Received: 17 January 2024 | Revised: 8 October 2024 | Accepted: 16 December 2024

IET Cyber-Physical Systems: Theory & Applications

DOI: 10.1049/cps2.12107

The Institution of Engineering and Technology WILEY

CASE STUDY

Analysing a multi-stage cyber threat and its impact on the power system

Leen Al Homoud[1] | Namrata Barpanda[1] | Vinicius Bobato[1] | Ana Goulart[1] | Kate Davis[1] | Mark Rice[2]

[1]Texas A&M University, College Station, Texas, USA

[2]Pacific Northwest National Laboratory, Richland, Washington, USA

Correspondence

Ana Goulart and Leen Al Homoud.
Email: goulart@tamu.edu and leen.alhomoud@tamu.edu

Funding information

U.S. Department of Energy, Grant/Award Number: DE-CR0000018; National Energy Technology Laboratory, Grant/Award Number: DE-OE0000895

Abstract

Electric power systems are composed of physical and cyber sub-systems. The sub-systems depend on each other. If the cyber sub-system is compromised by a cyber threat, what is the impact on the physical system? This paper presents a case study that shows the steps of a multi-stage cyber threat involving a database injection attack, and what happens to the power system if this threat is not detected in its early stages. The threat first affects one utility but it can spread to the balancing authority, which is responsible for keeping the voltage and frequency stable in the power grid. During the cyber threat, the authors also show defence tools, such as a cyber-physical data fusion tool that displays and analyses power and cyber telemetry.

KEYWORDS

computer network security, critical infrastructures, cyber-physical systems, power system reliability, power system simulation

1 | INTRODUCTION

Accounting for communication networks and how they can be trusted adds a new layer of complexity to power systems. The challenge is that a power system is a large-scale non-linear system. Based on its electrical properties alone, to operate a power system in a reliable and resilient way is already a complex task. The problem of resilience only increases when we consider the grid as the cyber-physical system that it is.

While the goal is grid resilience, achieving it is multifaceted. A system may move towards more resilience but may never perfectly achieve it. Similar to how there is no 'perfect security,' 'perfect resilience' may also not exist. Resilience remains the target to improve towards, and it must be addressed throughout the entire life-cycle of an event. The goal is for the system to maintain its essential functions. This means planning and preventative actions at different stages of an event's life-cycle such as:

- before an event,
- during an event to withstand and maintain critical operations,
- after an event to respond and return the system to normal, reliable operation.

From each stage, a feedback loop must exist to learn from those events and improve the system's resilience at the earlier stages. Hence, resilience requires a holistic event life-cycle perspective, that is, on how a utility will prepare for, withstand, and respond to different threats, while learning from events to better plan the system [1]. The study in ref. [2] portrays this closing-the-loop holistic approach to resilience and outlines the paradigm change of resilience-based grid planning and operation.

As illustrated in Figure 1, a cyber-physical resilience life-cycle approach encompasses modelling the system with a cyber-physical model, collecting and combining cyber and physical telemetry data, detecting the event accurately, and responding and recovering quickly. With focus on electric power systems, such as the Smart Grid, this approach can help power systems to achieve cyber-physical situational awareness and intrusion response [3].

Towards this goal of resilience-based planning and operation, the work in [4] introduces a next-generation cyber-physical Energy Management System (EMS) for cyber-physical detection, situational awareness, mitigation, and response. By comparison, this paper presents a new case study to test and improve the detection and response tools of the aforementioned next-generation EMS detailed in ref. [4]. In particular, emphasis is given in this paper to the response and recovery steps, using a cyber-physical data fusion tool, which was introduced in ref. [5].

The proposed case study demonstrates a multi-stage cyber threat event and how it impacts the physical system. The multi-stage cyber threat assumes the MITRE ATT&CK framework [6]. Its design and philosophy for industrial control systems is explained in ref. [7], which is a major reference work that has helped to synthesise a lot of the steps for researchers to take. The methodologies described in our case study also follow the steps of the MITRE's ATT&CK framework.

This case study was first introduced in the authors' conference paper [8]. In particular, the context of the multi-stage cyber threat event can be understood and analysed in this paper by the stages shown in Figure 2, where the black circles show the implemented cyber threat steps: Initial Access, Persistence, Privilege Escalation, Lateral Movement and Impact. The sequence of the steps in the proposed case study is illustrated in Figure 3, which also shows where prevention, detection, mitigation, response and recovery actions apply. The Steps 1–9 in Figure 3 are explained in detail in Section 3.

One key point of this case study is its ability to decompose the assessment and detection techniques in modules and generalise the analysis and multi-step nature. While we select specific instances, techniques and communication protocols for each of these, the response and end-to-end design and testing and detection are generic. Hence, a key part of this research is indeed to help others understand what can be detected from generic models and defence tools and what adversary knowledge and specific threat hypotheses are needed and must be applied in order for the detection tools to be successful. Details (on these capabilities and limitations) of intentionally designed cyber-physical fusion-based modelling and detection are given in ref. [5] and the goal is that it does not require the defenders to know the information about the threat ahead of time, making the assessment real-time and agnostic to a priori detailed threat information.

Thus, our previous work [8] is extended with these additions:

1. The conference paper outlines a multi-stage scenario, that focused on Stage 2—persistence and privilege escalation and Stage 3—lateral movement. In ref. [8], the physical impact analysis was proposed as future work. In this paper, we add Stage 4, which is the physical impact on a generator of a Western System Coordinating Council (WSCC) 9-bus power system.
2. This paper adds more details on the implementations and challenges that would be needed for others to more easily understand and extend that work, such as an updated architecture of the testbed, details of the industrial protocols used, such as Inter-Control Centre protocol (ICCP) protocol and how it is integrated with Distributed Network Protocol 3 (DNP3).
3. The conference paper [8] did not address the analysis and visualisation of collected data but simply concluded that it was possible at an early stage using cyber-only data to detect the threat. By comparison, this paper analyses the cyber-physical features in detail using different types of graphs.
4. The conference paper [8] compared data without the attack and data with the attack. However, the physical data in the power system simulation model had not changed. Now we

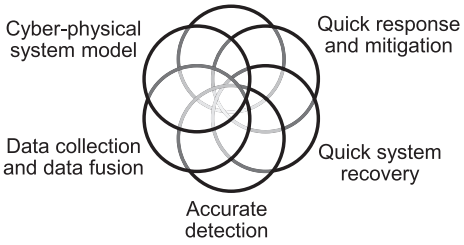

FIGURE 1 The adopted cyber-physical resilience life-cycle approach based on the cyber-physical energy management design principles outlined in [3].

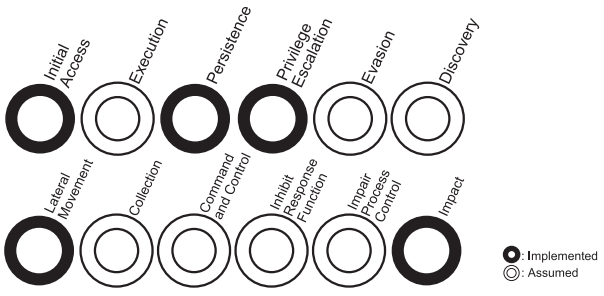

FIGURE 2 The MITRE ATT&CK threat context for this work, with its implementation and experimentation focus shown in the black circles. The MITRE context is detailed in [6, 7].

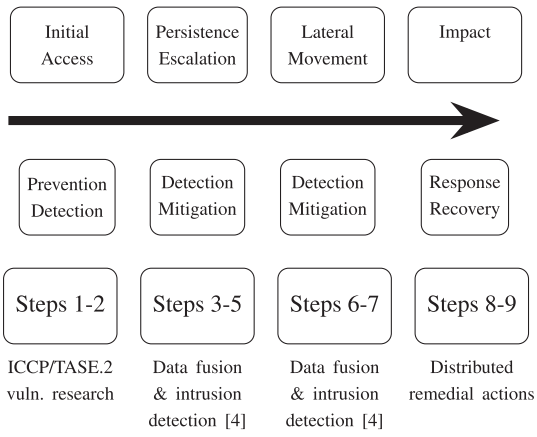

FIGURE 3 Multi-stage threat and defence using MITRE's framework. Earlier steps (i.e., Steps 1–7) were implemented in [8].

present data that has the physical impact on the 9-bus power system, and discuss changes we had to make to the power system model to protect it from frequency instability.

2 | RELATED WORK

Our goal is to show the event life-cycle of a multi-stage cyber threat and the defence against it. Previous studies have addressed multi-stage attacks in cyber-physical systems. They are also called advanced persistent threats, as in [9], where an intruder gets access to the utility's communications network. After this initial compromise, the intruder escalates privileges to perform reconnaissance on the system's operations.

Regarding threat analysis, we present a summary below of other related threat analysis work, including other testbed and *digital twin* studies, and how significant they are to our work.

In a recent study [10] on *digital twins* and testbeds, the authors did a comparative study on the MITRE ATT&CK threat context and testbeds. That work is quite related to our work. While their work addresses the broad context and how one would implement many different MITRE scenarios in the testbed, ours is very much a deeper dive into a certain use case scenario. Hence, that paper combined with this paper provides a good perspective of the combined capabilities of MITRE's framework, testbeds, and *digital twins*. Another paper [11] on testbeds differs from our work by its focus on microgrids. However, that study also follows a similar avenue as this paper. They also aim towards a very good *digital twin* or replica of the cyber-physical system so that one can rigorously study attacks and defenses in a safe environment. A recently published review article [12] sums up these points on the importance of *digital twins* or high fidelity testbed models and emulations for cyber-physical studies.

