Cyberattack Defense with Cyber-Physical Alert and Control Logic in Industrial Controllers

Hao Huang*, Student Member, IEEE, Patrick Wlazlo†, Zeyu Mao*, Student Member, IEEE, Abhijeet Sahu*, Student Member, IEEE, Katherine Davis*, Senior Member, IEEE, Ana Goulart†, Member, IEEE, Saman Zonouz‡, Member, IEEE, and Charles M. Davis §, Member, IEEE

Abstract—Power system substations have intelligent electronic devices (IEDs) that collect data and control other devices. As the bridge between the physical and cyber parts of the power system, IEDs capture some key system behaviors. Since adversaries can modify the system’s behavior, physical and cyber data can be used to infer characteristics about the adversary. In this paper, we present alert and control logic for hardware-based power system defense using the physical data and communication status in substation IEDs for cyber threat detection, cyber-physical contingency detection and response, and physical contingency identification and response. The proposed alert and control logic routines are implemented in an industrial real-time automation controller (RTAC) using IEC 61131-3 in the Resilient Energy Systems Lab (RESLab) testbed. The goal is to help operators identify adversaries and protect the grid in a cyber-physical environment. The logic schemes’ effectiveness and accuracy are validated under different adversarial scenarios. Comparing the proposed schemes with an intrusion detection system (IDS), Snort, our results show the benefits of using cyber and physical data to identify threats. The results also suggest the use of such hardware-based schemes with software algorithms in a next-generation cyber-physical energy management system (EMS), which can implement automatic control actions to protect power grids and its physical equipment against cyber threats.

Index Terms—Cyber-physical Security, Hardware-in-the-loop Testbed, Cyber-physical Power Systems, DNP3, IEC 61131

I. INTRODUCTION

Modern power grids consist of various Intelligent Electronic Devices (IEDs) to collect data, monitor systems, and control devices to improve grids’ reliability, observability, and controllability. The integration of communication networks introduces additional threats to power systems. Our previous work [1] introduced a method to establish a Distributed Network Protocol version 3 (DNP3) [2] communication between real-time power system simulation and an industrial real-time automation controller (RTAC) to analyze power system cyber-physical security from the perspective of IEDs.

Cyber incidents are continuing to gain attention worldwide, including the recent unidentified threat in European Network of Transmission System Operators for Electricity (ENTSO-E) [3], the Ukraine attacks in energy distribution companies [4], the Stuxnet compromises of programmable logic controllers (PLCs) to wear down fast-spinning centrifuges [5], and the recent Colonial Pipeline attack [6]. All above cyberattacks bypass the intrusion detection systems (IDS) and deceive the operators until certain conditions trigger their malicious functions. These events emphasize the importance to take a holistic approach for studying ways to improve power system security, including systematic incorporation of the cyber, physical, and device perspectives.

A. Literature Review: Defending cyberattacks in cyber-physical power systems

As discussed in [7], there are six directions of defending cyberattacks in cyber-physical power systems, including: temporally- and spatially-relevant detection, securing measurement sensors, model and algorithmic enhancement, data-driven approaches, moving target defense, and watermarking. Various approaches and methodologies have been proposed from the physical and cyber perspective, respectively, to improve the security of power systems against cyberattacks following above directions. From the physical perspective, most work focuses on the integrity of the data for ensuring security of power systems operation. For example, Valenzuela et al. utilize principal component analysis (PCA) to determine whether the data is compromised, which improves the data security in power system operations against false data injection (FDI) attack [8]. In [9], Yang et al. present the countermeasures against FDI attacks on state estimation to ensure the security of power system operation. In [10], Deng et al. formulate a least-budget strategy to defend power systems against FDI attacks. With the integration of renewable energies, Wang et al. propose a novel anomaly detection countermeasure from the perspective of state estimation considering the uncertainty of renewable energies [11]. From the cyber perspective, the proposed methodologies and techniques improve the security of communication network against the cyber kill chain of industrial control systems [12]. For example, Liang et al. utilize the blockchain technology to enhance the self-defense capability of power systems’ communication networks against cyberattacks [13]. In [14], Yang et al. introduce a multi-attribute SCADA-specific intrusion detection system with heterogeneous information from the SCADA cyber network. In [15], Premaratne et al. present an intrusion detection system specifically for IEC 61850 automated substations based on the simulated attack data within an IEC 61850 communication network. In [16], Ustun et al. present a machine learning based
intrusion detection system using IEC 61850’s Sampled Value messages to monitor communication traffic and identify FDI. Other approaches integrate the cyber and physical features of power systems to identify and defend cyberattacks. A tri-level optimization problem is formulated in [17] to allocate both physical and cyber resources for defending power systems against cyberattacks. In [18], Li et al. introduce attack detection logic for a cyber-physical power systems’ sensors with reconstructed attacks.

Even though the above works can improve power systems’ security and defend cyberattacks at different stages, their models are from the system perspective, hence they neglect new countermeasures that can be possible by including the IED perspective. Modern power grids consist of millions of IEDs with the communication capability and control capability. Cyber threats can stay silently in the communication network until the targeted device or action triggers its function and inflicts whatever the physical impact to the system might be. Thus, it is important to consider the defending strategies from the IED perspective. However, only a few studies of defending cyberattacks focus on the IEDs. For example, Nuqui et al. introduce a method of securing protective relay settings via peer-to-peer communication between IEDs against malicious changes for relay configuration [19]. In [20], a reliability assessment framework for power grids is proposed with the consideration of integrity attacks on protective relays. To the best of our knowledge, there is no work utilizing the data within the IEDs to proactively defend against cyberattacks in power systems.

### B. Defending cyberattacks from the IED perspective

In this work, we transit the attention from protective relays to data concentrator devices in substation automation system (SAS) [21] and supervisory control and data acquisition (SCADA) systems [22]. Such devices collect data from other IEDs in the system and have the ability to control them and the connected physical devices. As the bridge between cyber and physical networks, they have extensive online cyber and physical information. In [23], Sahu et al. observed a significant improvement in detection of cyberattacks by fusing features from cyber, physical, and security domains. Thus, the data concentrator devices have great potential to be used against cyber and physical threats.

The RTAC has been used widely in the field as a data concentrator. From the research perspective, several power system testbeds have integrated the RTAC as a remote terminal unit (RTU) to collect data from protective relays, send it to SCADA software, and perform the protocol conversion functionality [24]–[26]. Its IEC 61131-3 engine [27] has also been used for validating control algorithms to reconfigure the physical network structure for microgrids [28], control reclosers and tap-changers [29], and send the power setpoints to control the battery storage management system (BESS) [30], [31]. The high-fidelity cyber-physical power system testbed, Resilient Energy Systems Lab (RESLab) testbed, has integrated real-time power system simulation, real-time communication network emulation, and RTACs with detailed substation network architectures [32]. This enables the study of data flow from field devices to substation control center.

Within the detailed cyber-physical environment, this paper addresses the research question, how can we protect power systems against cyber and physical threats by fusing cyber and physical data within IEDs?

A multi-tagging technique is introduced in this paper that uses the RTAC’s IEC 61131-3 logic engine to protect power systems with fused cyber and physical data. With the physical data and communication status tags in the RTAC, we design and implement three logic for five cyber-physical adversarial scenarios. The logic are presented for cyber threat detection, cyber-physical contingency detection and response, and physical contingency identification and response, which detect the threat and secure the response against contingencies.

