This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TII.2018.2884728, IEEE Transactions on Industrial Informatics

TII-18-0785

Cyber Attack Resilient Distance Protection and Circuit Breaker Control for Digital Substations

Junho Hong, *Member, IEEE*, Reynaldo Nuqui, *Senior Member, IEEE*, Anil Kondabathini, *Member, IEEE*, Dmitry Ishchenko, *Senior Member, IEEE*, and Aaron Martin, *Senior Member, IEEE*

***Abstract*— This paper proposes new concepts for detecting and mitigating cyber attacks on substation automation systems by domain based cyber-physical security solutions. The proposed methods form the basis of a distributed security domain layer that enables protection devices to collaboratively defend against cyber attacks at substations. The methods utilize protection coordination principles to cross check protection setting changes and can run real time power system analysis to evaluate the impact of the control commands. The Transient Fault Signature (TFS) based cross correlation coefficient algorithm has been proposed to detect the false Sampled Values data injection attack. The proposed functions were verified in a hardware-in-the loop (HIL) simulation using commercial relays and a Real Time Digital Simulator (RTDS). Various types of cyber intrusions are tested using this test bed to evaluate the consequences and impacts of cyber attacks to power grid as well as to validate the performance of the proposed research-grade cyberattack mitigation functions.**

***Index Terms*— Cyber-physical security test bed, collaborative cyber defense models, substation cybersecurity, domain based mitigation, digital substation, smart grid cybersecurity.**

I. Introduction

Substations are one of the critical infrastructure components in power grids as they interconnect with critical physical assets, e.g., circuit breakers, transformers, bus bars and transmission lines. Moreover, substation measurements are commonly used for Energy Management System (EMS) in Supervisory Control and Data Acquisition (SCADA) system applications. In the past, substations usually had limited connectivity with other systems, typically via dedicated communication lines and local area networks. Nowadays, advanced technologies including intelligent electronic devices (IEDs), standardized protocols, Ethernet based communications and remote access controls have enabled digital substation technologies with provisions for enhanced operations and simplified engineering. Particularly, adaptation of IEC 61850 standards brought many benefits, specifically: (1) reduced engineering effort and costs, (2) resolved interoperability problems between different vendors, and (3) enhanced reliability of substation operation. However, new technologies have also introduced new system vulnerabilities that may result in security breaches and could be an attractive target for adversaries, such as unauthorized remote access to substations through misconfigured security devices (e.g., firewalls). As shown in [1], misoperations and malfunctions or hidden failures [2] in protective relays may trip a line that could lead cascading outages and system collapse. For instance, misconfiguration of a distance relay zone 1 setting to overreach to the next line, will result in multiple line outages as a fault outside this distance relay's protected line will also trip the line. Hence, successful attacks on substations may trip multiple circuit breakers, and could trigger cascaded sequences of events with potential impact to substations [3]. In the worst scenario, this will lead to a power system blackout causing severe economic consequences. In fact, a coordinated cyber attack on the Ukrainian power grid [4, 5] clearly showed the need for reliable cyber-physical security measures at substations and SCADA systems. The first cyber attack (Dec. 23rd 2015) caused outages (about 6 hours) to approximately 225,000 customers' after malicious disconnection of seven 110 kV and twenty three 35 kV substations from the grid. The attackers successfully compromised the utility's industrial control system via virtual private network (VPN) and the malware virus "BlackEnergy3." The second attack (Dec. 17th 2016) impacted a single transmission level substation. The new malware ("CRASHOVERRIDE") has evolved from the knowledge what has been learned through past attacks. It is therefore crucial to enhance the cybersecurity of substations and analyze cyber and physical system security holistically to enhance the resiliency and reliability of power systems. In order to address these problems, the North American Electric Reliability Corporation (NERC) has developed the Critical Infrastructure Protection (CIP) 002-009 Standard for bulk power system (BPS) that covers the security of critical cyber assets, physical and cybersecurity, electronic security perimeters as well as personnel training and security management [6]. The International Electrotechnical Commission (IEC) Technical Committee (TC) 57 Working Group (WG) 15 on data and information security for utility communications has established the IEC 62351 standard series for security of the industrial communication protocols [7]. The work embodied in reference [8] proposed Information and Communication Technology (ICT) based intrusion and anomaly detection systems for substation automation systems. The work of [9] discussed DER resilience concepts and challenges against cybersecurity (threats and vulnerabilities)

US Department of Energy under Award Number, DE-OE0000674 "Collaborative Defense of Transmission and Distribution Protection and Control Devices against Cyber Attacks", sponsors this research.

J. Hong, R. Nuqui, A. Kondabathini, and D. Ishchenko are with ABB US Corporate Research Center (USCRC), Raleigh, NC, USA (e-mails: junho.hong@us.abb.com, anil.kondabathini@us.abb.com, reynaldo.nuqui@us.abb.com, dmitry.ishchenko@us.abb.com). A. Martin is with BPA, Vancouver, WA, USA (e-mails: akmartin@bpa.gov).

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TII.2018.2884728, IEEE Transactions on Industrial Informatics

of power grids. Reference [10] shows impact of implementation attacks on substation security. The research in [11] proposed collaborative intrusion detection systems with control and protection IEDs in order to secure the digital substations. By the proposed concept, the IEDs can detect both power system faults and cyber intrusions. In [12], physical response of power systems to malicious attacks on protection system settings and parameters has been studied. The authors of [13] proposed multidimensional intrusion detection system that can detect anomalies of communication protocols, access control and system model for IEC 61850 based substations. An intrusion based quantitative analysis has been proposed and it presents overview of ten substation network architectures and evaluates the architectures as to their effectiveness at intrusion prevention [14]. However, ICT (cyber layer) based detection and mitigation methods (e.g., intrusion detection systems, firewalls and advanced network switches) may sometimes exhibit high false negative/positive ratio. Additionally, these methods offer little or no barriers to a successful intrusions into industrial control systems that have breached the cyber layer of defense. In order to bridge the gaps, the authors of [15] proposed an anomaly detection system to use the characteristics of the physical domain, and the work of [16] shows machine leaning based correlation coefficient methods to detect the cyber intrusions.

This paper proposes both an ICT and power system domain based security layer for mitigating attacks targeting digital substations. Through the use of the test bed, it is demonstrated that the proposed novel mitigation methods provide operational benefits and overall improvement for cyber defense methods. Such benefits and contributions include: (1) additional security against successful intrusions; (2) improved accuracy of conventional intrusion detection and anomaly detection systems in a substation network; and (3) minimized human errors by potentially blocking incorrect operator commands before the control action is executed. This is accomplished by incorporating power system domain knowledge into the security system's final decisions.

