Detecting data manipulation attacks on the substation interlocking function using direct power feedback

Eniye Tebekaemi, Edward Colbert, Duminda Wijesekera

▶ **To cite this version:**

Eniye Tebekaemi, Edward Colbert, Duminda Wijesekera. Detecting data manipulation attacks on the substation interlocking function using direct power feedback. 11th International Conference on Critical Infrastructure Protection (ICCIP), Mar 2017, Arlington, VA, United States. pp.45-62, 10.1007/978-3-319-70395-4_3 . hal-01819136

HAL Id: hal-01819136
https://inria.hal.science/hal-01819136

Submitted on 20 Jun 2018

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Distributed under a Creative Commons Attribution 4.0 International License

Chapter 3

DETECTING DATA MANIPULATION ATTACKS ON THE SUBSTATION INTERLOCKING FUNCTION USING DIRECT POWER FEEDBACK

Eniye Tebekaemi, Edward Colbert and Duminda Wijesekera

Abstract Any form of deliberate physical or cyber activity that attempts to undermine the control mechanisms that maintain the key goals of reliability, efficiency and safety of a physical system can be considered to be an attack on the system. Indeed, an attack can be as subtle as a configuration change that prevents the optimal operation of a power system.

This chapter describes an approach that enhances the security of the interlocking function in a power distribution substation by using the power flow behavior of the physical system during switching events as direct power feedback. The approach detects potential over-the-network data modification attacks on the interlocking function using out-of-bounds sensor measurements. The direct power feedback adds an extra layer of security and redundancy to existing power substation interlocking function protection mechanisms.

Keywords: Smart grid, substation, interlocking function, attack detection

1. Introduction

When smart grids become operational, power substations will be expected to support bidirectional power flows between distributed energy sources, storage facilities and power consumers. Substations use switchgear to maintain the appropriate flow of power, protect equipment and provide redundancy during power source and equipment failures. Interlocking functions in substations prevent improper operations of switchgear by maintaining information about their operational states and permissible state transitions from their current states to the next states. This ensures correct switching sequences and prevents switch operations that could violate the integrity of the substations. Due to the significant role played by the interlocking function in the safe and reliable

operation of power systems, any attack that compromises the state information and state transition integrity of an interlocking function can have disastrous consequences.

The interlocking function implemented in intelligent electronic devices (IEDs) in an IEC 61850 based power substation relies exclusively on Generic Object Oriented Substation Event (GOOSE) status messages between switchgear controllers in order to maintain the state information of all the switchgear in the substation, This reliance on GOOSE status messages is potentially a single point of failure for the interlocking function. Moreover, it fails to provide the substation with the required resilience to cyber-physical attacks.

This chapter examines the unique physical system behavior characteristics in response to switchgear events and extracts useful consequent system behavior attributes in order to specify a method that uniquely identifies switchgear events and to provide a cyber-physical security solution that integrates these observations into traditional cyber security controls. The physical system behavior is an important, but often neglected, part of cyber-physical security research. Indeed, understanding and considering the physical behavior of a power substation plays a key role in designing a resilient security solution.

2. Related Work

Peripheral information from sensor measurements is often used to monitor the state and behavior of cyber-physical systems. However, little work has been done on integrating this information in intrusion detection systems. Colbert et al. [2] have developed a process-oriented method for intrusion detection in industrial control systems. Data from critical elements in a physical system are collected by sensors and used to estimate the system state. Control operations sent over the network are intercepted by the intrusion detection system and evaluated using the estimated system state and system guard conditions. An alert is raised when a control operation violates the guard conditions based on the estimated system state.

Koustandria et al. [5] have developed a hybrid control network intrusion detection system. Expected communications patterns and the limitations of a physical system are leveraged to detect a wide range of attacks. The system, which is designed for protective digital relays in power transmission grids, detects attacks using packet sequences, time gaps between packets and the measured current in relays. Every packet and communications flow are evaluated against the expected packet sequence, maximum allowed time delay and measured current in the relay. An attack is detected when any of these constraints are violated or a circuit breaker activation request is received when the measured current is less than the cut-off current.

Mitchell et al. [7] have created a behavioral-rule-based intrusion detection system for unmanned air vehicles. A set of system (physical) behavior rules and system state transformation rules are employed to identify attacks. The detection system comprises monitor nodes (sensors and actuators) that monitor other nodes (sensors and actuators) or a neighboring system (unmanned air

vehicle) that monitors another trusted system (unmanned air vehicle). The monitoring system evaluates the behavior of the monitored system against a set of predefined system behavior and transition rules, and identifies a violation as a potential attack.

Sawada et al. [12] and Harshe et al. [3] have proposed cyber-physical system security solutions that use local (backup) controllers, which kick in when remote (central) controllers are compromised or are unavailable. The central controllers usually optimize the networked control system to yield high performance while the local controller guarantees the minimum performance requirements of the logical subsystem. The security solutions continuously evaluate control signals received from the central controller against the physical system and switches to the backup controller when a violation is observed.

