Chapter 1

DETECTING DATA MANIPULATION ATTACKS ON IEC61850-BASED SUBSTATION INTERLOCKING FUNCTION USING DIRECT POWER FEEDBACK

Eniye Tebekaemi, Edward Colbert and Duminda Wijesekera

Abstract Any form of deliberate activity (physical or cyber) that attempts to undermine control mechanisms that maintain the objectives of reliability, efficiency, and safety of a physical system can be considered an attack on the system. Such attacks can be as subtle as configuration changes that prevent the optimal operation of the power system through data modification. In this work, we introduce a system that enhances the security of the interlocking functions in power distribution substations by using the power flow behavior of the physical system during switching events as a direct power feedback. This solution detects potential over the network data modification attacks on the interlocking function using out of bounds sensor measurements as direct power feedback. This direct power feedback adds an extra layer of security and redundancy to any existing security mechanisms of power substation interlocking.

Keywords: Cyber-Physical Security, Smart Grid, Smart Power Systems, Intrusion Detection, Cyber Attacks, IEC-61850 standard.

1. Introduction

In the age of smart grids, power substations will be expected to support bidirectional power flows between distributed energy sources, storage facilities, and power consumers. Substations use switchgears to maintain the appropriate flow of power, protect equipment, and provide redundancy during power source or equipment failures. Interlocking functions in the substations prevent mal-operation of switchgears by keeping information about the operational state of the switchgear and permissible state transitions from the current state to the next state. Doing so ensures the correct sequences of switching and prevents any switch operation that can violate the integrity of a substation. Due to the significant role played by interlocking functions on the safe and reliable operation of power systems any attack that compromises state information and state transition integrity of the interlocking function can have disastrous consequences on a power system.

Interlocking functions implemented as IEDs in IEC61850-based power substations rely exclusively on the *Generic Object Oriented Substation Event (GOOSE)* status messages among switchgear controllers in order to maintain the state information of all switchgears in the substation as shown in Fig. 1. Relying solely on GOOSE status messages result in a single point of failure for the interlocking function and fails to provide the required resiliency for a substation under cyber-physical attack. In this paper, we explore the unique physical system behavior characteristics in response to switchgear events, extract useful consequent system behavioral attributes to develop a method that uniquely identifies switchgear events, and design 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; understanding the physical behavior of power substation systems plays a significant role in the design of any resilient security solution.

2. Related Work

Using extraneous peripheral information from sensor measurements in physical systems to observe the system behavior and state is common in cyber-physical systems. However, there has been little effort to integrate this information into intrusion detection systems for cyber-physical systems. An example solution is discussed by Colbert et al. [1] who developed a process-oriented method for intrusion detection for use on Industrial Control Systems (iPoid). In their system, data from critical elements in the physical system are collected by sensors and used to estimate the state of the system by an intrusion detection system (IDS). Control operations sent over the network are intercepted by the IDS and evaluated using the estimated system state and system guard conditions. Alerts are raised if the network controlled operation violates the guard conditions based on the estimated system state.

Koustandria et al. [2] proposed the hybrid control network intrusion detection system (HC-NIDS). By using expected communications patterns and physical limitations of the physical system they developed an intrusion detection system that leverages the physical part of the system and able to detect a wide range of attack scenarios. Their work was limited to protective digital relays for power transmission grids and focused primarily on attack detection using packet sequence, the time gap between packets, and the measured current value of relays. They evaluate each packet and communications flow against the expected packet sequence, the maximum allowed time delay, the current measurement of the relay, and detects an attack if 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. [3] created a behavioral rule-based unmanned air vehicles IDS (BRUIDS). BRUIDS is an adaptive intrusion detection mechanism, focusing on unmanned air vehicles using behavior rule specifications. They use a set of the systems physical behavioral rules and the system state transformation rules to identify attacks. Their system consists of monitor nodes (sensors and actuators) monitoring other nodes (sensors and actuators) or a neighbor system (UAV) monitoring another trusted system (UAV). The monitoring system evaluates the monitored systems behavior against a set of predefined behavioral and transition rules and identifies any violation as an attack.

Sawada et al. [4] and Harshe et al. [5] propose a solution to the cyber-physical security problem by using local (backup) controllers that kicks in when the remote (central) controller becomes compromised or unavailable. The central controllers usually optimize the networked control system (NCS) for high performance and the local controller guarantees minimum performance requirement for the logical subsystem. Their system continuously evaluates control signals received from the central controller against the physical system and switches to the backup controller if a violation is observed.

