS: Modeling and Simulation in Power Networks*, 1st ed., Hoboken, NJ, USA: Wiley, 2004.

[10] J. Zha, J. Y. Wen, S. J. Cheng, and J. Ma, "A novel SVC allocation method for power system voltage stability enhancement by normal forms of diffeomorphism," *IEEE Trans. Power Syst.*, vol. 22, no. 4, pp. 1819–1825, Nov. 2007.

[11] B. Liu, K. Meng, Z. Y. Dong, P. K. C. Wong, and T. Ting, "Unbalance mitigation via phase-switching device and static var compensator in low-voltage distribution network," *IEEE Trans. Power Syst.*, vol. 35, no. 6, pp. 4856–4869, Nov. 2020.

[12] B. R. Lakshmikantha and K. S. Sundar, "A novel method for assessment of voltage stability improvement of radial distribution system using SVC at optimal location," in *Proc. ICEECCOT*, Msyuru, India, 2018, pp. 602–606.

[13] N. Gupta, "Probabilistic optimal reactive power planning with onshore and offshore wind generation, EV, and PV uncertainties," *IEEE Trans. Ind. Appl.*, vol. 56, no. 4, pp. 4200–4213, Jul. 2020.

[14] S. Chakraborty, S. Mukhopadhyay, and S. K. Biswas, "Coordination of D-STATCOM & SVC for dynamic VAR compensation and voltage stabilization of an AC grid interconnected to a DC microgrid," *IEEE Trans. Ind. Appl.*, vol. 58, no. 1, pp. 634–644, Jan. 2022.

[15] S. Keskes, S. Salleem, L. Chrifi-Alaoui, and M. B. Ali Kammoun, "Nonlinear coordinated passivation control of single machine infinite bus power system with static var compensator," *J. Mod. Power Syst. Clean Energy*, vol. 9, no. 6, pp. 1557–1565, Nov. 2021.

[16] D. Maiti, S. Mukhopadhyay, A. Banerji, S. K. Biswas, and N. K. Deb, "Harmonic cancellation in a three-phase thyristor controlled reactor using dual banks," *IEEE Trans. Ind. Electron.*, vol. 64, no. 12, pp. 9201–9209, Dec. 2017.

[17] C. Liu, H. Liang, and T. Chen, "Network parameter coordinated false data injection attacks against power system AC state estimation," *IEEE Trans. Smart Grid*, vol. 12, no. 2, pp. 1626–1639, Mar. 2021.

[18] H. Wang, J. Ruan, B. Zhou, C. Li, Q. Wu, M. Q. Raza, and G.-Z. Cao, "Dynamic data injection attack detection of cyber physical power systems with uncertainties," *IEEE Trans. Ind. Informat.*, vol. 15, no. 10, pp. 5505–5518, Oct. 2019.

[19] Y. Li, Y. Wang, and S. Hu, "Online generative adversary network based measurement recovery in false data injection attacks: A cyber-physical approach," *IEEE Trans. Ind. Informat.*, vol. 16, no. 3, pp. 2031–2043, Mar. 2020.

[20] Z. Kazemi, A. A. Safavi, F. Naseri, L. Urbas, and P. Setoodeh, "A secure hybrid dynamic-state estimation approach for power systems under false data injection attacks," *IEEE Trans. Ind. Informat.*, vol. 16, no. 12, pp. 7275–7286, Dec. 2020.

[21] K. Jhala, B. Natarajan, A. Pahwa, and H. Wu, "Stability of transactive energy market-based power distribution system under data integrity attack," *IEEE Trans. Ind. Informat.*, vol. 15, no. 10, pp. 5541–5550, Oct. 2019.

[22] S. Lakshminarayana, A. Kammoun, M. Debbah, and H. V. Poor, "Data-driven false data injection attacks against power grids: A random matrix approach," *IEEE Trans. Smart Grid*, vol. 12, no. 1, pp. 635–646, Jan. 2021.

[23] B. Ajao, P. Khaledian, B. K. Johnson, and Y. Chakhchoukh, "Implementation of remedial action scheme for transient stability index improvement of power system Island," in *Proc. IEEE Power Energy Soc. Innov. Smart Grid Technol.*, Washington, DC, USA, Jun. 2020, pp. 1–5.

[24] O. G. M. Khan, E. F. El-Saadany, A. Youssef, and M. F. Shaaban, "Cyber security of market-based congestion management methods in power distribution systems," *IEEE Trans. Ind. Informat.*, vol. 17, no. 12, pp. 8142–8153, Dec. 2021.

[25] E. Naderi and A. Asrari, "A remedial action scheme to mitigate market power caused by cyberattacks targeting a smart distribution system," *IEEE Trans. Ind. Informat.*, vol. 20, no. 3, pp. 3197–3208, Mar. 2024.