The remainder of this paper is divided as follows. Section II summarizes the background and research framework. Threat modeling using attack trees, impact of cyber attacks to power systems are studied, and an authentication based solution for GOOSE communication using cryptography is introduced in Section III. Both cyber and power system domain based mitigation methods are explained in Section IV. The cyber-physical security test bed used to validate the developed methodologies, the system modeling, implementation, simulation of mitigation strategies and case studies conducted at the Bonneville Power Administration (BPA) are presented in Section V. Finally, Section VI concludes this paper.

II. Research Background and Framework

An on-going cyber security research program under Department of Energy (DOE) called Cyber Security for Energy Delivery Systems (CEDS) is focused on advancing the state-of-the-art in cyber defense. The methods presented in this paper developed with DOE CEDS funding include extensive utilization of power system domain knowledge [17]. Whereas other cyber defense methods have relied exclusively on ICT domain knowledge, the use of physics of power systems to counter cyber attacks brings a novel aspect. The ultimate goal is to develop a distributed security domain layer that enables transmission and protection devices to collaboratively defend against cyber attacks in a substation environment. The main research framework of cyber security research consists of five parts as shown in Fig. 1, (1) modeling of cyber-physical system, (2) threats modeling, (3) cyber attack simulation, (4) mitigation strategy, (5) system update, and then (6) new threats modeling. This paper contributes to areas (3) and (4). First, vulnerability assessment has been conducted to find any existing cybersecurity flaws in electrical substations. In order to consider the worst case scenario, the final goal of each threat modeled is to trip circuit breakers in a substation. All cyber attack scenarios are subsequently conducted in a HIL environment with realistic power system model in order to evaluate the realistic impact of an attack. The power system domain based mitigation solutions are then actively applied to all threat models. The results confirmed the feasibility of using domain based mitigation algorithms to detect, block and alarm on all evaluated attack scenarios in real-time without interrupting the regular substation operations. The mitigation algorithm performance needs to be consistently faster than the main protection functions, for instance distance or overcurrent elements.

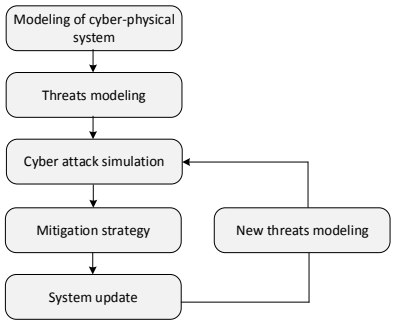


Fig. 1. Main research framework

III. Tools and Approaches for Cybersecurity Development

A. Attack tree

For threat modeling, attack trees were used to describe the potential threats and attack paths for cyber intrusions. Fig. 2 shows an attack tree on how a cyber attack can open circuit breakers in a substation. Note that cyber attackers may intrude into the substation from outside or inside of the facility.

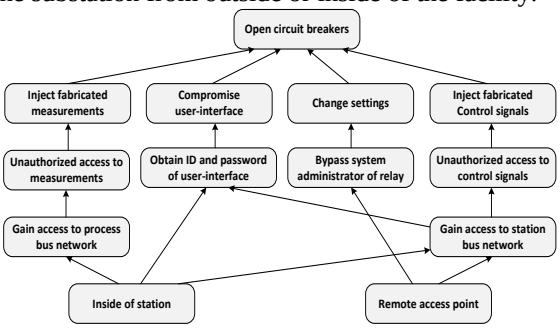


Fig. 2. An example of potential cyber attacks

From inside the substation, an adversary may inject false streaming measurement data (currents and voltages). The

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TII.2018.2884728, IEEE Transactions on Industrial Informatics

station communication bus can be accessed either from the external network (remote access points) or from inside the communication network. Once attackers have gained access, they could compromise either or both the station equipment (protective relays, remote terminal units or user-interfaces) or communication protocols. For instance, they could issue malicious control or commands to open circuit breakers. Another potential attack scenario is to change the protective relay settings so that the relay will be tripped on normal operation, which may create a cascading problem. Additional attack trees have been created to analyze the attack paths and potential cyber threats for designing supplementary cyber intrusion scenarios.

B. *Impact analysis*

Impact analysis is necessary to analyze the consequences of a cyber attack on the substation and the power system as a whole. We assume that the final action of the attack results in circuit breaker opening or closing. Such action could be the outcome of a cyber attacker performing the malicious actions. Fig. 3 illustrates an integrated cause/effect modeling approach that captures both power system vulnerabilities and the resulting impacts on the real-time operation.

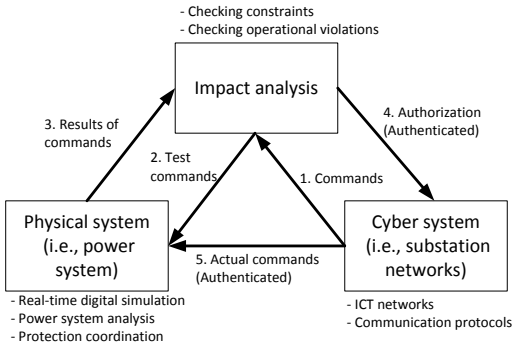


Fig. 3. The model of impact analysis

In the developed algorithms, any commands (e.g., circuit breaker control and setting change) from the cyber system will be analyzed and verified by an impact analysis module before issuance of the actual commands. The analysis sometimes involves evaluating the steady-state and dynamic behavior of a power system under a cyber attack or operator's command. Other impact analysis could be applying basic coordination rules between protective relays. As time is of essence, evaluation of a power system under cyber attacks can be performed quickly on a system in proximity to the compromised systems.

C. *Security Filter*

The proposed collaborative intrusion detection framework requires secured signal for authorization and actual command. One such approach to secure the signal via authentication was introduced, a security filter. Security filters can be inserted between the devices and secure the communication in IEC 61850 digital substations by providing end-to-end authentication for multicast messages. The design of security filter is out of the scope of this paper, and more details can be found in [18]. The security filter authenticates and verifies the designated multicast packets transmitted between protection and control devices by appending a message authentication code (MAC) called GMAC (Galois MAC) to the extended IEC 61850 packets (e.g., GOOSE and SV) [19, 20, 21].

