Substation Anomaly Detection System – A Substation & Distribution Network Cybersecurity Early Warning System

Eric Hawthorne[*], Moein Manbachi[*], Alif Gilani[**]
British Columbia Institute of Technology (BCIT)[*], Siemens Canada Limited[**]
CANADA

SUMMARY

Power grids are transitioning to a fully digital data-network-driven paradigm. While digitalization provides great benefit in terms of flexible, adaptive, and efficiency-optimized operation of the power-grid, it introduces substantial new risks of cyberattack on the power grid, including the risk of disruptive and damaging mal-operation of control and protection. While IT security best-practices and IT security technology such as firewalls, intrusion and malware detection systems, asset management software and Security Information and Event Management (SIEM) systems can help to detect and prevent such attacks, it is wise to assume that well-resourced mal-actors may still penetrate the control network, and either take manual actions or place persistent malware for later triggering. Therefore, an additional important aspect of critical infrastructure cybersecurity is real-time situational awareness of potential system mal-operation due to digital monitoring and control system misbehavior. A pathway to such situational awareness is to understand system vulnerabilities to different cyberattacks, and to note the characteristic effects of each category of attack. Hence, it is important for operators of an infrastructure system such as digital substations to investigate potential cyberattack scenarios, and prioritize detection and mitigation efforts according to different cyberattack impact levels. This paper enumerates and describes attack types particular to the OT (control and monitoring system) of the substation and distribution segment of the grid, on the assumption that access to the OT networks has already been gained by mal-actors or their malware. With research still in progress, this paper examines specific cyberattack test case scenarios carried out on an IEC61850 digital substation emulated by a designed test platform. The emulated substation and distribution grid has an advanced double bus-bar scheme and includes Distribution Energy Resource (DER) assets. Multi-vendor protection relays adopt typical protective schemes of a real substation environment, and power flow simulation is carried out over process bus (IEC61850-9). This paper first introduces the designed and developed real-time test platform for cybersecurity studies. Then, it briefly enumerates plausible cyberattack cases to IEC 61850 substation and distribution grid. It then investigates two noteworthy and diverse IEC 61850-based cyberattack test cases, i.e., forged breaker failure and reverse polarity of DR/DER operation. For these two test cases, data collection, training Machine Learning (ML) algorithm, attack sequences, anomaly detection methods and testing the trained detection system on attack-contrasting normal operations use cases are discussed.

KEYWORDS

Anomaly Detection, Cyberattacks, Cybersecurity, Distribution Networks, Early Warning System, IEC 61850, Substation

1. Introduction

In recent years, the IEC 61850 standard has provided power grids with remarkable capabilities such as substation IED interoperability. However, with the advent and the expansion of new IEC 61850 monitoring-and-control features, cyberattacks potentially increased vulnerability levels of the grids. As cyberattacks could negatively affect substations and/or distribution grid operational performance, studying IEC 61850-based cyberattacks seems essential. IEC 61850 Ethernet–based Generic Object Oriented Substation Event (GOOSE) can send indications that subsequently trigger control commands from an Intelligent Electronic Device (IED) to a breaker and/or an actuator to change its status and send the status changes from one IED to another to co-ordinate power-switching and power-protection functions across different feeders of the power distribution substation. In contrast, IEC 61850 Sampled Value (SV) is comprised of digitized analog values (e.g., node voltages, branch currents, etc.) that are measured in the field. Both GOOSE and SV use a non-protected multicast messaging system to perform very fast data transmission, which makes them more vulnerable to cyberattacks. Investigating IEC 61850-based cyberattack impacts on the substation and distribution grid can be done by using a similar approach to that of this paper; designing and developing a real-time test platform able to emulate different types of attack use cases, aiming to provide substation automation systems with effective cybersecurity anomaly detection solutions. In the last decade, many efforts have been devoted to address substation automation cybersecurity issues. Some tried to evaluate power system reliability considering cybersecurity in substations [1]-[4]. Others have focused on improvements in security measures [5] and vulnerability assessment [6]. Modeling of substation intrusion discussed in [7] and an integrated anomaly detection method proposed in [8]. Moreover, many utilities and research institutes aimed to setup cybersecurity test-beds [9]-[16]. The main goal of these testbeds is to measure the performance of industrial control systems when equipped with cybersecurity protections in accordance with best practices by the existing standards and guidelines. In addition, some reports focused on different recent aspects of cybersecurity [17]-[20]. In 2010, NISTIR 7628 [17] presented a guideline for smart grid cybersecurity and NESCOR [20] introduced and explained failure scenarios threat models and impact analyses according to NIST 1108. From the literature and guidelines, it can be concluded that more specific IEC 61850 cyberattack investigation is required, describing vulnerable subsystem domains and information/communication-system interfaces, reviewing some of the attacks, their potential motivations and several dimensions of distribution grid cyberthreat features, attack sequences, and possible detection methods. Hence, this paper will dive deeper into cyberattacks on the IEC 61850 substations and distribution grids. While most attack methods and use cases are on the IEC 61850 power monitoring, protection, and control system of the substation, a use case attacking the smart distribution grid of the near future, in which distribution grid management (DGM) involves the control of distributed energy resources (DER) and demand response (DR), is studied as well.