This paper presents a systematic framework of fusing online cyber and physical features (Figure 2) within IEDs to identify and defend threats in power networks. Following the methodology and technique introduced in [1], the major contributions of this work are:

1. With the RTAC, we design a series of cyber-physical alert and automatic control logic to proactively defend the system against different cyber and physical threats with fused cyber and physical data. This approach has not been proposed before nor subjected to stringent examination in a high-fidelity cyber-physical power system testbed.

2. With the RESLab testbed, we implement the proposed logic in a realistic cyber-physical power system environment. Under the real Man-in-the-Middle (MitM) attacks in the communication network, the proposed logic identifies the cyber threats and enacts countermeasures to stop them.

3. In RESLab, we analyze and compare the proposed logic against Snort, a software-based IDS. Results demonstrate the effectiveness and accuracy of proposed logic at detecting cyber threats with fused cyber-physical information and the potential to implement automatic control actions to protect power grids from cyber and physical threats.

4. These actions proactively protect the system from further cascading failures. It enables more timely protection of power systems to take place right before cascading failures begin in the systems.

This paper is organized into the following sections. Section II introduces the background of the RESLab testbed and its development to mimic the realistic substation network architecture. Section III presents the framework of fusing cyber and physical information within substation IEDs and the design of alert and control logic to detect and protect the grid against cyber and physical threats. Section IV introduces the cyber and physical contingency scenarios with critical elements in the synthetic 2000-bus case. Section V implements the proposed logic in RESLab and compares it with Snort to examine its accuracy and effectiveness under different threats. Further discussion about the case studies are in Section VI. Finally, Section VII is a summary of contributions this paper provides.
II. BACKGROUND AND DEVELOPMENT OF RESLab

The RESLab testbed is a high-fidelity cyber-physical hardware-in-the-loop testbed. It provides a realistic cyber-physical environment for power system studies with detailed cyber and physical information [32], with main elements as follows:

- Communication Protocol: DNP3 [2] is used to transmit data between two points through serial and IP communications. There are 5 object groups in DNP3 packets including Analog Input (AI), Analog Output (AO), Binary Input (BI), Binary Output (BO), and Counter Input (CI) for data collection and control.
- PowerWorld Dynamic Studio (PWDS) [33]: The real-time power system simulation software is running the real-time power system of a 2000-bus synthetic grid [34] and generating DNP3 packets for all physical devices [35], [36]. The PWDS represents the physical network of a power system and the conversion between analog and digital data in physical and cyber networks.
- Common Open Research Emulator (CORE) [37]: The communication emulation software is establishing an emulated communication network with detailed traffic. It bridges the physical network in PWDS with the data concentrator devices for upstream applications and services of monitoring and control of the system through the emulated network. This emulated communication network provides the environment to implement cyberattacks and study their impacts in the system after they bypass the IDS within substation.
- RTAC [27]: The automation platform for substation and industrial control applications is configured as the data concentrator to collect data from a physical network over CORE for monitoring, control and delivering data to upstream utility control centers. The substation devices, such as circuit breaker, protective relay, generator governor, etc., are modeled within PWDS and their data are captured in the DNP3 packets from PWDS.
- MiTM attack library [38]: The python library is launching MiTM attacks on DNP3 data packets in the emulated network in CORE, which achieves false data injection (FDI) and false control injection (FCI) attacks. The impact of such attacks can thus be analyzed considering both the physical system and the communication traffic.
- Layer-3 network switch: The network device is routing data among different local area networks (LANs). This new device completes a realistic communication network architecture in a substation that collects data from the physical network (Substation LAN) and serves the data for the utility control center (Utility LAN). Since the cyberattacks are only in CORE (Substation LAN), they will not affect the functionality and traffic in Layer-3 network switch (Utility LAN). It helps us to log the reaction of RTAC when the Substation LAN is compromised by cyberattacks.
- Wireshark [39]: The open-source packet analyzer is capturing the communication packets in the network for troubleshooting and analyzing.

Figure 1 shows the current architecture of the RESLab testbed. It is hosted in vSphere with multiple virtual machines (VMs) running CORE and PWDS in separated virtual local area networks (VLANS). Each VM has Wireshark [39] to capture the communication traffic flow through RESLab. RESLab provides detailed information for analysis and defense of cyber and physical threats in power systems. RTAC communicates with PWDS through DNP3 to collect data and control devices in the real-time power system simulation over CORE, enabling the hardware-in-the-loop feature to study and develop RTAC’s functionality. The frequency of data collection is based on RTAC’s Integrity Polling Period and Class 1,2,3 Polling Period for normal data and event data from the physical system (PWDS). The Integrity Polling Period is configured as 60000 ms and the Class 1,2,3 Polling Period is configured as 5000 ms, respectively [40]. The MiTM attack resides in the emulated communication network silently until particular event triggering its function of modifying the data [38]. The newly integrated Layer-3 switch is a special network device functioning as a router and a switch on the data-link layer (Layer 2) and network layer (Layer 3) of the Open Systems Interconnection model (OSI model) [41]. Through Access Control Lists (ACLs), it connects LANs of RTAC and Utility Operators, representing a realistic communication architecture of a substation network, from physical devices to control and monitoring systems. This also provides a separate channel to analyze the RTAC’s reaction under compromise in cyber-physical power systems. With the isolated channel, we can study and validate the performance of the RTAC-based hardware logic against these threats in the RESLab testbed.

III. DESIGN OF ALERT AND CONTROL LOGICS

Figure 2 presents a framework of using the collected data in RTAC to design generic logic against cyber and physical contingencies in power systems. Its purpose is to identify cyberattacks and, if one occurs, to interrupt its function just ahead of time. Thus, it can avoid the potential for cascading failures in both cyber and physical networks.

In Figure 2, the Data Concentrator Device collects all devices’ Measurement and Status from physical network. Meanwhile, the valid Communication Status ensures the
data transition from field device to the **Data Concentrator Device** over the communication network. Using the RTAC as a representative of the **Data Concentrator Device**, it has physical data from field devices and the internal program organizational unit (POU) tags that can indicate the communication status. With the embedded IEC 61131 engine, we can design and implement specialized algorithms in RTAC to detect and defend cyberattacks in power systems using the online cyber and physical information.

Once the cyber adversary enters the communication network bypassing the software based IDS, it can interrupt communication and falsify the data (measurement and command) between clients and servers, causing the physical system to be operated under stress [38]. The RTAC and other IEDs are the last line of defense against cyber threats and the first line against physical contingencies in power systems. Fortunately, cyberattacks can leave a digital fingerprint within data, which can be used with RTAC’s IEC 61131 logic engine. Thus, this paper proposed the following logic: **Cyber Threat Detection**, **Cyber-Physical Contingency Detection and Respond**, and **Physical Contingency Identification and Respond**, to identify the threat and secure the response against the contingencies. Furthermore, the synthesis of the results from above logic can help operators better locate the adversaries are in cyber network or/and physical network.

This logic-based multi-tagging technique fuses the cyber and physical features in RTAC to identify more than one cyber and/or physical threat occurring simultaneously in power grid. The logic is agnostic to whether the threat source is from cyber or physical domain. Once the abnormal data triggers the logic, it can identify and present the concrete information about the cyber threat to operators to help with forensics and investigation. In this paper, the proposed logic and their implementation targets the cyberattacks in DNP3 protocol.