IV. Domain Based Collaborative Mitigations

Cyber intrusions to substations in a power grid are of particular importance since most substations are unmanned and have limited physical security. One vulnerability is remote access to a substation network from corporate offices or locations external to the substation for control and maintenance purposes. This paper assumes that the remote access point is the main intrusion point to substations. An intruder may be able to access the substation network after the firewall is compromised. When remote access points have been compromised by an intruder, malicious attacks to operate circuit breakers and/or to access critical information, such as Substation Configuration Description (SCD), can be launched. For example, IEDs may have a web server to allow remote configuration change and control. As mentioned, state-of-the-art cybersecurity mitigation techniques for cyber attacks on power grids protection and control devices are performed at the ICT layer. The main problems of ICT layer-based cybersecurity mitigations are as follows: (1) sometimes they perform with unacceptable false positive/negative ratio, (2) they can be compromised by new type of cyber attacks, and (3) they need a system update or patch when new type of Operating System (OS) and ICT are available. This paper proposes a new type of cybersecurity mitigation methods called "power system domain based collaborative mitigation methods." The proposed mitigation methods can be used independently or/and can complement existing ICT layer measures so as to reduce the false ratio of ICT based methods. In this paper, we have chosen three most cyber attack scenarios from the impact analysis: configuration change, sensor data injection and direct CB control attacks. The final goal of these attacks is to open circuit breakers in order to induce a potential cascading event that could lead to a power system blackout.

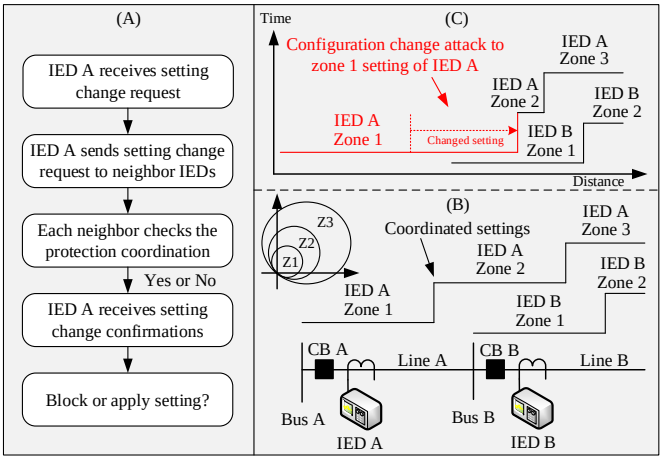


Fig. 4. Configuration Change (CC) attack

A. *Line protection configuration change security*

It is a well-known fact [1] that misconfigured distance relays may result in unwanted trips to transmission lines and trigger

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TII.2018.2884728, IEEE Transactions on Industrial Informatics

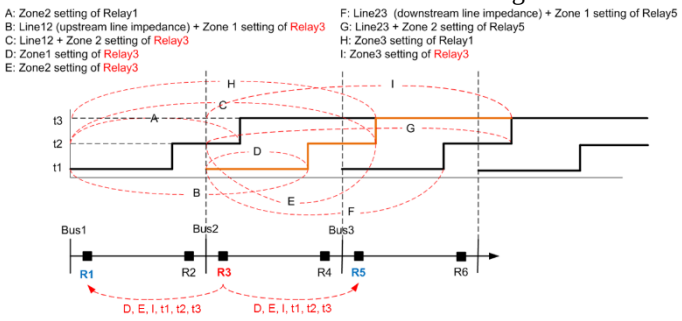
cascading outages leading to a blackout. The misconfiguration could be due to human error but also could be caused by malicious change in distance relay settings. Distance protection is one of the key schemes used to protect transmission lines [22].

It responds to impedance calculated from fundamental measurements (voltage and current phasors) between the location of IED and fault. Generally, the reach of Zone 1 and 2 settings are between 85 ~ 90 %, and 120 ~ 150 % of the transmission line, respectively. Whereas Zone 3 setting will be between 120 and 180 % of the next transmission line as shown in Fig. 4-(B). Therefore, if a fault occurred at the beginning of the line B (e.g., 20% of line B), the distance protection of IED B will see the fault and then trip the circuit breaker B for the isolation of the fault on the line B. However, if it is assumed that attacker(s) have enough knowledge of basic protection principles to change the Zone 1 setting of IED A as described in Fig. 4-(C), they could extend the Zone 1 setting of IED A by overreaching to 130 % of line A, which will be a violation of distance protection coordination. Once attackers have successfully changed the Zone 1 setting of IED A, the same fault at line B will be seen by both IED A and B. The consequence of this attack will be an unintended or false trip of circuit breaker A possibly resulting in dropping of more customer loads. Fig. 4 illustrates the developed domain based collaborative mitigations scheme to secure distance relays from configuration change attacks It is based on principles from protective relaying. If IED A gets a configuration change request (could be normal setting change by operator or cyber attack attempts by intruder), it requests a confirmation from its neighboring IEDs, e.g., IED B and IED C. Once the adjacent IEDs receive a setting confirmation request, they will independently evaluate protection coordination to target IED (i.e., IED A) as described in impact analysis framework (Fig. 3). If there is no loss of coordination, the adjacent IEDs will send a permissive (*true)* response to target IED via GOOSE. Otherwise, they send a blocking (*false)* response. Then target IED (IED A) makes the decision as,

$$D_A^{CC} = \begin{cases} 1, \text{if } D_B^{CC} \wedge D_C^{CC} = true \\ 0, \text{if } D_B^{CC} \wedge D_C^{CC} = false, \end{cases} \quad (1)$$

where D_A^{CC}, D_B^{CC} and D_C^{CC} in (1) is a final decision of IED A, B and C, respectively. As described in (1), if any of neighbor IEDs send a blocking response, the target IED rejects the configuration change request, and send alarms to the operator.

More detailed conditions can be found in the Fig. 5 as follows.



R1 Algorithm
Accept, if
1. t1 = 0
2. 0 < t2 <= t3
3. t2 < t3 <= Max_timedelay
4. A < B
5. A < C
6. D < E < I
7. H < I
8. H < C
Otherwise, reject

R5 Algorithm
Accept, if
1. t1 = 0
2. 0 < t2 <= Max_timedelay
3. D < Line23
4. E < F
5. E < G
6. D < E < I
7. I < G
Otherwise, reject

Fig. 5. CC Attack Detection Algorithm

An underlying foundation for the developed solutions is security of the data between the IEDs. The communications between IEDs and gateway is secured by security filters (refer to Section III-c) so attackers cannot inject fabricated confirmation from/to the IEDs for all mitigation scenarios. Other protective relays, e.g., overcurrent, directional, and differential relays, are equally vulnerable to malicious misconfiguration. Their actions will only affect the tripping decision to the extent of their coordination with the compromised relay.

