3-19-2022

Cascading verification initiated by switching attacks through compromised digital relays

Koji Yamashita
University of California, Riverside

Zhiyuan Yang
Guangdong Electric Power Design Institute

Chee Wooi Ten
Michigan Technological University, ten@mtu.edu

Soummya Kar
Carnegie Mellon University

Andrew Ginter
Waterfall Security Solutions

Recommended Citation

Yamashita, K., Yang, Z., Ten, C., Kar, S., & Ginter, A. (2022). Cascading verification initiated by switching attacks through compromised digital relays. *IET Smart Grid*. http://doi.org/10.1049/stg2.12062
Retrieved from: https://digitalcommons.mtu.edu/michigantech-p/15850

Follow this and additional works at: https://digitalcommons.mtu.edu/michigantech-p
Part of the Electrical and Computer Engineering Commons

Received: 28 October 2021 | Revised: 16 February 2022 | Accepted: 1 March 2022

DOI: 10.1049/stg2.12062

The Institution of Engineering and Technology WILEY

ORIGINAL RESEARCH

Cascading verification initiated by switching attacks through compromised digital relays

Koji Yamashita[1] | Zhiyuan Yang[2] | Chee-Wooi Ten[3] | Soummya Kar[4] | Andrew Ginter[5]

[1]Department of Electrical and Computer Engineering, University of California Riverside, Riverside, California, USA

[2]Department of System Technology, Guangdong Electric Power Design Institute Company, Guangzhou, China

[3]Department of Electrical and Computer Engineering, Michigan Technological University, Houghton, Michigan, USA

[4]Department of Electrical and Computer Engineering, Carnegie Mellon University, Pittsburgh, Pennsylvania, USA

[5]Waterfall Security Solutions, Calgary, Alberta, Canada

Correspondence

Koji Yamashita, Department of Electrical and Computer Engineering, University of California Riverside, 900 University Ave, Riverside, CA 92521, USA.
Email: kyamashi@ucr.edu

Funding information

US National Science Foundation, Grant/Award Numbers: 1739422, 1837607

Abstract

Attackers are able to enumerate all devices and computers within a compromised substation network. Digital relays deployed in the substation are the devices with IP addresses that can be discovered in the process of trial-and-error search. This paper is concerned with studies of cyberattacks manipulating digital relays to disruptively disconnect the associated breakers. The plausible enumeration of such disruptive attack for each relay in a substation is verified with the dynamic simulation studies with the special protection system for frequency, voltage, and rotor angle stability. A pertinent approach with smaller scale contingency analysis results is proposed to reduce the enormous computation burden. The devised enumeration reduction method is evaluated using IEEE test cases. The proposed method provides an extensive enumeration strategy that can be used by utility engineers to identify the pivotal relays in the system and can be further strengthened with security protection.

KEYWORDS

Big Data, distributed control, power system cyber-security and privacy, power system security, power system simulation, relay protection, substation automation

1 | INTRODUCTION

Internet Protocol (IP)-based information communication technology is increasingly deployed in today's power grids. Digital relays are the crucial components of protection in substations. According to the IEC61850 standards [1, 2], intelligent electronic devices (IEDs) are deployed on the local area network within substations based on Ethernet and IP communications [3]. Other deployment modes using older communications standards, such as DNP3 and IEC60870-5, are also possible. Convenient remote connections allow protection engineers to visualise the connections and relationships between the control functions and the physical components through the human-machine interface. With such remote connectivity, protection engineers are able to customise the functional settings of relays to meet the reliability of the power grid. Such flexibility to remotely connect the software systems on substations could also introduce a way for the intruders to log in. Upon successful hacking onto the control system, the attackers are able to learn from the system and perform strategically a series of switching actions associated with the compromised substation network.

The digital protective relay deployed in a substation can be a target [4–6]. The 2015 Ukraine attack, for example, exploited remote access to IP-based substation equipment to covertly disconnect circuit breakers and then erase the hard drives of that equipment. While the attack was not reported to affect cascading failure, it demonstrated the vulnerabilities of IP-based substation equipment to cyberattacks [7]. More recently, the United States Department of Homeland Security issued an alert indicating that Russian threat actors targeted American electric facilities with remote access attacks [8]. Another alert indicated that safety equipment at industrial sites had been targeted [9].

Available hacking tools, for example, Shodan, Nmap, and Wireshark, can help attackers enumerate all the IP-based devices in an interconnected communication network [10, 11]. These software tools identify nearby devices if they are alive [12–14]. The vulnerabilities of remote connectivity to protective relays are summarised in [15], categorised as software security vulnerabilities, network security vulnerabilities, such as denial-of-service (DoS) attacks, system vulnerabilities, and other miscellaneous malware. The cyberattack against the individual IED, for example, the false data injection attack, has already been rigorously discussed, mainly focussing on the unwanted or undesired IED operation [4, 16]. However, subsequent IED operations that could result in large-scale power outages have been well investigated [6]. Such studies are limited to multiple IED operations at a single substation.

One of the hackers' adversary strategies is to perturb the grid-wide instability and pose brownouts or blackouts, disconnecting components of a power grid via circuit breakers [17]. Breakers are generally tripped by switching maneuvers done by system operators or protective relays. Therefore, compromising Supervisory Control and Data Acquisition (SCADA) or IEDs allows hackers to manipulate switchgears in hand [18]. If a large number of substations are out of service due to the substation attack, the brownout is inevitable, and the blackout could occur. A partial power outage is defined here as the brownout in this paper. The majority of recent work related to the cyber-incurred power outages focusses explicitly on hacking onto the local SCADA system, but a granular detail on protective device levels is not performed [19–22]. Reference [18] proposes derivation of the probability that SCADA and IEDs are compromised in terms of the steady-state probability (Figure 1). However, the impact of those compromised SCADA and IEDs is not discussed. Reference [23] proposes a risk index and attempts to quantify which IED would give a more significant impact, refining the relevant work [19–22]. Despite the best efforts using the steady-state approach, the measure to identify worse-case combinations should be verified with dynamic simulation, including cascaded events.

References [19–22] have evaluated substation outages via the SCADA, enumerating all the possible combinations of substations. Combinations of cyberattacks via compromised IEDs would be extendable to a more complicated combinatorial problem because a single IED may be associated with one or more circuit breakers. On the contrary, different IEDs also disconnect the same circuit breakers. Such studies are crucial in determining if some cases may detrimentally affect operation that could lead to cascading implication where it requires time-domain simulation with models to verify.

Extreme contingency studies against switching attacks would provide a perspective beyond *status quote* N-1 contingency. It can be computationally taxing but the formulation of problem based on data flow of the control network provides a guidance of potential intrusion plausibility. To the best of the authors' knowledge, impact studies of substation attacks towards an exhaustive enumeration of IED-initiated contingencies using dynamic models have not been studied. Although time-domain simulation starts to be leveraged for the impact analysis for hypothetical cyberattack studies [24, 25], [24] restrain the anomaly detection. Reference [25] only covers transmission line events with underfrequency relays, which does not capture a wide variety of cascaded events.

The main contributions of this paper are summarised below:

- Dynamic control and protection models are implemented into IEEE standard system models to represent cascaded events more precisely than the power flow calculation. Specifically, special protection scheme models are detailed.
- A strategy capitalising on simulation results against a smaller number of equipment failures is proposed to decrease the explosively growing computation burden in response to the number of component outages.

The organisation of the paper is as follows: Section 2 gives the details on the IEDs (i.e. digital protective relays that assure technical compliance with IEC61850) and circuit breakers. Section 3 models the disruptive switching actions via the

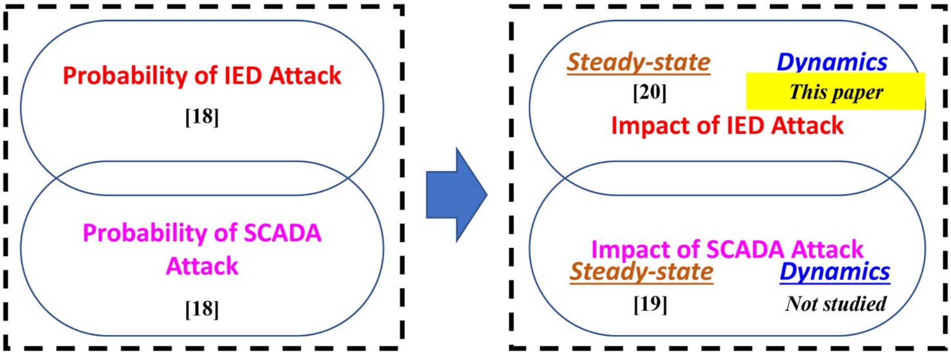


FIGURE 1 Summary of hypothesised switching attacks using different validation methods

associated digital relays, including special protection schemes (also known as special protection system; SPS). Refined IED combination enumeration that is suited for dynamic simulations is also proposed. Section 4 presents simulation results using IEEE test systems. Section 5 concludes with future work.