For cyber-physical systems, security solutions must be designed to understand the physical system's unique process behavior. The solutions discussed above do not directly address data manipulation attacks of the substation interlocking process, but they provide a useful starting point in reasoning about security for cyber-physical systems.

3. Substation Interlocking

Switchgears implement protection and control functions which 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, overcurrent, and overvoltage protection. Types of switchgear used in substations include; isolator Switches, contactor Switch, earthing switches, and circuit breakers.

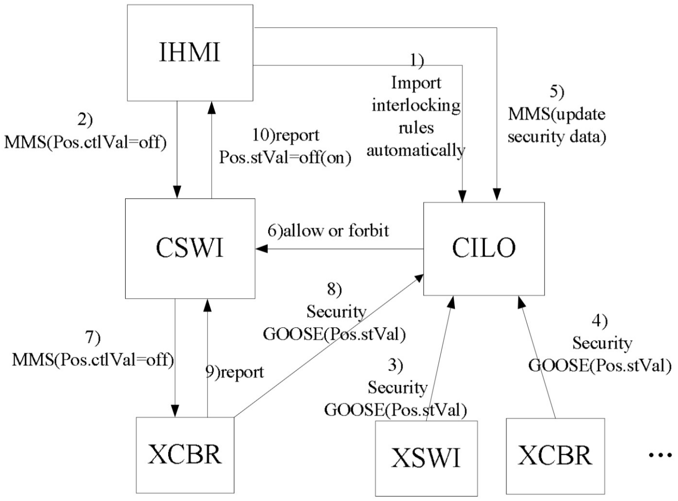

Figure 1. IEC-61850 CILO Controlled Switchgear Operation [6]

3.1 Substation Switching

The IEC61850 standard recommends switchgears be triggered by IEDs that implement the circuit breaker (XCBR) or circuit switch (XSWI) logical nodes at the process level. In turn, the XCBR and XSWI logical nodes are controlled by IEDs that implement protection and control functions like time over-voltage protection (PTOV), instantaneous overcurrent protection (PIOC) and switch controller (CSWI). The first letter of the logical node name is used as a group identifier for logical nodes with similar functions. For example, the ”I” in ”IHMI” (human machine interface) identifies IHMI as belonging to the interface group I.

A typical example of an operation sequences of the IEC61850 substation interlocking function discussed in Pan et al. [6] is shown in Figure 1.Human experts create interlocking rules and feed them to the system through the human machine interface (IHMI). Message 1, the interlocking function (CILO) imports the rules, validates the state of all the switchgear devices (Mesaages 3,4, and 8), and waits for a request from the switch controller (CSWI). Message 2, the human controller issues a switch OPEN command to the CSWI and in turn, the CSWI requests the CILO to verify if the execution of the command violates any interlocking rule. Message 6, the CILO responds with an allow if no rule is violated or a forbid otherwise. Message 7, The CSWI proceeds with a switch OPEN command if an allow response was received by instructing the XCBR/XSWI to OPEN. Message 9, the XCBR or XSWI notifies the CSWI about the failure or success of the operation and in turn, the CSWI notifies the IHMI of any success or failure. Finally, the XCBR notifies the CILO of the state change if any in message 8. In Pan et al. [6], the GOOSE update messages are protected with a keyed-hash message authentication code (HMAC). From time to time the XCBR and XSWI are expected to send status messages to the CILO to ensure the state information maintained by the CILO correctly reflects that of the physical switchgears.

3.2 Interlocking Function Operation

The IEC 61850 standard implements substation automation functions as logical nodes. The CILO logical nodes (LN) are implemented at the station level or bay level and contain the set of rules governing all valid switchgear configurations, the current state of each switchgear, and transition sequences. From the interlocking rules imported from the IHMI, the CILO generates the valid configurations table and transition sequences. In our testbed, we implement a single bay substation with two separate power sources. The testbed consists of five switchgears; one earthing switch (ES), two contactor switches (CS1 and CS2), one isolator switch (IS) and one circuit breaker (CB). We also implemented an interlocking logical node (CILO) containing eleven valid switchgear configurations as shown in table 1. The zeros (0) indicate that the switchgear is in an *OPEN* position and the ones (1) indicate that the switchgear is a *CLOSE* position.

