ARCSG: Advancing Resilience of Cyber-Physical Smart Grid: An Integrated Co-Simulation Approach Incorporating Indicators of Compromise

Mohammed Asiri, Neetesh Saxena, and Pete Burnap
School of Computer Science and Informatics
Cardiff University,
Cardiff, UK
{*asirima,saxenan4,Burnapp*}*@cardiff.ac.uk*

***Abstract*—Modelling and simulation techniques offer cost-effective solutions for developing frameworks and modules that address the intertwined cyber-physical security challenges in the Smart Grid (SG) domain. While some existing co-simulation approaches consider both communication networks and power systems, they often overlook the importance of incorporating Indicators of Compromise (IOCs) in their analysis, which are crucial for detecting and mitigating cyber threats.**

In response to this gap, we introduce ARCSG, a co-simulation approach to study and enhance the resilience of complex cyber-physical power systems against cyber threats, with a particular focus on incorporating IOCs. Our design employs the Common Open Research Emulator (CORE) to emulate the cyber network and uses PowerWorld to model the power system processes. We incorporate control system components such as OpenPLC and ScadaBR. The co-simulation supports various protocols for monitoring and controlling the grid, such as Modbus, DNP3, ICCP, and PCCC. We demonstrate the effectiveness of our design by validating it through a false command attack on a PowerWorld case. Our approach aims to bolster the detection and mitigation of cyber threats by facilitating an advanced post-incident analysis. Such analysis empowers operators to rapidly identify the severity of a security violation, understand the strategies the adversary employed to initially breach security defences, and evaluate the comprehensive impact of the incident.

1. Introduction

Cyber-security has become a crucial concern in power generation, transmission, and distribution systems [13]. The potential for cyber adversaries to manipulate or fabricate data that disrupts the grid's regular functioning and causes cascading failures poses significant challenges. For instance, the European Network of Transmission System Operators for Electricity (ENTSO-E) experienced a breach in its administrative systems. The breach of transmission compromised 42 transmission systems across 35 member states in Europe [28]. Additionally, well-known attacks such as those in Ukraine [7] and Pivnichna [26] have resulted in power outages, while Stuxnet [4] gained control over Programmable Logic Controllers (PLCs) in a nuclear plant. These events reveal the need for corporate organizations and government agencies to strengthen their power systems to withstand any digital attack.

Implementing a continuous, efficient, real-time monitoring and cyber-physical security assessment for heightened situational awareness is essential. This implementation can help ensure a secure, dependable, and resilient Smart Grid (SG). Moreover, such a system can detect various cyber-physical attacks and quantify and mitigate their impacts [5]. In recent years, the frequency and severity of cyber-attacks on SGs have increased, resulting in blackouts and, in some cases, the loss of sensitive information [24]. These attacks can disrupt power system applications, such as demand response, voltage control, and device control over wide area networks, as well as impair the decision-making capabilities of Independent System Operators (ISOs) or Regional Transmission Organizations (RTOs) within their Energy Management Systems (EMS). This disruption can further result in cascading failures and instability within the grid. In addition to the fact that compromised confidential power system information may provoke improper actions by operators, cyber-physical attacks can ultimately cause permanent physical damage to power devices in the field. This paper aims to address these challenges and improve overall system security by designing and evaluating a co-simulation framework for cyber-physical SG.

1.1. Context and Motivation

The SG has become instrumental in addressing the escalating global energy demands. The incorporation of sophisticated computing, communication, and control technologies engenders a highly efficient and robust power system. This intelligent network facilitates the seamless integration of renewable energy sources, demand-side management, and enhanced grid reliability, among other benefits [16]. Nonetheless, as the SG continually evolves and integrates with cutting-edge technologies, the power system becomes more susceptible to cybersecurity threats. These threats pose potentially catastrophic consequences for the power system and its stakeholders. These potential risks underscore the necessity of fortifying the smart grid's resilience and security against cyber-physical attacks.

Developing a cyber-physical co-simulator to identify and recognise Indicators of Compromise (IOCs) of security incidents is essential for a more comprehensive understanding of cyber-physical attacks and their impacts on power systems. This co-simulator can help deepen the understanding of cyber-physical attacks' behaviour on

power systems and identify effective mitigation strategies for cyber-attacks [24].

The motivation for this work stems from the need for a holistic and unified framework capable of facilitating an in-depth understanding of the SG's operations while offering valuable insights for detecting and identifying potential cyber-physical attacks related footprints. Existing research in SG security mainly focuses on individual aspects, such as vulnerability assessments, intrusion detection systems, and encryption techniques. While these approaches are valuable, they may not fully encapsulate the intricacies of the SG's interconnected cyber and physical components. Hence, the co-simulator is a valuable resource for the broader research community and forensic analysts, facilitating efforts to enhance system resilience to cyber threats and conduct thorough incident analyses [29].

1.2. Challenges and Contributions

Previous research on SG simulation tools has identified a gap in existing solutions, which usually concentrate on either power systems or communication networks [5] [20]. To overcome this limitation, some efforts have introduced an integrated cyber-physical co-simulator capable of simultaneously modelling and simulating both power systems and communication networks. The co-simulator should assess potential vulnerability states, system state changes, and situational awareness under various cyber-attacks. Accurate modelling and simulation of the dynamic behaviour of smart networks present significant challenges due to the system's extensive and intricate nature, consisting of thousands of sensors, electrical devices, transmission and distribution lines, communication nodes, routers, and authentication servers. A critical aspect of this research is to understand and characterise the dynamic behaviour and interdependencies between communication and electrical systems within this vast network, along with the role of IOCs in detecting and responding to threats. Current co-simulations and testbeds within the realm of SG security have made considerable progress in evaluating and addressing cyber-physical risks. Nevertheless, these efforts are fraught with various obstacles and constraints. Some of the most prominent challenges and limitations are as follows:

• *Complexity and Scalability:* The SG has a complex, large-scale, varied architecture with many interconnected components. Existing co-simulations and testbeds may not adequately model and mimic such a complex system, limiting their ability to evaluate cyber-physical threats.

• *Interoperability:* Many co-simulations and testbeds use various tools, platforms, and standards, which might cause problems. Customising and developing tools and platforms to build a unified simulation environment is difficult.