B. Security against sensor data injection attacks

The consistency of the fault current signatures measured across all IEDs in a substation can be used to secure against data injection attacks. IEDs in conventional substations get measurements from current transformers (CTs) and voltage transformers (VTs) via hardwired analog inputs, whereas IEDs in digital substation receive currents and voltages using sampled value messages from merging units (merging units are connected to conventional or non-conventional CTs and VTs). Fig. 6 illustrates how false data injection attack can be performed in digital substations, and how it can be detected and blocked by the power system domain layer mitigation described in this paper. If the attackers can access the substation ICT networks, they could compromise the measurement signals of IED A or any other IED within the same network. For example, they could create fabricated fault currents and inject them into the target IED inducing IED A to trip circuit breaker A, as shown in Fig. 6-(B). When a fault occurs in the power system, detection of fault transients and associated characteristics (including transient direction) can also be extracted through evaluation of sampled values from other monitored points (e.g., through merging units) in the substation. Hence, IEDs can evaluate whether to trip a CB in response to the detection of the fault and based on confirmation of an indication of detection of fault transients at the other monitored points of the power system. In the proposed mitigation method as illustrated in Figure 6-(A), the IEDs check for a transient fault signature (TFS) by analyzing multiple Sampled Values (currents) messages whether they are satisfied at designated nodes and line currents with transformer ratio. Once an IED detects a transient fault signature, it will distribute the TFS signal to all other IEDs. Then the IEDs calculate the cross correlation coefficient, Ψ, of TFS - a measure whether the measured fault signals are correlated to each other. In this approach, a High Pass Filter (HPF) filters the measured current signals in sampled values messages and then Π_{TFS} will be calculated on time and frequency domain.

$$\Pi_{TFS}(t, f) = TFS(HPF(t, I_t)). \quad (2)$$

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TII.2018.2884728, IEEE Transactions on Industrial Informatics

If one of the fault signals is modified by attackers, the TFS of current measurements at different location will show some discrepancy. The differences between TFS results can be calculated by, if the fault signal is modified by attackers, the TFS of current measurements at different location will show some discrepancy. Then the differences between TFS results can be calculated by,

$$\Psi(\Pi_m, \Pi_n) = \frac{1}{N-1}\sum_{k=1}^{N}\left(\frac{\Pi_{m,k}-\mu_{Im}}{\sigma_{Im}}\right)\left(\frac{\Pi_{n,k}-\mu_{In}}{\sigma_{In}}\right) = \frac{cov(\Pi_m, \Pi_n)}{\sigma_{Im}\sigma_{In}} \quad (3)$$

$$D_A^{FDI} = \begin{cases} 1, & \text{if } \Psi(\Pi_{TFS1}, \Pi_{TFS2}, \Pi_{TFS4}) > T \\ 0, & Otherwise, \end{cases} \quad (4)$$

The similarity of multiple TFS signals can be identified and calculated by the cross correlation coefficient defined in Eq. (3), where $\Psi(\Pi_m, \Pi_n)$ is the index of cross correlation coefficient, μ_{Ic} and μ_{It} are means of Π_m and Π_t, respectively. The σ_{Im} and σ_{In} are standard deviation of Π_m and Π_n, where D_A^{FDI} is the decision from IED A, and Π_{TFS} is the result of TFS. If the measured currents of line 1, line 2 and line 3 are not cross correlated (e.g., higher than the threshold value, T), it will set D_A^{FDI} as *true*, in which case IED A blocks the trip signal or sends an alarm to the operator.

C. *Security against Direct Circuit Breaker control attack*

EMS operators sometimes need to remotely control the CBs at the substation. They issue the direct commands to CBs via DNP 3.0 communication from the control center to the substation. In a manned substation, substation operators can issue the direct CB control command from local Human Machine Interface (HMI). Sometimes operators may issue incorrect command to open breakers resulting in potentially serious operational problems (i.e., human error). Furthermore, most of direct control signals are not encrypted presenting a vulnerability that could be exploited by cyber attackers. Fig. 7 shows how direct CB control attack can be performed and mitigated by the proposed algorithms. If the attackers have gained access to the substation's ICT networks, they could fabricate a direct CB control signal, send it to the target IED A, and trip the breaker. However, with the proposed mitigation method, the IED A will first send a confirmation request to the security gateway, which analyzes the impact of the action, particularly with regards to potential line overload condition and bus voltage violation. If a confirmation is not received then the tripping action will not start.

Potential overload can be predicted by checking whether the affected line conductor temperature will exceed its thermal overload trip threshold, θ_{TRIP}. This involves the extra step of predicting the final temperature θ_{final} based on the new line current I (if the breaker is opened) in (5).

$$\theta_{final} = \left(\frac{I}{I_{base}}\right).\theta_{base} + \theta_{amb} \quad (5)$$

$$\theta_n = \theta_{n-1} + \left(\theta_{final} - \theta_{n-1}\right).\left(1 - e^{-\frac{\Delta t}{\tau}}\right) \quad (6)$$

$$t_{operate} = -\tau.ln\left(\frac{\theta_{final}-\theta_{TRIP}}{\theta_{final}-\theta_n}\right). \quad (7)$$

Where,

I	Steady state RMS line current
θ_{final}	Final temperature rise corresponding to I
I_{base}	Given reference for the RMS current
θ_{base}	Steady state temperature rise corresponding to I_{base}
θ_{amb}	Ambient temperature
θ_n	Calculated present temperature
θ_{n-1}	Calculated temperature at the previous time step
θ_{final}	Calculated final temperature with the actual steady state RMS current
Δt	Time step between calculation of the actual temperature
τ	Thermal time constant for the protected line
$t_{operate}$	Calculated time to send trip signal with present temperature
θ_{TRIP}	Trip temperature corresponding to protected line thermal limit

Eq. (7) shows the impact of the issued direct CB control action (open CB A) on potential system overload resulting from direct CB control action. For instance, if the result of (7) is not infinite, IED B trips Line 2 through line thermal overload protection after IED A has tripped CB A. Therefore, the system operator can know that the consequence of tripping Line 1 will cause another line tripping action (i.e., Line 2). Circuit breaker opening could potentially violate operational voltage limits. To evaluate the operational impact of a circuit breaker opening on the voltages and the line flows a power flow model could be constructed composed of the substation and nearby stations. Eq. (8) shows the linear relationships between the changes in powers and voltages. When a breaker opening results in line outage, the Jacobian elements would have been modified as indicated in Eq. (9). If the determinant of the new Jacobian is close to zero, Eq. (10), then it could be a potential voltage stability problem.