Algorithm 1 Validate CSWI Request

```
 1: procedure VALIDATECSWIREQUEST(request)
 2:     temp = FALSE
 3:     if request $\neq$ 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:         CALL transSeqFn(request,curConfig)
11:     RETURN temp
```

The behavior of the CILO is described using the validate CSWI request algorithm (Algorthm 1). The validate CSWI request algorithm request is called whenever a new request is received. In line 4, the CILO

Table 1. Valid configurations table of switchgears in the testbed

Config.	**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

checks for the number of switchgears that would be affected by the request, obtains the current switchgear configuration in line 5, and the new configuration based on the change request in line 6. In line 7, the CILO checks to ensure that the request does not violate any interlocking rule and returns a true or false. If the number of switchgear that would be affected by the request is no more than one and the new configuration is valid, the CILO returns a true to the CSWI meaning the change is allowed. If more than one switchgear is affected by request, the algorithm proceeds to line 10 calling transition sequence function. The transition sequence specifies the order in which the switchgear affected by the change request should be implemented. Usually, an execution interval of between $1ms$ to $10ms$ delay is allowed for concurrent switchgear operations.

3.3 Substation Communication Protocols

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

3.3.1 The GOOSE Protocol. The GOOSE protocol, specified in the IEC 61850-8-1 standard is a multicast/broadcast protocol that uses a publisher-subscriber communication model to send and receive data between IEDs. Bay-level IEDs use the GOOSE protocol to report the switch state changes (ON and OFF). The GOOSE protocol uses the

Status Number (StNum) and the *Sequence number (SqNum)* to distinguish between state change events and re-transmissions. StNum starts from 1 and is incremented for every state change (OPEN or CLOSE) event. The SqNum, starting from zero, indicates re-transmissions of a previous notification. For example, the first status change in the switchgear will have StNum=1 and SqNum=0. The switchgear will keep broadcasting its state information at time intervals less than 60s until a new state is recorded. For each re-transmission, the StNum remains the same but the SqNum is incremented.

3.3.2 The SV Protocol. The SV communication protocol defined in IEC 61850-9-2 is a multicast/Broadcast protocol using a publisher-subscriber communication model to send and receive data streams of sampled values from sensors in the substation. The SV 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. The SmpCnt is incremented for every new sample and there are no re-transmissions. The substation uses the SV protocol primarily to send voltage and current measurements obtained from current and voltage sensors to all subscribing IEDs.

4. Attack Description

The CILO 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 any given instant. The valid configuration table is the collection of all possible valid configurations. Let s be the number of switchgear devices in the substation, then all possible switchgear configuration $C \in \{0,1\}^s$. Assuming $\vec{C'}$ is a valid configuration, and n be the total number of valid configuration, we can define the valid configuration table as a set $T = \{\vec{C'_1}, \vec{C'_2}, \cdots, \vec{C'_n}\}$. Therefore a state change request τ_{i+1}, can only be allowed to change the CILO current configuration state from $\vec{C'_i}$ to $\vec{C'_j}$ if and only if $F : \vec{C'_i} \times \tau_{i+1} \Rightarrow \vec{C'_j} \in T$, 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 the XCBR or XSWI, a status update message is sent to the CILO, and the CILO updates its current configuration state from $\vec{C'_i}$ to $\vec{C'_j}$.

Process level communications is time critical as IEC 61850 requires a delay of not more than 4ms in the transmission of GOOSE and SV messages. This requirement makes implementing encryption based security solutions difficult. IEC 61850 does not recommend the encryption of SV and GOOSE messages and says that encryption-based message integrity checks can be used for GOOSE only if it meets the 4ms time requirement. IEDs in the process LAN depend on the timestamps, StNum, and SqNum for GOOSE messages and SmpCnt for CV messages to detect any data manipulation. Tebekaemi et al. in [7] demonstrate successful GOOSE attack when the attacker has physical access to the process LAN. Attacks on SV messages are more difficult to detect especially at high SmpRate values, as it becomes more difficult to predict the next SmpCnt value.