2 | HYPOTHETICAL SWITCHING ATTACKS VIA COMPROMISED IEDS IN SUBSTATIONS

2.1 | Theoretical difference between compromised IED and compromised substation from enumeration perspective

Extended enumerations of substation outages via the compromised SCADA have already been established in [19, 20]. They define hypothesised substation outages as an S-select-k contingency, linking it with *N-1 contingency*.

The number of the complete combinations of substations is $\sum_{k=1}^{|S|} \mathbf{C}_k^{|S|}$, where S is the substation set and k is the number of out-of-service substations.

On the other hand, once hackers successfully compromise the protective equipment, that individual would be able to remotely change relay settings, which may initiate (1) undesired/unwanted relay operation if the grid is in a healthy condition or (2) failure to operate against a fault condition. The impact of cyberattacks on IEDs is nontrivial and could lead to a cascading failure.

As shown in Figure 2, this proposed study extends the previous work to presume switching attacks via compromised relays/IEDs associated with the breakers (hereafter, we call it R-select-k contingency as contrasted with S-select-k). Let $\tilde{\mathbf{R}}$ denotes the set of IEDs in the entire system:

$$\tilde{\mathbf{R}} = \mathbf{R}_1 \cup \mathbf{R}_2 \cdots \cup \mathbf{R}_i \cup \cdots \cup \mathbf{R}_{|S|} \tag{1}$$

where $\mathbf{R}_i$ is the set of IEDs that are deployed at the substation i, such as:

$$\mathbf{R}_i = \left[r_1^i, r_2^i, \ldots, r_b^i, \ldots, r_{B^i}^i \right] \tag{2}$$

where r_b^i denotes the bth IED on a specific substation i. The variable, B^i, denotes the total number of the set of IEDs with respect to a particular protection zone of the substation i. It is noted that one set of IEDs at a substation corresponds to a particular protection type, such as bus protections, line protections, transformer protections, and generator protections (see Figure 3). Thus, the total number of the IED combination enumerations, $\mathbb{S}_R$, is:

$$\mathbb{S}_R = \sum_{k=1}^{|\tilde{\mathbf{R}}|} \mathbf{C}_k^{|\tilde{\mathbf{R}}|} = 2^{|\tilde{\mathbf{R}}|} - 1 = 2^{\sum_1^{|S|} B^i} - 1 \gg \mathbb{S}_S = 2^{|S|} - 1 \tag{3}$$

Variables, $\mathbb{S}_R$ and $\mathbb{S}_S$, denote the total number of enumerations of R-select-k and S-select-k contingencies, respectively. It is evident that the total number of combination enumerations increases enormously when hacking IEDs for substation outages are considered. For example, let us assume 10 substations in the system and three IEDs on each substation. $\mathbb{S}_R$ is 2^{20} times larger than $\mathbb{S}_S$.

2.2 | Simulation-based verification against simultaneous IED outage and sequential IED outage

In addition, the evaluation volume would further increase if the sequential operation between IEDs is considered. The sequential order of those operations would significantly increase the complexity of the problem. An R-select-k contingency analysis result using the IEEE 14-bus system with and without the sequential order of substation outages is illustrated in Table 1. The sequential events are simulated every 5 seconds. The number of studied sets of IEDs are fixed as three among bus protection, generator protection, transmission line protection, and feeder protections at each substation to limit the

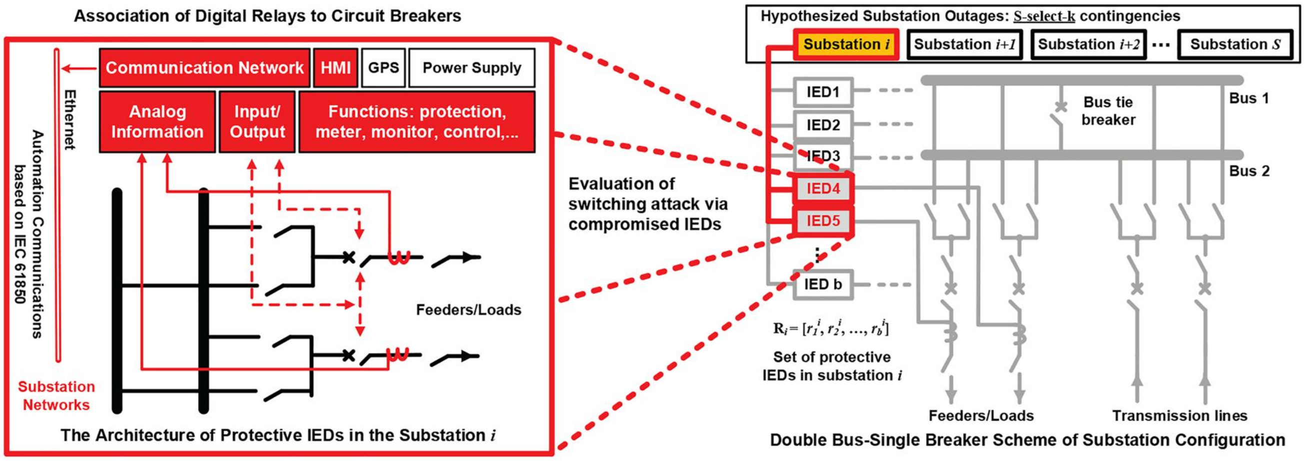
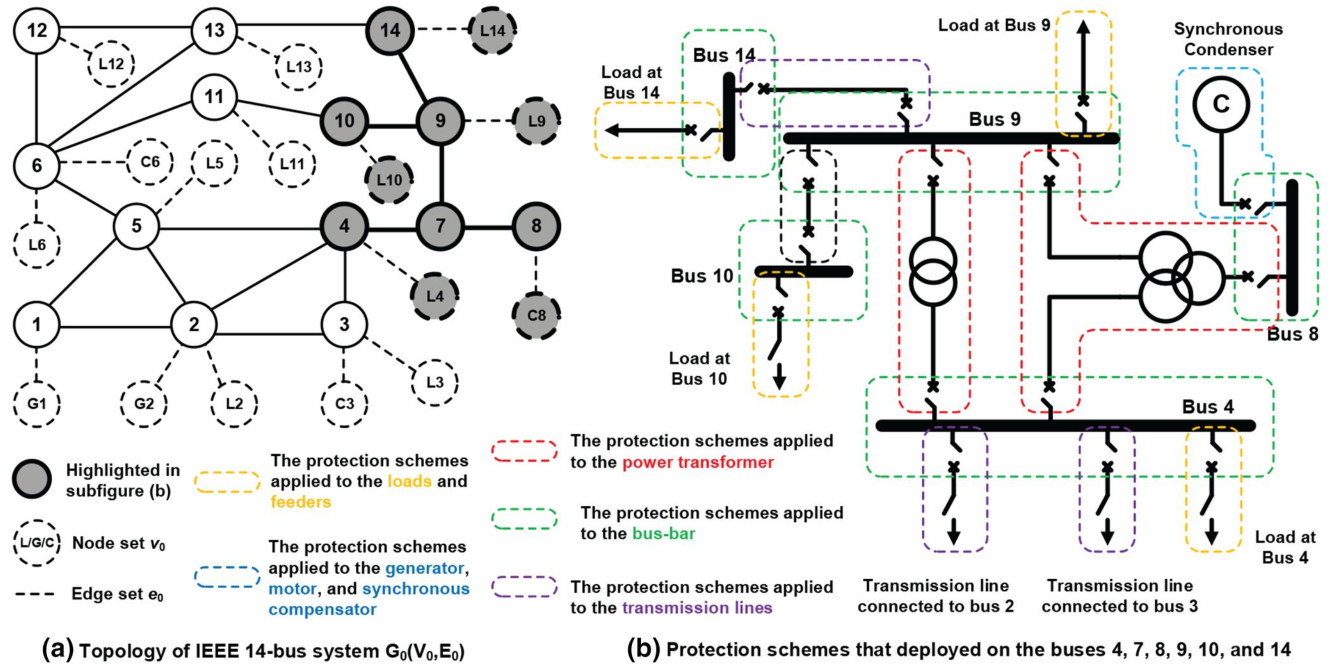