• *Cyber-Physical Coupling:* The main problem of co-simulation is how to represent the smart grid's cyber-physical interdependencies. Many co-simulations and testbeds focus on cyber or physical components, neglecting their linkages and dependencies and disregarding coupling risks.

• *Demanding Decision Making:*Understanding the immediate effects of cyber-physical attacks and assessing response plans requires quick and complete observation. During a cyber-physical attack, decision-makers must quickly assess the situation and make decisions that could have a major impact on the security of the system. These decisions are often made under pressure and with limited information, which can make them even more challenging.

• *Insufficient Attack Data:* The varied data formats of indicators of compromise (IOCs) add a layer of complexity to their integration, as co-simulation systems often require to handle the combination of multi-source data. The accuracy of IOCs can influence the effectiveness of threat detection, with inaccurate or incomplete data leading to false positives or negatives.

Our main objective in this work is to develop a comprehensive and integrated co-simulation environment that accurately represents a cyber-physical power system and monitors attacker activities. Such activities are simulated and based on real-world attack patterns, replicating the tactics and procedures an actual attacker might employ. To this end, our main contributions are three-fold:

1. The design of a scalable representation of power system and network infrastructure: By incorporating the Common Open Research Emulator (CORE) network emulator to represent the three network zones (internet, corporate, and industrial), the co-simulation provides a more comprehensive understanding of the end-to-end communication infrastructure and its impact on the security of the SG network.
2. The development of an integrated cyber-physical simulation: The co-simulation combines the capabilities of OpenPLC, ScadaBR, and PowerWorld to create an integrated environment that represent both the cyber and physical aspects of the power system. This integrated approach can help operators at utilities to understand the complex interactions between the cyber and physical systems, and to identify potential vulnerabilities that could be exploited by attackers.
3. The development of a security analytics module to monitor the cyber-physical power system for potential attack footprints. This module involves data collection, analysis, and evaluation of potential indicators using techniques and tools for incident analysis, which are integrated within the co-simulation environment. This can help operators at utilities to identify potential attacks early, before they have a chance to cause significant damage

2. Related Work

Co-simulation of power systems and communication networks has gradually become scholars' favourite option as the power system is restructured. Table 1 summarises the associated research in this direction. Each co-simulation tool is evaluated based on its target SG application, network and power simulators used, scalability, and IOCs monitoring capability. Scalability is measured on the capacity to handle an increasing number of heterogeneous simulators and manage the interconnected relationships for simulating large-scale complex systems. Lin *et al.* [15] proposed a Global Event-Driven Co-Simulation (GECO) framework to study power systems and communication networks as a single distributed cyber-physical system.

TABLE 1: COMPARISON OF INTEGRATED POWER/NETWORK SIMULATORS

Ref	Target	Network Simulator	Power System Simulator	Scalability	Monitoring IOCs
[24] CPSA	Power system monitoring	GridSim	PowerWorld/MATLAB	High	partially
[6] GridSim	Wide area measurement systems	GridStat	TSTAT	Moderate	✗
[14] VPNET	Network control	OPNET	Virtual Test Bed (VTB)	Low	✗
[17] TASSCS	SCADA security	OPNET	PowerWorld	High	✗
[8] FNCS	Real-time pricing	NS-3	PowerFlow/ GridLAB-D	High	✗
[12] EPOCHS	Wide area measurement systems	NS-32	PSLF	High	✗
[15] GECO	Wide area measurement systems	NS-2	PSLF	High	✗
[23] OPNET/Simulink	SCADA security	OPNET/OMNeT ++	Simulink	-	partially
ARCSG	Power system monitoring	CORE	PowerWorld	High	✓

They found that the framework could improve the investigation of smart grids and evaluate wide area measurement/control schemes. However, this system could not address cybersecurity concerns or provide guidelines for selecting appropriate simulation parameters. The co-simulator Cyber-Physical Situational Awareness (CPSA) was used to evaluate the impact of malicious commands on CPS [24]. The tool could also detect bad measurement data in real-time and provide visualisation dashboards to guide operators to take actions to mitigate the impacts of cyber-attacks. Electric Power and Communication Synchronizing Simulator (EPOCHS) [12], integrated multiple research and commercial off-the-shelf systems, was used to address the gap between existing models and real-world scenarios involving networked control of power grids. VPNET, an integration of Virtual Test Bed (VTB) software with OPNET, was introduced in [14] for simulating remotely operated power electronic devices in the system. The synchronisation approach employed in this paper is similar to that utilised by EPOCHS. The co-simulation coordinator samples receive values from both simulators using a global simulation time step. It collects the same kinds of system defects as EPOCHS. Rajkumar and Manzur [6] developed a simulation toolkit called GridSim to model and simulate entities in parallel and distributed computer systems. GridSim creates diverse resources for computation and data-intensive applications. A resource's processing nodes can vary in capability, configuration, and availability. Another form of merging power systems with communication networks, featuring the establishment of a SCADA cybersecurity testbed, was presented in [17]. The main purpose of this testbed was to assess the power system communication infrastructure's susceptibility to cyber assaults. Based on this objective, static power system simulations are sufficient, and synchronisation concerns can be disregarded. Similarly, SCADA cyber security test bed, which integrates Simulink and OPNET/OMNeT ++, was proposed in [23]. The Framework for Network Co-Simulation (FNCS) co-simulation platform was developed by the Pacific Northwest National Laboratory (PNNL) for dynamic simulations of transmission and distribution systems [8]. These co-simulations primarily focus on studying the impact analysis of attacks and potential threats that may contribute to grid instability. However, differently from ARCSG, most of the existing work has not considered forensic analysis and collecting threat information in their frameworks. Our approach uniquely combines these two critical components, which leads to enhanced incident investigation and better decision-making. By incorporating forensic analysis, we can gather crucial details about the nature of attacks, enabling a more thorough understanding of the attacker's techniques, tools, and objectives. Meanwhile, the collection of threat information allows for a better grasp of the current threat landscape and helps prioritise resources effectively.

