electronics

MDPI

Article

Innovative Testbed Configurations and Interfacing Techniques for Real-Time Digital Simulation of Cyber-Physical Energy and Power Systems

Al Hussein Dabashi [1], Dongmeng Qiu [2], Xin Zhang [2] and Gareth Taylor [1,*]

[1] Brunel Interdisciplinary Power Systems (BIPS) Research Centre, Brunel University of London, London UB8 3PH, UK; alhussein.dabashi@brunel.ac.uk
[2] Control and Power Systems (CAPS) Laboratory, University of Sheffield, Sheffield S10 2TN, UK; dqiu4@sheffield.ac.uk (D.Q.); xin.zhang1@sheffield.ac.uk (X.Z.)
* Correspondence: gareth.taylor@brunel.ac.uk

Abstract

Testbed configurations and interfacing methods for real-time digital simulation of cyber-physical power systems (CPPS) remain complex and fragmented across the literature, limiting the clarity with which researchers can compare tools, reproduce testbeds, and select suitable platforms for communication-aware control and cyber security studies. This paper addresses this issue by first comparing the latest works with particular focus on the method of interfacing and configuration architecture, and second, by showcasing two representative testbeds, used for analysing the impact of cyber events on distribution system and microgrid operation. The first testbed interfaces HYPERSIM (OPAL-RT Technologies) with MATLAB (version R2025a) using Modbus over TCP/IP for data exchange. This testbed configuration is capable of capturing the impacts of communication delays on Volt-VAR control in a modified IEEE 13-node test feeder. The second testbed uses two real-time power simulators, OPAL-RT and Typhoon HIL, both interfaced with the discrete-event simulator (DES) EXata Network Modelling (by Keysight Technologies) through modular Python-based scripts. This interfacing effectively enables the simulation of cyber attacks in microgrids. These testbeds show how recent advances in real-time simulation are enabling more practical cross-domain analysis of communication effects, control performance, and cyber vulnerabilities, while informing the design of more capable and future-ready CPPS simulation environments.

Keywords: real-time digital simulation; cyber-physical systems; cyber-physical power systems; cyber security; interoperability; hardware-in-the-loop; software-in-the-loop; discrete-event simulation; ns-3

Academic Editors: Federico Rossi, Cinzia Bernardeschi and Gloria Gori

Received: 29 May 2026
Revised: 9 August 2026
Accepted: 13 August 2026
Published: 19 August 2026

1. Introduction

1.1. Background

The increased usage of the term 'cyber-physical system' (CPS) reflects a shift in research perspective, placing greater emphasis on holistic system-level analysis rather than isolated elements such as individual components, interfaces, and processes. A CPS describes one that is heterogeneous with close interdependencies between its cyber and physical parts [1]. Examples of systems that traditionally fall under the physical domain include the following: vehicles, manufacturing plants and factories, and buildings. When sensors, communication systems and control devices, which are part of the cyber domain, are integrated into

these physical systems, they become smart/autonomous vehicles, smart manufacturing plants, and smart homes/buildings, respectively, where, due to the combination of the two domains, the holistic CPS has improved its viewability, controllability, flexibility, and its ability for automation. Besides the mentioned examples of CPS, a prominent example is a smart grid, also referred to as cyber-physical power systems (CPPS).

CPPS describe modern-day and future electrical power systems that are inseparable from their cyber technologies. These cyber technologies comprise three categories as shown in Figure 1: (1) computing parts such as sensors, instrument transformers, phasor measurement units (PMUs), intelligent electronic devices (IEDs), remote terminal units (RTUs), and programmable logic controllers (PLCs), (2) communication infrastructure such as wired and wireless communications, protocols such as International Electrotechnical Commission (IEC) 61850 and (3) control schemes such as automatic generation control (AGC), Volt-VAR Control (VVC), Load Frequency Control (LFC). Within each category, example technologies are further classified into mature/established technologies and advanced/emerging technologies based on their level of deployment maturity, operational adoption, and relevance to modern smart-grid and CPPS applications [2].