2. Real-time Test Platform Design and Setup

The main goal of the test environment is to emulate in real-time the operation of a non-trivial power-distribution substation and a moderately complex power distribution grid fed by the substation. An emulation platform was designed and developed at BCIT to provide real-time testing for substations and distribution grid cybersecurity studies. This platform emulates the required power-flow layer of the desired SuT (System under Test) using HIL (hardware-in-the-loop) process, while the command & control layers are implemented with a power automation system. This platform utilizes IEC-61850 communication protocol and emulates a fully functional medium voltage substation with various types of distribution grid loads and resources such as PV, Battery Energy Storage (BESS), and EV chargers using a Real-time Digital Simulator (RTDS). RTDS enables the platform to implement key levels of substation topology, i.e., process level, bay level and station level (see Fig. 1). This includes real-field substation protection and control IEDs such as protection relays and Merging Units (MU) using IEC 61850 GOOSE, SV and MMS protocols. The system has a real substation automation controller and HMI (from Siemens) that is able to control and monitor the whole system in real-time. As the substation topology (shown in Fig. 1) supports different power flow paths, it is flexible enough to emulate diverse grid operation scenarios. This topology enables supporting various protection schemes and short circuit levels. Moreover, the substation and distribution grid design for real-time emulation can provide a cybersecurity test platform with an adequate amount of power-metric data and P&C

signal data from normal and normal-rare (e.g. typical fault occurrence and handling / maintenance) operating conditions.