Association of Digital Relays to Circuit Breakers
Communication Network
HMI
GPS
Power Supply
Analog Information
Input/ Output
Functions: protection, meter, monitor, control,...
Ethernet
Automation Communications based on IEC 61850
Feeders/Loads
Substation Networks
The Architecture of Protective IEDs in the Substation i
Evaluation of switching attack via compromised IEDs
Hypothesized Substation Outages: S-select-k contingencies
Substation i
Substation i+1
Substation i+2
Substation S
IED1
IED2
IED3
IED4
IED5
IED b
Bus tie breaker
Bus 1
Bus 2
$\mathbf{R}_i = [r_1^i, r_2^i, \ldots, r_b^i]$
Set of protective IEDs in substation i
Feeders/Loads
Transmission lines
Double Bus-Single Breaker Scheme of Substation Configuration

FIGURE 2 Architecture of protective intelligent electronic devices (IEDs) and possible path enumeration within a substation network by hacking tools


12
13
14
L14
L12
L13
11
10
9
L9
6
C6
L5
L11
L10
L6
5
4
7
8
L4
C8
1
2
3
G1
G2
L2
C3
L3
Highlighted in subfigure (b)
L/G/C
Node set v_0
Edge set e_0
The protection schemes applied to the loads and feeders
The protection schemes applied to the generator, motor, and synchronous compensator
The protection schemes applied to the power transformer
The protection schemes applied to the bus-bar
The protection schemes applied to the transmission lines
Load at Bus 14
Bus 14
Load at Bus 9
Bus 9
Synchronous Condenser
C
Bus 10
Load at Bus 10
Bus 8
Bus 4
Load at Bus 4
Transmission line connected to bus 2
Transmission line connected to bus 3

(a) Topology of IEEE 14-bus system $G_0(V_0,E_0)$

(b) Protection schemes that deployed on the buses 4, 7, 8, 9, 10, and 14

FIGURE 3 Modified topology of the original graph G_0 and fundamentals of protection deployment in the IEEE 14-bus system

TABLE 1 Simulated brownout and blackout cases of R-select-k contingency analysis using IEEE 14-bus system with and without sequential outages, indicating the potential threats of system collapse

$R-k$	Brownout cases (simultaneous outages)	Blackout cases (simultaneous outages)	Brownout cases (with sequential outages)	Brownout cases (with sequential outages)	Blackout rate (simultaneous outages)	Blackout rate (with sequential outages)
$R-1$	23	22	23	22	0.27	0.27
$R-2$	258	177	507	363	0.41	0.42
$R-3$	1835	2225	10,710	13,650	0.55	0.56
$R-4$	9233	18,172	206,883	450,837	0.66	0.69

explosively increasing volume of contingency cases. It is noted that the total substation number is 10. The used models are illustrated in Section 4. As shown in Table 1, the contingency analysis results are overall the same with and without sequential outages. Strictly speaking, sequential order of outages is prone to provide pessimistic results as k of R-select-k increases. Although this is not always the case, the difference in blackout rates with and without sequential substation outages is likely to be negligible, especially for the smaller k. In light of the above, the sequential operation between the set of IEDs is out of scope in this paper and treated as the future work in the paper.

3 | *R*-SELECT-*k* CONTINGENCY

3.1 | Modelling of IED outages

Compromised advanced digital relays (i.e. IEDs) can be manipulated by hackers to trip those associated breakers in a substation. Generally, the protective schemes, defined as relays, would overlap with some circuit breakers in a substation. In other words, it is common to deploy two or more protective relays on the same equipment. The relay deployment and applications of r_b^i can be found in Table 2, which details the basic relaying fundamentals, applications, and electrical components [26]. As shown in Table 2, each substation may deploy numerous relays for single or multiple power components, which would create a massive set of switching attack combinations. It is observed that on the one hand, multiple relays are protecting the same equipment, which may cause the same impact to the system; on the other hand, the impact level can also be different depending on the schemes. For example, compared to bus protection, which connects multiple components, such as generators, feeders, and transmission lines, the line protection obtains a lower level of impact to the system. A ranking method is introduced for each substation to sort and collect the first R relays that can cause higher impacts. By accumulating the number of N relays for each substation, to differentiate from $\tilde{\mathbf{R}}$, the relay set $\hat{\mathbf{R}}$ is introduced where the impactful relays from power balance perspectives are selected, that is, $\hat{\mathbf{R}}$-k contingencies.

Let $G(V, E)$ represents the graph topology of the power system, where V and E denote the set of bus nodes and the set of edges. The original topology may not represent the deployment of the generators and loads. Therefore, the set of generator and load buses, v_0, and the corresponding incident set of edges, e_0, are incorporated. Thus, the graph $G_0(V_0, E_0)$, where $V_0 = V \cup v_0$ and $E_0 = E \cup e_0$, is introduced to evaluate attack combinations through IEDs as depicted in Figure 3. Figure 3 also illustrates the correlation of the various protection schemes and the corresponding electrical components of a substation with buses 4, 7, 8, 9, 10, and 14. The dashed circles with different colours represent the different electrical components and their corresponding protection zones comprising sets of IEDs. The R-select-k contingency analyses introduced in the paper presume that each set of IEDs can be compromised independently. On the other hand, it is assumed that IEDs in the same protection type (e.g. bus protection) at a substation are all compromised once one particular IED is hacked. The protection coordination and backup protections are not included. The initial event of compromised IED outages, $K(V_K, E_K)$, is presented in Figure 4.

Figure 4 represents the modelling process of the initial IED outage event, K. Based on Table 2, the configuration of IEDs within the system can be initialised by aligning corresponding substation i, connected transmission lines, feeders, and generators, for the bth IED, r^i_b. The IED set, $\hat{\mathbf{R}}$, can be derived from (1) and (2). Then, the $\hat{\mathbf{R}}$-k relay contingency list, $\mathbf{T}$, is generated, which satisfies the event, $K \in \mathbf{T}$. The initial event $K(V_k, E_k)$ is modelled by collecting all the substation nodes and lines affected after the set of IEDs, r^i_b, is compromised. The event, K, would be leveraged for the dynamic verification study in the following subsection.

TABLE 2 Fundamental of relay deployment and application on substation i [27]

Protection zone	Typical relays r^i_b (if available)	Component
Generator	Over/underfrequency relay	Generator
	Inverse time overcurrent relay	
	Over/under-voltage relay	
Power transformer	Percentage differential relay	Transformer
	Inverse time overcurrent relay	
	Overload relay	
Transmission line	Distance relay:	Line
	Three-zone phase fault relay	
Feeder and load	Distance relay:	Lumped load
	Three-zone phase fault relay	
Busbar	Differential relay	Generator
		Load/Feeder
		Line
		Transformer

3.2 | Contingency case reduction

Let us define a hypothetical IED switching attack that leads to a blackout in R-select-k contingencies with R-select-k critical IEDs. We define the critical IEDs as an IED-initiated attack that incurs direct and cascaded outages in this paper. Once the critical IEDs are specified in small R-select-k combinations, any larger R-select-k combinations that include critical IEDs generally result in blackouts. This idea was applied to the power flow-based approach and enabled to reduce the volume of the contingency cases tremendously [20]. However, that is not necessarily the case. That means, combinations of IED attacks containing critical IEDs can lead to the brownout (referred to as a blackout error). On the other hand, attack combinations through IEDs, including no critical IED, can lead to the blackout (referred to as a brownout error). Such an exceptional case more emerges in the dynamic simulation. This exceptional circumstance affects both the accuracy of blackout and brownout, and those errors increase as k of R-select-k increases. Therefore, the trade-off reducing R-select-k contingency cases and mitigation of increase in blackout and brownout errors needs to be carefully examined. In addition, a power flow-based approach can recursively identify critical IEDs for each R-select-k contingency. However, the same procedure cannot be applied to dynamic simulations due to the heavier computation burden than power flow calculations. This paper proposes two countermeasures using critical IEDs obtained from R-select-1 contingencies: (1) Decrease in brownout error slightly increasing R-select-k contingency cases and (2) decrease in R-select-k contingency cases slightly increasing in blackout error. Features of countermeasures are summarised in Table 3. The procedure of those countermeasures is illustrated in Figure 5. As shown in Table 3, the examined R-select-k contingency cases are IED-outage combinations that include critical IEDs obtained from the

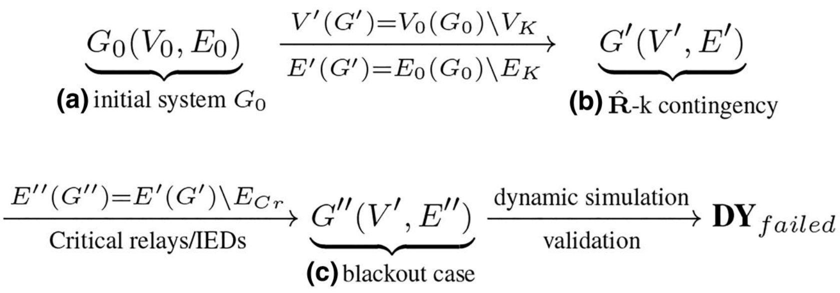


FIGURE 4 Modelling process for switching attack through compromised associated intelligent electronic device (IED)

R-select-1 contingency for countermeasure 1 and IED-outage combinations that exclude R-select-1 critical IEDs for countermeasure 2, that is, there are no overlapped examined cases in both countermeasures. The right flowchart corresponds to countermeasure 1 in Table 3, while the left corresponds to countermeasure 2 in Table 3.