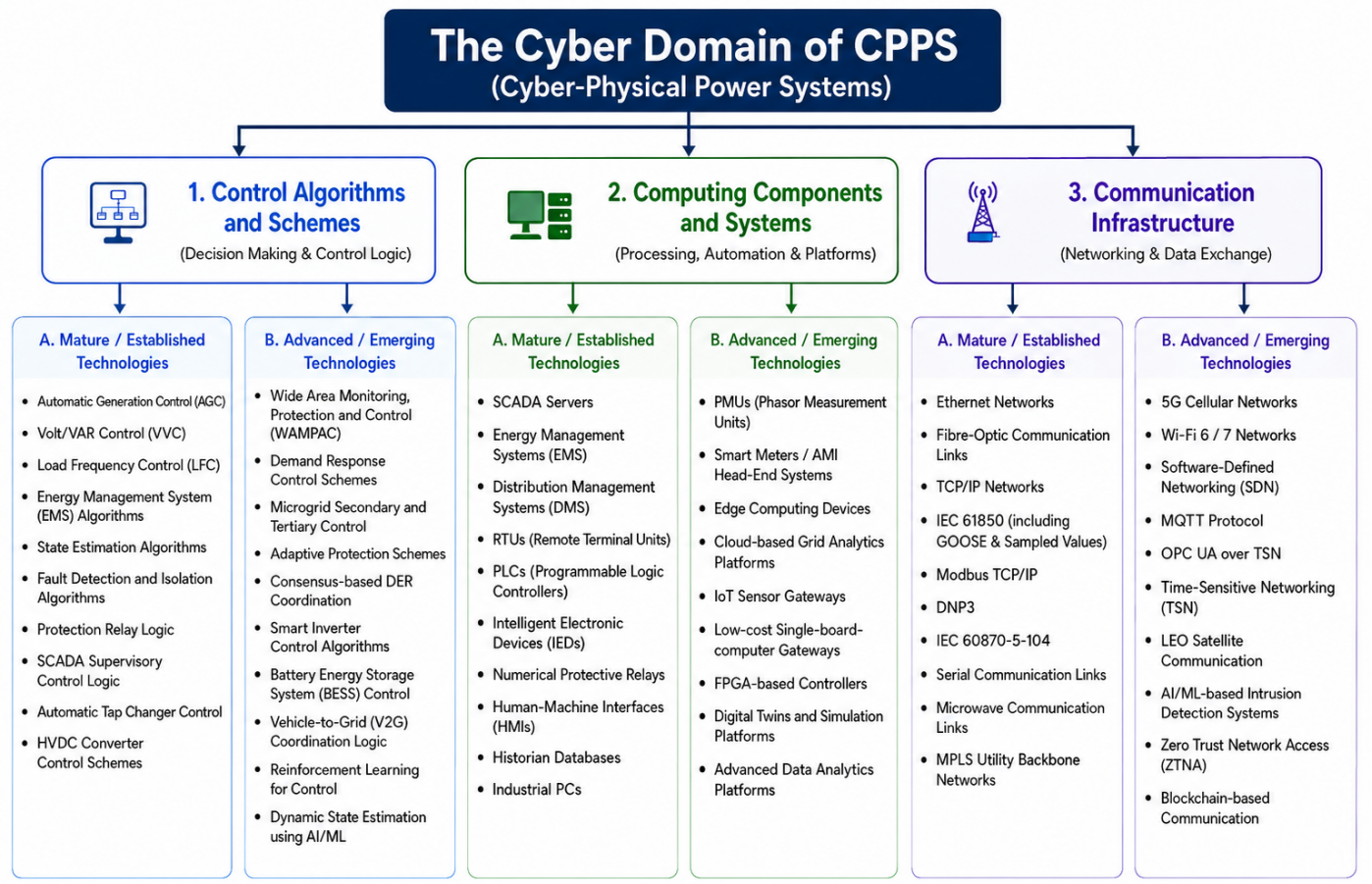

Figure 1. Overview of the cyber domain of CPPS, categorised into three principal areas: (1) control algorithms and schemes, (2) computing components and systems, and (3) communication infrastructure. Within each area, representative technologies are further classified into mature/established technologies and advanced/emerging technologies. Mature technologies include widely deployed operational systems and protocols such as supervisory control and data acquisition (SCADA), energy management systems (EMS), and IEC 61850, while advanced/emerging technologies include AI/ML-enabled control and cybersecurity methods, edge and cloud computing platforms. The figure highlights the increasing convergence of OT, IT, and advanced communication and computing paradigms within modern CPPS environments.