3. Proposed System Architecture

In this section, we introduce the design and configuration of our co-simulation framework tailored for cyber-physical power systems. We delve into the primary elements of the architecture and elaborate on their functions and the interplay among them. Next, we highlight the system's hierarchical structure and modular nature, which facilitates the smooth incorporation of diverse models and ensures efficient co-simulation execution.

3.1. Functional Requirements

In this section, we outline the core functionalities and capacities of ARCSG. Designed to tackle the intricate challenges in simulating cyber-physical power systems, these features cater to the unique demands of researchers and industry experts in this field. Our co-simulation framework can execute the following functions:

(1) Provide flexibility to model a large-scale grid system by linking power systems, control centres, and communication networks.
(2) Model and analyse a cyber-physical attack to assess grid stability, resilience, and security.
(3) Provide a modular and customisable co-simulation environment for diverse research needs and requirements.
(4) Generate and collect logs from different components and identify suspicious events, which helps operators to perform forensic analysis and respond quickly to such events.

3.2. ARCSG System Module

This subsection presents various sub-modules constituting ARCSG environment. A high-level representation of the considered architecture is provided in Figure 1. This figure illustrates an example that includes one substation and one control centre, along with their components and data flows. The primary data flow depicted in Figure 1 is Modbus traffic. This traffic originates from the control centre, where a Modbus master and SCADA server function as the central control and Human-Machine Interface (HMI) applications. At the substation level, a Modbus outstation (PLC/Remote Terminal Unit(RTU)) gathers data from field devices for monitoring.

Devices, such as RTUs and relays at the bay level monitor system status, collect data and manage physical

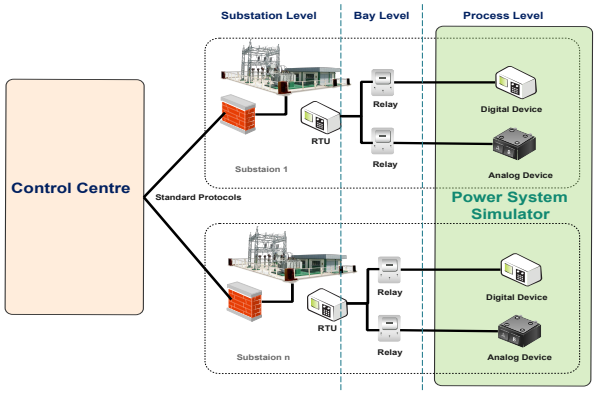

Figure 1: Power system architecture with substations and control centre

analogue and digital devices at the process level. Physical devices encompass circuit breakers, referred to as digital devices due to their two states, and generators and load, called analogue devices. Relays can trip circuit breakers to disconnect a faulty circuit. Data from the process level, collected by instrument transformers, for example, is consolidated in RTUs before being transferred to the substation level. Within the control centre, the PLC master gathers information from each substation and provides a comprehensive view for understanding and controlling the system. An Intrusion Detection System (IDS) is mirrored at the connected port of every substation and at the control centre. The following sub-modules constitute the developed system:

3.2.1. Cyber Communication Module. To represent realistic communication networks, we employ Common Open Research Emulator (CORE), a network emulator that provides a framework for running various applications such as iptables for firewalls, Snort for intrusion detection, and services such as Secure Shell (SSH) for remote access. CORE, an open-source network emulator developed by the United States Naval Research Laboratory, is used to emulate SG networks in [27], in which the authors analysed prior works on co-simulation and discovered CORE to be suitable for large-scale simulations. The software enables the establishment of many BSD jails, similar to Linux containers, that can be coupled to build communication networks. These containers are used to emulate routers, firewalls, personal computers, and Linux servers in the communication network. CORE can also connect to external networking devices and vSphere-hosted VMs via the hosts' Ethernet connections.

As illustrated in Figure 2, the CORE tool is hosted as one of the VMs in our simulator, with each of its virtual network interfaces connected to distinct VLANs to simulate a wide-area network (WAN) between the substations and the control centre. CORE also contains a bridge connecting the Energy Management System (EMS) application that analyses real-time traffic from PowerWorld as well as network traffic in CORE. The WAN configuration has direct links between the control centre's gateway routers and the substation subnets. The routes in this architecture are built by running Quagga [25] services and are designed to use the Open Shortest Path First (OSPF) protocol. Figure 2 shows the logical connections between the cyber and physical system from left to right: (1) VM running CORE, (2) VM hosting the PLC master and HMI, which are OpenPLC and ScadaBR in our system design, and (3) Host machine that implements the power system functions. As shown in Figure 2, we consider the network topology of a typical ICS network based on the Purdue standard architecture for ICS. A virtual interface connects the control centre systems to the CORE. In this direction, the interface passes the power system information from the control centre to the RTUs and back to the control centre. In the same way, another interface connects the VM running the large-scale synthetic electric case in PowerWorld with the control centre.

3.2.2. Control Centre Module. This module comprises OpenPLC and ScadaBR, which represent the control centre and serve as the key components in modelling the cyber-physical power system. While OpenPLC and ScadaBR may not be widely deployed in the real world, they are designed to use the same protocols and closely have similar functionalities to those of their proprietary counterparts.

• ***Modbus Master:*** This module monitors and controls various devices and equipment within the system. We employ an open-source PLC called OpenPLC to act as the Modbus Master in the control centre. In SCADA systems, PLCs are commonly employed as control devices due to their built-in input and output modules and processing capabilities for executing control logic. Various PLC providers exist, with Allen-Bradley, Siemens, Schneider (formerly Modicon), and Omron being among the most well-known PLC providers. However, these commercial devices feature closed-source implementations. This means vendors do not disclose hardware and firmware information necessary for virtualisation.

Consequently, much of the research on virtual SCADA testbeds relies on actual PLCs as hardware-in-the-loop [11], network-level emulators that solely simulate the SCADA protocols utilised by PLCs [18], or basic programs often written in scripting languages like Python to substitute the logic carried out by the PLC without offering equivalent programming functionality [19].

To virtualise a complete PLC, including its programming capabilities and network protocols, the most viable approach is to utilise an open-source PLC that allows for virtualisation and customisation. Doing so ensures compatibility with the developed virtual environment. To this end, we use an OpenPLC controller to run as a Modbus master in the proposed co-simulator [4].