TABLE 3 Pros and cons of two countermeasures

Countermeasure	1	2
R-select-k contingencies	R-select-k including critical IEDs obtained from R-select-1 contingency	R-select-k excluding critical IEDs obtained from R-select-1 contingency
R-select-k contingency cases	Increase	Decrease
Brownout/blackout evaluation accuracy	Increase	Decrease

Abbreviation: IEDs, intelligent electronic devices.

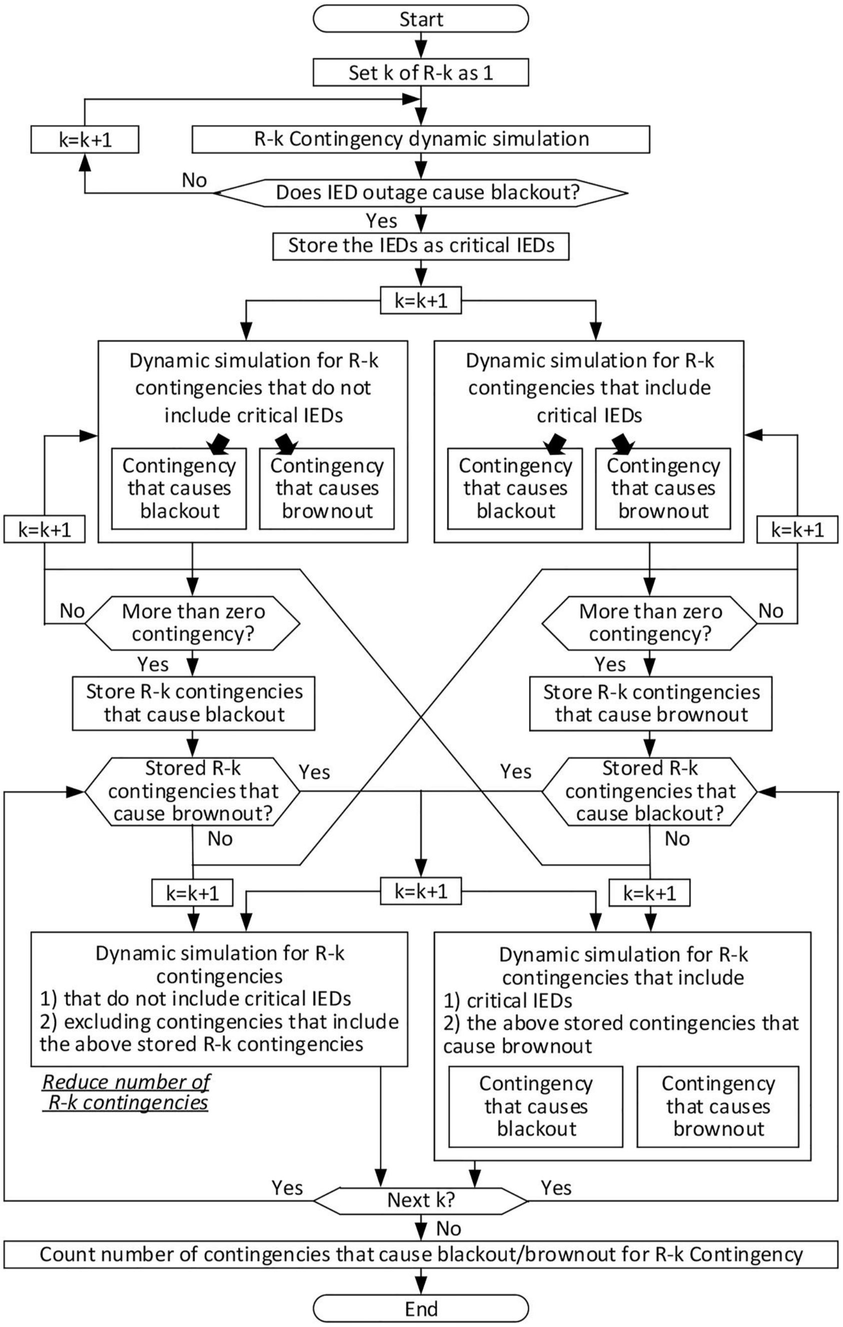

Start
Set k of R-k as 1
k=k+1
R-k Contingency dynamic simulation
No
Does IED outage cause blackout?
Yes
Store the IEDs as critical IEDs
k=k+1
Dynamic simulation for R-k contingencies that do not include critical IEDs
Contingency that causes blackout
Contingency that causes brownout
Dynamic simulation for R-k contingencies that include critical IEDs
Contingency that causes blackout
Contingency that causes brownout
k=k+1
k=k+1
No
More than zero contingency?
Yes
More than zero contingency?
No
Yes
Store R-k contingencies that cause blackout
Store R-k contingencies that cause brownout
Stored R-k contingencies that cause brownout?
Yes
Yes
Stored R-k contingencies that cause blackout?
No
No
k=k+1
k=k+1
k=k+1
Dynamic simulation for R-k contingencies
1) that do not include critical IEDs
2) excluding contingencies that include the above stored R-k contingencies
Reduce number of R-k contingencies
Dynamic simulation for R-k contingencies that include
1) critical IEDs
2) the above stored contingencies that cause brownout
Contingency that causes blackout
Contingency that causes brownout
Yes
Next k?
Yes
No
Count number of contingencies that cause blackout/brownout for R-k Contingency
End

FIGURE 5 Flowchart of two countermeasures

3.3 | Computational environment and test case setup

This simulation study evaluates IEEE 14- and 30-bus systems using a commercially available time-domain simulation tool, Central research institute of electric power industry's Power Analysis Tool [28], in the Unix operating system. For each hypothesised scenario, the dynamic simulation time is set as 11 s, including the pre-disturbance time of 1 s.

This simulation study investigates the $\hat{\mathbf{R}}$-k contingency with N set to 3, which includes the top three IEDs (protection categories) with the highest impacts on the system based on the fundamentals and applications in Table 2. From the viewpoint of the demand and supply balance following the switching attack, the bus protection is highly likely to cause the largest loss of electricity and is ranked as level 1. In the same manner, the generator and line/feeder protections are ranked to levels 2 and 3, respectively, grouping feeder protections and transmission line protections together as the line protection. The double-circuit line is assumed for all the transmission lines in the model. Then, compromised single line protection is assumed, that is, the disruptive tripping by attackers on one of the double circuit lines.

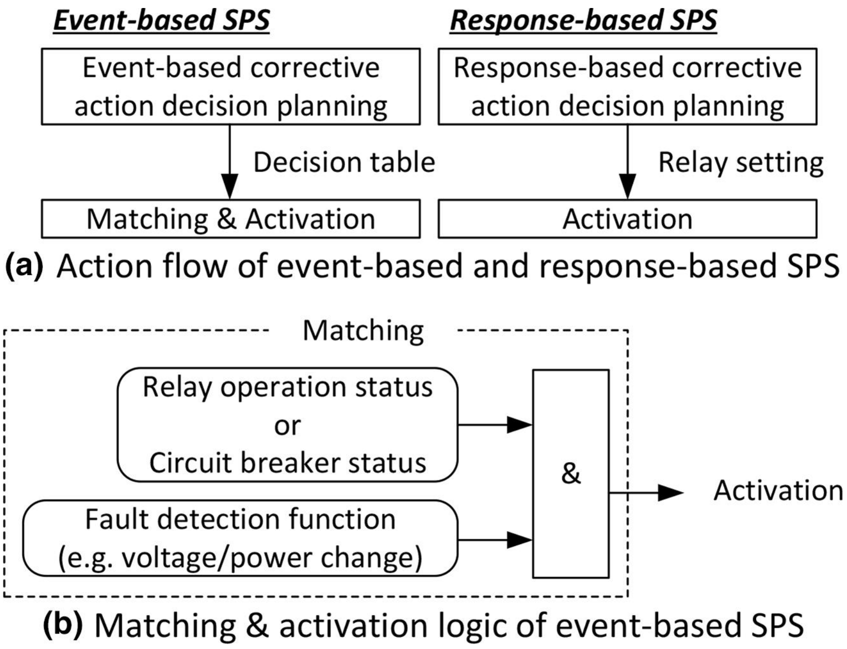
3.4 | Implementation of response-based SPS model

The special protection system (SPS) is widely used to prevent cascaded events that pose a blackout. The SPS is classified into two types: (1) response-based SPS and (2) event-based SPS [29] (see Figure 6a). The response-based SPS is provoked by detecting the dynamic behaviour following a severe disturbance. Because remote or system-wide electric quantities are not generally required, this type has been typically implemented and used by utilities across the globe. On the other hand, the event-based SPS normally requires system-wide information to initiate the corrective action earlier than the response-based SPS, matching the event with decision tables. As shown in Figure 6b, a fault detection function is often applied to activate the event-based SPS for higher reliability. The disruptive switching actions lead to the disconnection of the power equipment without any faults. Therefore, the event-based SPS does not initiate the corrective control action. At the same time, the response-based SPS can take that action regardless of the fault occurrence. In light of this, the event-based SPS is out of the scope of this study.