Unlike the physical power system domain, which is typically modelled using continuous-time or discrete-time electromagnetic and electromechanical simulation tools, many cyber-domain technologies are modelled using discrete-event simulation (DES), which focuses on packet-level communication behaviour, event scheduling, routing, latency, congestion, and protocol operation. Consequently, the physical and cyber domains inherently operate according to different simulation principles, timescales, and computational paradigms. This creates a major challenge for realistic cyber-physical analysis, since disturbances or vulnerabilities originating within the communication and control layers, such as packet loss, communication latencies, false data injection attacks (FDIAs), or denial-of-service (DoS) attacks, can propagate into the physical power system and influence stability, protection, monitoring, and operational performance. Therefore, cross-domain analysis through co-simulation, hardware-in-the-loop platforms, and integrated cyber-physical testbeds becomes essential for accurately capturing the dynamic interactions between the power, communication, and control domains of modern smart grids. In this context, interoperability becomes a central requirement, since CPPS testbeds must enable heterogeneous power-system simulators, communication-network models, control algorithms, protocols, and hardware interfaces to exchange data consistently and operate as a coordinated cyber-physical environment.

1.2. Recent Developments in CPPS Testbeds

In recent CPPS research and in response to next-generation demands, various research works employ novel interfacing techniques and unique testbed configurations to study the impacts of communication events, mainly communication latencies and different types of cyber attacks, on power system models, mainly distribution systems and microgrids. In doing so, the common simulators used for real-time power system simulation are from the Canada-based engineering companies OPAL-RT Technologies and RTDS Technologies. The prominent cyber tool used is ns-3, an open-source DES designed primarily for research and educational use, to model, experiment, and analyse the behaviour of modern communication networks.

The literature review was limited to recent CPPS studies that execute an electrical power-system model using a real-time simulation platform and interface it with a communication-network simulation or emulation environment. Studies were included where sufficient information was available regarding the selected simulators, interface method, communication protocol, synchronisation mechanism, or associated communication hardware. Studies limited to physical protection equipment, individual component digital twins, offline power-system simulation, or communication systems without an integrated real-time power-system model were excluded. Alternative co-simulation and interoperability frameworks, including HELICS, FMI/FMU, HLA, and OPC UA, remain relevant to the wider field; however, they are included in the comparative review only where their implementation satisfies these real-time cyber-physical modelling criteria.

Acharya et al. [3] focus on a deep learning-based approach for the detection, classification, and mitigation of cyber attacks in distribution systems. A CPPS testbed is employed to validate the proposed approach, structured across three layers: the physical layer, the cyber layer, and the control layer. The physical layer consists of RTDS and an RTU, which are connected through GTNETx2, which are network interface cards developed by RTDS for interacting with real external devices via protocols like IEC 61850, Modbus, and Distributed Network Protocol 3 (DNP3) over Ethernet. For the cyber layer, the authors use Wireshark to capture real-time communication traffic alongside an unspecified "communication network emulator". The control layer consists of a workstation for device configuration and HMI monitoring and a real-time automation controller (RTAC).

Haseeb et al. [4] use RTDS and ns-3 in their testbed to develop four variants of man-in-the-middle (MITM) attacks, analyse their impacts on communication latency, and introduce corresponding mitigation schemes using the US National Institute of Standards and Technology (NIST)-approved lightweight cryptography algorithm ASCON. The connection between RTDS and ns-3 is achieved using a bridging interface termed TapBridge, which acts as a virtual gateway by capturing data from RTDS, injecting it into the ns-3 network, and returning processed data back to RTDS via TCP/IP communication. This creates a closed-loop system where the physical and cyber layers interact in real time, enabling realistic analysis of communication delays and cyberattacks on power system operation.