Another study [13] further connects the points of how a cyber event impacts the physical system. The authors in that paper illustrate in detail the connection between the steps of a cyber threat scenario on the cyber network side, and the physical impact. They further analyse and compare how these can lead to severe negative consequences, and in particular, cascading failures. This helps improve our understanding on how failures propagate through the physical system and the causes of the failures.

Many other papers focus on defence mechanisms and how important it is to utilise testbeds and threat scenarios to collect data. For instance, the authors in ref. [14] present an attack graph model for cyber-physical power systems using hybrid deep learning. The work in ref. [15] addresses the development and application of graph-based deep learning, and connecting it with real-world operational technology environments and real-time systems. Another work [16] also uses GNNs and offers an observability/controllability study that highlights the cyber-physical systems testbed experimentation and validation from end-to-end as a foundation for which we can validate structural detectability. These types of mathematical and data-driven models are important to develop side-by-side with realistic intrusion and defence scenarios, which is the focus of our work.

The variety of ways the threats can be effectively modelled and monitored, in risk assessment, are highly relevant to our research. In performing a risk assessment whose results will be valuable to the system stakeholders, it must capture the threat scenarios and the range of time scales. It also must contain the sufficiently high-fidelity modelling of the system assets to accurately understand the potential impacts, and for that, it also requires a strong inference mechanism, and how one pulls that data, and associates it with the models to perform the reliable and trustworthy inference to obtain the true decision support or actionable results. Thus, studies on risk analysis also have clear ties to our work, such as a recent paper assessing risk quantitatively in ref. [17] and the review of static risk-based security assessment in power systems presented in ref. [18]. This key point is further extended and evolved to dynamic risk analysis and to multi-criteria decision making based on such analyses, such as where [19, 20] review state-of-the-art works in dynamic cyber-physical risk assessment. The recent work [21] presents an approach for the analysis for distribution power systems which connects risk and resilience. It shows the diversity of the ways that such threat modelling and end-to-end risk and resilience enhancing measures are important and adopted.

In summary, these studies support and help to highlight the significance of our research and results. Furthermore, the data fusion and high-fidelity modelling of our testbed are essential proving grounds for such models, and the case study in this paper is one example.

In the next sections, we introduce the steps of the adopted multi-stage scenario. As we describe how to implement each step, we add references and related work that can provide a background on the context and the key technologies used in the adopted use case.

This paper's novelty and contribution lie in helping researchers and practitioners to understand the steps of a multi-stage cyber event, its consequences, and visualise this event's lifecycle from a cyber-physical perspective. Detection and defence are presented for two stages of the cyber threat: persistence and escalation, and physical impact. Multiple industrial communication protocols are applied and analysed for the adoption of this scenario and its defenses, including the ICCP messages between utility and balancing authority (BA) which is infrequently included in other *digital twin* platforms or case studies.

This case study's steps, implementation details, and the meaning of the cyber-physical features are described in the next sections.

3 | MULTI-STAGE THREAT SCENARIO

The communication network for this use case is shown in Figure 4. The use case assumes the intruder moves laterally from the corporate network to the public demilitarised zone, where the intruder injects false data in a utility's database. If

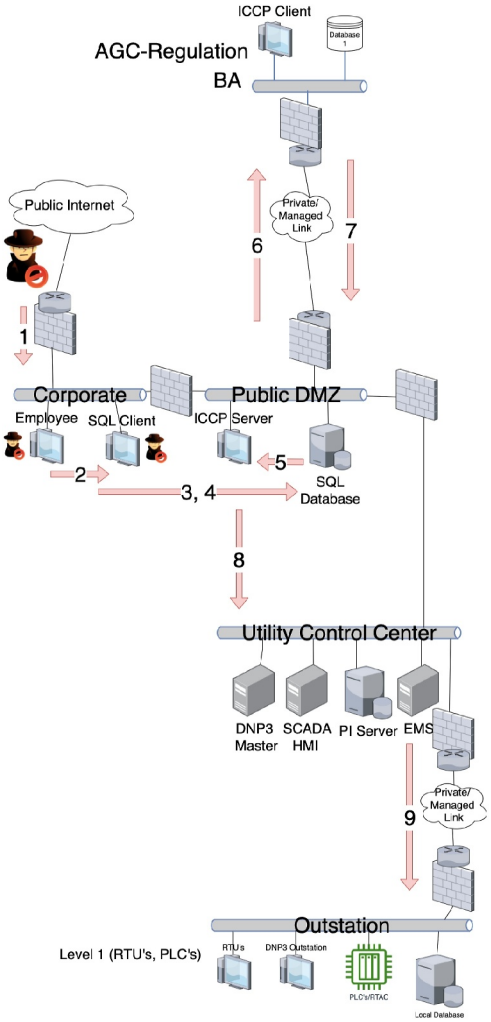

FIGURE 4 Communication network has a balancing authority (BA), corporate network, public demilitarised zone (Public DMZ), utility control centre (UCC), and outstation.

successful, this false data goes unnoticed at the BA, which calculates new setpoints. These wrongfully calculated setpoints are sent back to the utility control centre and substation.

The cascading impact of this multi-stage threat lies in the ability of the intruder to follow through this access path from the corporate network all the way to the outstation. Our main assumption is that the intruder is able to pass through all defence mechanisms undetected to consider a worst-case scenario of how a realistic and complex multi-stage threat can affect power systems. The power system in our use case is the 9-bus power system model of the WSCC (Figure 5). It has three generators and two areas. It is simulated using PowerWorld Dynamic Studio (PWDS), an interactive transient stability environment. The generators' data are retrieved from the PowerWorld Simulator using DNP3 read requests. Their responses are stored in the database.

The arrows in Figure 4 show the scenario stages as follows:

Stage 1 - Reconnaissance and Initial Access

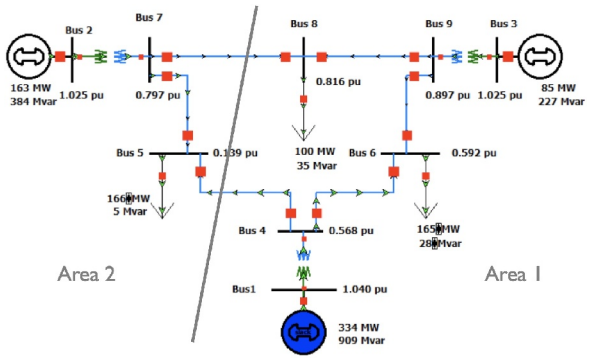

FIGURE 5 Power system scenario is the Western System Coordinating Council (WSCC) 9-bus system [8].

- **Step 1:** Intruder scans and finds an open virtual port to the corporate network.
- **Step 2:** Intruder reaches corporate network. Intruder uses an internal computer to access the utility's database.

Stage 2 - Persistence and Privilege Escalation

- **Step 3:** Intruder gets login credentials to database.
- **Step 4:** Intruder manipulates generator values in database.

Stage 3 - Lateral Movement

- **Step 5:** Utility's ICCP server reads data from database.
- **Step 6:** Utility reports false data to BA.

Stage 4 - Physical Impact

- **Step 7:** BA calculates new generator setpoint values using false data. Then, it sends a new setpoint command to this utility (or another utility).
- **Step 8:** Supervisory Control and Data Acquisition (SCADA) master receives new generation setpoints.
- **Step 9:** SCADA master sends new setpoint command to the outstation.

The progression from Stage 1 all the way to Stage 4 happens in the order of minutes. For example, after the database is modified, it takes a few steps and several messages for the false data to cause the physical impact. Thus, this scenario is not a fast attack, compared with some others, such as a man-in-the-middle (MiTM) or a fast DoS, which may cause the impact to be almost immediately experienced by the network. This is one of the reasons we are evaluating our data fusion tool. In a previous work, the data fusion tool was evaluated for a set of MiTM use cases, based on DNP3 messages [5] and cyber features, like higher round-trip times, where it is seen that, for example, small increases in the network delays on the order of milliseconds, could indicate a MiTM attack.

4 | SCENARIO IMPLEMENTATION

4.1 | Performing the SQL injection

4.1.1 | Background

The authors in ref. [9] explain the vulnerability of utility data that is stored in databases. They explain how smart metres regularly send their power consumption information to be stored in a database. Most databases use SQL—Structure Query Language—a client-server application protocol that is used to manage, programme, and query relational databases. These database are used by utilities to store physical system's data, such as power consumption and power generation information.

A common threat to these databases is called an SQL injection attack, where a malicious user injects malformed queries or runs scripts that can modify the contents of the database. If the queries are not accurately verified, then an SQL injection attack happens. As a result, data confidentiality is compromised because unauthorised users can gain access to the data, and the integrity of the data is compromised because the stored data about the physical system can be manipulated. According to ref. [9], SQL injection attacks have the potential to cause severe disruptions.

Another research study [22] shows examples of SQL injection attack on power dispatching systems, which may occur when an individual with malicious intent infiltrates the utility's network. Expanding on this issue, an IBM report [23] explains that a significant proportion (60%) of incidents targeting energy utilities in 2016 were data injection attacks.

4.1.2 | Implementation details

A web-based interface is typically used on the computer that is running the SQL client. Through this interface, the client makes requests to the SQL server, where the data is stored. If this web interface is poorly designed and does not properly validate user inputs, then there is a possibility of an SQL injection attack on the client. Any user data that is provided to a vulnerable web application and that is subsequently processed by a supporting database can be used as an SQL injection attack vector. Hypertext Transfer Protocol (HTTP) requests such as GET and POST requests are the two most frequently utilised attack channels.