[26] H. Huang, M. Kazerooni, S. Hossain-McKenzie, S. Etigowni, S. Zonouz, and K. Davis, "Fast generation redispatch techniques for automated remedial action schemes," in *Proc. 20th Int. Conf. Intell. Syst. Appl. Power Syst. (ISAP)*, New Delhi, India, Dec. 2019, pp. 1–8.

[27] S. Hossain-McKenzie, M. Kazerooni, K. Davis, S. Etigowni, and S. Zonouz, "Analytic corrective control selection for online remedial action scheme design in a cyber adversarial environment," *IET Cyber-Phys. Syst., Theory Appl.*, vol. 2, no. 4, pp. 188–197, Dec. 2017.

[28] R. Tan, H. H. Nguyen, Eddy. Y. S. Foo, D. K. Y. Yau, Z. Kalbarczyk, R. K. Iyer, and H. B. Gooi, "Modeling and mitigating impact of false data injection attacks on automatic generation control," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 7, pp. 1609–1624, Jul. 2017.

[29] N. G. A. Aysheh, T. Khattab, and A. Massoud, "Cyber-attacks against voltage profile in smart distribution grids with highly-dispersed PV generators: Detection and protection," in *Proc. IEEE Electr. Power Energy Conf. (EPEC)*, Edmonton, AB, Canada, Nov. 2020, pp. 1–6.

[30] R. Deng and H. Liang, "False data injection attacks with limited susceptance information and new countermeasures in smart grid," *IEEE Trans. Ind. Informat.*, vol. 15, no. 3, pp. 1619–1628, Mar. 2019.

[31] P. Khaledian, B. K. Johnson, and S. Hemati, "Power grid security improvement by remedial action schemes using vulnerability assessment based on fault chains and power flow," in *Proc. IEEE Int. Conf. Probabilistic Methods Appl. Power Syst. (PMAPS)*, Boise, ID, USA, Jun. 2018, pp. 1–6.

[32] M. Bahrami, M. Fotuhi-Firuzabad, and H. Farzin, "Reliability evaluation of power grids considering integrity attacks against substation protective IEDs," *IEEE Trans. Ind. Informat.*, vol. 16, no. 2, pp. 1035–1044, Feb. 2020.

[33] E. Naderi, S. Pazouki, and A. Asrari, "A remedial action scheme against false data injection cyberattacks in smart transmission systems: Application of thyristor-controlled series capacitor (TCSC)," *IEEE Trans. Ind. Informat.*, vol. 18, no. 4, pp. 2297–2309, Apr. 2022.

[34] EPRLAB. *Static VAR Compensator (SVC)*. Accessed: Jun. 20, 2024. [Online]. Available: http://www.eprlab.com/static_VAr_compensator.html

[35] J.-H. Chen, W.-J. Lee, and M.-S. Chen, "Using a static VAr compensator to balance a distribution system," in *Proc. Conf. Rec. IEEE Ind. Appl. Conf. 31st IAS Annu. Meeting*, San Diego, CA, USA, Oct. 1996, pp. 2321–2326.

[36] I. A. Erinmez, "Static VAR compensators," Conseil International des Grands Reseaux Electriques (CIGRE), Paris, France, Working Group 38-01, Task Force no. 2, 1986.

[37] C. W. Taylor, G. Scott, and A. Hammad, "Static VAR compensator models for power flow and dynamic performance simulation," *IEEE Trans. Power Syst.*, vol. 9, no. 1, pp. 229–240, Feb. 1994.

[38] H. R. Baghaee, B. Vahidi, S. Jazebi, G. B. Gharehpetian, and A. Kashefi, "Power system security improvement by using differential evolution algorithm based FACTS allocation," in *Proc. Joint Int. Conf. Power Syst. Technol. IEEE Power India Conf.*, New Delhi, India, Oct. 2008, pp. 1–6.

[39] E. Naderi, H. Narimani, M. Fathi, and M. R. Narimani, "A novel fuzzy adaptive configuration of particle swarm optimization to solve large-scale optimal reactive power dispatch," *Appl. Soft Comput.*, vol. 53, pp. 441–456, Jan. 2017.

[40] B. Mahdad and K. Srairi, "Adaptive differential search algorithm for optimal location of distributed generation in the presence of SVC for power loss reduction in distribution system," *Eng. Sci. Technol., Int. J.*, vol. 19, no. 3, pp. 1266–1282, Sep. 2016.

[41] S. R. Najafi, M. Abedi, and S. H. Hosseinian, "A novel approach to optimal allocation of SVC using genetic algorithms and continuation power flow," in *Proc. IEEE Int. Power Energy Conf.*, Putra Jaya, Malaysia, Nov. 2006, pp. 202–206.