4.1 Scenario 1: Dropped Update Message

We assume the attacker has physical access to the process LAN at the substation and is able to block GOOSE update messages to the CILO. When a status change request is received by the CSWI, the CSWI queries the CILO to validate the request. The CILO validates the request against the system's current state $\vec{C}_i'$ and instructs the XSWI to execute the request. The XSWI executes the request and broadcasts its new status which is blocked by the attack. Since no update message is received by the CILO, the CILO still thinks the system is in the state $\vec{C}_i'$ instead of the new state $\vec{C}_j'$. The current state of the CILO no longer reflects the actual state of the physical system. Although The CILO and the physical system may still be in a valid configuration, any new change request will result in the F using the wrong input $\vec{C}_i'$ instead of $\vec{C}_j'$.

4.2 Scenario 2: Corrupt Update Message

We assume the attacker has access to the process LAN and modifies the GOOSE update messages, injects new GOOSE packets, or arbitrarily sends GOOSE update messages. The attacker may be able to deceive the CILO that an update has occurred and its current state should be updated, causing the CILO to update its current state to $\vec{C}_j'$, while the system remains in $\vec{C}_i'$.

Both scenarios have the same impact of poisoning the CILO configuration state. If the malicious update is a valid configuration state, no flag is raised and the attack goes unnoticed by the IED. If an attacker is able to successfully put the CILO in an invalid state the result could be disastrous. For example, from Table 1 we know that CS1 and CS2 cannot be closed at the same. Assuming we want to disconnect the bay for maintenance autonomously, both CS1 and CS2 need to be open before ES closes. The CILO configuration table is poisoned to think that both CS1 and CS2 are open and then validates an ES close request when ei-

Table 2. Voltage and Current Measurements in p.u. During ON/OFF Switchgear 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

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

ther CS1 or CS2 is closed. Executing the request will raise current values astronomically (since the voltage is suddenly reduced to approximately 0) which could damage equipment and cause fatal accidents. In Table 2 row 14, we see that executing such request raised the current value to 850 times the nominal current value.

5. Proposed Solution

Electrical equipment and appliance show unique physical attributes properties when triggered by ON/OFF commands, which can be seen

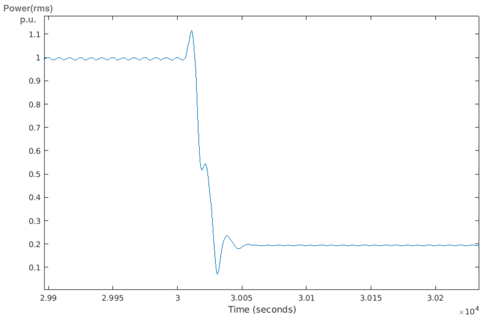

Figure 2. Transient and steady state voltage behavior during switch close operation (p.u. = measured value/nominal value)

as transients, steady state changes, amplitude and frequency changes in the voltage and current waveforms. These properties can be used to provide *direct power feedback* on physical and cyber controlled events by observing disturbances in the voltage and current waveforms. It is possible to monitor and detect such turn ON or OFF events of electrical equipment and trace these events to the originating equipment using their transient state, steady state, or frequency changes of the measured voltage and current [8, 9]. Similar techniques have been used to detect and locate of faults in power systems [10], [13], and [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, over-voltage and over-current protection. Current and Voltage sensors give information about which part of the system is energized. IEDs can use this information to determine the switchgear position (OPEN or CLOSE) at any given instant. Switchgear events are also observable through the electrical waveforms they generate, as switching ON or OFF generates transients seen as spikes in their waveforms and steady state amplitude changes as seen in Figure 2. Monitoring these events can provide useful information about the time an event occurs and the originating switchgear, that can be used to detect illegal switchgear manipulations.

5.1 Switchgear Event Detection

Event detection algorithms compare measured values of a signal to a reference value and if there is any significant difference an event of interest is declared to have occurred. To increase event detection accuracy in power signals, the change event is computed on properties of the signal over a time frame usually called the event detection window. This helps to reduce the effects of noise in the signal and reduce false event detection ratio. In our initial simulated testbed, the electrical noise is normally distributed, which may not be the case for an actual substation. The detection algorithm is a simple mean change detector that compares the detection window w_i to 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 $|\frac{\sum_{i=1}^{n} x_i - \sum_{i=1}^{n} y_i}{n}| > \xi$ indicates the occurrence of an event, where μ is the mean value, x_i and y_i represent sample points of the DC component of the signal, and ξ is a predetermined threshold value.