OpenPLC supports multiple communication protocols, including DNP3, Modbus, and IEC 61850. It enables seamless interaction with a diverse range of devices and systems in industrial automation and control applications. Modbus/TCP, in particular, is widely adopted by electric utility companies for communication between various equipment [9]. This protocol employs a master/slave architecture, where one Modbus master can be configured to communicate with multiple Modbus slaves (outstations) in a distributed network configuration. Alternatively, the setup can involve a single Modbus master communicating with just one Modbus outstation.

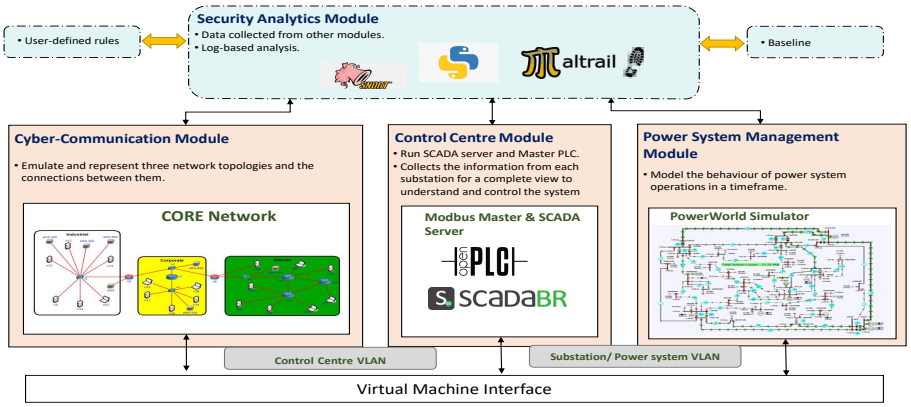

Figure 2: The logical connections between cyber-physical components

In our system module, the OpenPLC Modbus master constantly monitors the condition of circuit breakers, generators, and loads within the slave outstations operating in the PowerWorld simulator VM. An overcurrent protection relay control logic is implemented on the OpenPLC to monitor the overcurrent relays and control the breaker based on the relay's trip signal. Therefore, the OpenPLC forwards the responses of the Modbus slave outstations and communication status to the SCADA server locally using Modbus TCP, which is supported by both platforms. The OpenPLC can be customised to modify polling rates and display real-time traffic. Thus, The OpenPLC polling rate was set to 100 ms (10 Hz), a sufficient rate to monitor the station in real-time.

• ***SCADA Server:*** The SCADA Server module is specifically designed for operators to analyse the CPS system behaviour based on the process information provided by the Modbus master module. In our system, we use ScadaBR as the SCADA Server. In a real-world scenario, the HMI is a critical component of the SCADA system. This interface allows operators to interface with the system successfully. The HMI serves as the primary interface for remote monitoring and control. There are two types of HMIs: (i) physical HMIs, which are integrated with the process panel and automation devices and (ii) software-based HMIs, which run on computers in the control room.

Physical HMIs can be difficult to virtualise because of their proprietary, closed-source nature, which prohibits access to critical firmware and hardware information. Software-based HMIs, on the other hand, are easier to implement in virtual environments because they do not require virtualisation. ScadaBR, an open-source HMI program, is used and configured as a SCADA server in this module.

ScadaBR is a Java-based application compatible with various operating systems, including Windows and Linux. It is compatible with any platform that supports an application server, such as Apache Tomcat. ScadaBR, which was originally created by MCA Sistemas and is now provided under an open-source licence, allows for smooth integration into the virtual environment [1].

The ScadaBR in our proposed tool receives data from the Modbus master, including slave outstation responses and the current state of the power system. This application analyses this data and displays it in a user-friendly interface, allowing operators to monitor and control the system effectively. In this direction, the operator can issue control commands to the Modbus master, which are then forwarded to the Modbus slaves. ScadaBR also supports a variety of communication protocols and ensures compatibility with numerous devices and systems in industrial automation and control applications. As ScadaBR software provides support for Modbus, the communication channel with OpenPLC Modbus master was straightforward.

3.2.3. Power System Management Module. The Power System Management Module is a critical component of the CPS system. It is designed to supervise and scrutinise the power generation system to maintain stability and achieve optimal efficiency. In our implementation, we select PowerWorld as the foundation for this module.

PowerWorld, a highly-regarded and widely-employed power system simulation software, is designed to visualise, simulate, and analyse power systems. The software is extensively utilised in various settings, such as electric utilities, industrial plants, and research institutions, for power system planning, operation, and analysis purposes.

As a widely-used simulation tool, PowerWorld enables in-depth analysis of power systems [3]. With its capabilities, the software can conduct power flow analysis on systems encompassing up to 250,000 buses. In addition, PowerWorld offers an interface to carry out other analyses, including transient stability, optimal power flow, voltage stability, and contingency analysis. To control the simulator from the Modbus slave outstation, we employ Simulator Automation Server (SimAuto) as a COM object, seamlessly integrating it with our SCADA system.

• ***Connection Interface between PowerWorld and the Slave Outstation:*** SimAuto is a component of the PowerWorld software bundle that enables automated simulation control and interaction. SimAuto exposes a set of functions and interfaces that allow users to manipulate and access the simulator's capabilities and features programmatically. This automation server allows PowerWorld Simulator to be integrated with external applications, scripts, or custom programmes. The slave modbus cannot directly interface with PowerWorld. It must be done through SimAuto. In this direction, the OpenPLC slave aggregates and fetches data through SimAuto. Then, it reprocesses the flow measurements and sends them through Modbus/TCP back to the OpenPLC master. The interface between the power system and the slave modbus

is governed by SimAuto (OpenPLC slave outstation ⇔ SimAuto ⇔ PowerWorld).

3.2.4. Secuirty Aanlytics Module. This module is specifically designed for operators to analyse the behaviour of the CPS system based on various observations provided by other modules. To this end, we developed Python scripts that facilitate data aggregation and analysis, enabling pattern recognition and anomaly detection using predefined rules. Snort, an intrusion detection system, is employed to monitor network traffic for known attack signatures and suspicious activities. Additionally, the Maltrail framework is utilised at the endpoint and network level to investigate network traffic and uncover behavioural irregularities by leveraging publicly available heuristic analysis and blacklists [2]. Lastly, continuous baseline comparisons reveal deviations in system behaviour that may indicate potential cyber-attacks or malfunctions.