In the Resilient Energy System Laboratory (RESLab) testbed, we performed Stage 2 of the scenario on the SQL's database Web interface using HTTP GET and POST requests (using the *Postman* platform). A query is sent to the authentication page. This query uses the "OR 'a'='a'" expression which causes the authentication check to be ignored [24]. Then, we can retrieve all the user data in the database such as account details, time stamps, generator values, area correction and setpoint values. We can also delete the generator data from the tables or drop the tables completely. In this study, we modified all the Generator 2 data in one of the columns of the database. Algorithm 1 shows the steps we performed.

Algorithm 1. SQL Injection on Generator SQL Server

```
1. Client sends query to log in
2. SELECT * FROM users WHERE username =
'X' AND password = 'example' OR 'a' = 'a'
3. Server returns TRUE. Bypass
 authentication
4. Client accesses data and modifies one
column
5. Use Postman API to change gen2 columnn
```

4.2 | Inter-control centre protocol

4.2.1 | Background

Utilities and software vendors continuously monitor the National Vulnerability database, which publishes vulnerabilities for different protocols. A Common Vulnerability and Exposure [25] has been found for ICCP [26, 27]. Inter-control centre protocol is a communication protocol used between control centres, such as a utility control centre reporting data to a BA or regulatory agency. Inter-control centre protocol is also known as IEC 60870–6/TASE.2, where IEC is the International Electrotechnical Commission and TASE means Telecontrol Application Service Element.

For instance, some CVEs describe how an intruder can cause problems to the SCADA system and ICCP nodes. For SCADA systems, in CVE-2022-29490, an intruder is able to login to the utility's Web interface, and then execute the SCADA system's internal scripts. For ICCP nodes, CVE-2022-2227 explains a validation flaw in ICCP messages when an adversary sends data with timestamps in the future. The ICCP node then forwards this malicious data to remote ICCP clients. If all ICCP nodes experience the same time validation flaw, it can lead to a denial-of-service (DoS) threat. This shows how an initial threat escalates and moves to other parts of the system.

Ilgner et al. [28] present an ICCP/TASE.2 message generator software tool, which can be used to test and verify the configuration of ICCP network nodes. They explain in detail the message exchange used in ICCP, which can follow two different models: a *PUSH* model in which the control centre passively receives updates from remote ICCP nodes, or a *PULL* model in which the control centre requests the information from the remote nodes. In their software tool, the performance tests were done using ICCP over Transport Layer Security (TLS), which means that the messages were encrypted. The ICCP/TASE.2 IEC 60870-6 software libraries they used [29] are the same ones we use in this paper. However, our experiment does not implement ICCP over TLS. TLS relies on

public key infrastructure (PKI) certificates [30]. According to ref. [31], the availability and interoperability between many utilities and balancing authorities becomes difficult to achieve where there is a need to manage and implement a large number of PKI certificates.

At the application layer, ICCP uses the manufacturing message specification (MMS) protocol, which is defined by the International Standards Organization (ISO) and IEC and it is named ISO/IEC-9506. It allows the exchange of real-time data among manufacturing control systems. Manufacturing message specification data format is also used in IEC 61850 protocols, for *Communication Networks and Systems in Substations*. An easy way to understand this architecture is that MMS defines how to name and format the data [27], while ICCP defines methods to request and to report data, as shown as the top of Figure 6.

Inter-control centre protocol and MMS are interoperable across different vendors, but each software implementation may have its own interface to access the ICCP libraries. Examples of software applications that use ICCP include an EMS, a SCADA database with real-time data, a historian database, and any ICCP node, such as field devices, that collects or reports data.

Manufacturing message specification has simple data types such as discrete variables to represent a state value, and real variables to represent an analog values, where even more complex data types are also represented in these ways. In ICCP, each MMS data item is called an *indication point*. A named list of MMS indication points is called a *data set*, and it needs to be agreed upon first between the two control centers.

4.2.2 | Implementation details

We assume in our experiments that the client ICCP node is the BA and the ICCP server is at the utility. We also assume the *PULL* method in ICCP. For example, in Figure 7, we can see the client, that is, the BA, requesting the list of variables for the domain *icc1* and dataset *DSTrans1*; then, the client can read those variables by sending a request to the server. The last four arrows show how the ICCP client can send a Select-Before-Operate (SBO) request followed by a new Generator 2 set-point command. A portion of this Wireshark packet capture is shown in Figure 8.

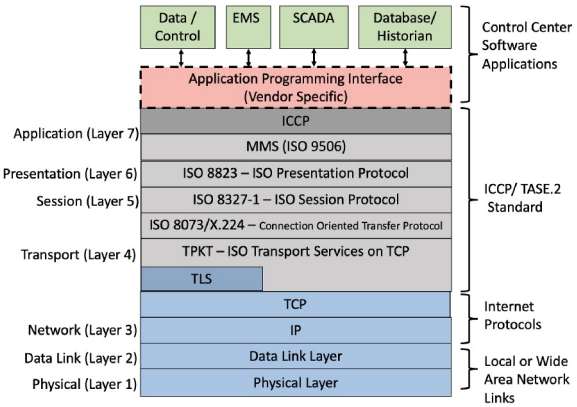

FIGURE 6 Inter-control centre protocol (ICCP) protocol stack and its software applications.

4.3 | Automatic Generation Control

4.3.1 | Background

Additionally, an important component of our multi-stage threat scenario is the Automatic Generation Control (AGC) system. An AGC receives power flow and frequency measurements from sensors at substations, and it outputs control commands to keep the frequency stable. AGC is a real-time control application, and it is sensitive to the measurements it receives. An example of an AGC attack is described in [32]. They simulated data integrity threats on AGC, and how it

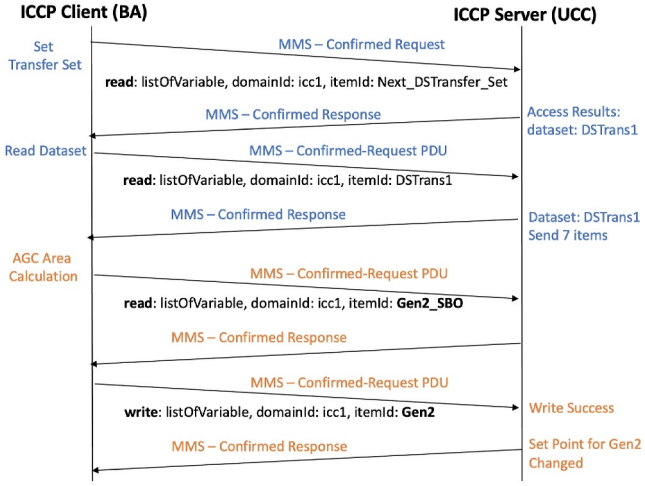

FIGURE 7 Inter-control centre protocol (ICCP) client and server exchanging data set information.

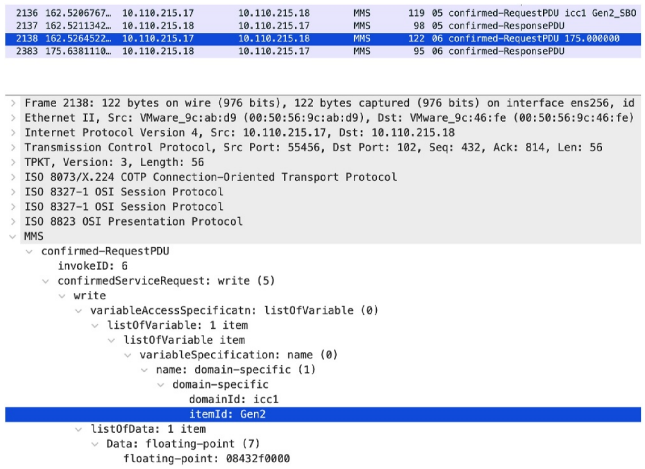

FIGURE 8 This inter-control centre protocol (ICCP) packet shows the new setpoint command of 175 MegaWatt (MW) being sent.

impacted the SCADA system. In [33], the authors studied cyber attacks that caused frequency disturbances in the power system and proposed mitigation techniques. A threat scenario where false data is injected to an AGC is presented in the paper by Sridhar and Govindarasu [34], where the AGC's integrity is compromised by corrupted measurements. Scaling, random, and pulse attacks were used to change the measurements, which triggered the AGC to modify the generator operating points, or setpoints. Their intrusion detection used machine learning models that were trained with load forecast data. The authors simulated load and generation data, but did not use any cyber data. In our paper, both the cyber and physical systems are emulated/simulated to show their real-world interactions.

For power system applications and operation, the purpose of an AGC system is to minimise the Area Control Error (ACE). The ACE is the difference between the actual and scheduled power flow between two different areas. The ACE value [35] considers the produced electricity's nominal and measured frequencies, the frequency bias factor, and the sum and initial values of the power flow, as in (1),

$$ACE = \left(f_{meas} - f_{nom}\right) * 10 * B + \left(tieflows_s - tieflows_i\right) \quad (1)$$

where f_{meas} is the measured bus frequency, f_{nom} is the nominal frequency of 60 Hz, B is the frequency bias factor in MegaWatt per 0.1 Hz or MW/0.1 Hz, $tieflows_s$ is the sum of tie flows between two areas at a specific time, and $tieflows_i$ is the initial sum of tie flows between two areas. The measured frequency f_{meas} should be close to 60 Hz with no disturbance to the system.

4.3.2 | Implementation details

To calculate the tie flows in the WSCC 9-bus model (Figure 5), four values are collected: the power flows in both directions for each of the two branches in the power system (Branches 4–5 and 7–8). Specifically, the $tieflow_s$ for Area 1 is the summation of the tie flows going from Bus 4 to 5 and Bus 8 to 7. For Area 2, the $tieflow_s$ is the summation of the tie flows going from Bus 5 to 4 and Bus 7 to 8. At the beginning of the simulation, the $tieflow_i$ is set to the initial tie flow measurement from the simulation. As the simulation runs, the tie flows are collected continually.