A security solution for a cyber-physical system must be designed to comprehend and respond to the unique process behavior of the system. The solutions discussed above do not directly address data manipulation attacks on a power substation interlocking process, but they do provide a useful starting point for reasoning about the security of cyber-physical systems.

3. Substation Interlocking

Switchgear implement protection and control functions that are triggered in response to system guard conditions, automation and optimization functions or by human intervention. Substations are equipped with switchgear devices that are independently controlled and perform functions such as fault isolation, sectionalization, and over-current and over-voltage protection. The types of switchgear used in substations include isolator switches, contactor switches, earthing switches and circuit breakers.

3.1 Substation Switching

The IEC 61850 Standard recommends that switchgear be triggered by intelligent electronic devices that implement circuit breaker (XCBR) or circuit switch (XSWI) logical nodes at the process level. In turn, the circuit breaker and circuit switch logical nodes are controlled by intelligent electronic devices that implement protection and control functions such as time over-voltage protection (PTOV), instantaneous over-current protection (PIOC) and switch controller (CSWI). The first letter of a logical node name is used as a group identifier for logical nodes with similar functions. For example, the first "I" in "IHMI" (human-machine interface) identifies IHMI as belonging to interface group I.

Figure 1 shows a typical example of the operation sequence of an IEC 61850 substation interlocking function discussed in [8]. Human experts create interlocking rules and feed them to the system via the human-machine interface (IHMI). In Message 1, the interlocking function (CILO) imports the rules, validates the state of all the switchgear devices (via Messages 3, 4 and 8), and waits for a request from the switch controller (CSWI). In Message 2, the human controller issues a switch OPEN command to the switch controller and, in turn,

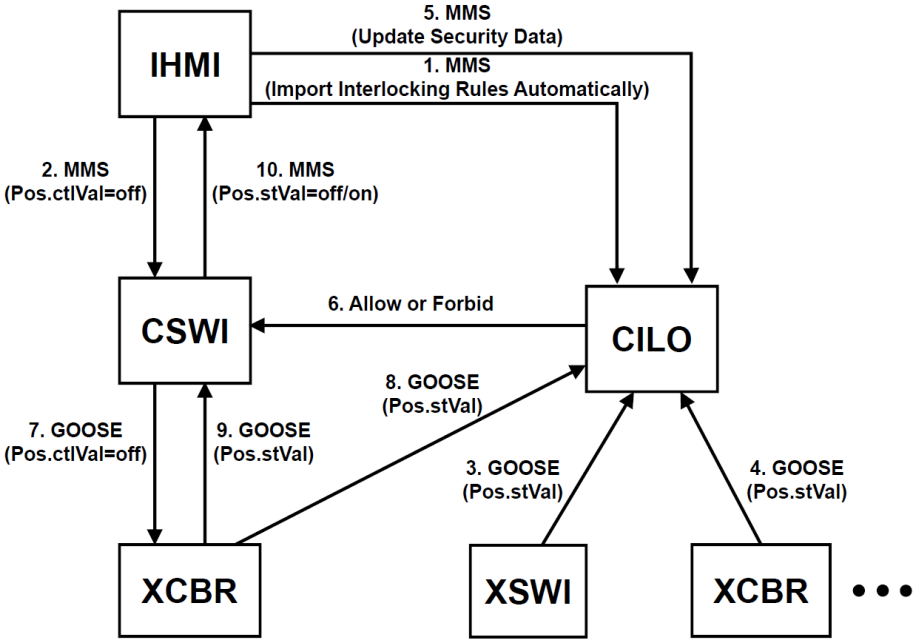

Figure 1. IEC 61850 CILO-controlled switchgear operation [8].

the switch controller requests the interlocking function to check if the execution of the command violates an interlocking rule. In Message 6, the interlocking function responds with an allow if no rule is violated and a forbid otherwise. In Message 7, the switch controller proceeds with a switch OPEN command if an allow response was received by instructing the circuit breaker/circuit switch (XCBR/XSWI) to OPEN. In Message 9, the circuit breaker/circuit switch notifies the switch controller about the failure or success of the operation and, in turn, the switch controller notifies the human-machine interface of success or failure. Finally, in Message 8, the circuit breaker notifies the interlocking function of the state change if any. As described in [8], GOOSE update messages are protected with a keyed-hash message authentication code (HMAC). From time to time, the circuit breaker and circuit switch are expected to send status messages to the interlocking function to ensure that the state information maintained by the interlocking function correctly reflects that of the physical switchgear devices.

3.2 Interlocking Function Operation

The IEC 61850 Standard refers to substation automation functions as logical nodes. The interlocking function logical nodes (LNs), which are implemented at the station level or bay level, contain the rules that govern all valid switchgear

Table 1. Valid configurations of the switchgear devices in the testbed.

Configuration	CS1	CS2	CB	IS	ES
1	0	0	0	0	0
2	0	1	0	0	0
3	0	1	1	0	0
4	0	1	1	1	0
5	0	0	0	0	1
6	0	0	0	1	1
7	0	0	1	0	1
8	0	0	1	1	1
9	1	0	0	0	0
10	1	0	1	0	0
11	1	0	1	1	0

configurations, the current states of switchgear devices and the transition sequences. Based on the interlocking rules imported from the human-machine interface, the interlocking function generates the valid configuration table and transition sequences.