### A. Communication Disruption Alert Logic

Due to the importance of the communication network, the goal of the Detection logic is to identify both cyber and physical threats in the system that result in communication loss. Through RTAC’s internal tag processor [27], we propose the **Communication Alert Logic** in Algorithm 1 to promptly inform the operators about the loss of communication using the RTAC’s internal tags. In RTAC, the POU has specific tags to indicate the communication status, including the **Offline**, **Message_Success_Count**, **Message_Failure**, etc., for each communication link between RTAC and other device [1]. Any interruption of communication, regardless the source, such tags will reflect the contingencies immediately. The POU offline tag is an internal tag that can be directly obtained within RTAC’s tag processor. It is a simple utilization of communication status to see whether there is a cyber interruption in the network. Other tags can also be used for the same purpose, which can be explored in future work. If the communication of any DNP3 client served by the RTAC is interrupted, this logic can send a signal to indicate the threat through LED lights or annunciation system, informing the operator about disruption in the communication network. The interruption of communication between field devices to control centers can come from sabotage of physical links, the cyber adversary in communication network, or a mis-configuration of the communication network devices. Considering different sources of threats, the proposed logic only focuses on the detection and alert of the threats in communication networks. With the following logic, the synthesis of results can help operator better locate the source of adversaries. It is recommended that the loss of communication should be fixed manually by substation operators to ensure the network’s security and integrity. However, with the integration of other network devices, such as the Layer-3 switch, this signal can also be
used as a trigger to reconfigure the communication network to isolate or disable the compromised part.

**Algorithm 1 Communication Alert Logic**

1. Input = All Clients’ POU Offline Status
2. if One of Clients’ POU Offline == TRUE then
   3. Status = Alert
   4. else
   5. Status = Normal
   6. end if
7. Send Status to Indicator Device

**B. Cyber-Physical Contingency Detection and Response**

When an adversary bypasses the security controls of the communications network, (s)he is able to launch various malicious programs that can be intended to mislead the operators. Even though the control actions are issued from an authorized device or operator, the cyberattacks can falsify the data within cyber networks. In [32], the authorized DNP3 client issues a Trip command to open a branch, but the control center still shows that branch is closed because of the MiTM attack. PWDS converts all physical devices’ data, such as measurement, status, generator setpoint, etc., into DNP3 packets, and the packets are then sent to the RTAC through CORE. Thus, the MiTM attack in RESLab testbed can manipulate the communication between a location in the physical network and the RTAC. When a branch status is falsified by the MiTM attack, all connected circuit breakers’ status are also falsified. This misguided information can make operators unaware of potential threats and vulnerabilities in the system. To deal with this situation, we have created the **Cyber-Physical Contingency Alert and Control Logic** in Algorithm 2. Its sole purpose is to validate whether the issued control command is received and executed as expected in the system. While the control logic and settings in protective relays protects the system against physical faults, Algorithm 2 serves to protect the system against malicious cyberattacks that falsify the data and control actions from authorized devices with online data collected by an RTAC.

In Algorithm 2, after a BO control command is sent from the control center to a field device through an RTAC, the system will execute the operation and update the device’s status through DNP3 protocol to the RTAC based on the communication settings. If the device’s updated status is not aligned with the command as expected, the logic will identify the issue. It will send an alert to the operators and simultaneously re-send the same control command to reattempt to validate its execution. If the successive control commands cannot be executed correctly, there must be issues in the communication network or in the field devices, such as the circuit breaker is locked or a permanent fault in the physical system. The issue with field devices has to be fixed manually. However, if the issue comes from the cyber attacks, the Re-send Control Command will cause large amounts of traffic in a short time that may exhaust the resources of the cyberattacks. This will interrupt the communication within the network. Two benefits are that (1) communication loss will interrupt the cyberattacks’ function, and (2) the Communication Loss Alert will allow operators to catch the issue in an early stage, which can prevent the cyberattacks causing cascading failures from the cyber domain to the physical system. Similar to the Communication Alert Logic, this logic also takes advantage of POU Offline tag as input to ensure there is no communication error between clients and servers. If the communication between clients and servers is interrupted, no control command needs to be issued. The Communication Alert Logic should react first, as operators need to validate the communication network before issuing any control command. Since the DNP3 event data is polled based on its Class Number and the Integrity Polling Period, the system status may not update immediately. Thus, Algorithm 2 has an input Delay, which allows the logic to get updated status and data, so it does not trigger the Alert signal immediately. Once the Alert Status stays On after the Delay (based on settings), the **Cyber-Physical Contingency Alert and Control Logic** will issue a signal to alert devices and re-send the same control command.

Different from the status control using BO, the setpoint control uses AO, which depends on the setpoint value and control status. For example, in RTAC, the AO consists of status and oper. The status is the value of setpoint and the oper is boolean value of the control action. Unlike computers, RTAC and other PLCs are memory storage deficient, so the control value cannot be stored with Delay function as the BO. Besides, the dynamic model in power systems cannot immediately set the output as the AO command, so the **Cyber-Physical Contingency Alert and Control Logic** cannot compare the AO command, such as generator setpoint control, with the real-time measurement data.

**Algorithm 2 Cyber-Physical Contingency Alert and Control Logic**

1. Input = Device Type, Client POU Offline Status, Control Command, Update Status, Delay
2. if POU Offline Status == False AND Control Command ≠ Updated Status then
   3. Status = Alert
   4. else
   5. Status = Normal
   6. end if
7. Keep the Status for Delay
8. if Status == Alert then
9. Send Status to Indicator Device
10. Re-send Control Command
11. end if

**C. Physical Contingency Identification and Response**

To complement the protection of AO command, we propose the **Physical Contingency Alert and Control Logic** in Algorithm 3. Based on the operating limits of each device, this logic protects physical equipment with local information when adversarial actions cause line overloads or generators’ operated out of its limits. It is designed to ensure the safety
of physical equipment in the event a protective device or remedial action fails to operate. Thus, Algorithm 3 functions as a backup protection to ensure the safety of local devices with local information through auxiliary PLCs, like an RTAC, when the protection devices do not operate as expected, such as the relay settings are falsified or the primary protection zone is not covered.

Algorithm 3 checks the operating limits of the device with consideration of communication status, where the limits information is given to the logic. For example, if there is a branch overload situation, this logic will issue an alert signal for operators to check the physical situation. Then, if no manual operation occurs to relieve the stress within a certain time interval, the device-safety operations can be implemented within the substation to protect other local devices. Examples of device-safety operation to relieve branch overload include: opening the branch, and/or reducing the generator’s output. As for generators, if the generators’ output is out of its limits, the pre-defined control action will either increase or decrease the setpoint to make the operation within limits. If the operators or protective devices cannot identify and resolve such contingencies on time, the physical system will experience cascading failures.

Algorithm 3 Physical Contingency Alert and Control Logic
1: Input = Device Type, Client POU Offline Status, Measurement, Max Limit Value, Min Limit Value, Time Limit
2: if Client POU Offline Status == False AND (Measurement > Max Limit Value OR Measurement < Min Limit Value) then
3: Status = Alert
4: else
5: Status = Normal
6: end if
7: Send Status Signal to Indicator Device
8: Operate the device to relief the stress locally if the contingency is not resolved within the Time Limit.