By integrating these tools, the module not only provides operators with a comprehensive understanding of the system's security but also enhances their accuracy in detecting IOCs. This involves identifying the footprints of various attacks, such as the source and impact on the system, from log files that reveal event timelines. Subsequently, operators can utilise additional tools for in-depth analysis to respond efficiently to emerging threats and maintain system resilience.

4. Applications of the Developed Co-Simulator

The co-simulator has been designed to be scalable. It can handle everything from a small power system with a few ten buses to a large system with tens of thousands of buses. The simulator can monitor both the behaviour of the real-time system and the impact of cyber-attacks on the power system. This tool is generally useful for the following power systems' applications:

4.1. Multi-Protocol Cyber Network Generation

One significant application of our co-simulation is the capacity to build and develop cyber networks for diverse industrial protocols. These protocols include Modbus TCP/UDP, DNP3, Programmable Controller Communication Commands (PCCC), and IEC 61850. This functionality enables smooth integration and communication across diverse industrial systems, demonstrating our co-simulator's versatility and applicability to a wide range of applications in the power and automation industries. This extends its potential use cases beyond power systems to various industries, such as oil and gas and water.

4.2. Cyber-Physical Behavior Impact Monitoring

• ***Behaviour-based Detection***: The cyber-physical monitoring application in our co-simulation improves system visibility and security by tracking communication logs and events across many components. In this scenario, the communication system logs events at the control centre, slave outstation, firewall, and routers. These logs contain message details, timings, sender and receiver information, and the route taken by each communication.
On the other hand, host-based monitoring systems such as ScadaBR can monitor data points, events, and alarms created by the system via its internal database. OpenPLC, which primarily focuses on PLC programming and execution, includes enhanced logging and monitoring tools for tracking mistakes, data table changes, and cycle times.

The monitoring module allows users to establish unique rules, such as permissible operational limitations, to ensure the integrity of control commands. The module logs and extracts relevant information as a JSON file if any suspicious activity is detected. An alert is sent to the operator if a control command violates the power system's health. This application also allows for aggregating and normalising log files acquired from various components. In the event of a security issue, IOCs are used to correlate and examine log files. This technique enables forensic analysts to create a timeline of events and identify additional artefacts to determine the source of the attack and analyse its impact on the affected asset.
• ***Intrusion Detection System (IDS)***: The IDS is installed at both the substation and the control centre. This system monitors Modbus packets transmitted and received by the substation's OpenPLC slave. It acts as a second line of defence. If the packet is suspected of being malicious, the IDS sends a notification (an alarm) to the control centre. Snort, an open-source solution, can be used for IDS implementation as it offers the broad capability for a customisable system [21]. Snort conducts Modbus deep packet inspection and evaluates functions on network messages. The IDS combines its signature with behavioural analysis from the previous module to protect the system from known, unknown, and advanced threats. Detecting suspicious behaviour considers various parameters, including measurement data thresholds, protocol changes, and monitoring IP addresses, port numbers, and predictable Modbus communication patterns, which are often steady in industrial networks.

• ***Power System Monitoring***: To model the power system, the IEEE 37 bus system is chosen. The system is comprised of 37 buses, 43 transmission lines, nine generators, 26 loads, 14 transformers and 12 load tap charges. It is built with three different voltage levels (69 kV, 138 kV, and 345 kV), and the system is designed per unit. The developed tool includes a capability that monitors the stability of the power system and focuses on monitoring the system's behaviour in real-time. It can also compare the system's current state to the baseline established under normal operational conditions. This comparison allows operators to correlate network communication alerts with anomalies in physical measurements, thus providing valuable insights into system performance and potential problems.

5. Evaluation and Impacts Analysis on Power Systems

In this section, we evaluate the functionality of the developed system by studying the impact of the false command attack on Modbus sessions between the control centre and outstations. The effectiveness of the attack is evaluated by examining its impact on communications and power systems.

5.1. False Command Injection

An adversary can perform a malicious command injection attack by sending a false control command, such as opening the circuit breakers, to a substation slave device (e.g. PLC or RTU) using the Modbus communication protocol. This attack aims to cause line overloading or other disruptions in the power grid [22].

If the adversary does not have complete knowledge of the system and simply injects a false command at random, the operator should be able to identify and stop the execution of the malicious command on the power system. However, if the intruder has complete or partial knowledge of the system, they can purposefully inject a specific malicious command to damage the system at large. The threat model we consider in this work is based on emulating a multi-stage attack in the large-scale synthetic system model. The attack consists of the following stages:

1) **Initial Access**: We assume the adversary gains access to a machine in the control centre. This is achieved by spear phishing activities that compromise third-party vendor user credentials, which are then used to access a dedicated workstation with privileges to carry out maintenance activities. The workstation runs a ScadaBR that constantly polls the OpenPLC master for process state and displays the status for the operator in real-time.
2) **Network Compromise**: The attacker, now with access to the control centre network, performs an ARP spoof attack, poisoning the ARP cache of both the substation's gateway and the Modbus outstation.
3) **False Command Injection**: The attacker modifies the control and monitoring traffic to have different implications on the power operations.