In the testbed used in this research, a single bay substation was implemented using two power sources. The testbed consisted of five switchgear devices, one earthing switch (ES), two contactor switches (CS1 and CS2), one isolator switch (IS) and one circuit breaker (CB). The interlocking function had the eleven valid switchgear configurations shown in Table 1. A zero indicates that a switchgear is in the OPEN position and a one indicates that the switchgear is the CLOSE position.

Algorithm 1 : Validate switch controller request.

```
1:  procedure validateCSWIRequest(request)
2:      temp = FALSE
3:      if request ≠ NULL then
4:          n = getNoSwitch(request)
5:          curConfig = getCurConfig()
6:          newConfig = getNewConfig(request)
7:          temp = isValid(newConfig, validConfigTable)
8:          if n == 1 then
9:              RETURN temp
10:         end if
11:         CALL transSeqFn(request,curConfig)
12:     end if
13:     RETURN temp
14: end procedure
```

The behavior of the interlocking function is described using the validate switch controller request algorithm (Algorithm 1). The algorithm is executed

whenever a new request is received. In Line 4 of the algorithm, the interlocking function checks for the number of switchgear devices affected by the request, Line 5 obtains the current switchgear configuration and Line 6 computes the new configuration based on the change request. In Line 7, the interlocking function checks that the request does not violate any interlocking rules and returns either TRUE or FALSE. If the number of switchgear devices that would be affected by the request is no more than one and the new configuration is valid, then the interlocking function returns TRUE to the switch controller, implying that the change is allowed. If multiple switchgear devices are affected by the request, then the algorithm proceeds to Line 11 and invokes the transition sequence function. The transition sequence specifies the order in which the switchgear affected by the change request should be implemented. An execution interval of 1 ms to 10 ms is typically allowed for concurrent switchgear operations.

3.3 Substation Communication Protocols

IEC 61850 specifies the use of the generic object oriented substation event (GOOSE) and sampled value (SV) protocols for power substation communications. GOOSE and SV are fast data transfer protocols that execute in the data link layer and are used in the substation local-area network to control, report events and transmit measured values.

GOOSE Protocol. The GOOSE protocol specified in the IEC 61850-8-1 Standard is a multicast/broadcast protocol that uses a publisher-subscriber communications model for sending and receiving data between intelligent electronic devices. Bay-level intelligent electronic devices use the GOOSE protocol to report switch state changes (ON and OFF). The GOOSE protocol uses the status number (StNum) and sequence number (SqNum) to distinguish between state change events and re-transmissions. StNum starts from one and is incremented for every state change (OPEN or CLOSE) event. SqNum, which starts from zero, indicates re-transmissions of a previous notification. For example, the first status change in the switchgear has StNum = 1 and SqNum = 0. The switchgear keeps broadcasting its state information at time intervals less than 60 s until a new state is recorded. For each re-transmission, StNum remains the same but SqNum is incremented.

SV Protocol. The SV communications protocol defined in IEC 61850-9-2 is a multicast/broadcast protocol that uses a publisher-subscriber communications model to receive data streams of sampled values from sensors in a substation. The SV protocol is primarily used to send voltage and current measurements obtained from current and voltage sensors to all the subscribing intelligent electronic devices. The protocol uses the sample count (SmpCnt) field in the SV protocol data unit to indicate every new sample and the sample rate (SmpRate) to specify the number of samples per second. SmpCnt is incremented for every new sample and there are no re-transmissions.

4. Attack Description

The interlocking function translates switchgear configuration rules into a valid configuration table as shown in Figure 1. A valid configuration is a vector that indicates the permitted state of all the switchgear devices at a given instant. The valid configuration table is the collection of all possible valid configurations.

Let s be the number of switchgear devices in a substation and let $C \in \{0,1\}^s$ correspond to all possible switchgear configurations. Let $\vec{C'}$ be a valid configuration and n be the total number of valid configurations. Then, the valid configuration table T is the set:

$$T = \{\vec{C'_1}, \vec{C'_2}, \cdots, \vec{C'_n}\} \tag{1}$$

A state change request τ_{i+1} is allowed to change the interlocking function configuration state from $\vec{C'_i}$ to $\vec{C'_j}$ if and only if:

$$F : \vec{C'_i} \times \tau_{i+1} \Rightarrow \vec{C'_j} \in T \tag{2}$$

where F is the transition mapping function and $1 \leq i, j \leq n, i \neq j$. Whenever a change request is successfully executed by a circuit breaker or circuit switch, a status update message is sent to the interlocking function, which updates its current configuration state from $\vec{C'_i}$ to $\vec{C'_j}$.