IV. CASE STUDIES OF PROPOSED LOGIC UNDER CYBER-PHYSICAL THREATS

This section introduces five cyber-physical contingency use cases to validate the effectiveness and accuracy of the proposed cyber-physical alert and control logic. These use cases are emulated under real MiTM attacks in RESLab testbed. With the generic attacks, we can validate the effectiveness of the proposed logic with online data in RTAC.

First, an N-1 substation contingency analysis for the 2000-bus case is performed, and its results identify several substations as critical. The events cause the power system case to experience limit violations of branch power flows and bus voltages. The sets of unexpected critical contingencies are found in [42], which consist of multiple branches spread throughout the system. The nearby generators are also important to the system’s security. Using combinations of FDI and FCI attacks targeting such critical assets, this paper considers 4 scenarios of cyber-induced contingencies and 1 scenario of physical-induced contingency to the synthetic grid, as listed in Table I. These scenarios are used to evaluate the effectiveness and accuracy of the proposed solution. If there is no prevention of such attacks, the system will experience cascading failures, as demonstrated in [32], [38]

The MiTM console presented in [38] is used to perform the above cyber attacks on the DNP3 protocol. To give a brief overview, a Python script that utilizes Scapy’s open-source libraries [43] to dissect clear-text network traffic was created. The script is designed to first perform an address resolution protocol (ARP) attack on both the gateway and victim devices (modeled in PWDS) in a LAN. Then, once the adversary places itself within the communication channel, it can not only sniff traffic but perform FDI/FCI attacks on DNP3 traffic.

A. Use Case Description

Use Case 1 is an FCI attack on DNP3’s BO data, which falsifies the binary control command. It interchanges the Trip and Close operation when the operator issues the command. From contingency analysis with the system model, it is observed that the disconnection of Substation San Juan (ID: 266) can cause a cascading failure with multiple branches overflow. Thus, we implement the proposed logic to monitor and protect the controls in Substation San Juan. In normal operation, the operator is able to close or open branches in the substation. During the attack, with the same control commands, we analyze how the RTAC reacts and logs the attack, based on the proposed logic.

Use Case 2 is an FCI attack on DNP3’s AO data, meaning that the analog control data is falsified by the adversary through MiTM console. To help illustrate the control logic, the generator setpoint is falsified to a value of zero, regardless of the real analog setpoint issued from the operator. For this use case, we apply the proposed logic for five large capacity generators in the system. These generators are located at Substation Glen Rose 1 (ID: 560), Substation Riesel 1 (ID: 631), and Substation Wadsworth (ID: 968). During normal operation, we slightly change the generators’ output, as in automatic generation control (AGC). During the attack period, we perform the same command and see how the RTAC reacts and logs the attack.

Use Case 3 is similar to Use Case 2, but it considers a combination of FDI and FCI attacks on DNP3’s AI and AO data, respectively. The FDI attack first changes AI data of

<table>
<thead>
<tr>
<th>Use Case</th>
<th>Threat Type</th>
<th>Protected Substations</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>FCI on BO</td>
<td>Substation San Juan</td>
</tr>
<tr>
<td>2</td>
<td>FCI on AO</td>
<td>Substation Glen Rose 1, Substation Riesel 1, Substation Wadsworth</td>
</tr>
<tr>
<td>3</td>
<td>FDI on AI and FCI on AO</td>
<td>Substation Glen Rose 1, Substation Riesel 1, Substation Wadsworth</td>
</tr>
<tr>
<td>4</td>
<td>FDI on AI, FCI on AO, and FDI on AI</td>
<td>Substation Glen Rose 1, Substation Riesel 1, Substation Wadsworth</td>
</tr>
<tr>
<td>5</td>
<td>Maliciously Disconnect Substation San Juan</td>
<td>Substation Edinburg 2, Substation Mission 4, Substation McAllen 1</td>
</tr>
</tbody>
</table>
generators’ measurement to zero, which forces the operators to send a control command that will make the generators’ reset their real power output. However, due to the FCI attack, the command will be falsified and make the generators’ setpoint become zero.

*Use Case 4* is similar to *Use Case 3*, but there is one more FDI attack on DNP3’s AI. After the control command is falsified, the attack will falsify AI data of the generators’ real power output measurement to the issued setpoints value. The extra FDI attack is supposed to disguise the FCI attack.

*Use Case 5* assumes the adversary entered the communication and controlled the Substation San Juan, which is like the Ukraine Attack [4]. After the adversary disconnected Substation San Juan, it caused several branches to overload in the neighboring areas. Thus, we implement the proposed logic in neighboring substations at Substation Edinburg 2 (ID: 244), Substation Mission 4 (ID: 265), and Substation McAllen 1 (ID: 310) to detect and protect the substations from the physical contingencies. The logic will identify the overloaded branches in those substations and protect them if there are no other control actions taken to relieve the stress.

### B. Logic Implementation Specifications and Challenges

As introduced in Section III, the internal POU of RTAC have different tags indicating the status of communication status between RTAC and connected devices and services. Such tags can be utilized with the internal tag processor for different purposes. The tag processor logs tag values for IEC 61131 logic design and complex calculations, visualizes the data in the RTAC web interface, converts data from different sources to SCADA/HMI, etc. [40]. With the embedded IEC 61131 logic engine, users can code flexible control and alert logic using the internal tag data and the data collected from local devices. To preserve the functionalities of different application, we create two types of DNP3 tags for data in this paper: one is for DNP3 clients that achieves the functionality of data concentration, the other one is for the RTAC’s tag processor that is used for implementing the proposed cyber-physical contingency detection and control logic.

In [15], [16], [18], cyber attack detection is demonstrated through analyzing off-line data in computers or servers. By contrast, the proposed cyber-physical contingency detection and control logic uses the online data in the RTAC. However, the RTAC does not have the capability to store the data for a complicated algorithm. Thus, Algorithm 2 has an input of *Delay* to wait for the system’s status to get updated for the comparison. With the IEC 61131 logic engine, we are able to achieve these functions to *temporarily store* the contingency information within the RTAC. It can ensure the accuracy of the proposed logic against cyber and physical adversaries. However, for the sophisticated control actions for generators, shunts or loads against cyber threats, the RTAC or other PLCs still need assistance from superior computers or the decision to come from the EMS.

### C. Alert Log Assignment

To better analyze the effectiveness and accuracy of proposed logic, we create specific alert logs to capture the reaction of proposed logic under threats. They are configured as DNP3 BI data with seven bits. They are assigned *Communication Lost* (1), *Cyber-Physical Contingency on Branch* (2), *Cyber-Physical Contingency Protection on Branch* (3), *Branch Overflow* (4), *Branch Overflow Protection Action* (5), *Cyber-Physical Contingency on Generator* (6), and *Cyber-Physical Contingency Protection on Generator* (7). The numbers listed here are their respective indices in the DNP3 BI data. Wireshark captures all communication traffic within *RESLab Testbed*, which allows us to analyze and visualize the logic reactions in the following section.

For *Use Case 1* and *Use Case 5*, there are no generators in the substations where the threat is located, so in these cases, the RTAC only detects the first five types of alert logs. For the other cases, all seven logs are considered. When the tag of *Communication Lost* is shown *True*, the *MiTM* console will manually be stopped and the control logic performance is analyzed.

### V. Results and Analysis

In this paper, Algorithms 1-3 are implemented based on the DNP3 protocol to test above cyber and physical threats. For other communication protocols, such as Modbus, SEL, Mirrorbits, etc., the proposed logic can also be implemented with the appropriate tags and data. This section analyzes the accuracy and effectiveness of the proposed alert and control logic for all use cases.