Once the ACE value is calculated in each area, the generation values and the participation factor $\left(P_f\right)$ for each generator in that area are used to calculate each generator's $Gen_{setpoint}$, as in (2),

$$Gen_{setpoint} = Gen - 2 * ACE * P_f \quad (2)$$

where Gen is the generator's power output, and $Gen_{setpoint}$ is generator's setpoint. For Areas 1 and 2, $Gen3$ and $Gen2$ values are used, respectively. The P_f value is assumed to be 1, meaning both generators contribute equally to changes in generation. If the data used in these calculations comes from rogue sensors or is altered, the AGC's integrity will be compromised.

5 | SCENARIO TIMELINE

To describe the timeline of events, the use case's events are illustrated in Figure 9. The implementation of the scenario uses four virtual machines (VMs) in our RESLab cyber-physical testbed [36]. To interpret the scenario and timeline, it is helpful to refer to the architecture of RESLab testbed updated for this scenario (Figure 10) which shows the VMs used and elucidates their functionalities for the scenario. The VMs are implemented using VMWare's vSphere virtualisation environment.

In the timeline, first the 9-bus simulation in PWDS (PW-DS) is launched as a continuous, real-time simulation. At the utility control centre, a Python script is launched as a DNP3 master, and it sends DNP3 read commands to the PW-DS outstations, from which it collects analog datapoints about the generators. Figure 9 shows a read command, where these are sent periodically throughout the duration of the experiment runs. The DNP3 messages are denoted by the blue arrows in Figure 9, that is, by the first two arrows and the last arrow of the overall timeline.

With the measurements it receives, the DNP3 master calculates ACE and setpoint values and stores them in the database. Both the control centre and database are hosted in the Substation A VM. This is done using a Python script at the utility control centre of our RESLab tested.

Also at Substation A VM, we assume the *Reconnaissance and Initial Access* stage has already happened. After that, an adversary performs the SQL injection step using a malicious query on the databases web interface. From this point, the adversary can log in to the database, and it can also perform other queries to change the Generator 2 data values stored in the SQL database. This corrupts the data for Generator 2. The

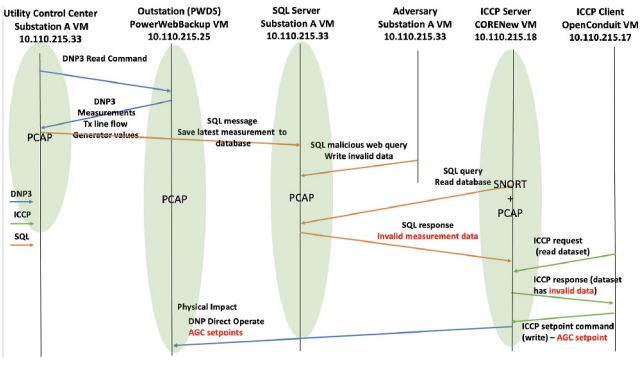

FIGURE 9 Scenario timeline include three different protocols (Distributed Network Protocol 3 (DNP3), inter-control centre protocol (ICCP), and SQL). Cyber telemetry collected at each virtual machine (VM) is shown in the oval shapes.

SQL messages are represented as light brown arrows (i.e., the four arrows after the two DNP3 arrows), in the timeline.

The ICCP Server periodically reads the SQL database, and then it sends a dataset report to the ICCP Client at the BA. In the dataset report, one of the reports includes the compromised Generator 2 data. The ICCP messages are represented as green arrows (i.e., the three arrows preceding the last arrow), in the timeline.

At the public demilitarised network, when the utility's ICCP server queries the SQL server database to get the latest measurements, the ICCP server will receive compromised data. This data is sent as an ICCP dataset to the BA.

At the BA, the AGC algorithm runs for an area, and calculates new setpoints. The ICCP client can send an ICCP *select before operate* followed by an *operate* command to update the new setpoint. We assume that these ICCP commands are sent directly to the ICCP server at the utility. The utility ICCP node also acts as a DNP3 master, and it sends the DNP3 Direct Operate command to the outstation. In the testbed, the outstation is modelled with the VM running PW-DS, which has been configured to receive commands from two different masters. As a result, the SQL injection now causes a physical impact on the power grid. This concludes our scenario timeline, and the results are illustrated in the following sections.

6 | CYBER-PHYSICAL FEATURES

Following the description of the case study in our testbed, here we explain how we test the cyber fusion detection tool and visualise the cyber-physical data at each stage of the cyber attack, which we use as a defence tool to prevent the physical system impact.

6.1 | Cyber telemetry

We ran the Wireshark packet sniffing tool to collect data packets at the utility control centre (Substation A VM), outstation (PowerWebBackup VM), and at the ICCP Server (CORENew VM). These machines are the network nodes shown in the timeline of Figure 9. In Wireshark, packets are filtered to allow Transmission Control Protocol (TCP) ports 20000 (DNP3), 102 (ICCP), 443 (secure web traffic), and 3306 (MySQL protocol).

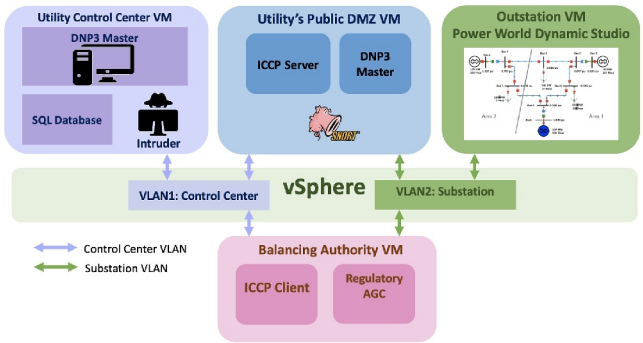

FIGURE 10 The updated RESLab testbed has four virtual machines (VMs): utility control centre VM (Substation A VM), outstation VM (PowerWebBackup VM), public demilitarised zone (DMZ) VM (CORENew VM), and balancing authority (BA) VM (OpenConduit VM).

The second component of the cyber telemetry is the intrusion detection system (IDS) logs. Using SNORT version 2.9.14–1 as the intrusion detection software, SNORT detects suspicious activity from packets, based on the rules defined in Figure 11. These rules aim to detect SQL injection using the Web interface (TCP port 443). We assume that for the specific Internet Protocol (IP) source addresses defined in this rule, the use of TCP port 443 is not normal traffic and should trigger an alarm. In Figure 12, an operator can see SNORT alert messages after the SQL injection attack.

6.2 | Physical telemetry

To calculate the ACE as in Eq. 1, eight DNP3 data points are collected, based on the WSCC 9-bus power system simulation model:

- Point0 (Gen): real power output of Generator 3 (90 MW)
- Point1 (f_{meas}): frequency of Generator 3 (59.998 Hz)
- Point2 $(tie flow)$: tie flow from Bus 5 to 4 (64.135 MW)
- Point3 $(tie flow)$: tie flow from Bus 7 to 8 (−63.4748 MW)
- Point4 (Gen): real power output of Generator 2 (126.335 MW)
- Point5 (f_{meas}): frequency of Generator 2 (59.998 Hz)
- Point6 $(tie flow)$: tie flow from Bus 4 to 5 (−63.6673 MW)
- Point7 $(tie flow)$: tie flow from Bus 8 to 7 (63.8081 MW)

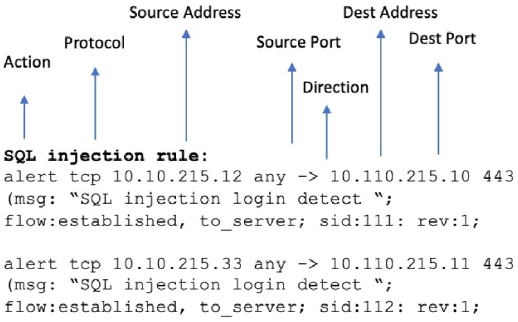

FIGURE 11 SNORT rules that check for the SQL Injection attack, on the database's Web interface (TCP port 443).

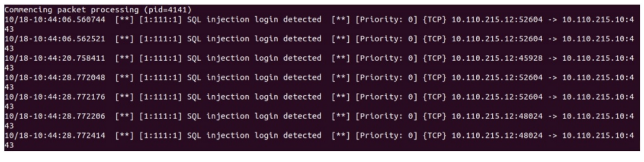

FIGURE 12 SNORT detected the SQL Injection login attack.

A view from PowerWorld's configuration of these DNP3 analog data points is shown in Figure 13. This physical system data is used to calculate the ACE and new setpoint values, which are stored in the SQL database's table shown in Figure 14. Note the ACE values for generators 2 and 3 are close to zero, which means the actual power flow almost matches the scheduled power flow. This figure also shows the result of the SQL injection attack where an intruder modified all the data in Generator 2's column to 175 MW.

6.3 | Data fusion features

Our data fusion tool [4, 5] combines information from multiple sources to produce a more complete and accurate representation of the cyber and physical sub-systems. A summary of the steps that the data fusion tool performs, as enumerated in our earlier work [8], are as follows:

- Collect packet captures using Wireshark (*cyber_table*),
- Collect logs from the IDS SNORT (*snort_table*),
- Extract physical data from DNP3 (*physical_table*),
- Extract DNP3 payload data points (*dnp3_table*),
- Merge the *snort_table* with the *cyber_table*,
- Merge *cyber_table*, *physical_table* and *dnp3_table*,
- Encode and normalise the data in the tables,
- Analyse the data using machine learning techniques. In our earlier work [8], we used an autoencoder to improve detection of the threat.