3.4.1 | Response-based SPS model for frequency stability

The response-based SPS for frequency stability generally contains the frequency drop using underfrequency relays with or without the timer or rate-of-change-of-frequency (ROCOF) relays. Because most IEEE standard models were assumed to be the grid in the 1960s, the underfrequency relay without the timer is modelled as the response-based SPS for frequency stability. This is the simplest and most widely used SPS around the world, and the relay setting values may be determined according to the following conditions:

- The frequency nadir is no lower than the lower limit of the operating frequency of synchronous generators.
- The total load shedding amount is nearly the same as the assumed largest single generator tripping amount.


Event-based SPS
Response-based SPS
Event-based corrective action decision planning
Response-based corrective action decision planning
Decision table
Relay setting
Matching & Activation
Activation
Matching
Relay operation status or Circuit breaker status
Fault detection function (e.g. voltage/power change)
&
Activation

(a) Action flow of event-based and response-based SPS

(b) Matching & activation logic of event-based SPS

FIGURE 6 Event-based SPS and response-based SPS

- The post-fault frequency should not exceed the steady-state frequency.

The relay settings of underfrequency relay models are set, referring to a publicly available source [30] (see Figure 7).

It is noted that underfrequency relays are locked in the model when the voltage is below 0.4 (p.u.).

3.4.2 | Response-based SPS model for rotor-angle stability

The response-based SPS for transient stability generally disconnects the out-of-step (OOS) synchronous generators or (tie-) lines to prevent cascaded failure. The role of this SPS is different depending on the disconnected equipment. If the OOS occurs at the local level (i.e. when regional synchronous generators are out of synchronism), the response-based SPS for transient stability removes some operating units from the main grid to stabilise the entire system. If the OOS occurs at the grid-wide level, the bulk power system is split into two or more sub-grids by disconnecting tie lines. OOS relays are designed using the impedance or the voltage angle difference [31]. Although OOS relays are not always placed in all transmission lines in many countries, it is desired to implement OOS relays to all lines, especially to cope with disruptive switching attacks. It is known that the relay characteristics are not easily determined for the impedance-type OOS relay. On the other hand, the relay setting values are easily determined for the voltage angle difference type OOS relay because the definition of the OOS condition is 180° of a voltage angle difference. For its simplicity, the voltage angle difference is employed not only for lines but also for generators (See Figure 8). It is noted that voltage angle difference type OOS is applied here as the line protection in some countries, while impedance-type OOS is often used as the generator protection in many countries. Because the time-domain simulation tool can calculate the internal induced voltage, the angle difference between the terminal voltage and the internal induced voltage is used to detect the OOS generators.

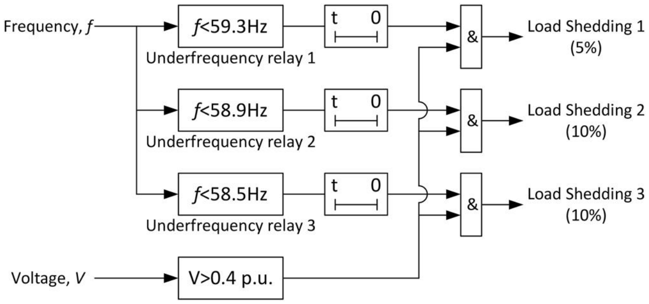


FIGURE 7 Underfrequency relay logic

3.4.3 | Response-based SPS model for voltage stability

There is no event-based SPS for voltage stability, and the response-based SPS for voltage stability is known as the under-voltage load shedding system, while the self-disconnection of loads during sub-second voltage sags is not paid much attention. The load self-disconnection characteristics are equivalent to that of the under-voltage load shedding system at a system level expressed as Equation (4) [32]. The starting and saturated voltage levels are set as 0.8 p.u. and 0.6 p.u., individually. The amount of self-disconnected loads is assumed to linearly increase with the upper limit of 25% of the initial load. It is noted that this relay is not applied to reactive power compensators.

$$P_{\mathrm{drop}} = \begin{cases} 0 & (V_{\min} > 0.8) \\ -1.6V_{\min} + 0.8 & (0.8 \geq V_{\min} \geq 0.4) \\ 0.25 & (0.4 > V_{\min}) \end{cases} \tag{4}$$

where P_{drop} denotes the amount of the load self-disconnection, and $V_{\min}$ denotes the lowest voltage at the load bus.

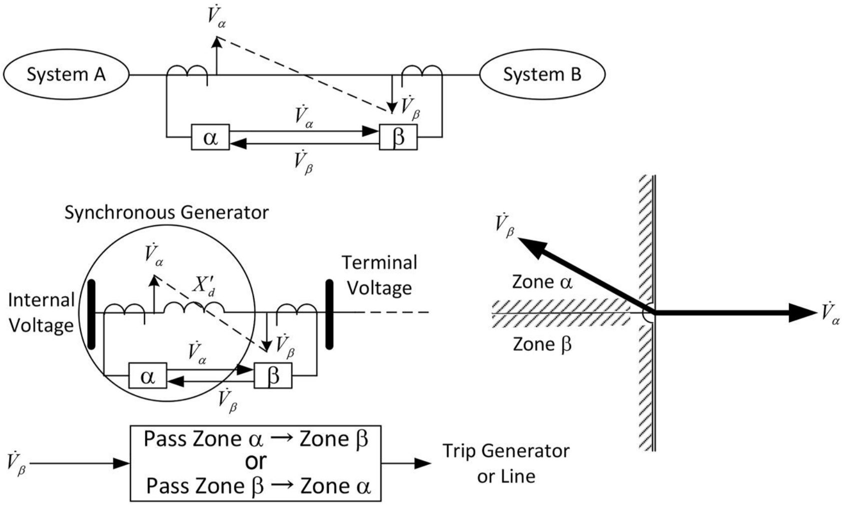


FIGURE 8 Out-of-step relay characteristics for lines and generators

3.4.4 | Response-based SPS model for overload

Disruptive switching actions electrically de-energise not only lines and transformers, but also loads connecting to a substation. Therefore, overloaded power equipment is unlikely to occur. If a generator is overloaded in terms of active power, the frequency drops due to the deficiency of generations. If a generator is overloaded in terms of reactive power, the implemented over-excitation limiter (OEL) of the generator resolves this issue, which results in the further decline of the grid voltage and further load reduction. In the light of this, the frequency relay and the automatic voltage regulator models with OEL are implemented to all generators instead of response-based SPS for overload. In addition, the overvoltage relay model is implemented because IEEE models include synchronous condensers that can cause overvoltage during cascaded events.

3.4.5 | Example dynamic study with and without SPS

Table 4 shows brownout and blackout rates with and without SPS in the IEEE 14-bus system. The dynamic simulation model without SPS excludes the response-based SPS models for frequency stability and rotor angle stability. As shown in Table 4, the mismatch of the blackout rate with and without SPS is at most 3%, and it decreases as k of R-select-k increases. It is noted that the cascaded/sequential tripping of lines, generators, and other power grid components following hypothesised contingencies is considered in this simulation using the SPS models.