For each use case, the data of the protected devices and the generated alert logs are captured in *Wireshark* and plotted using the method from [23]. Figures. 3 - 7 show the captured data from all five use cases, respectively. The *MitM* console saves all its attack actions. It provides an accurate timestamp for the *attack period* as reference. When the alert is detected by the proposed logic, the log toggles from *False* to *True* and keep the status until the alert is cleared or the timer is off (the alert signal will stay on for 60 seconds after the contingencies are resolved.). In the plot, *False* is 0 and *True* is 1.

To better analyze the effectiveness and accuracy of the proposed logic, we also run *Snort*, an open source IDS, on a router in the emulated communication network as comparison. Following [44], the *Snort* is configured with an ARP cache overwrite rule and a DNP3 protocol specific rule for *MitM* attack on DNP3 data. In a normal operation, ARP tables are updated whenever a new device is connected to a Layer 2 device. There can be benign gratuitous ARP sent, usually for detecting IP conflicts. Hence, only considering ARP cache overwrite alerts would result in numerous False Positives. To reduce the alert rates, alerts associated with DNP3 function codes are also considered using the *AND* logic with the ARP cache overwrite. Thus, within a time period, if there are both ARP cache overwrite and DNP3 operation, it is treated as an *attack* [23].

The legends of the DNP3 data show the DNP3 outstation number/DNP3 server address and the data’s index in the DNP3 protocol. The indexes starts with *BI*, *BO*, *AI*, and *AO* for one DNP3 packet. For example, Figure 3(a) shows the status of all branches in Substation San Juan. The legends start at 266_1
and top at 266.9, which indicate all devices’ status (BI data) in the DNP3 packet. Similarly, Figure 3(b) shows the real power flow measurements (P) for all branches in Substation San Juan, and their indices represent the AI data in the DNP3 packet. Since there are BI and BO data ahead, the index of AI doesn’t start at 1. We create both real and reactive power measurements for devices in substations, so each of the indices is increased by 2. For RTAC logs, we assign the server address as 3, so the alert log legend is from 3.1 to 3.5 for Use Case 1 and 5. For Use Case 2, 3, and 4, since the attacks are on generators, the plots show the log legend of 3.1, and 3.4 to 3.7.

A. Analysis of Use Case 1

For the use case of FCI on BO in Substation San Juan, Figure 3(a) shows the status of all branches; Figure 3(b) shows the real power flow measurements on all branches; Figure 3(c) shows the alert logs from the proposed logic.

In the normal operation, when we Close, Open, and Close the same branch (266.1), the Snort detects the DNP3 operation and a fixed-interval detection of ARP cache overwrite. Since there is no overlap of the DNP3 operation and ARP cache overwrite at the same time interval, there is no attack detected. The alert logs from the proposed logic also do not show any alert during normal operation.

When the MitTM console starts, we can observe there are more ARP cache overwrites. However, the DNP3 operation depends on the operators’ command from RTAC. Thus, there is only one attack being identified with Snort logs. For comparison, Figure 3(c) shows the detection of FCI using proposed logic. The proposed logic identifies all compromised control actions and they are earlier than the Snort logs. Since the Cyber-Physical Contingency Alert and Control Logic detects the alert and issues the control command at the same time, the plots are overlaid onto one another.

After the FCI attack is identified, the Cyber-Physical Contingency Alert and Control Logic sends the original control command several times. Since the MitTM console is left running, the re-sent commands are also falsified, leading to more control actions. These extra actions make the Snort logs detect the attack. There are supposed to be six actions (one initial action and five triggered actions) captured by the WireShark. However, the polling period of RTAC is not as frequent as the actions. Thus, there are only three alert status shown during attack period in Figure 3(c). With so many actions happening in a short period, overwhelming packets trying to traverse the network caused the lost of communication. Then, the Communication Alert Logic detects the attack and the MitTM console is manually turned off. After the communication network is back to service, the original control command has been correctly issued and executed.

During the attack period, the proposed logic was able to detect the MitTM attack. However, the Snort was only to detect the attack after the attack period ends. Moreover, the overwhelming DNP3 traffic are because of the automatic control actions from the proposed automatic control logic. Meaning, if there is no extra operations, the Snort logs can not detect this attack. Due to the stochastic nature of IP based communication networks, the pure cyber log based intrusion detection can cause a false alarm or omit the alarm entirely. The presence of physical data can reduce the detection delay time, while increasing the detection accuracy. Moreover, the pattern of alert logs also indicates the contingency is because of cyberattack since the Communication Loss is raised right after the Cyber-Physical Contingency Protection on Branch for this case. The proposed framework can help operators more accurately locate the issue.

B. Analysis of Use Case 2

For the use case of FCI on AO, Figure 4(a) shows the AO data for generators’ real power setpoint values in Substation Glen Rose 1, Riesel 1, and Wadsworth; Figure 4(b) shows the output of real power flow from each generator; Figure 4(c) shows the alert logs from the proposed logic.

In the normal operation, when we slightly change the generators’ setpoint (1200 MW and 1000 MW, respectively for generator 5262 and 5263) in Substation Glen Rose 1, the Snort detects the DNP3 operation and a fixed-interval detection of ARP cache overwrite alerts. Since there is no overlap of DNP3 operation and ARP cache overwrite during the same time interval, there is no attack detected. Snort, which is the same as the proposed logic.

When the MitTM attack starts, we send the same control to Generator 5262 in Substation Glen Rose 1 and the setpoint is falsified to zero. Then, the generator’s real power output is suddenly reduced. This event triggered the Physical Contingency Alert and Control Logic for Generator 5263 in the same substation. The reduced generation output of Generator 5262 causes the increased generation output of Generator 5263, making it produce over its capacity. Then, the automatic control issued a control command to reduce its output within the normal operating limits. However, due to the attack, the control is also falsified to zero, making Generator 5263 reduce its real power output. These actions induce large amount of DNP3 traffic and cause the communication between client and server to become interrupted, triggering the Communication Alert Logic. Then, we turn off the MitTM console. After communication is restored, the Physical Contingency Alert and Control Logic successfully issues the control and increases the generators’ output to a normal range.

Since the Physical Contingency Alert and Control Logic is to ensure generators’ operation is within their limits, after the falsified control issued to generators, the dynamic model gradually reduces the output. Only when the output is out of the operating limit, the logic is triggered. Thus, the Snort detects the attack earlier than the proposed logic. The alert log of the proposed logic keeps on after the MitTM console is off; that is because the alert status will stay on for 60 seconds to notify the operators. Similar to Use Case 1, the pattern of alert logs also indicates the contingency is in cyber network since the Communication Loss is raised right after the Cyber-Physical Contingency Protection on Generator for this case.
C. Analysis of Use Case 3

For the use case of FDI on AI and FCI on AO, Figure 5(a) shows the AO data for the generators’ real power setpoint values; Figure 5(b) shows the output of real power flow from each generator; Figure 5(c) shows the alert logs from the proposed logic.

The normal operation is the same as Use Case 3. However, the cyber threat in Use Case 3 is different. In the beginning, the FCI falsify all generators’ real power output measurement to zero, and this actions triggers the alert and control logic for all monitored generators. From Figure 5(a) and 5(b), we can see all generators’ output are set to zero at the same time. With so many actions happening concurrently, the communication is interrupted early on, and it is able to be detected by the Communication Alert Logic in the RTAC. After the MiTM console is off and the communication is restored, the automatic control logic in RTAC restores generators’ output within their limits.