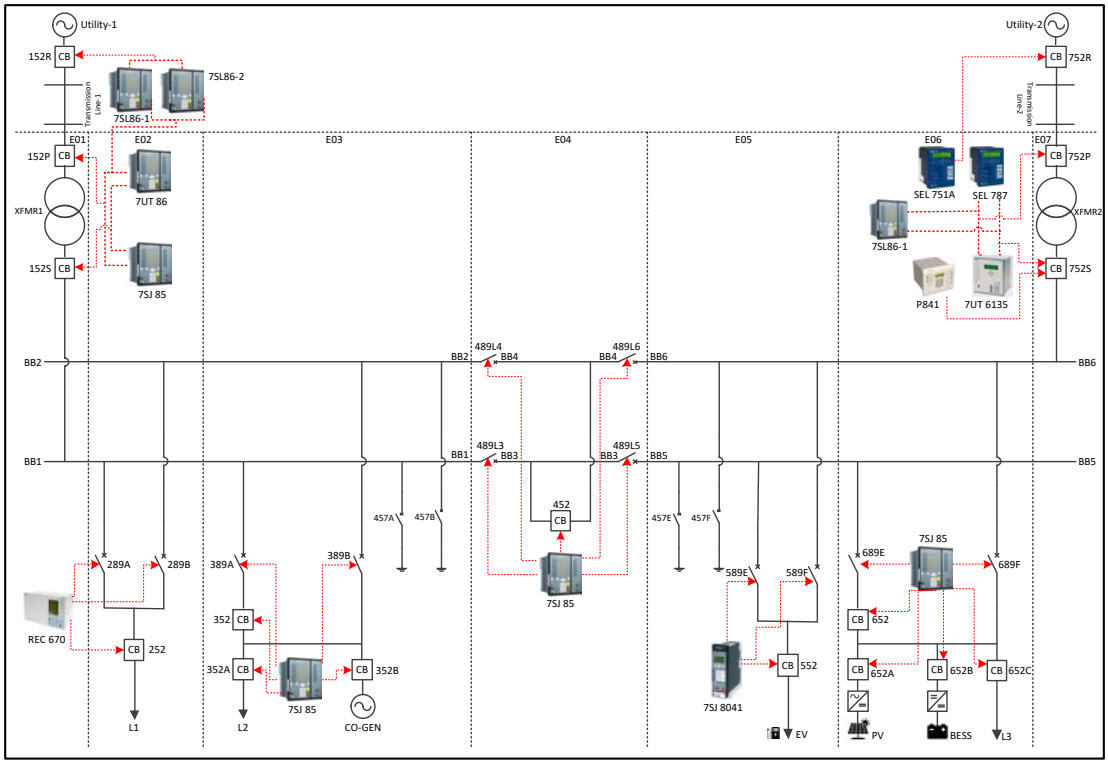

Fig. 1 Single line diagram of designed substation and distribution network

For the emulation of substation, distribution grid and the sequence of attack actions, RTDS scripting is used. For the attacks that involve testing the rate and pattern of occurrence of events which have minutes or hours between them, sped-up simulation time is used. Collection of discrete-event data and power-data masurements from the substation and distribution grid into a standardized timeseries data archive allows operating data pattern replay of use cases to ML/Attack Detection (ML/AD) algorithms, to allow flexible scheduling of trials of substation operation and cyberattack testing vs trials of ML training and anomaly detection. Fig. 2 depicts the test platform and anomaly detection data flow. A hybrid platform for training and execution of ML/AD algorithms, consisting of Google Cloud Artificial Intelligence (AI) platform and a local high-performance GPU-equipped computer server is used. Most ML/AD algorithms run on the TensorFlow-2 platform with KERAS, either on the local server or Cloud AI. The anomaly detection data processing & analysis chain also includes running of several BCIT-developed timeseries-data and event-sequence-learning algorithms, alongside standard ML and statistical algorithms running in TensorFlow/KERAS platform.

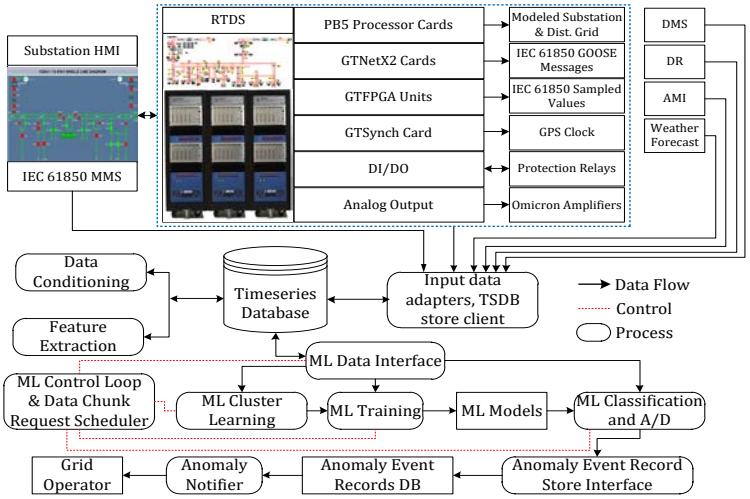

Fig. 2 Test Platform and Anomaly Detection System Data Flow

3. IEC 61850 Cyberattack Test Cases

This section enumerates a range of technically diverse cyberattack cases on a substation and distribution-network monitoring and protection-and-control system.

3. 1. GOOSE-based Attack: Forged Breaker Failure (FBF)

As a high-impact, simple GOOSE-based attack, a forged breaker failure message can create a severe condition, where the substation's co-ordinated protection scheme assumes that the breaker-in-charge cannot trip a fault. The consequence of such an attack can be high as forged breaker failure message can trip upstream breaker(s), causing wide outage and potentially damaging equipment.

3. 2. Command-based Attack: Forged Earth Switch Operating (ESO) Sequence

In this command-based attack, a forged switch-status message can defeat safety interlocking between breakers and earth switch, and can potentially cause a short-circuit. The consequence of such an attack can be very high as it can damage equipment and create significant safety hazard for the grid crew. Alternatively, forging switch-closed status could prevent power-restoring breaker operations.

3. 3. Sampled Value-based Attack: Forged Sampled Value (FSV)

The Sampled Value-based attack is one of the more difficult attacks to implement. This is due to the communications principle of publishing sampled values, the short time interval between the messages and the lack of repetition mechanism. In this attack, a forged SV stream can create trips and/or outages by mal-operation of an IED that subscribes to that stream.