Process level communications are time-critical because IEC 61850 requires a delay of no more than 4 ms in the transmission of GOOSE and SV messages. This requirement hinders the implementation of an encryption-based security solution. IEC 61850 does not recommend the encryption of GOOSE and SV messages and mandates that encryption-based message integrity checks may be used for GOOSE only if they meet the 4 ms time requirement. Intelligent electronic devices in the process local-area network depend on the timestamps, StNum and SqNum for GOOSE messages, and SmpCnt for CV messages to detect data manipulations. Tebekaemi and Wijesekera [13] have demonstrated a successful GOOSE attack when the attacker has physical access to the process local-area network. Attacks on SV messages are more difficult to detect when the SmpRate has a high value because it is harder to predict the next SmpCnt value.

- **Scenario 1: Dropped Update Message:** This scenario assumes that the attacker has access to the process local-area network at the substation and can block GOOSE update messages to the interlocking function. When a status change request is received by the switch controller, it queries the interlocking function to validate the request. The interlocking function validates the request against the current system state $\vec{C'_i}$ and instructs the switch controller to execute the request. The switch controller executes the request and broadcasts its new status, which is blocked by the attack. Since no update message is received by the interlocking function, it still believes that the system is in state $\vec{C'_i}$ instead of

the new state $\vec{C}'_j$. The current state of the interlocking function no longer reflects the actual state of the physical system. Although the interlocking function and physical system may still have valid configurations, any new change request results in F using the wrong input $\vec{C}'_i$ instead of $\vec{C}'_j$.

- **Scenario 2: Corrupt Update Message:** This scenario assumes that the attacker has access to the process local-area network and can modify GOOSE update messages, inject new GOOSE packets or arbitrarily send GOOSE update messages. The attacker may be able to deceive the interlocking function to believing that an update has occurred and that its current state should be updated, causing the interlocking function to update its current state to $\vec{C}'_j$ while the system remains in $\vec{C}'_i$.

Scenarios 1 and 2 poison the configuration state of the interlocking function. If the malicious update is a valid configuration state, then no flag is raised and the attack goes unnoticed by the intelligent electronic device. The result could be disastrous if an attacker can successfully place the interlocking function in an invalid state. For example, according to Table 1, CS1 and CS2 cannot be in the CLOSE position at the same time. Assuming that the bay is disconnected autonomously for maintenance purposes, both CS1 and CS2 must be OPEN before ES can be in the CLOSE position. The interlocking function configuration table is poisoned to show that both CS1 and CS2 are OPEN and, thus, the interlocking function proceeds to validate an ES CLOSE request when either CS1 or CS2 is in the CLOSE position. Executing the request increases the current astronomically because the voltage is suddenly reduced to approximately zero – this could damage equipment and cause a fatal accident. Row 14 in Table 2 shows that such a request increases the current to 850 times its nominal value.

5. Proposed Solution

Electrical equipment exhibits unique physical attribute properties when triggered by ON/OFF commands; the properties manifest themselves as transients, steady state changes, and amplitude and frequency changes in the voltage and current waveforms. Observations of disturbances in the voltage and current waveforms can provide direct power feedback pertaining to physical- and cyber-controlled events. It is possible to monitor and detect ON/OFF events involving electrical equipment and trace the events to the originating equipment using their transient states, steady states or frequency changes of the measured voltages and currents [4, 10]. Similar techniques have been used to detect and locate faults in power systems [1, 9, 11].

Current and voltage sensors are used in substations to provide information about the voltage and current of the supplied electric power, which is used to drive substation functions such as voltage/voltage-ampere reactive (VAR) control, frequency control, power quality control, and over-voltage and over-current protection. Current and voltage sensors give information about the portions

Table 2. Voltage and current measurements during switchgear ON/OFF operations.

Device	Position	Type	Sensor 1	Sensor 2	Sensor 3
CS	ON	V	1.001	1.001	0.465
		A	0.528	0.525	1.229
	OFF	V	0.195	0.195	0.09
		A	0.103	0.102	0.24
CB	ON	V	1.001	1.001	0.465
		A	0.529	0.525	1.229
	OFF	V	1	0.102	0.047
		A	0.107	0.053	0.125
IS	ON	V	1.001	1.001	0.465
		A	0.528	0.525	1.229
	OFF	V	1	1	0.009
		A	0.066	0.012	0.023
ES	ON	V	0	0	0
		A	850	0	0
	OFF	V	1.001	1.001	0.465
		A	0.528	0.525	1.229

of the system that are energized. Intelligent electronic devices use this information to determine switchgear positions (OPEN or CLOSE) at any instant. Switchgear events are also observable via the electrical waveforms they generate; switching a device ON or OFF generates transients that appear as spikes in its waveform and steady state amplitude changes as shown in Figure 2 (note that p.u. = measured value/nominal value). Monitoring switchgear events provides useful information about the times when events occur and the originating switchgear devices, which help detect illegal switchgear manipulations.

5.1 Switchgear Event Detection

Event detection algorithms compare the measured value of a signal to a reference value; when a significant difference is detected, an event of interest is declared to have occurred. In order to increase the accuracy of event detection in a power signal, a change event is computed based on the properties of the signal over a time frame called the event detection window. This helps reduce the effects of noise in the signal and the false event detection ratio.