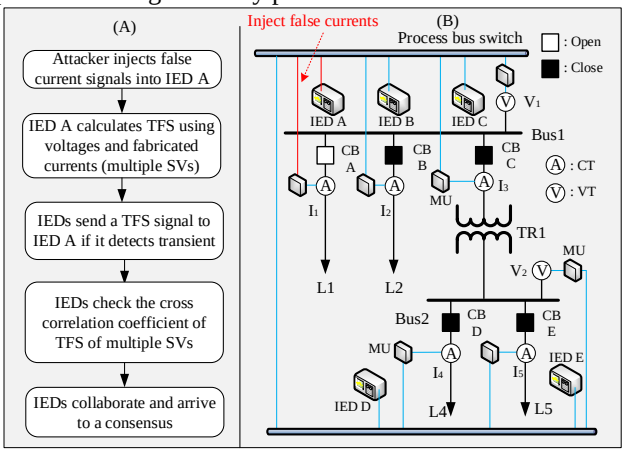


Fig. 6. False Data Injection (FDI) Attack

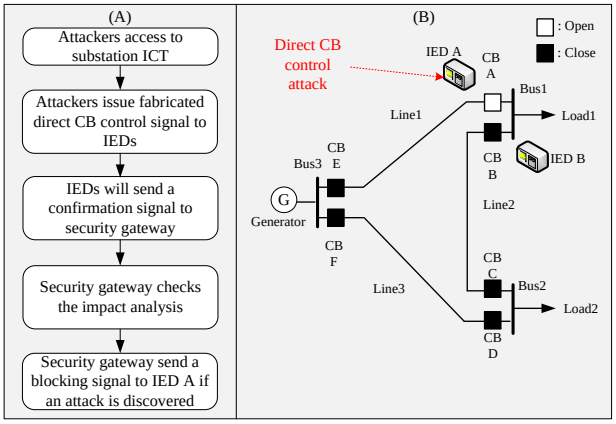


Fig. 7. Direct CB Control (DCBC) Attack

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TII.2018.2884728, IEEE Transactions on Industrial Informatics

$$\begin{bmatrix}\Delta P_{pre}\\ \Delta Q_{pre}\end{bmatrix}=\begin{bmatrix}J_{11} & J_{12}\\ J_{21} & J_{22}\end{bmatrix}\begin{bmatrix}\Delta\theta_{pre}\\ \Delta V_{pre}\end{bmatrix} \quad (8)$$

$$\begin{bmatrix}\Delta P_{post}\\ \Delta Q_{post}\end{bmatrix}=\begin{bmatrix}J_{11}+\Delta J_{11} & J_{12}+\Delta J_{12}\\ J_{21}+\Delta J_{21} & J_{22}+\Delta J_{22}\end{bmatrix}\begin{bmatrix}\Delta\theta_{post}\\ \Delta V_{post}\end{bmatrix} \quad (9)$$

$$\text{Determinant}\begin{bmatrix}J_{11}+\Delta J_{11} & J_{12}+\Delta J_{12}\\ J_{21}+\Delta J_{21} & J_{22}+\Delta J_{22}\end{bmatrix}=0 \quad (10)$$

The steady-state power flow algorithm could be running in a substation platform such as a security gateway and used to maintain situational awareness in the substation. Here P_{pre}, Q_{pre}, θ_{pre} and V_{pre} are the active and reactive power, bus voltage and angle, respectively. If there is any attempt to control the circuit breaker, the security gateway first update the Jacobian matrix J to reflect line equipment outage resulting from the intended action before issuing the control in order to check the consequence of the control. As shown in Eq. (9), the Jacobian matrix would have undergone changes in its elements. Here P_{post}, Q_{post}, θ_{post} and V_{post} are active power, reactive power, bus voltage and bus angle of the expected system state (after control), respectively. Alongside this calculation, the security gateway checks the determinant of J matrix to determine if it is close to null as this could indicate a trivial solution to the steady-state power flow Eq. (10). In this case the system cannot converge to a power flow solution and would suggest a voltage collapse condition. Therefore, if the result of tripping Line 1 by IED A will cause another line to trip (Line 2), the security gateway will send a blocking signal to IED A. The overall decision process is described as follows:

$$D_{SG}^{DCBC}=\begin{cases}1, \text{if } t_{operate}=\infty\\ 1, \text{if } V_{post}<V_{threshold}\\ 1, \text{if } Determinant\ J>DJ_{threshold}\\ 0, Otherwise,\end{cases} \quad (11)$$

where D_{SG}^{DCBC} is the decision from security gateway for the IEDs to accept (if it is "1")or block the direct CB control command. Additionally, the proposed domain based mitigations have the capability to evaluate the consequences and impacts of power system control actions, so it can help the operators make safe and secure decision and prevent misoperations due to human errors.

V. Proof of Concept Validation

A test bed representing a cyber physical system to test the concepts developed in the prior sections has been designed and implemented in a laboratory environment. However, to verify their performance in the field requires a testing environment that reflects field conditions. To test the developed concepts in near-field conditions require quite extensive historical operational data from an electric utility which is not practical to obtain during the course of the research. Therefore, a realistic utility-grade test bed is indispensable for completing this cyber-physical security research [23]. The test bed brings the developed solutions to a higher technology readiness level by testing in near field conditions. It provides a convenient way to generate the data, e.g., captured communication protocol traces, sequence of event records, system and security logs. Test beds enable system engineers and operators to design, implement and test the new algorithms and devices before they are deployed in a real system. Furthermore, any proposed cybersecurity mitigations or countermeasures can be verified and analyzed in real-time on a realistic test environment. Several national laboratories have established their own cybersecurity test bed in order to study system vulnerabilities, cyber intrusions, and implementation of remedies [3, 8, 24, 25, 26, 27, 28].

A. Utility Cyber Physical Testbed

A utility cyber physical test bed was built with the objective of testing the developed concepts in near-field environment. It was used extensively to validate the timing performance of the security algorithms. This testbed consists of commercially available substation protection, control and communication field devices that are integrated into a power system model (BPA) running in the real-time simulated environment as shown in Fig. 8. The testbed features a power system simulator (RTDS), substation protective devices, substation communication gateway, power amplifiers and time synchronization of physical protection and control hardware with the simulated environment. The detailed substation model in RTDS consists of ring bus bars, transformers, circuit breakers, and multiple 500kV transmission lines, analog measurements (e.g., voltages, currents, power factors, active and reactive powers) and digital values (circuit breaker status) from the RTDS simulator are transmitted to protective IEDs through a process bus and station bus, respectively. Time synchronization of physical protection and control hardware with RTDS simulated environment is implemented using an external clock through a pulse per second (1PPS) with an accuracy of 1µs. The 1PPS is generated using a GPS clock and merging unit's time synchronization module is used to replicates the 1PPS information on its 1PPS outputs. This ensures synchronous sampling of 3-phase voltage & current analog outputs from RTDS and merging units while publishing IEC 61850-9-2LE SV streams to the process bus.