5.1.1 Event Detection under Electrical Noise. 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 could cause detection systems to have an increase in the number false positives or a complete misdetection of the event. To address the effect of noise, the sensitivity of the detection system (threshold) needs to be set so that we can attain high detection rates (like 100%) given the noise level, and the lowest possible false positive rate in an acceptable response time. More sensitive threshold makes the system detect small events and responds quicker but with less accuracy, while a less sensitive threshold makes the system miss smaller events and responds slower but with better accuracy. In this work, we considered environments where the measured voltage and current signals contain noise and used change detection method discussed in Jin et al. [8]. We assume the noise e_i is 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 a detection sensitivity factor of k. An event is detected when $\sum_{i=1}^{n} \frac{(x'_i - y'_i)^2}{y'_i} > \xi$. The detection threshold can be pre-computed and fixed if the noise level is expected to be the same, or dynamically computed during the system operation if we expect the noise level 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 device may be 'CLOSE' or 'OPEN'. 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 maps to an ON of OFF state of switchgears in the substation. The switchgear state identification serves two purposes; firstly, to attribute a detected event to the originating switchgear and secondly, to validate the state of the physical system during the CILO request validation operation. Table 2 show the measured values of each switch when it is turned CLOSE and OPEN. The information contained in Table 2 is used to generate the switchgear event truth table in Table 3. The event truth table is used to predict which switchgear is OPEN or CLOSE based on sensor measurements. In the event truth table Table 3, a "0" indicates that the measured value from a given sensor is low and a "1" indicates the opposite.

5.3 CILO Security Controller

Switchgear status update information are sent from the XCBR or XSWI to the CILO using the process LAN as GOOSE packets. The IEC-61850 standard also supports sampled voltage and current measurements to be sent from the merging units to IEDs using the process LAN as sampled values (SV) packets. The CILO security controller using the SV messages can detect changes in the waveforms and obtain the direct power feedback for any switchgear event. The CILO security controller uses both GOOSE and SV messages which are two independent sources to validate the correct state of the switchgears in the system. The following algorithm describes the high-level the behavior of the proposed CILO security controller.

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 $\approx$ powFeedback.time then
6:                 return FALSE
7:         return TRUE
```

Algorithm 2 is called whenever GOOSE update messages (*updateMessage*) are received from switchgears (XCBR and XSWI). The security controller first checks whether the update message is a retransmission or a new event notification in line 2. If the update message is a new event notification, the security controller obtains the power feedback information from the SV messages in line 2. In line 3 the most recent

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
```

measurements from the sensors are obtained and used to estimates the current state of the switchgears. In line 4 and 5, the goose update message and the power feedback information are compared if the reported event is consistent and within the same time frame. The GOOSE update and SV feedback messages will arrive at the interlocking function at slightly times, so we approximate the time values and check if both messages arrives within an acceptable time frame. If any inconsistency is found in the reported event or the time frame, then there is a high probability the GOOSE update message has been modified.

Algorithm 3 runs continuously as a background process and checks for changes in voltage and current waveforms obtained from the SV messages. If any significant change is detected in line 3, the security controller proceeds to obtain the change information using line 4. The reported change is checked in line 5 to ascertain if the event is a result of a state change using, and returns *true* if the event is caused by a switchgear. If the event is a 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 consist of bays that connect feeders to power sources, and each bay contains switchgears that implement the bay-level protection and control function. The IEC61850 gives no preference where the interlocking function should be implemented (the station level or the bay level), instead it leaves this for the substation designer to decide. At the station level, the interlocking function will have to keep the state and configuration information of switchgears from all the bays in the substation. Thus for a substation with n number bays and x number switchgears per bay, the interlocking function will keep $n * x$ switchgear states with $(2^x)^n$ possible switchgear configurations. The configuration table can grow rapidly as x and n increases and can easily overwhelm the IED. Also, Our proposed solution relies on SV messages obtained from merging units by the interlocking function. SV messages are a continuous stream of currents and voltages sampled at high rates and transmitted as multi-cast packets. For a multi-bay substation, the interlocking function will need to process the continuous streams of multi-cast packets from all the merging units distributed across the bays in the substation. This will overburden the station LAN causing network congestion and may also lead to the failure of the interlocking function IED's network interface controller. For these reasons, we recommend that the interlocking function be implemented at the bay level, and our proposed solution is designed for bay-level interlocking function.