In the initial simulated testbed, the electrical noise was normally distributed, which may not be the case in an actual substation. The detection algorithm employed was a simple mean change detector that compared the detection window w_i against the pre-event window w_{i-1}. If $n = |w|$, $w_i = x_1, x_2, \cdots, x_n$ and $w_{i-1} = y_1, y_2, \cdots, y_n$, then:

$$|\frac{\sum_{i=1}^{n} x_i - \sum_{i=1}^{n} y_i}{n}| > \xi \tag{3}$$

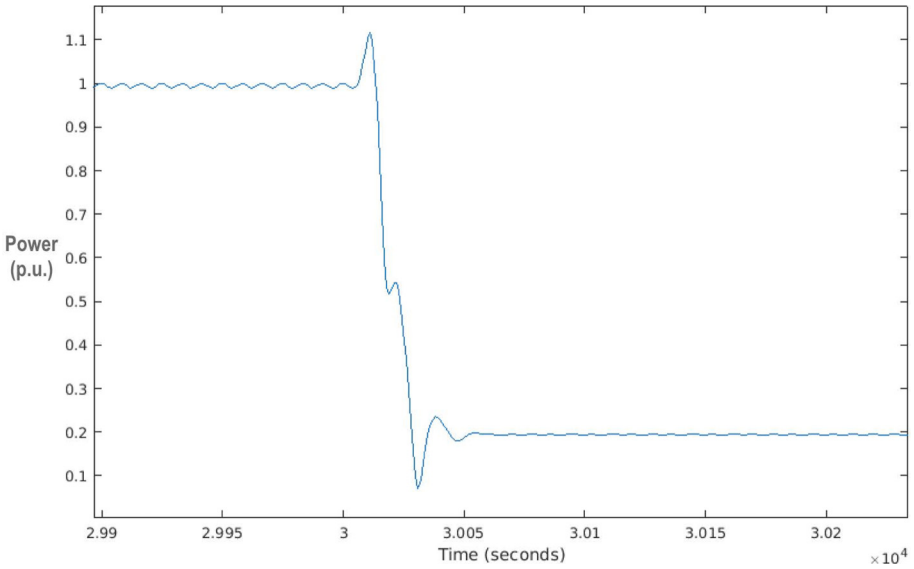

Figure 2. Transient and steady state voltage during switch CLOSE operations.

indicates the occurrence of an event, where μ is the mean value, x_i and y_i are sample points of the DC component of the signal and ξ is a predetermined threshold value.

Voltage and current signals usually contain noise caused by imperfections in electrical equipment and devices, thermal conditions, electrostatic interference, electromagnetic interference, radio frequency interference and cross-talk. Noise in measured signals can cause detection systems to increase the number of false positives or completely misdetect events. To address the effects of noise, the sensitivity of the detection system (threshold) must be set to achieve a high detection rate (e.g., 100%) given the noise level and the lowest possible false positive rate within an acceptable response time. A more sensitive threshold enables the system to detect minor events and respond quickly, but with less accuracy; in contrast, a less sensitive threshold causes the system to miss minor events and respond slowly, but with better accuracy.

This research assumes that the measured voltage and current signals contain noise, and employs the change detection method described in [4]. Specifically, the noise e_i is assumed to be a continuous white Gaussian process so that $x'_i = x_i + e_i$ and $y'_i = y_i + e_i$. The detection threshold $\xi = \chi^2_{\alpha,k-1}$ is a chi-square goodness of fit test with a confidence interval of $(100-\alpha)\%$ and detection sensitivity factor k. An event is detected when:

$$\sum_{i=1}^{n} \frac{(x'_i - y'_i)^2}{y'_i} > \xi \tag{4}$$

Table 3. Switchgear event truth table.

Close	Open	Type	Sensor 1	Sensor 2	Sensor 3
	CS	V	0	0	0
		A	0	0	0
CS	CB	V	1	0	0
		A	0	0	0
CB	IS	V	1	1	0
		A	0	0	0
IS		V	1	1	1
		A	1	1	1
ES		V	0	0	0
		A	1	0	0

The detection threshold can be pre-computed and fixed if the noise level is expected to be the same; alternatively, it can be computed dynamically during system operation if the noise level is expected to change.

5.2 Switchgear State Identification

The switchgear state detection process involves the determination of sections of the bay that are energized based on the sensor measurements. The sensor measurements are mapped using the switchgear state truth table (Table 3) to identify which switchgear devices are in the CLOSE and OPEN positions. The switchgear truth table is preconfigured and contains the combination of high and low voltage and current values measured by all the sensors in the testbed that map to the ON or OFF states of switchgear in the substation. The switchgear state identification serves two purposes: (i) to attribute a detected event to the originating switchgear; and (ii) to validate the state of the physical system during the interlocking function request validation operation. Table 2 shows the measured values of each switch when it is the CLOSE and OPEN positions. The information in this table is used to generate the switchgear event truth table shown in Table 3. The event truth table is used to predict which switchgear devices are in the CLOSE and OPEN positions based on the sensor measurements. In the event truth table, a zero indicates that the measured value from a given sensor is low while a one indicates that the value is high.