Forged fault-current SVs – impact amplified by forged-GOOSE defeat of reverse-interlock blocks

Here, a fault condition is forged, by alteration of a feeder load SV stream, causing an unwarranted breaker trip. To amplify impact of a forged fault, forged GOOSE messages can be injected to unblock reverse-interlock blocks. This second attack step has the potential to defeat the substation's selective time-grading and reverse-interlock co-ordinated protection scheme and cause cascading trips.

Temporal Cluster of FSV on multiple outgoing feeders (FSTORM): Forged SVs are used at different outgoing feeders of substation to simulate a storm condition, during which the likelihood of fault occurrence increases. Attackers may change voltage or current values in different outgoing points of substation in such a way that the difference between the forged SV attack and a real storm condition is difficult to detect.

Time Stamp Manipulation (TSMAN): here, the attackers publish forged SV streams with altered sequence counter numbers for current or voltage signals to mislead protection of a component in the system such as transformer. Thus, transformer differential protection can be wrongly activated.

3. 4 Multiple "Remote" Breaker-Open Commands

In this case, the attackers gain remote interactive access to the HMI or install MMS malware, and send control commands to multiple breakers to create a wide outage and/or black out. This type of attack can cause widespread and/or cascading tripping/opening of breakers or de-energizing of substation feeder(s). Alternatively or additionally, MMS power measurement or breaker-status data forgery can mask the change of state of grid in the HMI, misleading operators about system state.

3. 5. Attack to DMS: Reversed Polarity DR and DER Operation (DERKILL)

The main idea of this case is to emulate an attack that reverses the polarity of grid-balancing demand response (DR) and distributed energy resource (DER) operation. The substation and distribution-network are assumed to be managed by a distribution management system (DMS), including demand-response automation server (DRAS) and the grid-storage supervisory control system (DERMS).

4. Detailed Cyberattack Test Cases

This section investigates two significantly important IEC 61850-based cyberattack test cases on substation and distribution grids. A use-case specification of a specific application of the attack is given based on the emulated grid. Contrasting substation normal-operation use-cases are also described, so that an anomaly detection algorithm can train on normal operation patterns, to enable recognition of anomalous behaviour. For each attack, a specification of the application of an anomaly detection algorithm is specified, and a recipe is provided for testing the AD algorithm on both the attack event sequence and on contrasting normal-operations use cases.

4. 1. Forged Breaker Failure (FBF) Attack

4. 1. 1. Training ML on FBF-Contrasting Normal Operations Use Cases

The system is trained for normal operating sequences, normal fault clearing sequences and normal-rare (e.g., grid fault) conditions. Here, the IED of E06 section (Siemens 7SJ85) in Fig. 1, is properly set and configured to clear a fault on the feeder with L3. A GOOSE message from E06 7SJ85 relay to trip 652C breaker during fault, a GOOSE message from E06 7SJ85 relay to trip breaker-652A & 652B, and three-phase current measurements of L3 feeder (where the fault occurs) on E06 section are collected for the training purpose. GOOSE status-change events and Measurement Threshold Exceedance events are used to collect required training data. The anomaly detection algorithm to be tested on the FBF case is called **SEQT** (sequence tree). The SEQT algorithm recognizes novel sequences of events, and can be set to tolerate event re-orderings in clusters of almost simultaneous events. The algorithm searches for the event sequence in a sequence tree of previously encountered time-interval-ignored events, and in another tree which also represents the sequence of events, but considers subsequent events in a sequence to be different even if they are the same event-type, but occur after a substantially different time-interval than previous occurrences did. Training of SEQT can continue through the substation's operating life, by the mechanism of giving substation operating personnel a smartphone app or substation HMI button (green "Sequence OK" button) which allows them to confirm as OK (accepted behavior) any novel sequence that SEQT flags during normal operations. A Long Short-Term Memory (LSTM) Recurrent Neural Net (RNN) can also be applied to the event sequences of the fault-clearing and fault-with-breaker-failure normal-operation cases. We plan to compare LSTM to SEQT. LSTM or SEQT are trained on Normal-Normal (fault clearing by closest breaker tripping) and Normal-rare (breaker trip attempt with breaker failure and secondary protection operation) cases.