From Figure 5(c), we can see that the RTAC’s logic can detect the attack earlier than the Snort. There is also a False detection of attack in Snort when there is no attack. The
D. Analysis of Use Case 4

For a more complicated combination of FDI and FCI attacks, Figure 6(a) shows the AO data for generators’ real power setpoint values; Figure 6(b) shows the output of real power flow from each generator; Figure 6(c) shows the alert logs from the proposed logic.

In normal operation, the reaction in the system is the same as previous use cases. The difference of the attacks in Use Case 4 is that the extra FDI will falsify the generators’ real power output measurement after the FCI to make the operators believe the output of generator real power is normal.

From Figure 6(a), the FDI only successfully changes two generators’ AI data at first place, which are generators in Substation San Juan and Substation Riesel 1, respectively, because their setpoint control value suddenly becomes zero. After those generators’ output measurements are falsified to zero, the automatic control logic is triggered. Due to the FCI, the control of setpoints are falsified as zero. In Figure 6(b), the black line is real power output of the generator in Substation San Juan. After the first FDI, the automatic control logic was triggered. Then, the FCI set the real power output as zero so the generator reduced its output. Following a second FDI, the data was recovered to its original value. After the MitM attack is turned off and the communication between RTAC and PWDS is back, the automatic generator setpoint is issued normally and the generator’s real power output is the same value as the setpoint. The green dash line is the real power output of generator in Substation Riesel 1. Its pattern is similar to generator in Substation San Juan. Due to the latency of DNP3 event collection, there is a delay of showing the real power output becomes zero.

With the intensive data exchange among client, server and attacker, it caused the communication loss in an early stage, captured by the Communication Alert Logic. After the MitM console is turned off, the correct control commands are issued for both generators. From the Figure 6(c), we observe the Snort alert log is slightly earlier than the RTAC log, which is because of the generators’ dynamic model and polling frequency. While, the pattern of alert logs indicates the contingency is in cyber network. In Figure 6(b), it takes some time for generators’ output gets reduced and the collected data triggers the alert logic. There is also a drop of the falsified generators’ output real power because of the polling frequency and data mismatch in Wireshark.

E. Analysis of Use Case 5

Use Case 5 focuses on the physical contingency, where Substation San Juan is disconnected from the system. There are several branches in neighboring substations are affected and experiencing overflows. Figure 7(a) shows the status of all branches that are monitored in this use case, including all branches in Substation San Juan (ID: 266), one branch in Substation Edingburg 2 (ID: 244), one branch in Substation Mission 4 (ID: 265), and four branches in Substation McAllen 1 (ID: 310). Figure 7(b) shows above branches’ power flow. Figure 7(c) shows the alert logs generated by the logic. Since there is no cyber threat, there is no Snort alert log for comparison.

From Figure 7(a), all branches in the San Juan substation are disconnected (plots are overlapped). At the same time, Figure 7(c) shows there is an overflow on the monitored branches. Since there are no other actions to relieve line overflow, after 2 min, the logic automatically disconnects the overflow branch for its safety and flags the alert. However, this actions caused other branches overflow. After all monitored branches are disconnected, the overflow alert is off.
For this use case, we intentionally set a short time (2 min) to issue the predefined automatic control. In the field, the branches should have the capability to tolerate the overflow situation for a longer time. Otherwise, the protective relay should act. The logic implemented considers the protective relay fails to operate and the safety of the branch is in danger. For the protected substation, the contingency stems from physical network, so the pattern of alert logs indicates the contingency is in physical network network. From the results, we can see it is important to incorporate more actions with the control actions to ensure the overall reliability and security of the system.

VI. DISCUSSION

Unlike case studies in [32], [38], the DNP3 clients are modeled using PyDNP3 library [45]. Under the cyberattacks, there are no communication status tags like the POU Offline Status in RTAC, and the detection of cyberattacks only relies on the IDS. Therefore, the adversaries in [32] cause severe stress in the synthetic 2000-bus case. With the embedded IEC 61131 engine, RTAC provides an auxiliary method with its internal data to perform a more accurate detection for cyber-physical contingencies and provide countermeasures to interrupt the attack. And thus, it can prevent the cascading failures in the systems.

One common input for all proposed logic is the POU Offline Status, which is used to indicate the communication status:
online or offline. When the communication is interrupted, there should not be any controls, since these devices cannot be trusted to give accurate information to the operators. From the results of all use cases, the initial alert detected by the RTAC is because the issued control and updated data induce an alert tag. With automatic control actions, the logic disrupts an intruder’s steps and causes an intruder to lose control of the communication network. It shows the value of substation device logic using both cyber and physical data to identify cyber threats in the system.

From the analysis of both Snort and the proposed logic, the Snort logs detect the unusual rate of ARP cache overwrite after the MITM console starts, which provides more cyber situational awareness. However, only after the targeted DNP3 actions are issued, with two types of cyber logs (DNP3-based and ARP cache overwrite alert logs) can it help operators confirm the attack. Snort logs can also lead to False alarms, as in Use Case 1 and 3, when there is no attack in the system. Due to the stochastic nature of the systems, traditional IDSs face challenges that lead to inaccurate detection of cyber events. For pure cyber threat detection, the Snort detects the specified alerts more timely. However, as a cyber-physical system, the proposed logic detects the incidents more accurately.

On the other hand, the proposed logic provides a more accurate and timely detection and protection against adversaries. The pattern of alert logs can also be used to identify whether the contingency is in cyber network or physical network. For Use Case 1, the proposed logic detects the attack earlier than Snort after the control is issued. With the automatic control actions, the adversary runs out of resources to maintain the communication status. When communication is lost, the operators will take actions to fix the issue (In this paper, we have manually turn off the attack console). For Use Cases 2-4, the proposed logic is as accurate as the Snort logs. Due to the dynamic model of generators, Use Cases 2 and 4 detect the attack slightly slower than the Snort. However, the automatic control actions from the proposed logic disrupt the adversary’s control, and the surge of traffic interrupts the communications. The actions from the proposed logic enable Snort to detect the attack. After the communication network is restored, the control logic can immediately rescue the monitored generators by resetting their operating state to normal. In this way, the generators will be able to operate reliably through the attack. This also provides more time in the field for EMS to issue the optimal control vectors for the whole system’s security and resilience.

From Use Case 3 and 4, we can see that the attack period is much shorter. With the proposed defense logic, there will be a surge of traffic under this sophisticated attack. It will interrupt the communication, preventing the cyberattack’s function, and then notify the system about the threat in an early stage. The discontinuity of the attack could provide more situational awareness for operators, but Snort logs do not capture it. With the physical measurements in an RTAC, such situations draw more attention. This also emphasizes the importance of combining both cyber and physical data for situational awareness for cyber-physical power systems. It can be used for network reconfiguration to isolate the compromised networks with further development.

When there is no cyber threat, the proposed logic can also be used for physical contingency detection and operation. However, due to the limitation of PLCs, the control actions are pre-defined, and the logic only focuses on local devices and information. From Use Case 5, we can see that opening the overloaded branches can ensure their safety, but this action can cause other devices to be under stress, so it is only shown here as a hypothetical example which would require further coordination with operations. Thus, it is important to holistically consider the proposed logic with other enhancements to energy management system functions to better protect power systems against cyber-physical hazard scenarios.