5.3 Interlocking Function Security Controller

Switchgear status update information is sent from the circuit breaker or circuit switch to the interlocking function in the form of GOOSE packets over the process local-area network. The IEC 61850 Standard also allows sampled voltage and current measurements to be sent from the merging units to intelligent electronic devices via the process local-area network in the form of SV packets. The interlocking function security controller uses the SV messages to detect

Algorithm 2 : Check for modified GOOSE updates.

```
1: procedure isMessageModified(gooseUpdate)
2:     if stNumChange(updateMsg) then
3:         powFeedback == getPowFeedback()
4:         if updateMsg.stVal == powFeedback.val then
5:             if updateMsg.time ≈ powFeedback.time then
6:                 return FALSE
7:             end if
8:         end if
9:         return TRUE
10:    end if
11: end procedure
```

changes in the waveforms and obtains the direct power feedback for switchgear events. The security controller uses GOOSE and SV messages, which function as two independent sources, to validate the correct states of switchgear devices.

Algorithm 2 describes the high-level behavior of the proposed interlocking function security controller. The algorithm is invoked whenever a GOOSE update message (updateMessage) is received from a switchgear (circuit breaker or circuit switch). In Line 2, the security controller checks if the update message is a retransmission or a new event notification. If the update message is a new event notification, then the security controller obtains the power feedback information from the SV messages in Line 2. In Line 3, the most recent measurements from the sensors are obtained and are used to estimate the current states of the switchgear devices. In Lines 4 and 5, the GOOSE update message and the power feedback information are compared to check if the reported event is consistent and is within the same time frame. The GOOSE update and SV feedback messages arrive at the interlocking function at slightly different times, so the time values are approximate and a check is performed to see if both messages arrive within an acceptable time frame. An inconsistency in the reported event or time frame implies that there is a high probability that the GOOSE update message has been modified.

Algorithm 3, which runs continuously as a background process, checks for changes in voltage and current waveforms indicated by the SV messages. In Line 3, if a significant change is detected, the security controller proceeds to obtain the change information in Line 4. The reported change is checked in Line 5 to ascertain if the event is the result of a state change and returns TRUE if the event is caused by a switchgear. If the event is the result of a switchgear operation and no GOOSE update message is received, then there is a high probability that the update message has been blocked.

6. Implementation and Results

Power substations have bays that connect feeders to power sources. Each bay has switchgear that implement the bay-level protection and control func-

Algorithm 3 : Check for missing GOOSE updates.

```
1: procedure isUpdateMissing
2:     while TRUE do
3:         if eventDetected() then
4:             powFeedback == getPowFeedback()
5:             if stChange(powFeedback) == TRUE then
6:                 return TRUE
7:             end if
8:         end if
9:     end while
10: end procedure
```

tions. The IEC 61850 Standard does not have a preference regarding where the interlocking function should be implemented (i.e., station level or bay level); instead, it leaves the decision to substation designers. At the station level, the interlocking function has to maintain the state and configuration information of switchgear in all the bays in the substation. Thus, for a substation with n bays and x switchgear devices per bay, the interlocking function maintains $n \times x$ switchgear states with 2^{nx} possible switchgear configurations. The configuration table grows rapidly as n and x increase, and can easily overwhelm the intelligent electronic device.

The proposed solution relies on SV messages received by the interlocking function from merging units. SV messages transmitted as multicast packets provide a continuous stream of currents and voltages sampled at high rates. In the case of a substation with multiple bays, the interlocking function has to process the continuous streams of multicast packets from all the merging units distributed across the bays in the substation. This can cause congestion in the station local-area network and may also lead to the failure of the network interface controller of the intelligent electronic device with the interlocking function. For these reasons, it is recommended that the interlocking function be implemented at the bay level and, in fact, the proposed solution is designed for a bay-level interlocking function.

6.1 Implementation

Tebekaemi and Wijesekera [13] have designed and implemented a substation simulation testbed. Certain modifications were made to this testbed to support the substation interlocking function discussed in this chapter. Figure 3 shows a schematic diagram of the modified testbed with three virtual machines (VMs) running on a VMware ESXi server and a MacBook Pro computer.

Power System (VM1). The substation was simulated on the Intel core i7 MacBook Pro computer with a 2.5 GHz processor, 16 GB RAM and 512 GB SSD. The substation was a single-bay step-down station created with Matlab/Simulink that incorporated two contactor switches (CS1 and CS2), a groun-