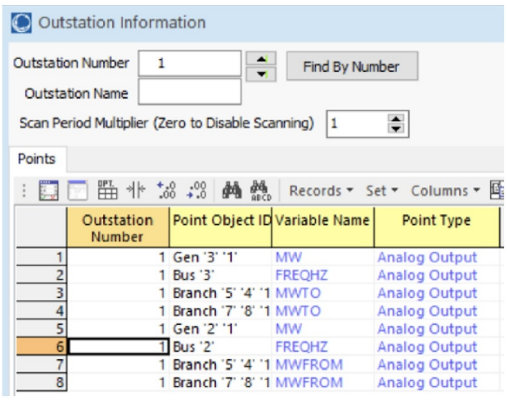

FIGURE 13 Distributed Network Protocol 3 (DNP3) data points configured in our power simulation.

id	time	gen2	gen3	ACEgen2	ACEgen3	spGen2	spGen3
1	11:27:19	175	90	0	0	126.335	90
2	11:27:19	175	90	0	0	126.335	90
3	11:27:24	175	90	-0.0001	0.0001	126.335	89.9998
4	11:27:29	175	90	0.00000000000000710543	0.0001	126.335	89.9998
5	11:27:34	175	90	0.00000000000000710543	0.0001	126.335	89.9998
6	11:27:39	175	90	0.00000000000000710543	0.0001	126.335	89.9998
7	11:27:44	175	90	0.00000000000000710543	0.00000000000000710543	126.335	90
8	11:27:49	175	90	0.00000000000000710543	0.00000000000000710543	126.335	90
9	11:27:54	175	90	0.00000000000000710543	0.00000000000000710543	126.335	90
10	11:27:59	175	90	0.00000000000000710543	0.00000000000000710543	126.335	90
11	11:28:04	175	90	0.00000000000000710543	0.00000000000000710543	126.335	90

FIGURE 14 SQL database after intruder changed Generator 2 values from 126 to 175 MW.

It is important to highlight that the cyber and physical telemetry are collected through a real-time cyber-physical emulation of the use case. As such, the physical and cyber data are correlated as a result of the inherent nature of the cyber-physical emulation setup in our testbed. In specific, the data fusion tool extracts cyber telemetry from Wireshark packet captures and SNORT alerts. This data is put in a Common Separated Value (CSV) file called a *cyber_table*. Physical telemetry comes from the information in the DNP3 packets and the power simulator. These are saved as a *physical_table*. The combination of both tables creates a *merged_table*.

Two samples of the *merged_table* are shown in Table 1, with features's values for one SQL packet sample (MySQL protocol on TCP port 3306) and also for a DNP3 packet (TCP port 20000). Both are normal traffic. The first 14 cyber features are collected from all sample packets, while features 15–24 are cyber features extracted from DNP3 headers. For example, *AL.dnp3.al.func* is the function code of the DNP3 packet. The value 129 in decimal is the same as 0x81, which is the function code for a solicited response. This packet is a response to a DNP3 read request.

At the bottom of Table 1, we have the physical features: eight DNP3 data points: Point0 to Point7. Although these data points can be considered a cyber feature, we consider them as physical features because we periodically read these values from the PW-DS outstation. In a *merged_table* the DNP3 packet (last column in Table 1) has a total of 30 features. While other packets such as SQL have only 14 cyber features.

Lastly, the feature *snort.alert* indicates whether an alert was triggered for a given packet. This feature is used to classify normal versus abnormal traffic.

7 | VISUALISING THE FEATURES

7.1 | Frame protocols and destination port

What kind of traffic is in our communication network? What is the percentage of DNP3 traffic? This information can be found by analysing feature *frame.protocols* as shown in Table 2. This feature shows the types of messages that flow through the network. It shows the packet headers at each layer of the network architecture, from the link layer, where all frames here are Ethernet frames, to the application layer such as MySQL or DNP3 protocols. Note there are only 137 DNP3 packets, or about four percent of all samples. These packets represent the communication between the DNP3 master at the utility control centre and the PW-DS outstation. These DNP3 packets have all the cyber and physical features in the *merged_table* of our data fusion tool (Table 1).

The TLS packets are exchanged between the client in the corporate network and the database's web interface. These are the *tcp:tls* packets and there are only four packets of this kind. Additionally, there are about 28 ICCP packets, or *mms* packets, which also played a role in the physical impact. The ICCP client at the BA receives modified or false data injected into the database. The four packets with frame protocol *acse:mms*

TABLE 1 Cyber-physical features.

Index	Feature	Example SQL Packet	Example DNP3 Packet
1	frame.len	132 bytes	122 bytes
2	frame.protocols	eth:ethertype:ip:tcp:mysql	eth:ethertype:ip:tcp:dnp3
3	eth.src	00:50:56:88:6b:b3	00:50:56:9c:fa:ed
4	eth.dst	00:50:56:9c:46:fe	00:50:56:9c:ce:96
5	ip.src	10.110.215.33	10.110.215.25
6	ip.dst	10.110.215.18	10.110.215.21
7	ip.len	118 bytes	108 bytes
8	ip.flags	0 × 02	0 × 02
9	tcp.srcport	3306	20000
10	tcp.dstport	38258	52887
11	tcp.len	78 bytes	68 bytes
12	tcp.flags	0 × 0018	0 × 0018
13	tcp.nxtseq	79	69
14	tcp.ack	1	19
15	LL.dnp3.src		1
16	LL.dnp3.dst		1
17	LL.dnp3.len		55
18	LL.dnp3.ctl		0 × 44
19	TL.dnp3.tr.ctl		0 x c0
20	AL.dnp3.al.func		129
21	AL.dnp3.al.ctl		0 x ca
22	AL.dnp3.obj		0 × 2803
23	DNP3.Obj. Count		8
24	DNP3.Objects		7
25	Point.0		90 MW
26	Point.1		60.1462 Hz
25	Point.2		64.1615 MW
26	Point.3		−63.4843 MW
27	Point.4		126.335 MW
28	Point.5		60.1462 Hz
29	Point.6		−63.6936 MW
30	Point.7		63.8176 MW
Label	snort.alert	0	0

include the Association Control Service Element, which means these are packets that the BA uses to send the new generator setpoint to the utility.

About the detection and defence method used in the earlier stages of our scenario, SNORT intrusion detection is able to detect malicious activity during the persistence and escalation stage. To illustrate this, Table 2 shows which packets had alerts from the SNORT intrusion detection software. We observe that the SNORT alert is detected on specific frame protocols. There are four *tcp:tls* packets and another four *ip:tcp* packets that received alarms. These alerts happened when the intruder accessed the SQL database, got its login credentials using the Web interface.

TABLE 2 Types of frames and SNORT alerts.

Type frame.protocols	Feature snort.alert	Number of Samples
eth:ethertype:ip: tcp	0	2710
eth:ethertype:ip: tcp	1	4
eth:ethertype:ip:tcp:dnp3	0	137
eth:ethertype:ip:tcp:mysql	0	425
eth:ethertype:ip:tcp:tls	1	4
eth:ethertype:ip:tcp:tpkt:cotp:ses:pres:acse:mms	0	4
eth:ethertype: ip:tcp:tpkt:cotp:ses:pres:mms	0	24

Regarding the different applications running in our scenario, a scatterplot for the destination port of each of the TCP packets is shown in Figure 15. The clients' requests have as destination port that is the *well-known* port number of their servers. Lower-numbered TCP ports in Figure 15 are ICCP on port number 102 and TCP on port 443. Other relevant protocols, such as DNP3 on port 20,000 and MySQL on 3,306, are easily observed. The larger port numbers are called ephemeral port numbers, which help us identify the connection between the client and server, as each TCP connection will have a unique pair of source and destination ports.

7.2 | Frame lengths

The feature *frame.len* tells us the total packet length that travels over the network links, including all the packet headers. This cyber feature is plotted in ascending order in Figure 16. It shows also the frequency of certain packet sizes and which packets triggered SNORT alarms (where 1 in the *x*-axis means an alarm). Most packets have small sizes, with 60 bytes as the median frame size. There are some large packets, such as one packet with 990 bytes and one packet with 1,105 bytes. Those two large packets, as well as packets with about 330 bytes, signal anomalous traffic, which is confirmed because they triggered SNORT alerts. Comparing this information with the *frame.protocols* in Table 2, we conclude that these large packets are the four *tcp:tls* packets used in the SQL injection attack.

As an additional view of the cyber feature *frame.len*, Figure 17 shows the frame length for each packet versus time, as the packets were captured during the procedure. The large outlier frames occurring a little before the 20:00 h. The time is important as we will see when we analyse the DNP3 function code and the generator values.

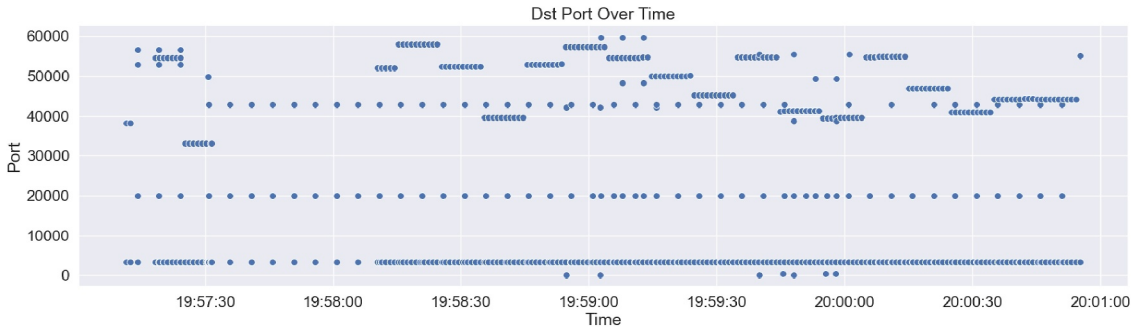

FIGURE 15 Cyber feature: TCP destination port.