In proving physical damage caused by cyberattacks, Masood et al. [5] show how an FDIA causes severe voltage and line loading violations, and how a DoS attack exacerbates cascading failure by preventing accurate FDIA detection. Their SIL-based testbed integrates ns-3, GridLAB-D and HELICS. GridLAB-D [6] is an open-source, agent-based power distribution system simulation software, whilst HELICS (Hierarchical Engine for Large-scale Infrastructure Co-Simulation) [7] is an open-source framework designed to synchronise multiple simulation tools, primarily for energy systems.

In Hueros-Barrios et al. [8], a real-time Digital Twin Prototype (DTP) testbed for green hydrogen production is developed using OPAL-RT for the physical power layers, and both InfluxDB [9] and Grafana [10] for the cyber information layer for data management and visualisation, respectively. InfluxDB and Grafana run on a Raspberry Pi, which is connected to the OPAL-RT hardware target by Ethernet and communicates via User Datagram Protocol (UDP) at 100 ms intervals.

In McCornack et al. [11], which focuses on analysing the impacts of PMU communication network anomalies on wide area monitoring and control (WAMC) applications, they interface ns-3 with OPAL-RT hardware. The TapBridge module of ns-3 is employed (similar to Haseeb et al.'s [4] use of the module) to interface with an IEEE 39-bus power system model running using OPAL-RT's eMEGASIM.

In contrast to packet-level network simulators such as ns-3 or OMNeT++, some works adopt software-defined networking (SDN)-based network emulation tools such as Mininet to enable real-time, controllable cyber environments, as shown in the work of Girdhar et al. [12]. These approaches prioritise flexibility and integration with HIL and digital twin platforms over detailed communication modelling. OMNeT++ and ns-3 provide high-fidelity behavioural modelling, whereas Mininet provides a real-time, controllable execution environment using actual network stacks and protocols.

Seshasai et al. [13] present a study on the real-time impact assessment of sensor measurement falsification attacks in cyber–physical power systems, with a particular focus on load redistribution (LR) attacks in smart grids. The primary aim of the paper is to design and evaluate a framework for quantifying the impact of such cyber attacks using newly proposed metrics, namely the cyber resiliency index (CRI), cyber severity index (CSI), and cyber market index (CMI), while also formulating the attack design as a multi-objective optimisation problem. To validate the proposed framework under realistic conditions, the authors implement a real-time cyber–physical testbed using the Typhoon HIL simulator, where the power system model is executed in real time and interfaced with a communication layer based on Ethernet, Modbus protocol, and IEEE 802.11 network switching. Sensor measurements generated by the Typhoon HIL are transmitted through this communication infrastructure and can be intercepted and manipulated via Internet of Things (IoT) devices to emulate attack scenarios, with the resulting data received by a SCADA system for analysis. This hardware-in-the-loop setup enables the authors to assess the real-time operational impact of cyber attacks and validate the effectiveness of the proposed metrics in a practical, closed-loop environment.

Works that focus on ML-based cyber attack detection and mitigation for wide-area damping control include Saini and Bhui [14], where they used OPAL-RT interfaced with ns-3 as the cyber tool. Their HIL-based testbed integrated OPAL-RT with industry-grade synchrophasor hardware, including PMU, RTAC, GPS clock and OpenPDC components, to create a realistic wide-area damping control (WADC) validation environment. Ns-3 was used to emulate the wide-area communication network, while OpenPDC acted as the control-centre/super-PDC platform. The environments were interfaced using an ns-3 tap bridge with OpenPDC, and the communication protocol was IEEE C37.118 for synchrophasor data exchange. The study focused on detecting and mitigating cyber attacks on WADC measurement and control signals using a semi-supervised generative adversarial network (SSGAN) with support vector machine-based synthetic minority oversampling technique (SVM-SMOT), with mitigation achieved by switching to alternative measurement and control signal pairs.