A substation gateway was used to host some of the cyber security functions and the communication modules. The other functions reside in the IEDs themselves (e.g., line differential, distance protection, and transformer protection). All power system analog and digital measurements are sent to the substation gateway via MMS and GOOSE, and then the IEDs coordinate the required information via communication through the substation gateway. Once the gateway receives all information from IEDs, it executes the implemented cybersecurity mitigation algorithms and then makes appropriate decisions, such as to block controls, send alarms or allow controls. A key requirement of the demonstration is that the security functions must not delay existing protection system's capability to detect and protect against faults in the system. It was confirmed in the lab set up that the distributed cybersecurity functions performed dependably in blocking simulated cyber attacks with timing performance that did not compromise the relays' protection times. The following

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TII.2018.2884728, IEEE Transactions on Industrial Informatics

sections describe the security functions introduced in Section IV and how they were implemented and demonstrated in the utility cyber physical test bed.

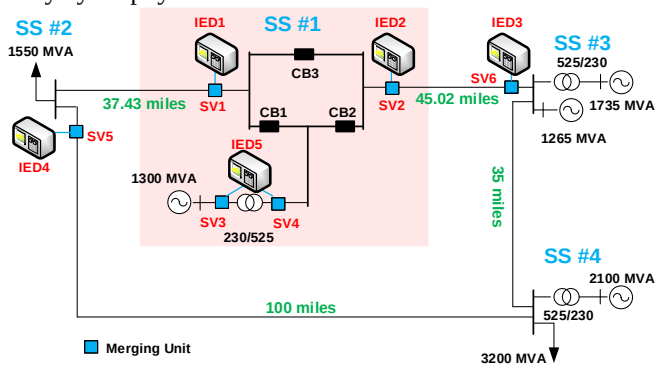


Fig. 8. Simplified test system

B. *Configuration change (CC) security demo*

This demonstration aims to confirm the performance of the developed secured configuration change function in this test bed. Here the relays were configured with realistic distance relay settings. For the security demonstration, on-line setting changes were attempted on the protective IED1 at the virtual 500-kV substation (SS #1 in Fig. 8) extending the reach of zone 1 into the next station (SS #2). As shown in Fig. 4, when an IED setting change was attempted, the IED sends the setting change request confirmation to other neighboring substation IEDs. After the request was received by the neighboring relays (IED3 and IED4), each execute the mitigation algorithms to check whether the attempted settings violate distance protection coordination. Since the setting change attempt was designed to overreach the Zone 1 of other IEDs, the neighboring IEDs did not issue a confirmation signal so the attempted changes were blocked by the secured configuration change function method.

C. *False data injection attack security (FDI) demo*

In this proposed false data injection security demonstration of the function described in Section IV IEDs will receive all corresponding SV streams from each merging unit in the substation. For instance, an IED1 in Fig. 8 must receive SV1 of the voltages and currents in its primary zone of protection to process distance protection but it will receive other measurements from other locations in the substation, e.g., SV2, and SV3, for the analysis. The IEDs will wait (do not process extra SVs) until they detect the first fault to calculate the TFS. Once they see the fault, the IEDs will calculate TFS using the subscribed multiple sampled values (SV2 and SV3) not used for the main protection. In this way, IEDs can perform cross-correlation in the beginning of the first fault. Once an IED detects abnormal cross correlation coefficients, it will send a binary TFS signal to other IEDs. As described in Fig. 6, the IEDs calculate the cross correlation coefficient regardless of the measurements violating any predefined rules. Once the relays detect abnormal cross correlation coefficients possibly indicating injected fabricated fault currents, they will let other relays know to prevent the fault trip signal. The TFS is designed to work with data windows shorter than the relay's window used in protection algorithms. Since the TFS signal is faster than the operating time of the existing protection functions, the proposed method successfully mitigates the malicious intent of any injected false data by blocking that action. In the case when correlation signals are not available (e.g., due to cyber attack or network error), the traditional protection function is not compromised but remains vulnerable. However, the attack surface for the cyber attacker would have been too complex because of this method.

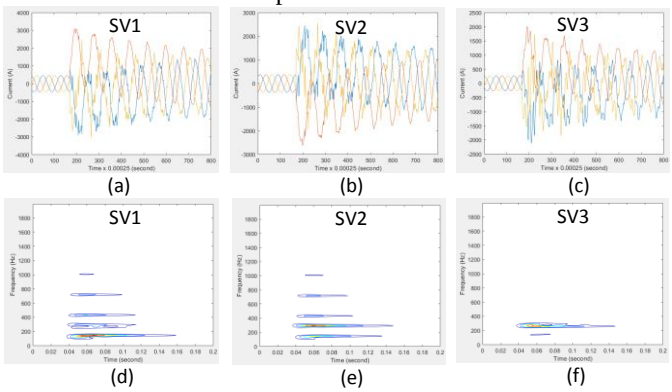


Fig. 9. Transmission line fault (between SS#1 and SS#2) and TFS

Fig. 9-(a), (b) and (c) show the current measurements of SV1, SV2 and SV3, respectively whereas Fig. 9-(d), (e) and (f) show the TFS (frequency-time domain graph calculated by Eq. (2)) of SV1, SV2 and SV3 when a fault occurred at between substations (SS #1 and SS #2), respectively. As Fig. 9-(a) to (f) show, the fault signatures propagate across the substation and all IEDs can detect the TFS from the three different measurement points, e.g., SV1, SV2 and SV3. Fig. 10-(a), (b) and (c) illustrate line currents from SV1, SV2 and SV3 under the normal operation whereas Fig. 10-(d), (e) and (f) describe TFS of SV1, SV2 and SV3. The TFS of SV1, SV2 and SV3 are almost same (cross correlation coefficient=0.86). However, when a false data was injected to SV1, as Fig. 11-(a) show, the TFS of SV1 (Fig. 8-(n)) shows significant difference (cross correlation coefficient=0.32) compared to SV2 (Fig. 10-(e)) and SV3 (Fig. 10-(f)). Even when the attackers try the replay attack after capturing the actual fault signals shown in Fig. 9-(a), the TFS of Fig. 9-(d) compared to Fig. 10-(e) and Fig. 8-(f) show a huge difference. In the improbable case when attackers replay a normal signal during the short duration of a real fault, the proposed system would vote in the majority and will make a decision (e.g., trip the breaker). Note that it is unlikely that an attacker could simultaneously replay a normal signal during the short duration of a real fault (it has been verified using testbed).