4. 1. 2. FBF Attack Sequence and Data Collection

A sophisticated attack can be executed by simulating breaker failure protection operation of E06 7SJ85. As the intruder has changed the stNum and the sqNum in the header of the GOOSE message according to the data from the last message published by 7SJ85, it is very tough to prevent the tripping of the upstream breaker (752S). The Breaker Failure Scheme has been configured for the double busbar scheme as follows within the relays:

1. On Fault tripping, feedback monitoring time of breaker open status together with current supervision will detect failure of the trip coil of the breaker or broken tripping circuit.
2. 50BF can be configured for multiple re-trips to confirm breaker failure (For our test only a single tripping with no re-trip has been configured)
3. Failure to trip the breaker associated with the fault (on 50/51(N)) will result in 50BF trip signal trigger over GOOSE upstream to the next breaker in the active path.
4. The 50BF trip indication will be sent to the next hierarchical upstream breaker to trip on External Trip Function to trip the upstream breaker (tripping time set to instantaneous)
5. Simulation of the trip coil / tripping circuit failure is realized within the RTDS by interrupting via logic the incoming tripping command from the associated relay.
6. Forging either the 50BF Trip signal or the simulated trip coil / trip circuit failure (increment the State number stNum by a large number, set the Sequence number (sqNum) to 0, and change the Binary value to RBRF1.OpEx.general = TRUE) results in the upstream breaker (752S) tripping.
7. Note that the forged 50BF trip signal should be one that is subscribed to by the IED controlling the highest order breaker closest to the HV source, for maximum outage impact.

For data collection, a forged GOOSE message that is similar to 7SJ85 relay message for breaker failure activation and three-phase current SV streams of load-3 feeder on E06 section are collected to check if the real fault occurred or not. GOOSE status-change events and Measurement Threshold Exceedance events are used for data collection.

4. 1. 3. Testing Trained Detection System on FBF Attack Sequence

Detection of an event sequence anomaly is the expected result. The FBF attack sequence is being run and data collected as described. Batches of data are being fed to a SEQT algorithm process which has as its model a sequence tree. Or batches of data are being fed to an LSTM RNN running in KERAS+TensorFlow, where the LSTM has a model that has been trained on multiple runs. Hence, it is expected that the SEQT algorithm will have output a "novel sequence" and/or "novel sequence

timing" status indications after processing the attack event sequence. The RNN is expected to have output an anomaly score above its significant anomaly threshold setting. Either of these indications could be the basis for a warning/alarm message to operators.

4. 1. 4. Testing Trained Detection System on FBF-Contrasting Normal Operations Use Cases

A lack of false-positive anomaly detection is the expected result. The training of SEQT and RNN on normal operations use cases, has taken place. The normal operations use cases are re-run and data collected. Batches of data are fed to a SEQT algorithm process which has as its model a sequence tree as trained on the first run. Or batches of data are being fed to an LSTM RNN running in KERAS+TensorFlow, where the LSTM has a model that has been trained on multiple prior runs. Hence, it is expected that the SEQT algorithm will have output a "novel sequence=false" and "novel sequence timing = false" status indications after processing the normal operations event sequences of the final run. The RNN is expected to have output a low, below-threshold anomaly throughout the final run.

4. 2. Reversed Polarity DR and DER Operation (DERKILL) Attack

Here, a DMS is assumed responsible for initiating both demand-response and charge/discharge energy storage commands. The context is a near-future smart power-distribution-network with a significant presence of smart loads (e.g. smart EV charging network, smart buildings) and large-capacity grid-scale or distributed energy storage. Forging power measurement inputs to the DMS, or hacking into the DMS and changing its control logic, can result in incorrect/reverse DER/DR commands being issued. For example, during already extreme peak consumption hours, or during low grid frequency events, when demand-response should curtail load and DERs should increase generation and storage discharge, this attack type could reverse this response, exacerbating the grid imbalance or a local overload condition. We describe 3 attack test cases: forged load measurement input to DMS, forged grid-frequency measurement input, and inverted DER+DR command output from a hacked DMS.

4. 2. 1. Training ML on DERKILL-Contrasting Normal Operations Use Cases

To train ML on the normal behaviour of the DMS DER and DR control system, we run the simulated DMS repeatedly during low, medium, and very high (peak) distribution-network demand times, and feed to an LSTM RNN (ML) the following data streams: 1) load active power measurements at all load feeder meter locations, DER and DR site meters, and a meter at the transformer HV side. To exclude the effect of usual load profile variation, derived data features (first and second derivatives, pair-wise measurement-point value correlations or subtractions, kirchoff's law sums and subtractions) are fed to the ML instead of raw power measurements. 2) Grid frequency measurements from several metered points including HV side of transformer and distribution-network meters such as at the DER and DR sites. 3) Optionally, the direct load control setpoints and/or price signals output by the DMS.