Kondu et al. [15] used OPAL-RT and ns-3 for their work on cyber-physical system-distributed energy resources management system (CPS-DERMS) cybersecurity and MITM attack impact analysis. The study developed a CPS-DERMS HIL/co-simulation platform that integrated OPAL-RT, ns-3 and a Python-based DERMS Volt-VAR control module. The authors used ns-3 to represent the communication network, including core and edge routers, and to emulate MITM attack insertion in DER-DERMS communication pathways. The interface relied on TUN/TAP bridges and DNP3 I/Os, with DER gateways modelled in OPAL-RT and connected into the ns-3 edge-router network. The case study used a model of a real utility DER-integrated feeder, and the simulated MITM attack manipulated VVC parameters, leading to overvoltage, reactive power imbalance and increased tap-changer operation.

In Srivastava et al.'s work [16] on cyber-physical security testbed development and cyber attack impact analysis, the authors used RTDS as the real-time power system simulator and ns-3 as the network simulation tool. The physical distribution system was modelled in RTDS, while the communication layer was modelled in ns-3 using a packet-level discrete-event simulation environment. The authors specifically focused on implementing Modbus communication, arguing that previous CPPS testbeds had not sufficiently addressed Modbus despite its widespread use in industrial automation. The RTDS and ns-3 environments were interfaced using a GTNETx2 card and a TAP interface, with ns-3 acting as a virtual Ethernet switch. The testbed was demonstrated using a modified IEEE 13-bus feeder with DERs, where a MITM attack manipulated DER flexibility offers and caused generator overloading and frequency decline.

In Ali and Mohammed's work [17] on cyber autonomous inverter-based microgrid control and communication QoS analysis, the authors also used OPAL-RT and ns-3 as the real-time power system simulator and communication simulator, respectively. The AC microgrid, including the inverter models, inner controllers and primary droop controllers, was modelled in MATLAB/Simulink and executed in real time on OPAL-RT, while ns-3 was used to emulate the communication network between the local droop controllers and a centralised voltage/frequency secondary controller. The authors explicitly justify ns-3 as a flexible open-source tool that can emulate network topologies, protocols, delays and data rates without additional computational cost. The OPAL-RT and ns-3 environments were interfaced using Docker containers and tap bridges, enabling bidirectional data flow between the physical and cyber layers. The study focused on validating the Cyber-HIL framework, secondary-control performance and communication QoS metrics such as delay and transmitted/received bitrate.

Overall, these recent studies prove no sign of slowing down in the race to develop practical CPPS testbed configurations, showing a clear and continuous movement from

stand-alone real-time power simulation towards integrated cyber-physical testbeds. However, the interfacing approaches remain diverse and inconsistently reported, which motivates the comparative summary in Table 1. The table compares the works, tabulating the selected real-time power system simulator, the cyber tool selected for communications design and simulation, whether the cyber tool is a packet-level DES or network emulation, whether the study involves real communication hardware such as IEDs, the interfacing method used to connect the real-time power simulator to the cyber tool, the smart grid standard/industrial control protocol used in the study.

Table 1. Summary of real-time CPPS testbeds and interfacing configurations.

Paper	Year	Power Simulator	Cyber Tool	Cyber Tool Type	Real Comms Hardware?	Interface Methods	Interface Protocol
Acharya et al. [3]	2026	RTDS	Other	Network Emulation	Yes	GTNETx2	DNP3
Haseeb et al. [4]	2026	RTDS	ns-3	packet-level DES	No	Virtual gateway	TCP/IP
Hueros-Barrios et al. [8]	2026	OPAL-RT	Other	Data Management & Visualisation	No	UDP Communication	UDP
McCornack et al. [11]	2025	OPAL-RT	ns-3	packet-level DES	No	Virtual gateway	Mixed
Girdhar et al. [12]	2025	OPAL-RT	Mininet	Network Emulation	Yes	OPAL-RT Signal Emulation Module	IEC 61850
Saini and Bhui [14]	2026	OPAL-RT	ns-3	packet-level DES	Yes	NS-3 tap bridge + OpenPDC	IEEE C37.118
Kondu et al. [15]	2025	OPAL-RT	ns-3	packet-level DES	No	TUN/TAP bridge + DNP3 I/Os	DNP3
Srivastava et al. [16]	2024	RTDS	ns-3	packet-level DES	No	GTNETx2 + TAP interface	Modbus
Ali and Mohammed [17]	2024	OPAL-RT	ns-3	packet-level DES	No	Docker containers + tap bridge	Unspecified