Algorithm 1 False Command Injection

function MODIFY_WRITE_SINGLE_COIL($recv\_pkt$)
  $openplc\_write\_coil\_ack \leftarrow recv\_pkt$[TCP].$ack$
  $mod\_pkt \leftarrow recv\_pkt$[TCP]
  DELETE($mod\_pkt.checksum$)
  $modbus\_query \leftarrow mod\_pkt.pl$[: $modbus\_query\_size$]
  $modbus\_payload \leftarrow mod\_pkt.pl[modbus\_query\_size$:]
  $modbus\_sniffed \leftarrow mod\_pkt.pl[modbus\_query\_size : coil\_loc]$
  $coil\_value \leftarrow mod\_pkt.pl[coil\_loc]$
  if $coil\_value == binary$'\x00' **then**
    $coil\_value \leftarrow binary$'\x01'
  else
    $coil\_value \leftarrow b$'\x00'
  end if
  $crafted\_pkt \leftarrow$ JOIN($modbus\_query, modbus\_sniffed,$) $coil\_value$
  $pl\_with\_crc \leftarrow$ UPDATE_CRC_PAYLOAD($crafted\_pkt$)
  $mod\_pkt.pl \leftarrow$ JOIN($modbus\_tcp\_layer, pl\_with\_crc$)
  $mod\_pkt \leftarrow$ SEND_TO_OUTSTATION(mod_pkt)
  return $mod\_pkt, openplc\_write\_coil\_ack$
end function

For this purpose, we employed Scapy, a powerful Python-based packet manipulation tool. Algrothim 1 demonstrates the procedure for performing the false command attack. The attacker focuses on the function code of a captured Modbus packet. If it is 5 (write single coil), it indicates an analogue write control command. The adversary modifies its value before forwarding the packet to the slave outstation. If the Modbus packet does not have the target function code, Scapy continues to sniff communication. To maximise the chances of success, the time between communication loops (100 ms) is exploited for the injection.

After a received packet `recv_pkt` is identified as a Modbus Write Single Coil packet, its TCP header checksum is removed, because Scapy automatically recalculates the TCP header checksum if it is not detected when forwarding the frame. The `recv_pkt`'s acknowledgement number is stored as `openplc_write_coil_ack`, so the response packet can be changed to the original value. Then, the Modbus write query is stored as `modbus_query`, and the packet's payload or `modbus_payload` is stored under `modbus_sniffed`. If the packet's data value of the circuit breaker is a CLOSE command ('00'), it is modified to be a TRIP command ('01'), or vice-versa. The Modbus payload is then reassembled by joining the `modbus_tcp_layer` and `modbus_sniffed` together as `crafted_pkt`. The reassembled payload is passed to the `update_crc_payload` function. Finally, the MAC address in the frame's header is updated to the MAC address of the OpenPLC slave outstation, and the adversary forwards the frame to the outstation.

By leveraging the capabilities we have previously discussed in the security analytics module, we can effectively identify and recognise IOCs within the CPS. This allows operators to proactively respond to potential threats, maintain system resilience, and enhance overall security.

```
11/30-07:22:15.080101  [**] [1:1111007:1] SCADA_IDS: Modbus TCP - Unauthorised
       Write Request to a PLC} [**] [Classification: Potentially Bad Traffic]
       [Priority: 1] {TCP} 172.16.192.20:43192 -> 172.16.192.30:502
11/30-07:22:15.080303  [**] [1:1111007:1] SCADA_IDS: Modbus TCP - Unauthorised
       Write Request to a PLC [**] [Classification: Potentially Bad Traffic]
       [Priority: 1] {TCP} 172.16.192.20:43192 -> 172.16.192.30:502
11/30-07:22:15.080798  [**] [1:1111007:1] SCADA_IDS: Modbus TCP - Unauthorised
       Write Request to a PLC [**] [Classification: Potentially Bad Traffic]
       [Priority: 1] {TCP} 172.16.192.20:43192 -> 172.16.192.30:502
```

Figure 3: An alert message sent from the IDS to the control centre

Footprints on the Communication Network: Under this attack, we can observe and monitor several IOCs. First, when an adversary compromises the network, they perform reconnaissance activities, such as port scanning. This reconnaissance causes sensors of material within the network to generate alert messages, as illustrated in Figure 4. These alerts demonstrate that the proposed tool can assess the performance of a security solution and identify potential bottlenecks within the tested system. The success of the proposed framework relies on the IDS's ability to detect suspicious commands based on their behaviour, goal, action, and timing. Consequently, the second IOC occurs when the IDS identifies potential ARP spoofing based on its rule-based filtering and pattern matching. Even if the IDS does not detect the malicious command and the command is successfully executed, ARCSG can achieve high accuracy of observation because the impact of each suspicious command is initially evaluated by the behaviour-based detection module. For instance, Modbus traffic between a master and a slave is highly periodic, with each communication process exhibiting its unique pattern length [10]. Therefore, another observable indicator that the behaviour-based module can monitor is the increased duration of Modbus queries. Such an increase in query time may indicate that an intruder intercepted

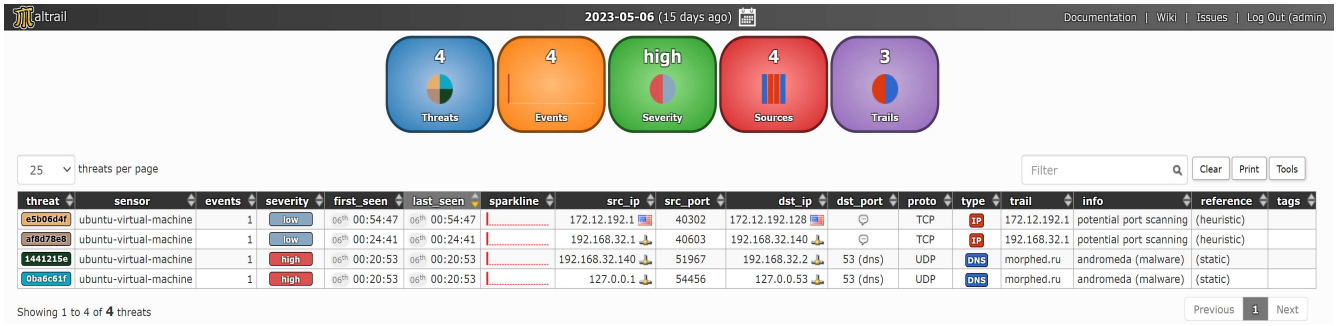

Figure 4: An alert message sent from the material sensor to the control centre.

the control command. A malicious command injection scenario is depicted in Figure 3, where the IDS alerts the system about an unauthorised command.

As mentioned in a previous section, our system maintains event logs detailing activities at intermediate routers, substation slave Modbus, and the control centre. An example of an event log captured at a slave outstation is illustrated in Figure 5. This log shows a series of normal Modbus queries, followed by a query with an increased duration. This increased query time may indicate that an intruder intercepted the control command.