Assuming that the DMS is also being employed as a frequency balancing service for the larger (near-future smart) grid, we also train the ML on extended time periods of simulated beyond-response-threshold low grid frequency, and simulated beyond-response-threshold high grid frequency, as well as periods of nominal grid frequency.

By this training during multiple sped-up-time simulation runs, the LSTM is expected to learn a model of the DMS's characteristic peak-shaving and frequency response, as well as learning the invariants in relationship and the typical evolutions in relationship of different power measurements.

4. 2. 2. DERKILL Attack Sequence and Data Collection

Test case 1 : intruders modify load-3 input values of the DMS. During a simulated high/extreme load-peak period in the distribution network, the load measurement SV stream is forged to indicate a very low load value. This should cause the DMS to issue DR commands that cancel any curtailment and in fact encourage or command high demand from discretionary or time-shiftable loads (we use a simulated network of EV chargers). Additionally, it should cause the DMS to change the DER (grid-scale BESS) command from discharge (grid support) to charge (increase demand). During the attack, power measurement SV and monitoring-direction MMS data are collected from measured buses in the substation and metered DR and DER locations. DMS DR and DER command signals are also collected. The expected result of the attack test is significant increase of already extreme peak load, due to maloperated DER and DR. A distribution-feeder protection relay IED may then trip on

"Undervoltage", causing local outage. Test case 2 : Forge beyond-response-threshold high grid-frequency measurement SVs on the HV side of the substation transformer, during a time when actual simulated grid frequency is beyond-response-threshold low. The DMS, relying on that grid frequency measurement and (attempting to) act as a grid balancing service, issues inappropriate DER and DR commands. Reversed polarity DER and DR activation (BESS charge, EVs max charging power) then exacerbates the wide-area grid frequency droop, although this effect is probably not measurable locally. Test case 3 : Alter the DMS simulator to issue reverse-polarity DER/DR commands in response to low or high grid frequency.

4. 2. 3. Testing Trained Detection System on DERKILL Attack Sequence

For test cases 1 and 2 : Detection of a power measurement integrity anomaly is the expected result. The training of the LSTM on DER/DR normal operations use cases, has taken place and the execution of the cyberattack is now taking place, with power measurement data collection and command data collection. Case 1 or 2 of the DER attack sequence is being run and data collected. Small batches (time windows) of the power measurement data and DER/DR command/price data are input successively and continuously, for comparison with the trained LSTM models.

The LSTM should detect unusual patterns of relationship and change of relationship between multiple power measurement timeserieses. Invariants in relationship of current/voltage/power/frequency measurement features will be violated as one measurement value is tampered with, and the LSTM will detect the evolution of these invariants as anomalous. This error signal in the LSTM could be the basis for a warning/alarm message to operators. When tested on attack case 3, the LSTM detects an unfamiliar (anomalous) association between low transmission-grid frequency and DER commands/prices designed to increase power demand further in the grid, and also detects the unusual increased power demand by meter measurements.

4. 2. 4. Testing Trained Detection System on DERKILL-Contrasting Normal Operations Use Cases

To verify lack of false positive detection by the LSTM, the normal operation use cases (4.2.1) are run again, with minor random power measurement differences simulated. Short time-windows (batches) of the measurement feature and command signal data are sent to the LSTM for comparison with its trained model. No anomaly detection is expected, as the system behaviour is consistent with trained/learned behaviour.

5. Conclusions

The smart digital substation will bring increased efficiencies, higher situational awareness, quicker response times and have a positive impact on operator safety and human error avoidance. With the increased connectivity capabilities come clear vulnerabilities from a cybersecurity perspective that need to be addressed. Cyber intruders and or malware sophistication increases will continue to have high impact on the changing distributed electrical network. A preemptive and proactive Early Warning Substation Anomaly Detection System will become a requirement for the future. This research advances the development of substation/distribution attack detection, by creating a substation and distribution-network HIL test environment, emulating real operational protection-and-control cyberattack scenarios, proposing anomaly detection algorithm application, and outlining methodology for testing anomaly detection algorithms on a digital substation's operational data.