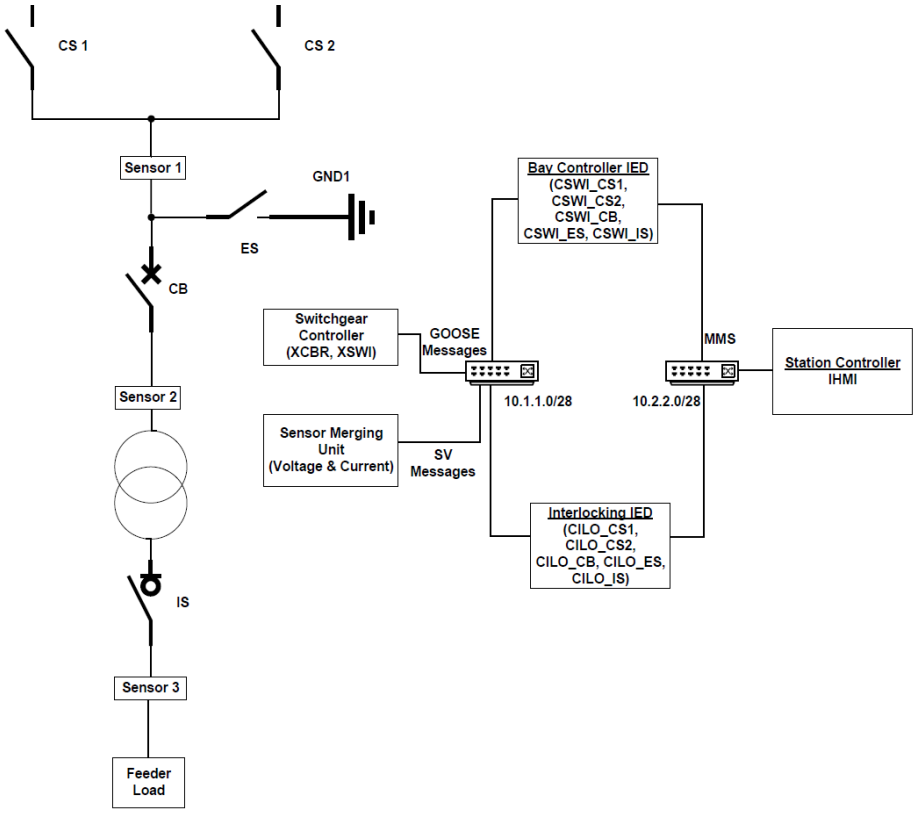

Figure 3. Implementation schematics of the substation testbed.

ding/earthing switch (ES), an isolator switch (IS) and a circuit breaker (CB). Voltage and current measurements were obtained from three sensors installed at different locations in the bay.

Virtual Intelligent Electronic Devices. The following virtual intelligent electronic devices were incorporated in the modified testbed:

- **Merging Unit and Switchgear Controller (VM1):** The merging unit and switchgear controller were implemented as standalone C/C++ applications based on the IEC 61850 Standard. These applications also ran on VM1 (Ubuntu 14.04.4LTS with two core processors, 2 GB RAM and 20 GB HDD). The merging unit and switchgear controller communicated with the simulated substation using UDP ports. The merging unit collected sampled measurements from all three sensors, timestamped them and broadcasted the values using the SV protocol. The switchgear

Algorithm 4 : Interlocking rules.

```
1: if CS2==CLOSE then DENY CS1 CLOSE
2: end if
3: if CS1==CLOSE then DENY CS2 CLOSE
4: end if
5: if ES==CLOSE then DENY CS1 CLOSE
6: end if
7: if ES==CLOSE then DENY CS2 CLOSE
8: end if
9: if CS1==CLOSE then DENY ES CLOSE
10: end if
11: if CS2==CLOSE then DENY ES CLOSE
12: end if
```

controller relayed the OPEN/CLOSE GOOSE commands from the bay controller to the appropriate switchgear devices.

- **Bay Controller IED (VM2):** The bay controller intelligent electronic device was implemented as a C/C++ application based on the IEC 61850 Standard that executed on VM2 (Ubuntu 14.04.4LTS with two core processors, 2 GB RAM and 20 GB HDD). The bay controller intelligent electronic device comprised five switch controller logical nodes (CSWI_CS1, CSWI_CS2, CSWI_ES, CSWI_CB and CSWI_IS), each corresponding to a switchgear device in the substation.

- **Interlocking IED (VM2):** The interlocking intelligent electronic device comprised five interlocking function logical nodes (CILO_CS1, CILO_CS2, CILO_ES, CILO_CB and CILO_IS), each of which maintained the state information of the corresponding switchgear device in the testbed. The interlocking intelligent electronic device executed the data manipulation detection algorithms and maintained the switchgear configurations and transition rules. The interlocking rules specified in Algorithm 4 were implemented in the interlocking intelligent electronic device based on Table 1.

Attacks. The following attacks were executed on the testbed:

- **Blocked GOOSE Update:** This attack requires access to the process local-area network and blocks GOOSE update messages from reaching their destinations. The attack was simulated by configuring the controllers not to send update messages after a state change operation.

- **Modified GOOSE Update:** This attack requires access to the process local-area network. GOOSE update messages are broadcast in plaintext to all the subscribing intelligent electronic devices. The TCPDump tool was used to capture network traffic and replay it unmodified using the

Table 4. Performance of the interlocking function with and without security.

	No Security	**Security (No Noise)**	**Security (Noise)**
Replay	✓	✓	✓
Modified Replay	×	✓	✓
Missing Update	×	✓	✓
Time (ms)	1.351	1.446	57.955

TCPReplay tool. Modified network traffic was transmitted using the Scapy traffic manipulation tool.