VII. Conclusion

In this paper, we take a unique perspective to protect power systems from cyberattack with the utilization of a substation’s data concentrator device. A systematic framework is presented to design the alert and control logic using fused cyber and physical data to detect and prevent cyber and physical contingencies in power systems. The pattern of alert logs raised from the proposed logic is able to identify whether the contingency is in cyber network or physical network. In the case studies considered, the automatic control actions can effectively interrupt the attacks in cyber network to prevent the cascading failures. It also indicates that the control actions that involve both the cyber and physical domains can better protect power systems.

With the RESLab testbed, we implement the proposed logic in the RTAC and validate its effectiveness and accuracy under different cyber-induced contingencies involving the DNP3 protocol. It shows the potential of the IEC 61131 engine to protect power grids and equipment with local information. From the comparison of the proposed logic-based alerting system with a Snort alerting system, it shows the alert logs directly from the RTAC are as accurate and produces less false alarms. Moreover, the logic in the RTAC can directly execute automatic control with pre-defined actions to disrupt an adversary and protect the grid. The case studies and analyses confirm the benefits of fusing the cyber and physical data for protecting power grids against cyber and physical threats in an early stage. It also suggests the use of such hardware-based schemes with software algorithms in a next-generation cyber-physical energy management system (EMS) for protecting a power grid and its physical equipment against cyber threats.

Acknowledgements

The work described in this paper was supported by funds from the US Department of Energy under award DE-OE0000895 and the National Science Foundation under Grant 1916142.

References

Hao Huang (Graduate Student Member, IEEE): received the B.S. degree in Electrical Engineering (Power System and Its Automation) from Harbin Institute of Technology, Harbin, Heilongjiang Province, China, in 2014 and the M.S. degree in Electrical Engineering (Electric Power) from University of Southern California, Los Angeles, CA, USA, in 2016. He is currently pursuing a Ph.D. degree in Electrical Engineering at Texas A&M University with Prof. Katherine Davis. His research focuses on power system resilience, power system situational awareness, cyber-physical security, etc.

Patrick Wlazlo: received his B.S. Degree in electrical engineering systems technology and his M.S. Degree in engineering technology from Texas A&M University in 2020 and 2022 respectively. He is currently working at Vistra Corp as Development Security Operations Engineer. His research interests involve studying cybersecurity as it relates to electrical transmission and generation systems.

Zeyu Mao (Graduate Student Member, IEEE) received the B.S. degree in electrical engineering from Chongqing University, Chongqing, China, in 2015, and the M.S. degree in electrical and computer engineering from the University of Illinois at Urbana–Champaign, IL, USA, in 2017. He is currently pursuing the Ph.D. degree in electrical and computer engineering with Texas A&M University, TX, USA. His research interests include power system cyber-physical modeling, data-driven power system control, and sparse matrix ordering.

Abhijeet Sahu (Graduate Student Member, IEEE) received his B.S. degree in Electronics and Communications from National Institute of Technology, Rourkela, India, in 2011 and his M.S. degree in Electrical and Computer Engineering from Texas A&M University, TX, USA in 2018. Currently, he is a Ph.D. candidate at Texas A&M University working with Prof. Katherine Davis and Prof. Ana Goulart on the Cyber-Physical Resilient Energy Systems project. His research interests include network security, cyber-physical modeling for intrusion detection and response, and Artificial Intelligence for cyber-physical security in power systems.

Katherine R. Davis (Senior Member, IEEE): received the B.S. degree from The University of Texas at Austin, Austin, TX, USA, in 2007, and the M.S. and Ph.D. degrees from the University of Illinois at Urbana–Champaign, Champaign, IL, USA, in 2009 and 2011, respectively, all in electrical engineering. She is currently an Assistant Professor of electrical and computer engineering with Texas A&M University. Her research interests include Operation and Control of Power Systems, Interactions between Computer Networks and Power Networks, Security-oriented Cyber-physical Analysis Techniques, Data-driven and Model-based Coupled Infrastructure Analysis and Simulation.

Ana E. Goulart (Member, IEEE) received a bachelor’s degree in electrical engineering from the Federal School of Engineering of Itajuba (EFET), Brazil in 1991; a M. Sc. degree in Information Systems Management from the Pontifical Catholic University of Campinas, Brazil, in 1997; a M. Sc. in Computer Engineering at North Carolina State University, Raleigh, NC in 1998; a Ph.D. in Electrical and Computer Engineering at Georgia Tech, Atlanta, GA, in 2005. She is currently an Associate Professor in the Electronics Systems Engineering Technology program at Texas A&M University, in College Station, TX. Her research interests include protocols for real-time voice and video communications and their performance, IP-based emergency communications, last-mile communication links and cybersecurity for the SmartGrid, wireless network systems, and rural telecommunications.

Saman Zonouz (Member, IEEE) is an Associate Professor in the Electrical and Computer Engineering Department at Rutgers University. His research has been awarded by Presidential Early Career Awards for Scientists and Engineers (PECASE) by the United States President in 2019, NSF CAREER Award in 2015, and National Security Agency (NSA) Significant Research in Cyber Security in 2015. He obtained his Ph.D. in Computer Science from the University of Illinois at Urbana-Champaign.

C. M. Davis (S’03-M’05) received the B.S. degree in electrical engineering from Louisiana Tech University in 2002 and the M.S. and Ph.D. degrees from the University of Illinois Urbana-Champaign. Currently he is working at the PowerWorld corporation. His research interests include linear sensitivities, power system analysis, power system visualization, and power system contingency modeling.
This section describes the implementation of Algorithm 1-3 in the RTAC using its embedded IEC 61131 engine. IEC 61131 is an International Electrotechnical Commission (IEC) standard for programmable controllers, where IEC 61131-3 is the third part of the open international standard IEC 61131 for PLCs [46]. The IEC 61131-3 deals with basic software architecture and programming languages of the control program within PLCs. It defines three graphical and two textual programming language standards: Ladder Diagram (LD), Function Block Diagram (FBD), Structure Text (ST), Instruction List (IL), and Sequential Function Chart (SFC). This section presents the implementation of the proposed logic in RTAC using ST.