[42] E. Naderi, S. Pazouki, and A. Asrari, "A region-based framework for cyberattacks leading to undervoltage in smart distribution systems," in *Proc. IEEE Power Energy Conf. Illinois (PECI)*, Urbana, IL, USA, Apr. 2021, pp. 1–7.

[43] A. Azizivahed, H. Narimani, E. Naderi, M. Fathi, and M. R. Narimani, "A hybrid evolutionary algorithm for secure multi-objective distribution feeder reconfiguration," *Energy*, vol. 138, pp. 355–373, Nov. 2017.

[44] L. Huang, J. Xu, Y. Sun, T. Cui, and F. Dai, "Online monitoring of wide-area voltage stability based on short circuit capacity," in *Proc. Asia–Pacific Power Energy Eng. Conf.*, Wuhan, China, Mar. 2011, pp. 1–5.

[45] *MATPOWER Package*. Accessed: Jun. 20, 2024. [Online]. Available: https://matpower.org/

[46] H. Pradeepa, T. Ananthapadmanabha, and C. Bandhavya, "Optimal allocation of combined DG and capacitor units for voltage stability enhancement," *Proc. Technol.*, vol. 21, pp. 216–223, Jan. 2015.

[47] S.-A. Yin and C.-N. Lu, "Distribution feeder scheduling considering variable load profile and outage costs," *IEEE Trans. Power Syst.*, vol. 24, no. 2, pp. 652–660, May 2009.

[48] A. Shafiu, T. Bopp, I. Chilvers, G. Strbac, N. Jenkins, and H. Li, "Active management and protection of distribution networks with distributed generation," in *Proc. IEEE Power Eng. Soc. Gen. Meeting*, Denver, CO, USA, Jun. 2004, pp. 1098–1103.

[49] F. Moazeni, J. Khazaei, and J. P. Pera Mendes, "Maximizing energy efficiency of islanded micro water-energy Nexus using co-optimization of water demand and energy consumption," *Appl. Energy*, vol. 266, May 2020, Art. no. 114863.

[50] J. R. S. Mantovani, F. Casari, and R. A. Romero, "Reconfiguração de sistemas de distribuição radiais utilizando o critério de queda de tensão," *SBA Controle Automa??o*, vol. 11, no. 3, pp. 150–159, 2000.

[51] N. G. Hingorani and L. Gyugyi, *Understanding FACTS: Concepts and Technology of Flexible AC Transmission Systems*. Piscataway, NJ, USA: Wiley, 2000.

[52] B. H. Alajrash et al., "A comprehensive review of FACTS devices in modern power systems: Addressing power quality, optimal placement, and stability with renewable energy penetration," *Energy Reports*, vol. 11, pp. 5350–5371, Jun. 2024.

EHSAN NADERI (Member, IEEE) received the Ph.D. degree in electrical engineering from Southern Illinois University (SIU), Carbondale, IL, USA, in May 2023.

He has been a tenure-track Assistant Professor with the Department of Electrical Engineering, College of Engineering and Computer Science, Arkansas State University (A-State), Jonesboro, AR, USA, since August 2023. Also, he has been the Director of the Department of Electrical Engineering since May 2024. The focus of his research is on the application of machine learning to smart grid security and operation of modern cyber-physical power systems. He was a recipient of the Dissertation Research Fellowship Award from the College of Engineering, Computing, Technology, and Mathematics at SIU, and his dissertation was nominated for the Richard and Donna Falvo Outstanding Dissertation Award. In addition to several the best paper awards from IEEE conferences (e.g., 2022 IGESSC, 2022 AIIoT, and 2021 icSmartGrid), he also received four outstanding reviewer awards from top-field journals (e.g., IJEPES, EAAI, and COR) in recognition of his professional services. He is an Editor for Frontiers in Smart Grids-Grid Efficiency and a reviewer for more than 40 scientific journals.

ARASH ASRARI (Senior Member, IEEE) received the Ph.D. degree in electrical engineering from the University of Central Florida, Orlando, FL, USA, in 2015.

From 2015 to 2017, he was a Senior Consulting Engineer with the Phasor Engineering, LLC, Winter Garden, FL, USA. From 2017 to 2023, he was an Assistant Professor with the School of Electrical, Computer, and Biomedical Engineering, Southern Illinois University (SIU), Carbondale, IL, USA. He is currently an Associate Professor with the Department of Electrical and Computer Engineering, Purdue University Northwest (PNW), Hammond, IN, USA. He has supervised 11 Ph.D./M.S. students in his research team at SIU and PNW. He was a recipient of the Outstanding Teacher of the Year Awards, in 2019 and 2022. He is also an Associate Editor for IEEE ACCESS.