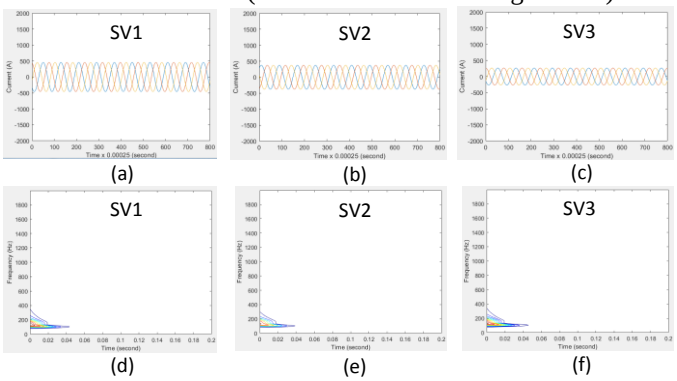


Fig. 10. Normal operation and TFS

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TII.2018.2884728, IEEE Transactions on Industrial Informatics

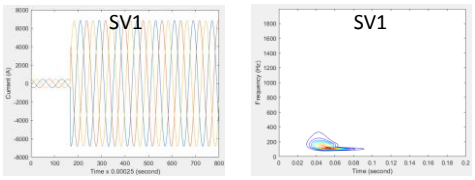


Fig. 11. Bad data injection attack and TFS

D. *Direct CB control security (DCBC) demo*

For the direct CB control security demonstration, MMS based Select Before Operate (SBO) control has been used. In the proposed mitigation scheme described in Section IV, a relay sends a confirmation request signal to the security gateway, after which the security gateway calculates the operational effect of opening the breakers in terms of potential system overload. The open command on the first breaker CB1 (at SS #1 in Fig. 8) does not create any line tripping so the security gateway sent a permissive confirmation signal to IED1 to open CB1. However, when attackers subsequently issued another direct CB control signal to open CB3, the security gateway detected an operational security violation, and sent a blocking signal to disallow the open breaker command on CB3.

VI. CONCLUSION

Cyber security threats to critical infrastructure assets have been increasing over the last decade. The efforts to mitigate these actions resulted in development of many cyber security standards and guidelines, and also produced lots of ICT based counter measures. This paper proposes novel power system domain based mitigation methods that have been developed, implemented and validated with the proposed cyber-physical security test bed. The proposed mitigation methods can be used even if ICT based solutions (e.g., firewall and intrusion detection system) are compromised. The proposed test bed can simulate cyber-attacks and validate the mitigation methods performance using real-time hardware-in-the-loop system. The methods have been validated by testing with realistic intrusion scenarios. The main contributions of this paper are: (1) introducing power system domain principles to detect and block a cyber-attack; (2) a system of IEDs collaborating in confirming the validity of changes based on their own measurements; (3) a collaborative scheme for IEDs to vote as a group to effect a change in the IED configuration; (4) a method for predicting the consequence of the control actions that includes cyber attack and normal operators commands; and (5) a method for helping operators make secure decisions and prevent human errors. We assumed that the code executing the proposed solutions are secured against cyber attacks. Furthermore, the developed functions require engineering efforts in integrate them in real substation systems. In future work, it will be useful to extend this research to include (1) other protective IEDs (overcurrent, directional, and differential relays), (2) coordinated simultaneous attacks on multiple devices, and (3) cybersecurity detection and mitigation of other substation automation communication protocols (e.g., MMS, SNTP, DNP, Modbus, and IEC 60870-5).

VII. REFERENCES

[1] P. Pourbeik, P. S. Kundur and C. W. Taylor, "The Anatomy of a Power Grid Blackout - Root Causes and Dynamics of Recent Major Blackouts," *in IEEE Power and Energy Magazine*, vol. 4, no. 5, pp. 22-29, Sept.-Oct. 2006.

[2] D.C. Elizondo, J. de La Ree, A.G. Phadke, and S. Horowitz, "Hidden Failures in Protection Systems and their Impact on Wide-area Disturbances", *IEEE Power Engineering Society Winter Meeting*, 28 Jan.-1 Feb. 2001.

[3] Y. Chen, J. Hong and C. C. Liu, "Modeling of Intrusion and Defense for Assessment of Cyber Security at Power Substations," *IEEE Trans. Smart Grid*, vol. 9, no. 4, pp. 2541-2552, July 2018.

[4] DRAGOS, "CRASHOVERRIDE: Analyzing the Threat to Electric Grid Operations," DRAGOS Inc., June 2017. [Online]. Available: https://dragos.com/blog/crashoverride/CrashOverride-01.pdf

[5] Industrial Control Systems Cyber Emergency Response Team (ICSCERT), Cyber-Attack Against Ukrainian Critical Infrastructure, Feb. 2016 [Online]. Available: https://ics-cert.us-cert.gov/alerts/IR-ALERTH-16-056-01

[6] North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) Reliability Standards 002-009. Available: http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx

[7] IEC 62351, Power Systems Management and Associated Information Exchange - Data and Communications Security, IEC TS 62351-1 Standard: Part 1: Communication Network and System Security - Introduction to Security Issues.

[8] J. Hong, C.-C. Liu, and M. Govindarasu, "Integrated Anomaly Detection for Cyber Security of the substations," *IEEE Trans. Smart Grid*, vol. 5, no. 4, pp. 1643-1653, July 2014.

[9] F. M. Cleveland, "Distributed Energy Resources (DER) Using IEC 61850 with Cyber Security and Resilience Guidelines," *Smart Grid Handbook*, John Wiley & Sons, Ltd., 2016.

[10] A. Chattopadhyay, A. Ukil, D. Jap and S. Bhasin, "Towards Threat of Implementation Attacks on Substation Security: Case Study on Fault Detection and Isolation," *IEEE Trans. Industrial Informatics*, vol. PP, no. 99, pp. 1-1, 2017 (Early Access Articles).

[11] J. Hong and C. C. Liu, "Intelligent Electronic Devices with Collaborative Intrusion Detection Systems," *IEEE Trans. Smart Grid*, vol. PP, no. 99, pp. 1-1, 2017 (Early Access Articles).

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

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

[14] R. Bulbul, P. Sapkota, C. W. Ten, L. Wang and A. Ginter, "Intrusion Evaluation of Communication Network Architectures for Power Substations," *IEEE Trans. Power Delivery*, vol. 30, no. 3, pp. 1372-1382, June 2015.

[15] J. Yang, C. Zhou, S. Yang, H. Xu and B. Hu, "Anomaly Detection Based on Zone Partition for Security Protection of Industrial Cyber-Physical Systems," *IEEE Trans. on Industrial Electronics*, vol. 65, no. 5, pp. 4257-4267, May 2018.