6.1 Implementation Details

In our earlier work [7], we designed and implemented a substation simulation testbed. Some modifications were made to our initial testbed to support the substation interlocking function discussed in this paper. The modified testbed is implemented as shown in Figure 3 using three virtual machines (VM) running on a VMware ESXi server and a MacBook Pro computer.

6.1.1 Power System (VM1). The substation is simulated in the MacBook Pro computer(Intel corei7 MacBook Pro computer with a processor speed of 2.5ghz, 16GB of RAM, and 512GB SSD.). The substation is a single bay step-down station designed with Matlab/Simulink and consists of contactor switches (CS1 and CS2), grounding/earthing switch (ES), isolator switch (IS) and the circuit breaker (CB). Voltage and current measurements are obtained from sensor1, sensor2, and sensor3 installed at different locations along the bay.

6.1.2 Virtual IEDs.

Merging Unit and Switchgear Controller (VM1): The merging unit and switchgear controller are both implemented as standalone C/C++ applications based on the IEC 61850 standard. These applications also run on VM1 (Ubuntu 14.04.4LTS 2GB RAM, 2 Core Processor, 20GB HDD). The merging unit and switchgear controller communicate with the simulated substation using UDP ports. The merging unit collects sampled measurements from all three sensors, timestamps them and broadcast the values using the SV protocol. The switchgear controller relays OPEN/CLOSE GOOSE commands from the bay controller to the appropriate switchgear.

Bay Controller IED (VM2): The bay controller IED is implemented as a C/C++ applications based on the IEC 61850 standard and runs on VM2 (Ubuntu 14.04.4LTS 2GB RAM, 2 Core Processor, 20GB

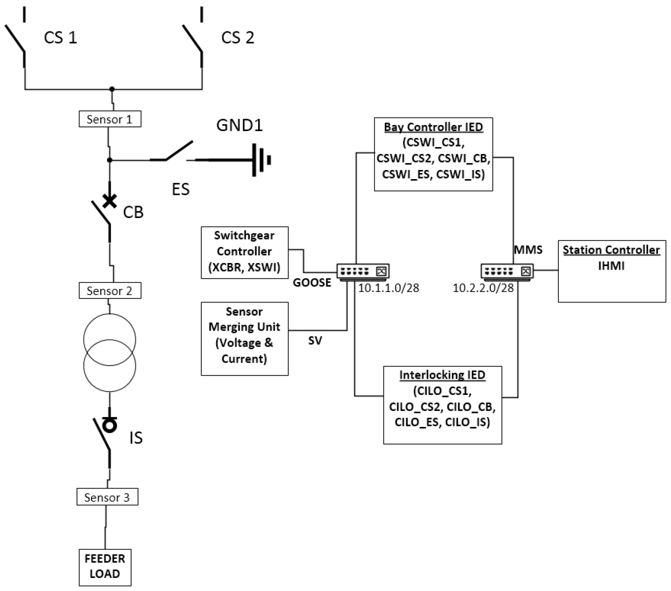
CS 1
CS 2
Sensor 1
GND1
ES
CB
Sensor 2
IS
Sensor 3
FEEDER LOAD
Bay Controller IED (CSWI_CS1, CSWI_CS2, CSWI_CB, CSWI_ES, CSWI_IS)
Switchgear Controller (XCBR, XSWI)
GOOSE
10.1.1.0/28
10.2.2.0/28
MMS
Station Controller IHMI
Sensor Merging Unit (Voltage & Current)
SV
Interlocking IED (CILO_CS1, CILO_CS2, CILO_CB, CILO_ES, CILO_IS)

Figure 3. Implementation Schematics of the Substation Testbed

HDD). The bay controller IED consists of 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 IED consists of five CILO logical nodes (CILO_CS1, CILO_CS2, CILO_ES, CILO_CB, and CILO_IS) each of which maintains the state information of the corresponding switchgear device in the testbed. The interlocking IED runs the data manipulation detection algorithms and maintains the switchgear configuration and transition rules. We created The following interlocking rules (Algorithm 4) for the Interlocking IED from Table 1.