6.2 Results

The simulation was first executed with the interlocking function security controller deactivated. The interlocking intelligent electronic device used the GOOSE StNum, SqNum and timestamp fields to detect replay attacks. However, if StNum, SqNum and timestamp were modified to mimic a new update message, it was possible to successfully modify the configuration state of the interlocking intelligent electronic device. In the case of missing and blocked update messages, the interlocking intelligent electronic device had no way of detecting the events and easily entered an inconsistent state. When the security controller was activated, the modified replay attacks and the missing update messages were detected. The security controller always validated the GOOSE update messages with the power feedback SV messages to ensure that the GOOSE update messages were valid. Also, by continuously listening to changes in the physical system, the security controller was able to detect configuration changes observed by the power feedback SV messages but not reported by the GOOSE update messages.

Table 4 summarizes the performance of the interlocking function with and without the security controller. The times (in ms) were measured from the instant the control operation was initiated by the switch controller to the instant the interlocking intelligent electronic device updated its configuration state.

7. Conclusions

Interlocking is a critical substation automation function that ensures the safety of human lives and power equipment, and the reliability and resilience of power systems. As a result, interlocking functions are high value targets for malicious entities. However, power systems have tight timing requirements that prevent the use of cryptographic techniques and tools to protect network traffic and data. This requires the design and implementation of other protection mechanisms for power systems.

This chapter has presented a novel method for detecting data manipulation attacks on interlocking functions in power distribution substations. The

method relies on knowledge about the behavior of the physical system and integrates it in conventional intrusion detection mechanisms. The method is applicable to other power system components and functions that involve automated switching functions, including distribution bus networks and ship power systems. The research also demonstrates that integrating knowledge about the physical behavior of a cyber-physical system in cyber security controls is vital to enhancing system reliability and resilience.

References

[1] A. Al-Mohammed and M. Abido, An adaptive fault location algorithm for power system networks based on synchrophasor measurements, *Electric Power Systems Research*, vol. 108, pp. 153–163, 2014.

[2] E. Colbert, D. Sullivan, S. Hutchinson, K. Renard and S. Smith, A process-oriented intrusion detection method for industrial control systems, *Proceedings of the Eleventh International Conference on Cyber Warfare and Security*, pp. 497–500, 2016.

[3] O. Harshe, N. Chiluvuri, C. Patterson and W. Baumann, Design and implementation of a security framework for industrial control systems, *Proceedings of the International Conference on Industrial Instrumentation and Control*, pp. 127–132, 2015.

[4] Y. Jin, E. Tebekaemi, M. Berges and L. Soibelman, Robust adaptive event detection in non-intrusive load monitoring for energy aware smart facilities, *Proceedings of the IEEE International Conference on Acoustics, Speech and Signal Processing*, pp. 4340–4343, 2011.

[5] G. Koutsandria, V. Muthukumar, M. Parvania, S. Peisert, C. McParland and A. Scaglione, A hybrid network IDS for protective digital relays in the power transmission grid, *Proceedings of the IEEE International Conference on Smart Grid Communications*, pp. 908–913, 2014.

[6] R. Liu, C. Vellaithurai, S. Biswas, T. Gamage and A. Srivastava, Analyzing the cyber-physical impact of cyber events on the power grid, *IEEE Transactions on Smart Grid*, vol. 6(5), pp. 2444–2453, 2015.

[7] R. Mitchell and I. Chen, Adaptive intrusion detection of malicious unmanned air vehicles using behavior rule specifications, *IEEE Transactions on Systems, Man and Cybernetics: Systems*, vol. 44(5), pp. 593–604, 2014.

[8] J. Pan, B. Duan, C. Qiu and G. Li, Research on interlocking CILO based on IEC 61499/62351, *Proceedings of the Asia-Pacific Power and Energy Engineering Conference*, 2012.

[9] P. Nayak, A. Pradhan and P. Bajpai, A fault detection technique for a series-compensated line during power swing, *IEEE Transactions on Power Delivery*, vol. 28(2), pp. 714–722, 2013.

[10] A. Rababaah and E. Tebekaemi, Electric load monitoring of residential buildings using goodness of fit and multi-layer perceptron neural networks, *Proceedings of the IEEE International Conference on Computer Science and Automation Engineering*, vol. 2, pp. 733–737, 2012.

[11] M. Riera-Guasp, J. Antonino-Daviu and G. Capolino, Advances in electrical machine, power electronics, and drive condition monitoring and fault detection: State of the art, *IEEE Transactions on Industrial Electronics*, vol. 62(3), pp. 1746–1759, 2015.

[12] K. Sawada, T. Sasaki, S. Shin and S. Hosokawa, A fallback control study of networked control systems for cybersecurity, *Proceedings of the Tenth Asian Control Conference*, 2015.

[13] E. Tebekaemi and D. Wijesekera, Designing an IEC 61850 based power distribution substation simulation/emulation testbed for cyber-physical security studies, *Proceedings of the First International Conference on Cyber-Technologies and Cyber-Systems*, pp. 41–49, 2016.