BIBLIOGRAPHY

[1] Y. Zhang, L. Wang, Y. Xiang, and C. Ten, "Power System Reliability Evaluation with SCADA Cybersecurity Considerations" (IEEE Transactions on Smart Grid, Volume: 6, Issue: 4, July 2015, pages 1713-1721).

[2] Y. Xiang, Z. Ding, Y. Zhang, and L. Wang, "Power System Reliability Evaluation Considering Load Redistribution Attacks" (IEEE Transactions on Smart Grid, Volume: 8, Issue: 2, March 2017, pages 889-901).

[3] Y. Zhang, L. Wang, and Y. Xiang, "Power System Reliability Analysis with Intrusion Tolerance in SCADA Systems" (IEEE Transactions on Smart Grid, Volume: 7, Issue: 2, March 2016, pages 669-683).

[4] Y. Zhang, L. Wang, Y. Xiang, and C. Ten, "Inclusion of SCADA Cyber Vulnerability in Power System Reliability Assessment Considering Optimal Resources Allocation" (IEEE Transactions on Power Systems, Volume: 31, Issue: 6, November 2016, pages 4379-4394).

[5] A. A. Al Jahil, and D. Giarratano, "Improvement of cyber-security measures in National Grid SA substation process control" (Saudi Arabia Smart Grid (SASG), December 2016).

[6] C. Jiwen, and L. Shanmei, "Cyber security vulnerability assessment for Smart substations" (IEEE PES Asia-Pacific Power and Energy Engineering Conference (APPEEC), December 2016, pages 1368-1373).

[7] Y. Chen, J. Hong, and C. Liu, "Modeling of Intrusion and Defense for Assessment of Cyber Security at Power Substations" (IEEE Transactions on Smart Grid, vol. 9, no. 4, September 2018, pages 2541-2552).

[8] J. Hong, C. Liu, and M. Govindarasu, "Integrated Anomaly Detection for cyber security of the substations" (IEEE PES General Meeting, Conference & Exposition, National Harbor, October 2014).

[9] National SCADA Testbed, [Online]: https://energy.gov/oe/technology-development/energy-delivery-systems-cybersecurity/national-scada-test-bed

[10] B. Rowe, K. Ladd, C. Scheper, S. Cornelia, K. Daniels, "Cyber Security Test Bed: Summary and Evaluation Results" (Final Report, RTI Project Number 0212782.000.001, October 2012).

[11] R. Candell, K. A. Stouffer, D. Anand, "A Cybersecurity Testbed for Industrial Control Systems" (Process Control and Safety Symposium, Houston, Texas, October 2014).

[12] R. Candell, T. Zimmerman, K. Stouffer, "An Industrial Control System Cybersecurity Performance Testbed" (NISTIR 8089, November 2015.
[Online]: http://dx.doi.org/10.6028/NIST.IR.8089)

[13] Autonomous Security Testbed, DAI Laboratory:
[Online]: http://www.dai-labor.de/en/testbeds/adaptive_cybersecurity_testbed/

[14] The DETER Project. [Online]: https://deter-project.org/

[15] Y. Yang ; H. T. Jiang, K. McLaughlin, L. Gao, Y. B. Yuan, W. Huang, S. Sezer, "Cybersecurity test-bed for IEC 61850 based smart substations" (IEEE Power and Energy Society General Meeting, Denver, USA, October 2015).

[16] J. Hong, Y. Chen, C. Liu, and M. Govindarasu, "Cyber-Physical Security Testbed for Substations in a Power Grid" (Chapter: Cyber Physical Systems Approach to Smart Electric Power Grid, Part of the series Power Systems, pp 261-301, 2015).

[17] National Institute of Standards and Technology, Cyber Security Working Group, "Guidelines for Smart Grid Cyber Security" (National Institute of Standards and Technology Interagency Report (NISTIR) 7628, August 2010).

[18] Electric Power System Research Institute, "Integrating Electricity Subsector Failure Scenarios into a Risk Assessment Methodology" (EPRI, Palo Alto, CA: 2013. 3002001181).

[19] J. Perks, J. Hyde, A. Falconer, "Study on Risk Governance of European Critical Infrastructures in the ICT and Energy Sector" (Final Report to European Commission, September 2009).

[20] Technical Working Group1, "Electric Sector Failure Scenarios and Impact Analyses" (National Electric Sector Cybersecurity Organization Resource (NESCOR) Version 1.0, September 2013).