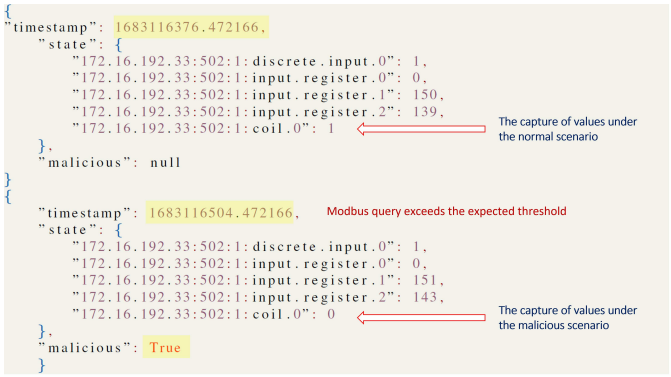

Figure 5: State monitoring between master PLC and slave outstation

Footprints on the Power System: To effectively monitor physical measurements of the power system for potential IOCs, we first identify and extract relevant indicators from the baseline module. The baseline is established by using load forecast information derived from historical data, which simulates the expected normal operational behaviour of the power system. The security module captures physical measurements every 5 seconds and compares them to the baseline profile. This comparison allows for the identification of any significant deviations from normal operations, which may serve as potential IOCs. In this scenario, one of the observations from our security analysis results indicates an increase in Aggregate Megawatt Contingency Overload (SysAMWCO) under malicious control command. The SysAMWCO is a reliable metric to measure the vulnerability of a power system to outages. A sudden increase in AMWCO could indicate that a power system is under attack. In response to detecting anomalous behaviour, the power system monitoring model promptly issues an end-user notification and generates detailed logs, as demonstrated in Figure 6.

Gen — Power System-normal scenario

Timestamp	BusNum	GenID	GenMW	GenMVR	GenMVRMa	GenMVRMin	GenVoltSet	GenMVABase	GenStatus	GenMWM	GenMWMin	GenParFac
00.00.05	14	1	0	0	5	0	1.01999998	100	Open	35	10.00000015	1
00.00.05	28	1	133.2525	-1.50511	60	-60.0000024	1.02999997	100	Closed	150	0	10
00.00.05	28	2	148.7289	-1.50511	60	-60.0000024	1.02999997	100	Closed	150	0	10
00.00.05	31	1	130.6879	49.25948	120	-89.9999976	1.02999997	100	Closed	220	0	10
00.00.05	44	1	20	24.14826	40	-20.0000003	1.01999998	100	Closed	150	20.0000003	1
00.00.05	48	1	0	0	26	-14.0000001	1	100	Open	52	15.99999964	1
00.00.05	50	1	42.09	-1.44762	33	-18.0000007	1.01999998	100	Closed	80	37.99999952	1
00.00.05	53	1	140	45	45	0	1.01999998	100	Closed	400	0	1
00.00.05	54	1	106.079	-2.18931	60	-20.0000003	1.00999999	100	Closed	110	15.0000006	1

Gen — Power System-under attack

Timestamp	BusNum	GenID	GenMW	GenMVR	GenMVRMa	GenMVRMin	GenVoltSet	GenMVABase	GenStatus	GenMWM	GenMWMin	GenParFac
00.00.10	14	1	0	0	5	0	1.01999998	100	Open	35	10.00000015	1
00.00.10	28	1	132.3747	-1.50652	60	-60.0000024	1.02999997	100	Closed	150	0	10
00.00.10	28	2	147.9868	-1.50652	60	-60.0000024	1.02999997	100	Closed	150	0	10
00.00.10	31	1	0	0	120	-89.9999976	1.02999997	100	Open	220	0	10
00.00.10	44	1	20	24.10597	40	-20.0000003	1.01999998	100	Closed	150	20.0000003	1
00.00.10	48	1	0	0	26	-14.0000001	1	100	Open	52	15.99999964	1
00.00.10	50	1	42.09	-1.51242	33	-18.0000007	1.01999998	100	Closed	80	37.99999952	1
00.00.10	53	1	140	45	45	0	1.01999998	100	Closed	400	0	1
00.00.10	54	1	106.079	-2.18931	60	-20.0000003	1.00999999	100	Closed	110	15.0000006	1

Figure 6: Normal vs. malicious command to open a generator breaker

Based on our evaluation, we claim that an ideal co-simulation should be designed to accommodate a wide range of systems and diverse applications while maintaining high scalability and low complexity during setup. By integrating innovative tools and piecing together threat artefacts within CPS co-simulation, operators can proactively respond to potential threats, maintain system resilience, and enhance overall security. Such tools enable researchers to investigate incidents, reconstruct timelines of events, and develop a deeper understanding of attack sources and their impact on the affected assets.

6. Conclusion

This research introduces an advanced co-simulation methodology that enhances cyber-resilience in intelligent electrical infrastructures. We create a robust co-simulation, ARCSG, for effective cyber-threat mitigation by integrating IOCs and employing monitoring and detection tools. A false command attack case study on a PowerWorld simulation validates our approach, demonstrating the potential for large-scale modelling and in-depth post-incident analysis.

We leverage modelling techniques and open-source control system components such as OpenPLC and ScadaBR to craft cost-effective cybersecurity solutions for SGs. Future work will incorporate the Elasticsearch tool for efficient IOC handling and real-time analysis, strengthening our capabilities to swiftly detect and respond to cyber threats. We also plan to produce real-time datasets to provide valuable insights for future threat mitigation. This research represents a significant stride towards more secure, resilient energy infrastructures.

References

[1] http://www.scadabr.com.br/. Accessed: 2023-04-16.

[2] Malicious traffic detection system. https://github.com/stamparm/maltrail. Accessed: 2023-04-16.

[3] The visual approach to electric power systems. https://www.powerworld.com/. Accessed: 2023-04-16.

[4] Thiago Rodrigues Alves, Mario Buratto, Flavio Mauricio De Souza, and Thelma Virginia Rodrigues. Openplc: An open source alternative to automation. In *IEEE Global Humanitarian Technology Conference (GHTC 2014)*, pages 585–589. IEEE, 2014.