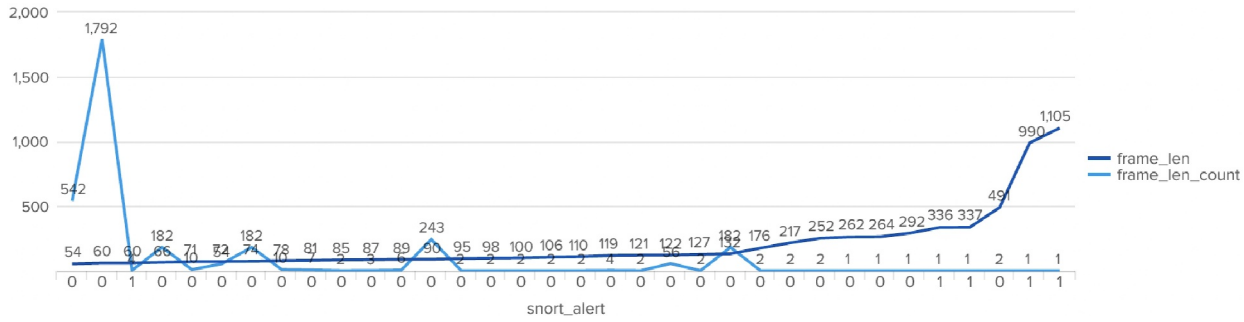

FIGURE 16 Frame lengths in bytes, in ascending order, with counts and SNORT alerts.

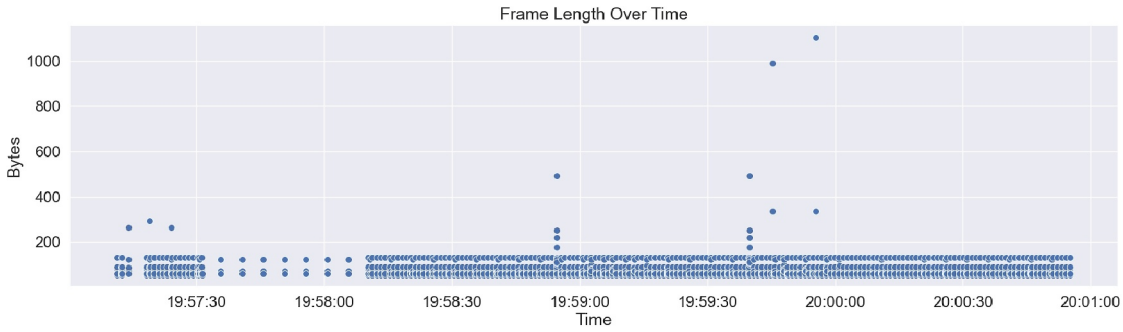

FIGURE 17 Cyber features: frame length. The database is compromised by the large frames that occurred a little before time 20:00 h.

7.3 | Distributed Network Protocol 3 function code

What types of packets did the DNP3 Master send to our 9-bus simulation model? Figure 18 shows the sequence of DNP3 function codes for the duration of the use case. There are many read requests and their responses. The important one is the *direct operate*, function code 5, which happens around time 20:00 h. It means the utility control centre sends the new setpoints to the 9-bus simulation model. This is Step 8 of our scenario, which causes the physical impact.

Figure 19 shows the number of packets with destination TCP port equal to 20,000 grouped by their function code. These packets are DNP3 requests. Most of them have function code 1, which means they are read request messages. Additional function codes and their type of request are explained in Table 3.

7.4 | Physical impact

If the SNORT alerts go undetected, the physical impact on the power system happens around time 20:00 h, as shown in Figures 20 and 21. The first figure shows the sudden change in the Generator 2 value from $126MW$ to $175MW$. This is caused by the false SQL data. This new Generator 2 value is a result of multiple actions taken by different parties throughout the attack. Upon reading the values from the database, the ICCP server forwards the value to the BA, which makes AGC calculations with false data, and reports back to the ICCP

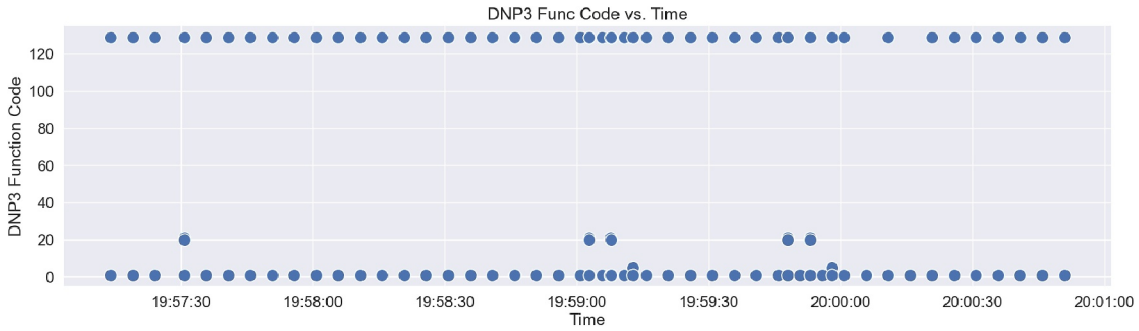

FIGURE 18 Physical feature: Distributed Network Protocol 3 (DNP3) function code. Note DNP3 function code 5, or direct operate, sent close to time 20:00 h.

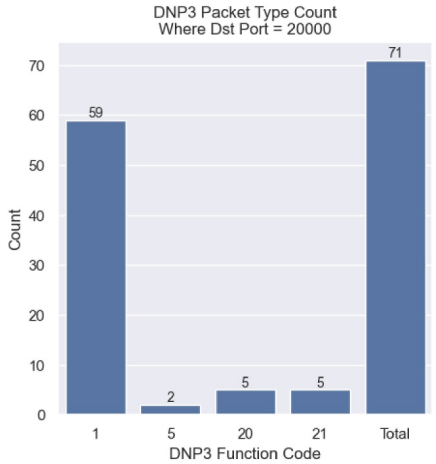

FIGURE 19 Distributed Network Protocol 3 (DNP3) function code count.

TABLE 3 Distributed Network Protocol 3 (DNP3) function codes observed in our experiment.

Function Code (Decimal)	Function Code (Hex)	DNP3 Request Type
1	0 × 01	Read
5	0 × 05	Direct operate
20	0 × 14	Enable unsolicited
21	0 × 15	Disable unsolicited
129	0 × 81	Response

server, which initiates a DNP3 *direct operate* command to Generator 2 in the outstation.

Figure 21 shows how this attack affects the power system frequency, assuming our 9-bus model does not have the dynamic model for generation control, which would control the frequency. The frequency of Generator 2 and 3 sink to values close to 0 Hz, then spike to more than 100 Hz, then changes to close to 0 Hz. It never stabilises. Because the frequency reaches very high and very low numbers, the 9-bus PowerWorld simulation case breaks. For this reason, the Powerworld simulation and the AGC configuration of the 9-bus model are

	Outstation Number	Zero-based Index	Object Type	Object ID By Number	Field Name	Analog Value
1	1	0	Gen	3 #1	MWSETPOINT	85.000
2	1	1	Bus	3	FREQHZ	60.017
3	1	2	Branch	5 TO 4 CKT 1	MWTO	74.763
4	1	3	Branch	7 TO 8 CKT 1	MWTO	-81.307
5	1	4	Gen	2 #1	MWSETPOINT	200.000
6	1	5	Bus	2	FREQHZ	60.017
7	1	6	Branch	5 TO 4 CKT 1	MWFROM	-74.080
8	1	7	Branch	7 TO 8 CKT 1	MWFROM	81.855

FIGURE 20 Physical features: Generator 2 value changes to 175 MW, after the SQL injection attack.

changed to create a defence mechanism at the physical level, as explained in the next section.

7.5 | Physical defence

Ongoing work for the presented use case is the physical system defence and how to prevent the consequence where the system frequency becomes unstable, even if false data is injected in the system and wrong setpoints are calculated by the AGC at the BA.

In order to help the system reach a steady-like state where the frequency remains somewhat constant, we had to make changes in the AGC configuration of the WSCC-9 bus system (Figure 5) on PowerWorld simulator. The adjustments made to the AGC system were a result of performing different case studies to see how different combinations of AGC configurations help stabilise the system frequency. These case studies were performed manually as this is a relatively smaller use case. The final AGC configuration adjustments include:

- Setting up two balancing authorities for the two areas within the 9-bus power system.
- Setting up an AGC for only one generator within each area. For Area 1, AGC was set up for Generator 1 (slack) but not for Generator 3, and for Area 2, AGC was set up for Generator 2.