4 | R-SELECT-k CONTINGENCY CASE REDUCTION IN IEEE 14-BUS SYSTEM AND 30-BUS SYSTEM

The proposed R-select-k contingency case reduction is applied to the IEEE 14- and 30-bus system models. The performance of the proposed case reduction schemes is reviewed and discussed using an F_1-score and relevant indicators, such as precision and recall.

$$F_1\text{score} = 2 \cdot \frac{\text{Precision} \cdot \text{Recall}}{\text{Precision} + \text{Recall}} \tag{5}$$

$$\text{Precision} = \frac{\text{True positive}}{\text{True positive} + \text{False positive}} \tag{6}$$

$$\text{Recall} = \frac{\text{True positive}}{\text{True positive} + \text{False negative}} \tag{7}$$

Due to a binary problem, that is, blackout/brownout problem, four relations are defined to apply the F_1 score shown below:

- True positive: predicted blackout and was blackout
- True negative: predicted brownout and was brownout
- False positive: predicted blackout and was brownout
- False negative: predicted brownout and was blackout

The 'precision' in Equation (6) presents the blackout accuracy, specialising in predicted blackouts cases. The 'recall' in Equation (7) illustrates the blackout accuracy, specialising in blackout cases. Therefore, the 'precision' addresses how credible the result is when it says blackout, while the 'recall' articulates how credible the result is when the contingency scenario results in the blackout. As shown in Equation (5), the F_1 score deals with both properties in a balanced manner. In other words, the high F_1 score is attained only when the 'precision' and 'recall' are both high. Therefore, the F_1 score can evaluate the blackout/brownout accuracy in terms of two different perspectives in a holistic manner. The case reduction performance is examined mainly with the F_1 score in Subsection 4.3.

The transition of the studied cases for R-select-k contingencies is presented in Figures 9 and 10. Due to the exponentially increasing computation burden, the studied range of k of R-select-k contingency for the IEEE 14- and 30-bus system models are up to seven and five, respectively. In the IEEE 14-bus system, seven IEDs that cause the blackout are extracted as critical IEDs in the R-select-1 contingency. No combination that excludes the above seven critical IEDs leads to the blackout in the R-select-1 through R-select-3 contingencies.

TABLE 4 Brownout/blackout case and rate with and without SPS in the IEEE 14-bus system

	Brownout (stable)		Blackout (unstable)		Fraction of blackout [%]	
R-k	**With SPS**	**Without SPS**	**With SPS**	**Without SPS**	**With SPS**	**Without SPS**
R-1	23	22	7	8	23.3	26.7
R-2	258	242	177	194	40.7	44.6
R-3	1835	1732	2225	2328	54.8	57.3
R-4	9233	8830	18,172	18,575	66.3	67.8
R-5	35,082	32,579	107,424	109,927	75.4	77.1
R-6	104,763	102,414	489,012	491,361	82.4	82.8
R-7	249,111	245,830	1,786,689	1,789,970	87.8	87.9

4.1 | Countermeasure 1

Right parts of Figures 9 and 10 show the process of countermeasure 1. R-select-2 contingencies are thoroughly analysed, and five 2-IED-outage combinations that include seven critical IEDs (Hereafter, we call it five exclusive IED sets) are extracted as brownout cases. In this study, those five exclusive IED sets are exhaustively exploited. For the R-select-3 contingency, if all 3-IED-outage combinations that include seven critical IEDs are assumed to result in the blackout, only 1771 case studies are required, skipping 2289 cases shown in Figure 9, which is treated as the benchmark case reduction method in this paper. The number of study cases of the benchmark case, $n_{case,k}$, for the R-select-k contingency is as follows:

$$n_{\mathrm{case},k} = \begin{cases} C_k^{|\tilde{\mathbf{R}}|} & (1 \le k \le 2) \\ C_k^{|\tilde{\mathbf{R}}|} - \sum_{p=1}^{k} C_p^{N_{\mathrm{CriticalRy}}} \cdot C_{k-p}^{|\tilde{\mathbf{R}}|-N_{\mathrm{CriticalRy}}} & \\ & (3 \le k) \end{cases} \tag{8}$$

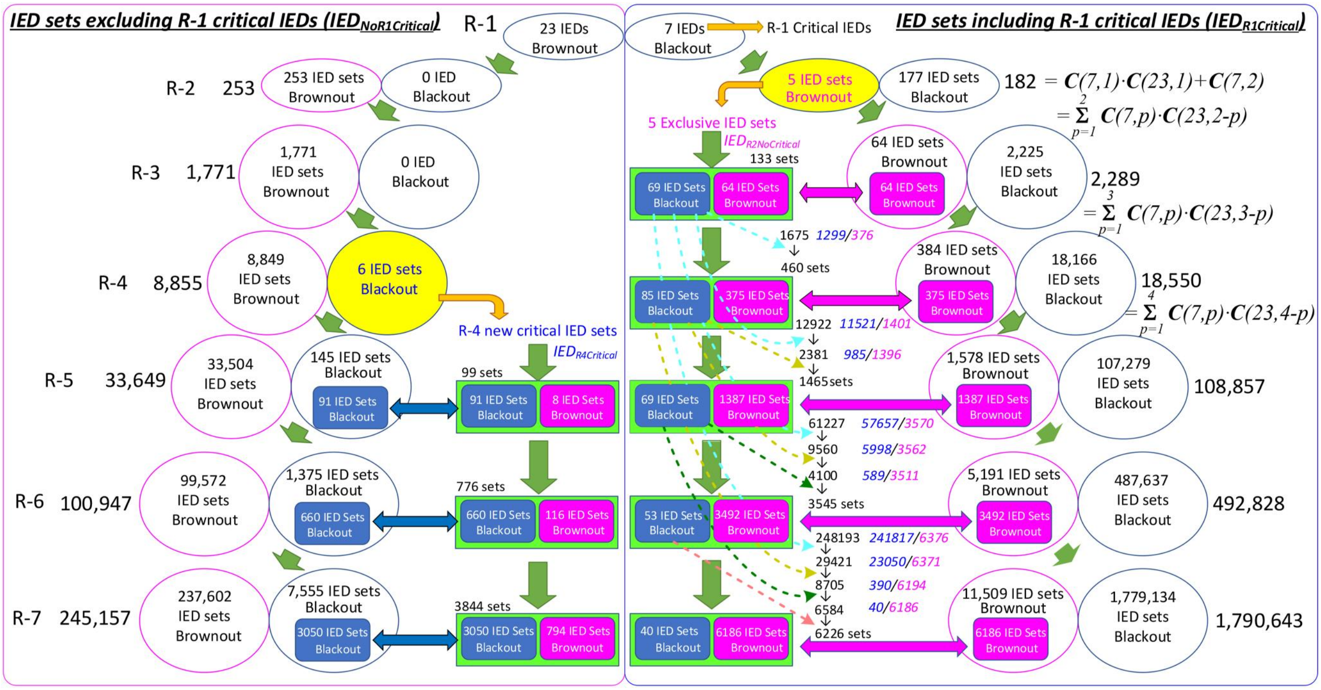


FIGURE 9 $R-1$ through $R-7$ simulation result in the IEEE 14-bus system

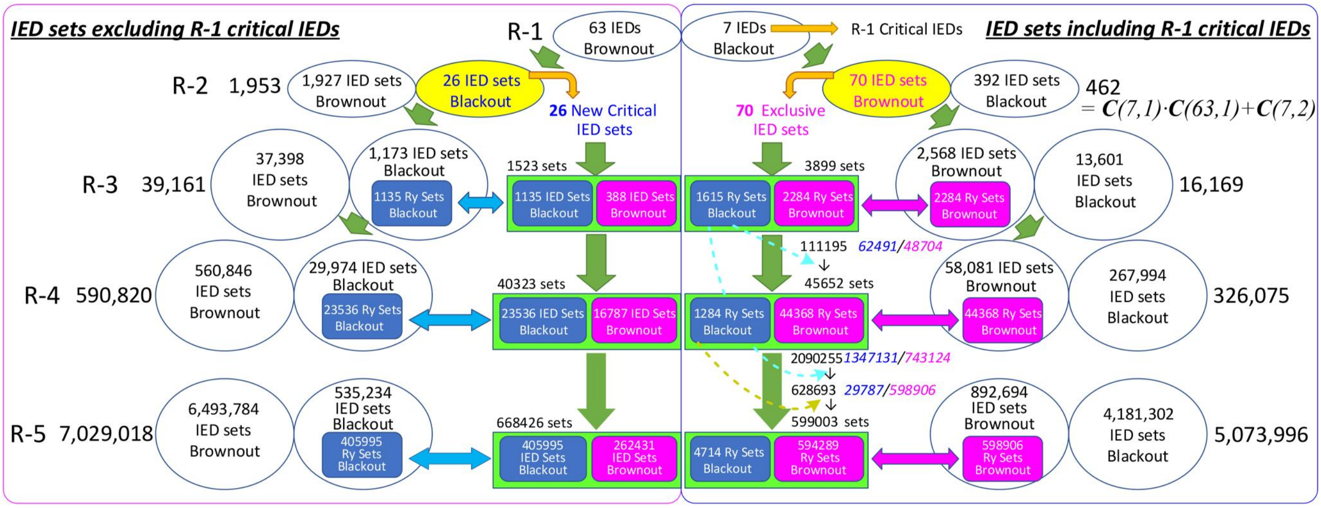


FIGURE 10 $R-1$ through $R-5$ simulation result in the IEEE 30-bus system

where $N_{\text{CriticalRy}}$ denotes the number of critical IEDs. The variable, $|\tilde{\mathbf{R}}|$, is 30 and 70 in the IEEE 14- and 30-bus systems, individually.