Relative to the reviewed studies, the contribution of this paper is threefold. First, it provides a focused comparison of recent real-time CPPS testbeds specifically from the perspective of their interfacing architectures, communication tools, protocols, and hardware integration. Second, the HYPERSIM-MATLAB testbed demonstrates a comparatively accessible approach in which communication-network and control modelling can be implemented without relying on a specialised network simulator. Third, the OPAL-RT/Typhoon HIL-EXata testbed makes the interfacing layer explicit through modular Raspberry Pi-based middleware and compares two real-time synchronisation approaches. Together, these contributions complement previous application-focused CPPS studies by placing greater emphasis on how heterogeneous cyber and physical simulation environments are practically interconnected and synchronised.

The rest of the paper is structured as follows: Section 2 details the architecture of the real-time SIL CPPS testbed based on HYPERSIM and MATLAB, aimed at studying distribution systems with high penetration of DERs. Section 3 details the CPPS testbed for microgrid cyber security analysis, with a focus on the synchronisation mechanisms of the interfacing framework. Section 4 highlights the benefits of the proposed testbeds and approaches, focusing on key features such as accessibility, in addition to discussing relevant future research directions pertaining to advancing CPPS testbeds.

2. CPPS Testbed for DER-Based Distribution System

In this section, the architecture of a real-time SIL CPPS testbed is detailed. The capabilities of this testbed include designing and simulating a suitable and corresponding cyber infrastructure for selected power system models, developing grid control schemes and introducing cyber attacks and faults to observe and analyse their impacts. Such a

testbed allows for specific cyber-physical research such as studies on improving CPPS resilience to cyber-induced contingencies by, for example, developing control schemes with improved robustness, or by optioneering different communication technologies and devices, forming new configurations. The testbed is capable of conducting studies on both transmission and distribution networks, making it flexible and suitable for the needs of modern power systems research. As a case study example, a PV-modified IEEE 13 Node Test Feeder (NTF) example has been selected, which represents the high penetration of renewable energy sources (RES) in modern distribution networks. The study focuses on the impact of communication contingencies on the effectiveness of the Volt-VAR control scheme of the network. For the power system simulation tool, HYPERSIM (version 2022.2.1) by the company OPAL-RT is selected, which is a real-time simulation software platform for power grids and includes models for power electronic devices. The corresponding communication network and the control scheme are modelled using MATLAB (version R2025a) on a separate desktop workstation, allowing for real-time data exchange over an Ethernet cable.

Other testbeds already depend on high-fidelity real-time power systems simulators; however, what separates this testbed from its counterparts in the literature is the incorporation of a cost-effective, accessible and flexible environment for modelling the cyber network, rather than depending on expensive commercial-off-the-shelf (COTS) solutions which not all researchers can access. Hence, this setup is invaluable for researchers aiming to investigate complex interactions between power systems and communication networks, assess control scheme resilience, and develop strategies for enhancing the robustness of grid operations against cyber threats in an accessible manner.

2.1. Architecture of Proposed Testbed

2.1.1. Overview

The architecture of this real-time testbed for CPPS studies incorporates three main hardware components and three simulated systems. As depicted in Figure 2, the three main hardware components are two PC workstations and the OPAL-RT hardware target. The initial computer workstation serves as a foundation, where HYPERSIM is used to design and evaluate various power system models. HYPERSIM also contains libraries for common and example test networks, such as the IEEE test feeders. The necessary computing power to execute the power system model and its interaction with external hardware through I/O ports is provided by the separate OPAL-RT hardware target. The other PC workstation is employed to model the corresponding communication network and also the centralised control scheme (CCS). The testbed allows for the transfer of critical network information (e.g., P injection by PV buses, P curtailment, tap positions, packet delays, etc.) between all three hardware parts via Ethernet cable and a network switch, employing the industrial control system (ICS) protocol Modbus. The three simulated systems are the designed/selected power network, the communication network, and the control scheme.