After updating our simulation with these changes, we sent and evaluated new setpoint commands to obtain results and insight on the physical impact of the threat. To demonstrate, we send a setpoint command to change the Generator 2 from 178 to 200 MW, where Figure 22 shows the resulting valus of

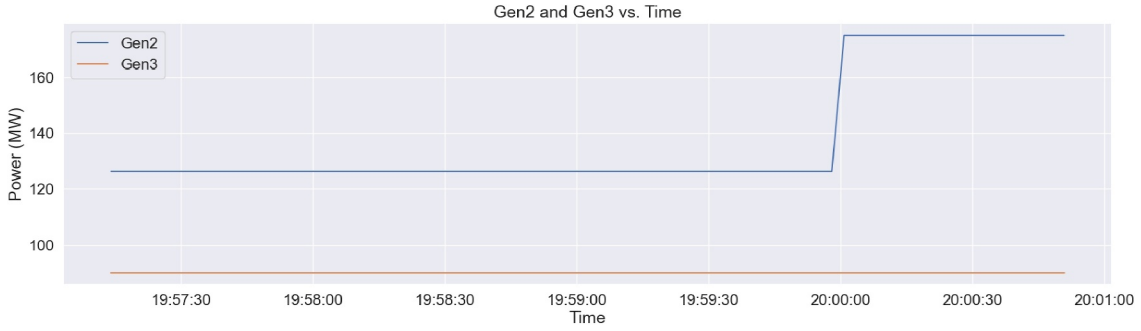

FIGURE 21 Sample of physical features: Freq 2 and Freq 3 values. The unstable frequencies beginning at time 20:00 h show the direct impact of the SQL injection in the physical system.

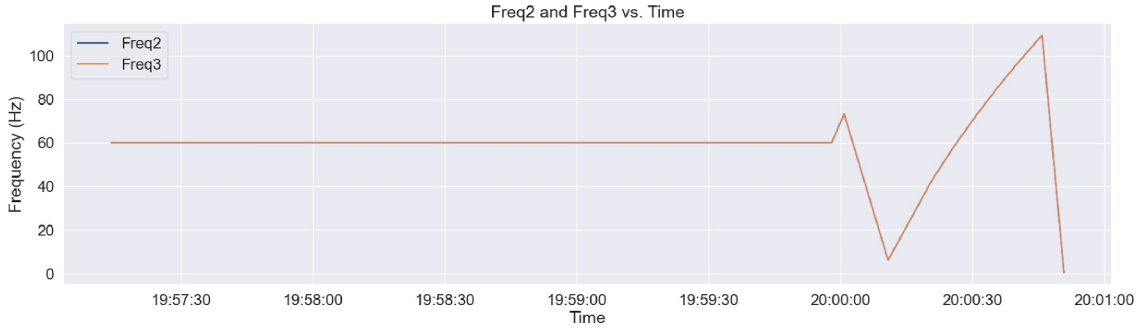

FIGURE 22 Physical values after the setpoint command to change Generator 2–200 MW.

the generator, frequency, and tie flow values in our simulation after the DNP3 *direct operate* command is sent. First, we observe that the frequency increases from 60 to 60.017 Hz, as shown in Figure 23. Additionally, the ACE values, generator values, and generator setpoints calculated by the AGC can be observed in Figures 24–26.

In Figure 24, we observe that the ACE values for each of the two areas in the system reflect the same magnitude of change, but in opposing directions. The reason for the ACE values being of the same magnitude is that we only have two areas in our power system model, which means the change in one ACE value is the same amount of change for the other area, but in opposite directions, due to the direction of the power flows. In Figure 25, we can observe the value change for when the command is sent to change the Generator 2 value from 178 to 200 MW, with the value of Generator 3 remaining unchanged at 85 MW. Since the ACE value changed, the generator setpoint values that would be sent back to the generators also change as shown in Figure 26. Specifically, the setpoint for Generator 2 has a peak value of 181 MW right after the command is sent, but saturates at 168 MW once the frequency settles. For Generator 3, the setpoint increases to 103 MW and continues to rise until it saturates at 116 MW once the frequency settles.

Ongoing investigations into the issue of frequency instability observed in our first attack have focused on optimising the transient stability models for the WSCC 9-bus system. Specifically, we have updated the synchronous machine, excitor, and governor transient stability models for all three

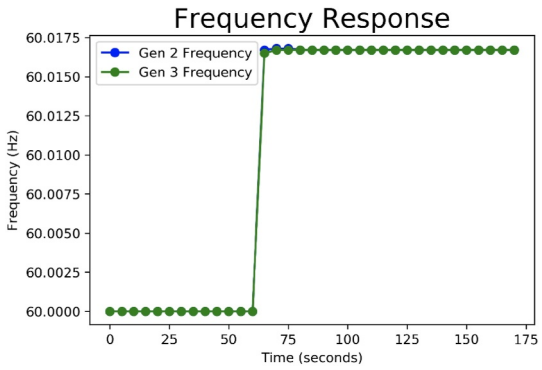

FIGURE 23 Frequency response after making changes to the Automatic Generation Control (AGC) setup in the power system simulation.

generators in the system. The inclusion of these models was a result of a set of case studies that were run to understand why the frequency was unstable following the threat. As such, the governor and excitor models were specifically added to help stabilise system frequency and allow for voltage control, respectively. Current work is ongoing to understand the stability models that should be included to ensure reaching and maintaining a stable system frequency in this use case and other threat scenarios. This work enables additional important rigorous analysis of different defence techniques' effectiveness, which is a natural next step. Further, it also provides an detailed case study and analysis that can serve as a gateway for

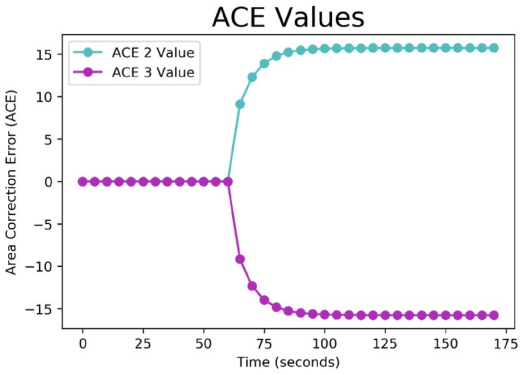

FIGURE 24 Changes in Area Control Error (ACE) values for both areas.

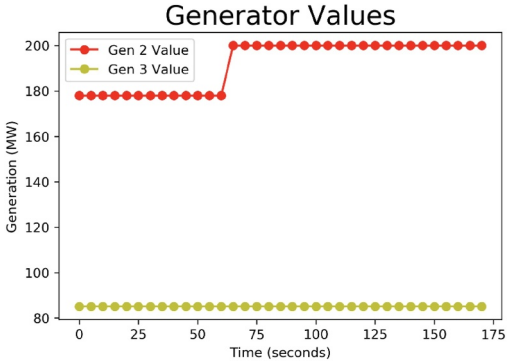

FIGURE 25 Changes in Generator 2 value after sending the command.

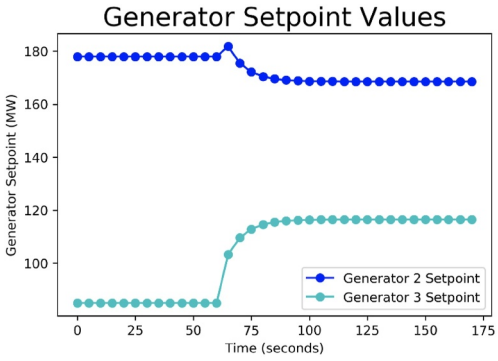

FIGURE 26 Generator setpoints for Generators 2 and 3 calculated by the Automatic Generation Control (AGC) system following the physical impact.

doing these studies in additional diverse contexts, for example, other critical infrastructures and other cyber-physical systems.

8 | CONCLUSION

The work in this paper highlights the importance of the multi-stage defence paradigm. Such defence is essential to maintaining the resilience of a system. The use case presented here shows a multi-stage threat scenario on a power utility, from Stage 1—initial access to Stage 4—physical impact. Stages 2, 3 and 4 are described in detail and they illustrate how intruders can compromise the integrity of the utility's data and cause serious consequences on its power generation system.

After integrating ICCP and DNP3 protocols in our testbed and implementing the multi-stage cyber threat, we observe physical impact. The reason is that we assume early-stage mitigation fails, that is, the intrusion detection alerts go undetected and Stage 4 is reached, to analyse and study the effect of a worst-case scenario on the system. As a consequence, we observe AGC actions, and their impact on the power system operational reliability and transient stability. After the system experienced frequency instability, we added a level of physical defence by adjusting the AGC configuration in our model. Current work is ongoing to understand the stability models that should be included as a physical defence technique to ensure reaching and maintaining a stable system frequency.

While this paper's scope is on just one use case, the results of this experiment have now enabled us to pursue in-depth defence tools, including designing and evaluating detection, mitigation, and response techniques, and even adding humans in the loop (at various roles, and in various scenarios). Such efforts would focus on modelling human behaviour into an AI-based response engine to aid in helping power system operators respond to threats and recover the system. Such AI-driven solutions can aid with providing automated and dynamic detection and mitigation of threats, which is a major focus of our future work. Other defence and analysis tools to pursue for the future work of this paper include cyber-physical interdependency quantification, real-time risk analysis and assessment, and cyber-physical network reconfiguration.

An important point is that the capabilities and motivations of potential adversaries is typically the most difficult part to figure out. For this reason, it requires a framework that can detect, analyse, and inform the response to an event, where that defence mechanism should be as *agnostic* as possible to the specific means and motivations of the adversary. Hence, the defence should be designed in support of this unknown and advanced threat model; thus, it is important to periodically make our scenarios take the following initial stance: we assume the adversary *does* get in, and we *do* see some impact indicators, *then* the question is, *how* do we respond automatically to protect the network? In this context, protection implies defence of both its physical functions (certainly, for the power grid, this includes keeping the lights on, keeping voltages and currents within normal bounds, keeping frequency within bounds, etc.) as well as its cyber functions (e.g., maintaining crucial communications while having a back up mechanism to ensure core functionalities are carried out even under severe complicated threat scenarios).

Additionally, to improve our data fusion method, we plan to extract features from the ICCP packet payload, such as the data values sent in ICCP reports. Also, we will evaluate a new protocol that is being developed for utilities and balancing authorities: the Universal Utility Data Exchange [37] protocol. It allows many utility control centres and balancing authorities

to exchange data in a secure way using new data types and a publish/subscriber messaging style. Comparative studies between both protocols will be included in future extensions of this work, as we believe the implementation, insights, and analysis would be detailed and fruitful.