However, sixty-four 3-IED combinations become wrong because five exclusive IED sets are the brownout case. In other words, sixty-four 3-IED-outages that include seven critical IEDs are wrongly treated as the blackout case. Countermeasure 1 enables to correct all wrong results, increasing 133 more study cases (see Figure 9).

For the R-select-4 contingency, 384 3-IED-outages that include seven critical IEDs are wrongly treated as the blackout case. The number of 4-IED combinations that include five exclusive IED sets is 1695. Because those combinations include 69 IED sets that result in blackout for the R-select-3 contingency, 4-IED combinations that include the 69 IED sets may be skipped. Thus, the number of additionally examined study cases is reduced from 1675 to 460. The 460 simulation cases as the countermeasure 1 demonstrate 375 brownout cases. Although 9 brownout cases are missing (i.e. the false negative still remains), a large number of contingency cases are omitted with tiny brownout errors shown below.

In the same manner, countermeasure 1 decreases the blackout error for larger k of R-select-k contingencies. However, the fraction of corrected cases decreases as k of R-select-k increases because countermeasure 1 uses only the above five 2-IED-outage combinations to fix the brownout rate accuracy. As shown in Figure 9, only 6186 out of 11,509 cases are corrected for the R-7 contingency.

4.2 | Countermeasure 2

Left parts of Figures 9 and 10 illustrate the process of countermeasure 2. The benchmark case reduction method examines all attack-through IED combinations that exclude seven critical IEDs acquired from the R-select-1 contingency. Once a blackout case is found in the above IED attack combinations for R-select-k contingency, IED combinations of such cases are treated as the additional critical IED sets. In the case of the IEEE 14-bus system, six 4-IED-outage combinations are identified for the R-select-4 contingency, and those six IED combinations are used for larger k of R-select-k contingencies.

For the R-select-5 contingency, ninety-nine 5-IED-outage combinations include the above six 4-IED-outage combinations, treated as the blackout case. Although 99 cases are skipped, the identified number of blackout cases is 91 out of 145. Thus, the false negative increases as k of R-select-k increases. Three thousand and fifty out of 7555 cases are identified as blackout cases (i.e. 4505 cases are mistakenly identified as the brownout) for the R-select-7 contingency in exchange for the 3844 case reduction.

Besides, eight 5-IED-outage combinations are wrongly treated as the blackout case for the R-select-5 contingency when the countermeasure 2 is exploited. Therefore, the countermeasure 2 also increases false positive cases other than false negative cases, although the number of simulation cases decreases.

4.3 | Case reduction performance

Case reduction rates and the F_1 score for the IEEE 14- and 30-bus systems are summarised in Tables 5 and 6. The 'precision' and 'recall' are also shown in those tables to demonstrate how much those two indicators contribute to the F_1 score. The performance of both countermeasures is shown against the benchmark case reduction method that uses only critical IEDs obtained from the R-select-1 contingency. Tables 5 and 6 indicate the following findings for the countermeasure 1:

- The F_1 score improvement against the benchmark's F_1 score decreases as the k of R-select-k increases (Tables 7 and 8).
- The F_1 score improvement against the benchmark's F_1 score augments as the grid size increases (Tables 7 and 8).

TABLE 5 Case reduction performance in the IEEE 14-bus system (part 1)

		Number of simulation cases/case reduction rate [%]			
R-k	**Total number of simulation cases**	**Benchmark case reduction with R-1 critical IEDs**	**Countermeasure 1 improving brownout accuracy**	**Countermeasure 2 reducing blackout cases**	**Blackout rate [%]**
R-1	30	30/0.0	30/0.0	30/0.0	23.3
R-2	435	253/41.8	435/0.0	253/41.8	40.7
R-3	4060	1771/56.4	1894/53.3	1771/56.4	54.8
R-4	27,405	8855/67.7	9316/66.0	8856/67.7	66.3
R-5	142,506	33,649/76.4	35,105/75.4	33,550/76.5	75.4
R-6	593,775	100,947/83.0	104,492/82.4	100,171/83.1	82.4
R-7	2,035,800	245,157/88.0	251.383/87.7	241,313/88.1	87.8

Abbreviation: IEDs, intelligent electronic devices.

- The additional performed IED combination rate with respect to benchmark IED combinations decreases as the k of R-select-k increases.
- The additional performed IED combination rate with respect to benchmark IED combinations increases as the grid size increases.

Tables 5 and 6 derive the following findings for countermeasure 2:

- The IED combination reduction rate with respect to benchmark IED combinations decreases as the k of R-select-k increases.
- The IED combination reduction rate with respect to benchmark IED combinations increases as the grid size increases.
- The F_1 score curtailment against the benchmark's F_1 score decreases as the k of R-select-k increases.
- The F_1 score curtailment against the benchmark's F_1 score augments as the grid size increases.

In the case of R-select-5 in the IEEE 30-bus system, countermeasure 1 improves the F_1 score from 0.914 to 0.970, increasing the studied IED combinations from 58.1% to 63.0%, while countermeasure 2 reduces the studied IED combinations from 58.1% to 52.6%, deteriorating the F_1 score from 0.914 to 0.877. Thus, both countermeasures have pros and cons. The countermeasure 1 may be leveraged when the blackout/brownout evaluation accuracy is more important than the case reduction. However, due to the tremendous volume of contingency cases for the larger grid, the countermeasure 2 can be exploited, especially for the bulk power system.

TABLE 6 Case reduction performance in the IEEE 30-bus system (part 1)

		Number of simulation cases/case reduction rate [%]			
R-k	**Total number of simulation cases**	**Benchmark case reduction with R-1 critical IEDs**	**Countermeasure 1 improving brownout accuracy**	**Countermeasure 2 reducing blackout cases**	**Blackout rate [%]**
R-1	70	70/0.0	70/0.0	70/0.0	10.0
R-2	2415	1953/19.1	2415/0.0	1953/17.3	19.1
R-3	54,740	39,161/28.5	43,060/21.3	37,398/30.1	31.7
R-4	916,895	590,820/35.6	636,472/30.6	560,846/39.5	38.8
R-5	12,103,014	7,029,018/41.9	7,628,021/37.0	6,360,592/47.4	39.0

Abbreviation: IEDs, intelligent electronic devices.

TABLE 7 Case reduction performance in the IEEE 14-bus system (part 2)

	Precision/Recall/F_1 score		
R-k	**Benchmark**	**Countermeasure 1 against brownout**	**Countermeasure 2 against blackout**
R-1	1.00/1.00/1.00	1.00/1.00/1.00	1.00/1.00/1.00
R-2	0.973/1.00/0.986	1.00/1.00/1.00	0.973/1.00/0.986
R-3	0.972/1.00/0.986	1.00/1.00/1.00	0.972/1.00/0.986
R-4	0.979/1.00/0.990	1.00/1.00/1.00	0.979/1.00/0.990
R-5	0.986/1.00/0.993	0.998/1.00/0.999	0.985/0.999/0.992
R-6	0.989/1.00/0.995	0.997/1.00/0.998	0.989/0.999/0.994
R-7	0.994/1.00/0.997	0.997/1.00/0.999	0.993/0.997/0.995

TABLE 8 Case reduction performance in the IEEE 30-bus system (part 2)

	Precision/Recall/F_1 score		
R-k	**Benchmark**	**Countermeasure 1 against brownout**	**Countermeasure 2 against blackout**
R-1	1.00/1.00/1.00	1.00/1.00/1.00	1.00/1.00/1.00
R-2	0.857/1.00/0.923	1.00/1.00/1.00	0.857/1.00/0.923
R-3	0.852/1.00/0.920	0.981/1.00/0.990	0.833/0.997/0.908
R-4	0.837/1.00/0.911	0.956/1.00/0.978	0.796/0.978/0.878
R-5	0.841/1.00/0.914	0.941/1.00/0.970	0.799/0.973/0.877

On the other hand, combining countermeasure 1 and countermeasure 2 can be an option to ensure the balance between accuracy and case reduction. Because both countermeasures are entirely independent, combined ones can reduce simulation cases, alleviating the deterioration of blackout/brownout accuracy. For R-select-5 contingency in the IEEE 30-bus system, the examined IED combinations are suppressed by 0.6% (from 58.1% to 57.5%), improving the blackout/brownout evaluation accuracy in terms of the F_1 score by 0.016 (from 0.914 to 0.930).