Algorithm 4 Interlocking Rules

```
if CS2==CLOSE then DENY CS1 Close
if CS1==CLOSE then DENY CS2 Close
if ES==CLOSE then DENY CS1 Close
if ES==CLOSE then DENY CS2 Close
if CS1==CLOSE then DENY ES Close
if CS2==CLOSE then DENY ES Close
```

6.1.3 Attacks.

Blocked GOOSE Update: We assume that the attack has access to the process LAN and blocks the sending of GOOSE update messages. To simulate this we configured the controllers not to send update messages after a state change operation.

Modified GOOSE Update: We assume that the attack has access to the process LAN. GOOSE update messages are broadcast in plain text to all subscriber-IEDs. Using TCPDump (network traffic capture tool) we were able to capture network traffic, and replay it unmodified using TCPReplay (network traffic replay tool) or modified using Scapy (network traffic manipulation tool).

6.2 Results

The simulation was first run with the CILO security controller deactivated. The interlocking IED used the GOOSE stNum, sqNum, and timestamp fields to detect replay attacks. However, if the stNum, sqNum, and timestamp is modified to mimic a new update message we were able to successfully modify the interlock configuration state. For missing or blocked update messages, the interlocking IED had no way of detecting such events and easily entered an inconsistent state. When the security controller was activated, both the modified replay attacks and the missing update messages were detected. The Security controller always validates the GOOSE update messages with the power feedback SV messages to ensure that the GOOSE update message is valid. Also, by continuously listening to changes in the physical system, security control can detect configurations changes observed by the power feedback SV messages but not report by the GOOSE update messages.Table 4 shows a summary of the performance of the interlocking function with and without the security controller. The time (ms) is the time in milliseconds it takes from when the control operation is initiated by the switch controller (CSWI) to when the interlocking IED updates its configuration state.

7. Conclusion

Interlocking is a critical substation automation function that ensures the safety of lives and equipment, reliability and resiliency of power systems. Failures of interlocking functions could result in loss of lives and property and therefore a high value target for malicious attackers. Power systems have very constraining time requirements which make the use of cryptographical techniques and tools to protect data undesirable

Table 4. Comparison 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

at present speeds. Therefore, other methods for securing the operation of power systems should be exploited.

In this work, we present a novel method to detect data manipulation attacks using the behavior of the physical system and integrating it into conventional intrusion detection mechanisms. The approach described in this paper is applicable to other areas of power systems were automated switching functions are desired, such as distribution bus networks and ship power systems. As this work show, Integrating the physical behavior of cyber-physical systems into the cyber security controls of the cyber-physical system is vital for the cyber-physical system is to operate resiliently.

References

[1] E. Colbert D. Sullivan, S. Hutchinson, K. Renard, and S. Smith, *A process-oriented intrusion detection method for industrial control systems*, International Conference on Cyber Warfare and Security, Academic Conferences International Limited, pp. 497, 2016.

[2] 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*, 2014 IEEE International Conference on Smart Grid Communications (SmartGridComm), pp. 908-913, 2014.

[3] R.Mitchell and R.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.

[4] K. Sawada, T. Sasaki, S. Shin, and S. Hosokawa, *A fallback control study of networked control systems for cybersecurity,* Control Conference (ASCC), 2015 10th Asian, pp. 1-6, 2015.

[5] O. A. Harshe N. T Chiluvuri, C. D. Patterson, and W. T. Baumann, *Design and implementation of a security framework for industrial*

control systems, 2015 International Conference on Industrial Instrumentation and Control (ICIC), pp. 127-132, 2015.

[6] J. Pan, B. Duan, C. Qiu, and G. Li, *Research on interlocking cilo based on iec 61499/62351*, 2012 Asia-Pacific Power and Energy Engineering Conference, pp. 1-4, 2012.

[7] E. Tebekaemi and D. Wijesekera, *Designing an IEC 61850 based power distribution sub- station simulation/emulation testbed for cyber-physical security studies*, CYBER 2016, The First International Conference on Cyber-Technologies and Cyber-Systems, International Academy, Research, and Industry Association (IARIA), pp. 41-49, 2016.

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

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

[10] 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.

[11] P. K. Nayak, A. K. Pradhan, and P. Bajpai, *A fault detection technique for the series-compensated line during power swing,* IEEE transactions on power delivery, vol. 28(2) pp. 714-722, 2013.

[12] 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 Transactions on Smart Grid, vol. 6(5) pp. 2444-2453, 2015

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