[5] Mohammed Asiri, Neetesh Saxena, Rigel Gjomemo, and Pete Burnap. Understanding indicators of compromise against cyber-attacks in industrial control systems: A security perspective. *ACM Trans. Cyber-Phys. Syst.*, 7(2), apr 2023.

[6] Rajkumar Buyya and Manzur Murshed. Gridsim: A toolkit for the modeling and simulation of distributed resource management and scheduling for grid computing. *Concurrency and computation: practice and experience*, 14(13-15):1175–1220, 2002.

[7] Defense Use Case. Analysis of the cyber attack on the ukrainian power grid. *Electricity Information Sharing and Analysis Center (E-ISAC)*, 388:1–29, 2016.

[8] Selim Ciraci, Jeff Daily, Jason Fuller, Andrew Fisher, Laurentiu Marinovici, and Khushbu Agarwal. Fncs: A framework for power system and communication networks co-simulation. In *Proceedings of the Symposium on Theory of Modeling amp; Simulation - DEVS Integrative*, DEVS '14, San Diego, CA, USA, 2014. Society for Computer Simulation International.

[9] Paulo Régis C De Araújo, Raimir Holanda Filho, Joel JPC Rodrigues, Joao PCM Oliveira, and Stephanie A Braga. Infrastructure for integration of legacy electrical equipment into a smart-grid using wireless sensor networks. *Sensors*, 18(5):1312, 2018.

[10] Niv Goldenberg and Avishai Wool. Accurate modeling of modbus/tcp for intrusion detection in scada systems. *international journal of critical infrastructure protection*, 6(2):63–75, 2013.

[11] Hannes Holm, Martin Karresand, Arne Vidström, and Erik Westring. A survey of industrial control system testbeds. In *Secure IT Systems: 20th Nordic Conference, NordSec 2015, Stockholm, Sweden, October 19–21, 2015, Proceedings*, pages 11–26. Springer, 2015.

[12] K. Hopkinson, Xiaoru Wang, R. Giovanini, J. Thorp, K. Birman, and D. Coury. Epochs: a platform for agent-based electric power and communication simulation built from commercial off-the-shelf components. *IEEE Transactions on Power Systems*, 21(2):548–558, 2006.

[13] Tim Krause, Raphael Ernst, Benedikt Klaer, Immanuel Hacker, and Martin Henze. Cybersecurity in power grids: challenges and opportunities. *Sensors*, 21(18):6225, 2021.

[14] W. Li, A. Monti, M. Luo, and Roger A. Dougal. Vpnet: A co-simulation framework for analyzing communication channel effects on power systems. In *2011 IEEE Electric Ship Technologies Symposium*, pages 143–149, 2011.

[15] Hua Lin, Yi Deng, Sandeep Shukla, J.s Thorp, and Lamine Mili. Cyber security impacts on all-pmu state estimator – a case study on co-simulation platform geco. 11 2012.

[16] Nian Liu, Xuejun Hu, Li Ma, and Xinghuo Yu. Vulnerability assessment for coupled network consisting of power grid and ev traffic network. *IEEE Transactions on Smart Grid*, 13(1):589–598, 2021.

[17] Malaz Mallouhi, Youssif Al-Nashif, Don Cox, Tejaswini Chadaga, and Salim Hariri. A testbed for analyzing security of scada control systems (tasscs). In *ISGT 2011*, pages 1–7, 2011.

[18] Peter Maynard, Kieran McLaughlin, and Sakir Sezer. An open framework for deploying experimental scada testbed networks. In *5th International Symposium for ICS & SCADA Cyber Security Research 2018 5*, pages 92–101, 2018.

[19] Bradley Reaves and Thomas Morris. An open virtual testbed for industrial control system security research. *International Journal of Information Security*, 11:215–229, 2012.

[20] Robin Roche, Sudarshan Natarajan, Ayan Bhattacharyya, and Siddharth Suryanarayanan. A framework for co-simulation of ai tools with power systems analysis software. In *2012 23rd International Workshop on Database and Expert Systems Applications*, pages 350–354, 2012.

[21] Martin Roesch et al. Snort: Lightweight intrusion detection for networks. In *Lisa*, volume 99, pages 229–238, 1999.

[22] Ahmad Mohammad Saber, Amr Youssef, Davor Svetinovic, Hatem H Zeineldin, and Ehab F El-Saadany. Anomaly-based detection of cyberattacks on line current differential relays. *IEEE Transactions on Smart Grid*, 13(6):4787–4800, 2022.

[23] Mohammad Ashraf Hossain Sadi, Mohd. Hassan Ali, Dipankar Dasgupta, and Robert K. Abercrombie. Opnet/simulink based testbed for disturbance detection in the smart grid. In *Proceedings of the 10th Annual Cyber and Information Security Research Conference*, CISR '15, New York, NY, USA, 2015. Association for Computing Machinery.

[24] Neetesh Saxena, Victor Chukwuka, Leilei Xiong, and Santiago Grijalva. Cpsa: A cyber-physical security assessment tool for situational awareness in smart grid. In *Proceedings of the 2017 Workshop on Cyber-Physical Systems Security and PrivaCy*, CPS '17, page 69–79, New York, NY, USA, 2017. Association for Computing Machinery.

[25] Carla Schroders. Dynamic linux routing with quagga. https://www.linux.com/topic/networking/dynamic-linux-routing-quagga/.

[26] Lev Streltsov. The system of cybersecurity in ukraine: principles, actors, challenges, accomplishments. *European Journal for Security Research*, 2(2):147–184, 2017.

[27] Song Tan, Wen-Zhan Song, Qifen Dong, and Lang Tong. Score: Smart-grid common open research emulator. In *2012 IEEE third international conference on smart grid communications (SmartGridComm)*, pages 282–287. IEEE, 2012.

[28] CBR Staff Writer. High voltage attack: Eu's power grid organisation hit by hackers. https://techmonitor.ai/technology/cybersecurity/eu-power-grid-organisation-hacked. Accessed: 2023-04-16.

[29] Yue Zhang, VVG Krishnan, Jiaxing Pi, K Kaur, Anurag Srivastava, Adam Hahn, and Sindhu Suresh. Cyber physical security analytics for transactive energy systems. *IEEE Transactions on Smart Grid*, 11(2):931–941, 2019.