5 | CONCLUDING REMARKS

This research study verifies the computational outcomes of disruptive switching attacks through protective IEDs using time-domain simulations. It is observed that the time-domain simulation provides more details of cyber-physical characterisation for IEDs in Ethernet-based substations based on an initial event, that is, hypothetical switching scenarios via one or more compromised IEDs. The results also demonstrate promising outcomes and can be further explored for online applications to identify critical protective IEDs. Although this research study has accomplished an extensive milestone in a contingency of hypothetical attack upon digital relays, dynamic studies can be carried out in the practically sized systems that may require a new parallelised computation paradigm to manage due to the computation burden over millions of simulations.

Future work includes establishing an effective comparison of S-select-k contingencies as well as R-select-k contingencies, considering a sequence of events using larger system models with renewable energy sources on cloud-edge-end orchestrated computing. The uncertainty caused by such distributed resources will also require myriad *new* load profiles, that is, power system conditions and configurations, to be additionally examined. Furthermore, cascaded line outages along with sequential hardware-in-the-loop corrective actions by operators are needed to explore in future study scenarios.

ACKNOWLEDGEMENTS

This work was supported by US National Science Foundation (NSF) Cyber-Physical System (CPS) projects 1739422 and 1837607 entitled ‘Collaborative Research: An Actuarial Framework of Cyber Risk Management for Power Grids’ and ‘Secure Computing and Cross-Layer Anomaly Detection in the Internet of Things.’

CONFLICT OF INTEREST

No conflict of interest.

PERMISSION TO REPRODUCE MATERIALS FROM OTHER SOURCES

None.

DATA AVAILABILITY STATEMENT

The leveraged numerical models are publicly available in books and papers. Simulation results are available on request from the authors.

ORCID

Koji Yamashita https://orcid.org/0000-0002-1892-2455

REFERENCES

1. Ingram, D.M.E., et al.: System-level tests of transformer differential protection using an iec61850 process bus. IEEE Trans. Power. Del. 29(3), 1382–1389 (2014). https://doi.org/10.1109/tpwrd.2013.2291789
2. IEC 61850-9-2, Communication Networks and Systems for Power Utility Automation - Part 9-2: Specific Communication Service Mapping (SCSM) - Sampled Values Over ISO/IEC 8802-3, 2nd edn. IEC, (2011)
3. Ericsson, G.N.: Cyber security and power system communication – essential parts of a smart grid infrastructure. IEEE Trans. Power. Del. 25(3), 1501–1507 (2010). https://doi.org/10.1109/tpwrd.2010.2046654
4. Chattopadhyay, A., et al.: Toward threat of implementation attacks on substation security: case study on fault detection and isolation. IEEE Trans. Ind. Informat. 14(6), 2442–2451 (2018). https://doi.org/10.1109/tii.2017.2770096. [Online]. https://ieeexplore.ieee.org/document/8097030
5. Yang, J., et al.: Anomaly detection based on zone partition for security protection of industrial cyber-physical systems. IEEE Trans. Ind. Informat. 65(5), 4257–4267 (2018). https://doi.org/10.1109/tie.2017.2772190
6. Hong, J., et al.: Cyber attack resilient distance protection and circuit breaker control for digital substations. IEEE Trans. Ind. Inf. 15(17), 4332–4341 (July 2019). [Online]. https://ieeexplore.ieee.org/document/8556464
7. ICS-CERT Alert (IR-ALERT-H-16-056-01). Cyber-Attack Against Ukrainian Critical Infrastructure. Feb. 25 2016. [Online]. https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01
8. U.S.-CERT Alert. (TA18-074A). Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors. Mar. 15 2018. [Online]. https://www.us-cert.gov/ncas/alerts/TA18-074A
9. ICS-CERT. Mar-17-352-01 Hatman-Safety System Targeted Malware (update a). Apr. 10 2018. [Online]. https://ics-cert.us-cert.gov/sites/default/files/documents/MAR-17-352-01%20HatMan%20-%20Safety%20System%20Targeted%20Malware%20%28Update%20A%29_S508C.PDF
10. Ameli, A., et al.: An intrusion detection method for line current differential relays. IEEE Trans. Inf. Forensics Secur. 15, 329–344 (2019). https://doi.org/10.1109/tifs.2019.2916331
11. Smith, H., Morrison, H.: Ethical hacking: a comprehensive beginnerś guide to learn and master ethical hacking. CreateSpace Independent Publishing Platform (2018)
12. Cable News Network (CNN). Shodan: The scariest search engine on the internet. [Online]. http://money.cnn.com/2013/04/08/technology/security/shodan/index.html Accessed 8 Apr 2013
13. NMAP.ORG. Chapter 15. nmap reference guide. (2011). [Online]. https://nmap.org/book/man.html
14. Sharpe, R., Warnicke, E.: Wireshark userś guide. (2014). [Online]. https://www.wireshark.org/docs/wsug_html/
15. Ward, S., et al.: Cyber security issues for protective relays; c1 working group members of power system relaying committee. In: Proc, 2007 IEEE Power Eng. Soc. General Meeting, pp. 1–8. Tampa (2007)
16. Khaw, Y.M., et al.: Preventing false tripping cyberattacks against distance relays: A deep learning approach. IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids. Beijing (2019). [Online]. https://ieeexplore.ieee.org/document/8909810
17. Piétre-Cambacédés, L., Tritschler, M., Ericsson, G.N.: Cybersecurity myths on power control systems: 21 misconceptions and false beliefs.

IEEE Trans. Power. Del. 26(1), 161–172 (2011). https://doi.org/10.1109/tpwrd.2010.2061872

18. Yamashita, K., et al.: Measuring systemic risk of switching attacks based on cybersecurity technologies in substations. IEEE Trans. Power Syst. 35(6), 4206–4219 (2020). https://doi.org/10.1109/tpwrs.2020.2986452
19. Ten, C.-W., Ginter, A., Bulbul, R.: Cyber-based contingency analysis. IEEE Trans. Power Syst. 31(4), 3040–3050 (2016). https://doi.org/10.1109/tpwrs.2015.2482364
20. Yang, Z., Ten, C.-W., Ginter, A.: Extended enumeration of hypothesized substations outages incorporating overload implication. IEEE Trans. Smart Grid. 9(6), 6929–6938 (2018). https://doi.org/10.1109/tsg.2017.2728792
21. Bulbul, R., et al.: Impact quantification of hypothesized attack scenarios on bus differential relays. In: Proc. IEEE Power Systems Computation Conference (PSCC), pp. 1–7. Wroclaw, Poland (2014)
22. Bulbul, R., et al.: Intrusion evaluation of communication network architectures for power substations. IEEE Trans. Power. Syst. 30(30), 1372–1382 (2015). https://doi.org/10.1109/tpwrd.2015.2409887
23. Yang, Z., Ten, C.-W.: Cyber-induced risk modeling for microprocessor-based relays in substations. In: Proc. 2018 IEEE Conf. Innov. Smart Grid Technol.–Asia (ISGT–Asia), pp. 856–861. Singapore (2018)
24. Sun, C.C., Hong, J., Liu, C.C.: A coordinated cyber attack detection system (ccads) for multiple substations. In: Power System Computation Conference (PSCC), pp. 114–129 (2016). [Online]. https://ieeexplore.ieee.org/document/7540902
25. Paul, S., Ni, Z., Ding, F.: An analysis of post attack impacts and effects of learning parameters on vulnerability assessment of power grid. In: Smart Grid Technologies Conference (ISGT) 2020. IEEE Power & Energy Society Innovative, Washington DC, USA (2020). [Online]. https://ieeexplore.ieee.org/document/9087639
26. Meter, Relay, Instrucment Division. Protective Relays Application Guide, 1st edn. The English Electric Company Limited (1968)
27. Anderson, P.M.: Power System Protection, 1st edn. The Institute of Electrical and Electronics Engineers, Inc., NY, USA (1998)
28. Power System Stability Study Group. Integrated analysis software for bulk power system stability. CRIEPI, Tech. Rep. ET90002 (1991)
29. Knight, U.G.: Power systems in Emergencies: from contingency Planning to crisis management, 1st edn. Wiley. Chichester, UK (2001)
30. Electric Reliability Council of Texas. Inc. (Jun. 1, 2018). ERCOT Nodal Operating Guides, Section 2: System Operations and Control Requirements. [Online]. http://www.ercot.com/content/wcm/current_guides/53525/02-060118.doc
31. CIGRE working group B5.19. Protection relay coordination, CIGRE, Tech. Rep. TB432, (2010)
32. CIGRE Working Group C4.605. Modelling and aggregation of loads in flexible power networks. CIGRE, Tech. Rep. TB566 (2014)

How to cite this article: Yamashita, K., et al.: Cascading verification initiated by switching attacks through compromised digital relays. IET Smart Grid. 1–14 (2022). https://doi.org/10.1049/stg2.12062