[16] Y. Xin et al., "Machine Learning and Deep Learning Methods for Cybersecurity," *IEEE Access*, vol. 6, pp. 35365-35381, 2018.

[17] R. Nuqui, "Collaborative Defense of Transmission and Distribution Protection and Control Devices against Cyber Attacks (CODEF)," U. S. Department of Energy (DOE) Office of Electricity Delivery and Energy Reliability (OE), 2015 [Online]. Available: https://www.energy.gov/sites/prod/files/2015/12/f27/CODEF%20fact%20sheet%20June%202015.pdf

[18] T. Cui, D. Ishchenko, and R. Nuqui "Security Filter: Secure Communication of Protection and Control Devices in IEC 61850 Substations," *Protection, Automation and Control (PAC) World Americas*, Raleigh, NC, USA, 2015.

[19] IEC 61850-8-1 Edition 2.0, Communication Networks and Systems for Power Utility Automation Part 8-1: Specific Communication Service Mapping (SCSM) – Mappings to MMS (ISO 9506-1 and ISO 9506-2) and to ISO/IEC 8802-3

[20] IEC 61850-9-2 LE, Implementation Guideline for Digital Interface to Instrument transformers Using IEC 61850-9-2, UCA International Users Group.

[21] IEC 61850-7-4 Edition 2.0, Communication Networks and Systems for Power Utility Automation Part 7-4: Basic Communication Structure – Compatible logical node classes and data object classes.
[22] P. K. Nayak, A. K. Pradhan and P. Bajpai, "Secured Zone 3 Protection During Stressed Condition," *IEEE Trans. Power Delivery*, vol. 30, no. 1, pp. 89-96, Feb. 2015.
[23] A. Martin, R. Nuqui, J. Hong, A. Kondabathini, W. Rees, D. Ishchenko, "Collaborative Defense of Transmission and Distribution Protection and Control of Devices against Cyber Attacks (CoDef)" *Western Protection Relay Conference*, October 2016.
[24] R. Liu, C. Vellaithurai, S. S. Biswas, T. T. Gamage and A. K. Srivastava, "Analyzing the Cyber-Physical Impact of Cyber Events on the Power Grid," *IEEE Trans. Smart Grid*, vol. 6, no. 5, pp. 2444-2453, Sept. 2015.
[25] C. Konstantinou, M. Sazos, A. S. Musleh, A. Keliris, A. Al-Durra and M. Maniatakos, "GPS Spoofing Effect on Phase Angle Monitoring and Control in a Real-time Digital Simulator-based Hardware-in-the-loop Environment," *IET Cyber-Physical Systems: Theory & Applications*, vol. 2, no. 4, pp. 180-187, 12 2017.
[26] Cyber Resilient Energy Delivery Consortium (CREDC) [Online]. Available: https://iti.illinois.edu/research/energy-systems/cyber-resilient-energy-delivery-consortium-credc
[27] S. Adepu, S. Shrivastava and A. Mathur, "Argus: An Orthogonal Defense Framework to Protect Public Infrastructure against Cyber-Physical Attacks," *IEEE Internet Computing*, vol. 20, no. 5, pp. 38-45, Sept.-Oct. 2016.
[28] A. Ashok, M. Govindarasu and J. Wang, "Cyber-Physical Attack-Resilient Wide-Area Monitoring, Protection, and Control for the Power Grid," *Proceedings of the IEEE*, vol. 105, no. 7, pp. 1389-1407, July 2017.

VIII. DISCLAIMER

This paper was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

IX. BIOGRAPHIES

Junho Hong (M'14) is a Senior Scientist at ABB Corporate Research in Raleigh, NC USA, since 2014. He received his Ph.D. in Electrical Engineering from Washington State University, in Pullman, WA USA, in 2014. Dr. Hong has been working on in the area of cyber-physical security of power grids more than 10 years and currently he is leading a US government funded cyber security project. His research interests are in the areas of cyber-physical security of power systems, substation automation, HVDC, Microgrid and high power EV charger.

Reynaldo F. Nuqui (SM'09) is a Senior Principal Scientist with the ABB Corporate Research in Raleigh, NC USA. He is employed by ABB for the last seventeen years. He received his Ph.D. in Electrical Engineering from Virginia Polytechnic Institute and State University, in Blacksburg, Virginia USA. Dr. Nuqui has been performing research and development in the general areas of high voltage transmission technologies. For the past eight years, he was involved in the modeling and simulation of HVDC Grids for control, protection and economic evaluation. He was Principal Investigator for two DOE funded projects related to cyber physical security. Dr. Nuqui is a Senior Member of the IEEE.

Anil Kondabathini (M'06) is a Sr. Research Scientist with ABB Inc. US Corporate Research Center in Raleigh, North Carolina. He received his Ph.D. in Electrical and Computer Engineering from Mississippi State University in 2009. He has more than 8 years of research and industry experience in the areas of power system, power electronics applications, microgrids and electrical cyber-physical security systems. Recently he is involved in several US government sponsored study and research projects related to Security of Energy Delivery Systems. His experience also include renewable energy integration, HVDC & FACTS, power system planning and economic analysis, real time modeling and simulations.

Dmitry Ishchenko (SM'04) is a Lead Principal Scientist at ABB US Corporate Research Center in Raleigh, NC, where he currently provides technical project leadership and supports strategic corporate technology development in the areas related to cyber-physical security for microgrids, power grids control and protection, renewable integration and utility communications. Dr. Ishchenko holds a Ph.D. degree in electric power systems. He is an active member of several Working Groups on DER integration and interoperability, and microgrid control functions, has published more than 30 technical papers and holds six patents. Additionally, he has extensive utility operations, new product development and application engineering experience in power systems control and protection.

Aaron Martin (SM'06) received a BSEE from University of Idaho in 2000, and a MEEE from the University of Idaho in 2007. He is licensed professional engineer in the state of Washington. In 1999 Aaron Martin began work for the Army Corp of Engineers as a Maintenance Engineer at Lower Granite Dam, located on the Snake River, in Washington State. In 2002 he left the USACE to work for the Bonneville Power Administration as a system protection field engineer in The Dalles, Oregon. In 2006 he transferred to BPA's Branch of System Protection and Control in Vancouver, Washington. His main duties involve system protection and substation automation issues on 115kv, 230kv, and 500kv transmission systems. He is currently working in that position. Aaron is also a member of the IEEE PSRCC Main Committee, the Vice Chair of the H-Subcommittee of the PSRCC, the Chair of the new Working Group H Monitoring and Diagnostics of IEC 61850 GOOSE and Sampled Values based systems, the Co-chair of the EPRI protection task force, and the Chair of the IEEE 1588 Power Conformity Assessment Steering Committee.