AUTHOR CONTRIBUTIONS

Leen Al Homoud: Conceptualisation; data curation; investigation; software; writing - original draft. **Namrata Barpanda**: Data curation; software; visualisation; writing - original draft. **Vinicius Bobato**: Software; visualisation; writing - original draft. **Ana Goulart**: Conceptualisation; data curation; investigation; software; writing - original draft. **Kate Davis**: Conceptualisation; data curation; funding acquisition; investigation; writing - review & editing. **Mark Rice**: Conceptualisation; methodology; writing - review & editing.

ACKNOWLEDGEMENTS

This research is supported by the US Department of Energy under awards DE-OE0000895 and DE-CR0000018.

CONFLICT OF INTEREST STATEMENT

All authors declare that they have no conflicts of interest.

DATA AVAILABILITY STATEMENT

The dataset for this multi-stage threat use case, without the physical impact, can be found in reference [38] in the paper. Additional data that supports the findings of this study are available upon request from the corresponding author.

ORCID

Ana Goulart https://orcid.org/0000-0001-7184-7485

REFERENCES

1. Toroghi, S.S.H., Thomas, V.M.: A framework for the resilience analysis of electric infrastructure systems including temporary generation systems. Reliab. Eng. Syst. Saf. 202, 107013 (2020). https://doi.org/10.1016/j.ress.2020.107013
2. Overbye, T.J., Davis, K.R., Birchfield, A.B.: The electric grid and severe resiliency events. Nat. Acad. Eng. Bridge 53(2), 73–79 (2023)
3. Davis, K.: An energy management system approach for power system cyber-physical resilience. In: Invited Position Paper for Virtual Workshop on Cyber Experimentation and Science of Security (CESoS) (2021)
4. Sahu, A., et al.: Design of next-generation cyber-physical energy management systems: monitoring to mitigation. IEEE Open Access J. Power Ener. 10, 151–163 (2023). https://doi.org/10.1109/oajpe.2023.3239186
5. Sahu, A., et al.: Multi-source multi-domain data fusion for cyberattack detection in power systems. IEEE Access 9, 119118–119138 (2021). https://doi.org/10.1109/access.2021.3106873
6. MITRE: Mitre ATT&CK: ICS matrix. [Online]. https://attack.mitre.org/matrices/ics/ (2022)
7. Alexander, O., Belisle, M., Steele, J.: Mitre Att&ck for Industrial Control Systems: Design and Philosophy. The MITRE Corporation: Bedford, MA, USA. 29 (2020). [Online]. https://attack.mitre.org/docs/ATTACKforICSPhilosophyMarch2020.pdf
8. Al Homoud, L., et al.: On grid resiliency: cyber-physical detection tool evaluated in a multi-stage attack scenario. In: 2023 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm). IEEE (2023)
9. Gunduz, M.Z., Das, R.: Cyber-security on smart grid: threats and potential solutions. Comput. Network. 169, 107094 (2020). [Online]. Available:. https://doi.org/10.1016/j.comnet.2019.107094
10. Mumrez, A., et al.: Comparative study on smart grid security testbeds using mitre att&ck matrix. In: 2023 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm), pp. 1–7. IEEE (2023)
11. Lin, W., Saifuddin, M.R., Chen, B.: The design and implementation of a cyber exercise on epic microgrid testbed. In: 2023 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm), pp. 1–7. IEEE (2023)
12. Srivastava, A., et al.: Digital twins serving cybersecurity: more than a model: cybersecurity as a future benefit of digital twins 2. IEEE Power Energy Mag. 22(1), 61–71 (2024). https://doi.org/10.1109/mpe.2023.3325196
13. Rajkumar, V.S., et al.: Cyber attacks on power grids: causes and propagation of cascading failures. IEEE Access 11, 103154–103176 (2023). https://doi.org/10.1109/access.2023.3317695
14. Presekal, A., et al.: Attack graph model for cyber-physical power systems using hybrid deep learning. IEEE Trans. Smart Grid 14(5), 4007–4020 (2023). https://doi.org/10.1109/tsg.2023.3237011
15. Presekal, A., et al.: Cyber forensic analysis for operational technology using graph-based deep learning. In: 2023 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm), pp. 1–7 (2023)
16. Touhiduzzaman, M., Hahn, A., Srivastava, A.: Arcades: analysis of risk from cyberattack against defensive strategies for the power grid. IET Cyber-Phys. Syst.: Theory Applicat. 3(3), 119–128 (2018). [Online]. Available:. https://doi.org/10.1049/iet-cps.2017.0118
17. Semertzis, I., et al.: Quantitative risk assessment of cyber attacks on cyber-physical systems using attack graphs. In: 2022 10th Workshop on Modelling and Simulation of Cyber-Physical Energy Systems (MSCPES), pp. 1–6 (2022)
18. Bhuiyan, M.Z.A., et al.: Review of static risk-based security assessment in power system. IET Cyber-Phys. Syst.: Theory & Applicat. 4(3), 233–239 (2019). [Online]. Available:. https://doi.org/10.1049/iet-cps.2018.5080
19. Cheimonidis, P., Rantos, K.: Dynamic risk assessment in cybersecurity: a systematic literature review. Future Inter. 15(10), 324 (2023). https://doi.org/10.3390/fi15100324
20. Bouramdane, A.-A.: Cyberattacks in smart grids: challenges and solving the multi-criteria decision-making for cybersecurity options, including ones that incorporate artificial intelligence, using an analytical hierarchy process. J. Cybersecurit. Priv. 3(4), 662–705 (2023). https://doi.org/10.3390/jcp3040031
21. Ju, J., et al.: Resilience enhancement strategy for cyber–physical distribution systems that considers cross-space propagation of information risk. IET Renew. Power Gener. 18(7), 1193–1203 (2024). [Online]. Available:. https://doi.org/10.1049/rpg2.12767
22. Sheng, J.: Research on SQL injection attack and defense technology of power dispatching data network: based on data mining. Mobile Inf. Syst. 2022, 6207275–6207278 (2022). https://doi.org/10.1155/2022/6207275
23. Kovacs, E.: Injection Attacks Common in Energy and Utilities Sector. IBM (2017). [Online]. https://www.securityweek.com/injection-attacks-common-energy-and-utilities-sector-ibm/
24. Dougherty, C.: Practical identification of SQL injection vulnerabilities. [Online]. https://www.cisa.gov/uscert/sites/default/files/publications/Practical-SQLi-Identification.pdf (2013)
25. National Institute of Standards and Technology: NIST) - information technology laboratory. CVE-2022-2277 detail https://nvd.nist.gov/vuln/detail/CVE-2022-2277 (2022)
26. Becker, D.: "ICCP user guide: TR-107176," electric power research institute (EPRI). Tech. Rep. (1996)
27. EPRI: "Inter-Control center communications protocol (ICCP, TASE.2): threats to data security and potential solutions," electric power research institute (EPRI). Tech. Rep. (2001)
28. Ilgner, P., Cika, P., Stusek, M.: SCADA-based message generator for multi-vendor smart grids: Distributed integration and verification of tase. 2. Sensors 21(20), 6793 (2021). https://doi.org/10.3390/s21206793

29. MZ Automation: Iccp/tase.2 iec 60870-6 protocol library. [Online]. https://libiec61850.com/tase-2-iccp-protocol-library-version-1-2/ (2022)
30. Schneier, B.: Applied Cryptography: Protocols, Algorithms, and Source Code in C. John Wiley & Sons, Inc., United States (1996)
31. Rice, M.J., et al.: "Secure iccp final report," Pacific Northwest National Lab. (PNNL), Richland, WA (United States). Tech. Rep. (2017)
32. Sridhar, S., Manimaran, G.: Data integrity attacks and their impacts on scada control system. In: IEEE Power and, pp. 1–6. Energy Society General Meeting (2010)
33. Hassan, M., Roy, N., Sahabuddin, M.: Mitigation of frequency disturbance in power systems during cyber-attack. In: 2016 2nd International Conference on Electrical, Computer & Telecommunication Engineering (ICECTE), pp. 1–4. IEEE (2016)
34. Sridhar, S., Govindarasu, M.: Model-based attack detection and mitigation for automatic generation control. IEEE Trans. Smart Grid 5(2), 580–591 (2014). https://doi.org/10.1109/tsg.2014.2298195
35. "Available generation control modeling," (2022). [Online]. https://www.powerworld.com/WebHelp/Content/MainDocumentation_HTML/Available_Generation_Control_Modeling.htm
36. Sahu, A., et al.: Design and evaluation of a cyber-physical testbed for improving attack resilience of power systems. IET Cyber-Phys. Syst.: Theory Applicat. 6(4), 208–227 (2021). https://doi.org/10.1049/cps2.12018
37. Neumann, S., et al.: Universal utility data exchange (UUDEX) protocol design - revision 1 - cybersecurity of energy delivery systems (CEDS) research and development. (2021). [Online]. https://www.pnnl.gov/main/publications/external/technicalreports/PNNL-32391.pdf
38. Al Homoud, L., et al.: Dataset of a cyber-physical detection tool evaluated in a multi-stage attack scenario. IEEE Dataport (2023). [Online]. Available:. https://doi.org/10.21227/21zx-9a54

How to cite this article: Al Homoud, L., et al.: Analysing a multi-stage cyber threat and its impact on the power system. IET Cyber-Phys. Syst., Theory Appl. e12107. (2025). https://doi.org/10.1049/cps2.12107