A. Communication Alert Logic

Listing 1 shows the program for Communication Alert Logic in RTAC to detect communication loss in the communication network. We focus on the communication with Substation 560, 601, 631, and 968 which contains the critical elements. The input for this logic is each substation’s POU Offline status and the output is the Alert status, represented by LED_on and LED_Off. When any of those substations’ communication is lost, the logic will assign the True to LED_on and False to LED_Off. To keep the alert signal on, there is a time-delay off function, TOF. For the connected LED light/alarm device, if the communication is back, the alert status will be turned off after a Delay (60 seconds). In this way, the connected LED lights/alarming device can notify operators the loss of communication.

```
PROGRAM Communication_Alert_Logic
VAR
  Substation560 : BOOL;
  Substation601 : BOOL;
  Substation631 : BOOL;
  Substation968 : BOOL;
  AlertStatus : BOOL;
  LED_on : BOOL;
  LED_off : BOOL;
  Delay : TIME:=T#60S;
  TOF_1 : TOF;
END_VAR

Substation560 := PWDS_Data.Substation_560_POU_Offline.stVal;
Substation601 := PWDS_Data.Substation_601_POU_Offline.stVal;
Substation631 := PWDS_Data.Substation_631_POU_Offline.stVal;
Substation968 := PWDS_Data.Substation_968_POU_Offline.stVal;
AlertStatus := Substation560 AND Substation601 AND Substation631 AND Substation968;
IF AlertStatus = TRUE THEN
  LED_on := TRUE;
  LED_off := FALSE;
ELSE
  LED_on := FALSE;
  LED_off := TRUE;
END_IF
TOF_1(IN:LED_on, PT:=Delay);
PWDS_Data.AUX1.operSet.ctVal:=TOF_1.Q;
PWDS_Data.AUX1.operClear.ctVal:=NOT(TOF_1.Q);
Listing 1: Communication Alert Logic

B. Cyber-Physical Contingency Alert and Control Logic

Listing 2 shows the Function Block to protect branches against falsified control command based on Algorithm 2. It can be used by all branches in the system with corresponding input. The input for this logic is the communication status (POU_Offline), the branch status (BranchStatus), and the control command (CloseCommand and OpenCommand). The output includes the Alert status, represented by the LED_On and LED_Off, to indicate the adversary for operators, and the automatic control command (Trip and Close) to issue the original control. Since the system status is updated based on the configuration of Polling Period in RTAC, there is a Delay in the logic to keep the control command status for the logic to validate the control command and device status. To achieve this goal, we use the on delay timer (TON) function and assign the delay with 60 seconds. If the issued control and updated status doesn’t align, the LED_On will be True and LED_Off will be False to indicate the operator about this contingency. To ensure the alert will last long enough for operators to notice, there is a HoldingTime that will keep the status constant for a set period of time (60 seconds). Besides, the logic will automatically re-send the original control command. We use the Counter to re-send the original control command 5 times with an interval of 5 seconds. The reason we want to re-send the original control command is to validate the execution of control command in the communication network. Meanwhile, it can create more traffic so that the attacker won’t have enough resource to maintain communication from attacker to targeted network. It will cause the communication lost as shown in Section V.

```
FUNCTION_BLOCK Branch_AntiAdversary_Control_Lo, V
VAR
  Trip : BOOL;
  Close : BOOL;
  TON_1 : TON;
  TON_2 : TON;
  TON_3 : TON;
  TP1 : TP;
  TP2 : TP;
  TON_offline : TON;
  TOF_Close : TOF;
  TOF_Open : TOF;
  Counter : CTU;
  Alert : BOOL := FALSE;
  HoldingTime : TIME := T#60S;
  Delay : TIME := T#60S;
  Duration : TIME := T#5S;
END_VAR

VAR_INPUT
  Offline : BOOL := FALSE;
  CloseCommand : BOOL;
  OpenCommand : BOOL;
  BranchStatus : BOOL;
END_VAR

VAR_OUTPUT
  LED_on : BOOL;
  LED_off : BOOL;
END_VAR

TOF_Close(IN:=CloseCommand, PT:=Delay);
TOF_Open(IN:=OpenCommand, PT:=Delay);
TON_offline(IN:=Offline, PT:=Delay);
IF TON_offline.Q = FALSE AND ((TOF_Close.Q = TRUE AND BranchStatus = FALSE) OR (TOF_Open.Q = TRUE AND BranchStatus = TRUE)) THEN
  Alert := TRUE;
```

Listing 2: Function Block
Listing 2: Branch Cyber-Physical Contingency Alert and Control Logic

C. Physical Contingency Alert and Control Logic

Listing 3 shows the Function Block for branches to monitor whether there is overflow based on Algorithm 3. The input includes the communication status (POU_Offline), the branch power flow measurement (BranchMW), and the branch limit (BranchLim). The output includes the Alert status, represented by the LED_on and LED_off, to indicate whether there is overflow, and Trip to open the overflow branch for physical safety. If the branch is experiencing overflow, the logic will assign the True to LED_on and False to LED_off. The connected alarming device will respond correspondingly to notify operators about the contingency. Since overflow can be relieved by other operations such as load shedding and generator re-dispatch, this logic will not trip the branch immediately after detecting the overflow. Unless the overflow stays too long in the system, causing physical damage to the branch, the Trip will not be executed. This is achieved using TON with the input delay, which is set as 120 seconds in this instance.

Listing 3: Branch Physical Contingency Alert and Control Logic

As mentioned prior, the RTAC doesn’t have the capability to store the entire cyber-physical dataset, so the AO control of generator setpoint value cannot be stored. Thus, unlike Listing 2, the Cyber-Physical Contingency Alert and Control Logic doesn’t apply to generators. However, the generators are operated within a range. Based on Algorithm 2 and 3, Listing 4 shows a Function Block to protect generators against falsified control command against generator setpoint to avoid the generators’ output is over limits. The input for this logic includes the communication status (POU_Offline), the generator’s online status GenStatus, the generator’s measurement (GenMW), and the generator’s operating limit (GenMax) and GenMin. Based on such information, Listing 4 will determine whether the online generator is operated within the limit. The output includes LED_on and LED_off, and a new generator setpoint AO control. If the generator is operated out of its limit, the LED_on is True and the LED_off is False. The connected device will notify the operator of this contingency. Based on the real output of the generator, the logic will automatically send an AO control command to set the output point of generator. If the output is over the maximum limit, the NewGenSet is reduced from the maximum value. If the output is under the minimum limit, the NewGenSet is increased from the minimum value. The amount of reduced/increased value depends on the input of Margin. Since the generator dynamic model changes the generator output gradually, there is also a Delay for the logic to determine the real-time value of the generator’s output. This time should consider both the data polling period in the SCADA system and the generator’s dynamic model.

FUNCTION_BLOCK Generator_Limit_Protect
VAR
  TON_1: TON;
  TP_1: TP;
  Delay: TIME := T#5S;
  Alert: BOOL := FALSE;
END_VAR
VAR_INPUT
  Offline: BOOL := FALSE;
  GenMW: REAL;
  GenMax: REAL;
  GenMin: REAL;
  GenStatus: BOOL;
  Margin: REAL;
END_VAR
VAR_OUTPUT
  NewGenSet: REAL;
  OperStatus: BOOL;
  LED_on: BOOL;
  LED_off: BOOL;
END_VAR

Counter(CU:=OperStatus, RESET:=NOT(Alert), PV:=100)

IF Offline = FALSE AND GenStatus = TRUE AND GenMW< GenMin THEN
NewGenSet := (1+Margin)*GenMin;
Alert := TRUE;
TON_1{IN:= Alert, PT:= Delay};
OperStatus := TON_1.Q;
LED_on := TRUE;
LED_off := FALSE;
ELSIF Offline = FALSE AND GenStatus = TRUE AND GenMW > GenMax THEN
NewGenSet := (1-Margin)*GenMax;
Alert := TRUE;
TON_1{IN:= Alert, PT:= Delay};
OperStatus := TON_1.Q;
LED_on := TRUE;
LED_off := FALSE;
ELSIF Offline = TRUE THEN
NewGenSet := 0;
OperStatus := FALSE;
ELSE
NewGenSet := 0;
OperStatus := FALSE;
LED_on := FALSE;
LED_off := TRUE;
END_IF

Listing 4: Generator Physical Contingency Alert and Control Logic

All control actions in List 2-4 are targeted to protect devices with local substation information, thus the automatic control to ensure the safety of monitored devices. However, with the integration of other EMS software, the input for the logic can be updated with optimal power flow solutions to better protect the system.