The architecture of the CPPS testbed is summarised in Figure 2 and Table 2. The table organises the functional purpose of each component of the testbed, and the final column lists the corresponding specifications of the implementations and platforms. The overall design of the testbed reflects a layered integration of real-time power system execution, communication infrastructure, and supervisory control, enabling controlled evaluation of cyber–physical interactions under both nominal and adversarial scenarios. This modular separation of functionalities supports flexible configuration of test conditions and facilitates systematic assessment of cross-domain dependencies within the CPPS.

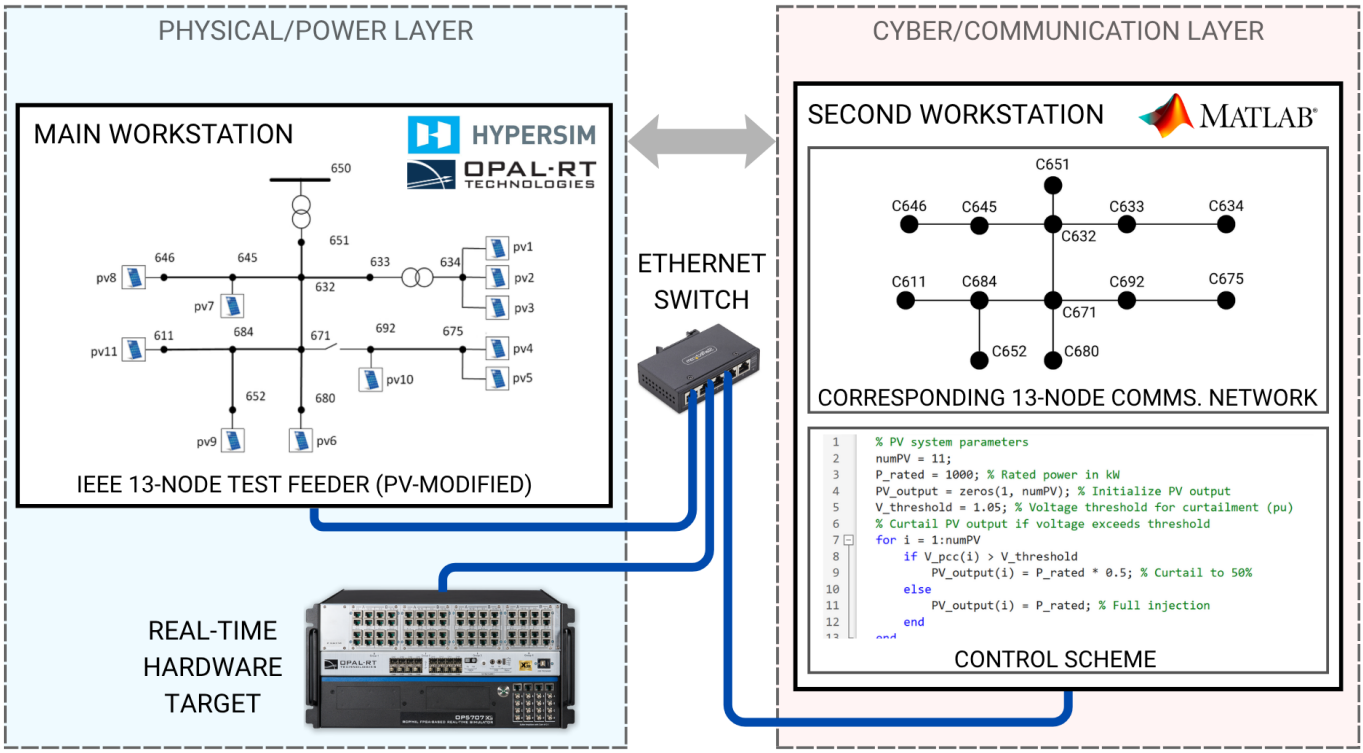

Figure 2. Architecture of real-time CPPS testbed for SIL studies.

Table 2. Element list of real-time CPPS testbed.

Testbed Component	Implementation/Platform	Functional Description
Main Workstation	i7-3770 @3.40 GHz, 16 GB RAM, Windows 10 Enterprise	Supports the development and configuration of power system models, and facilitates their deployment onto the real-time hardware platform (e.g., transmission, distribution, or microgrid systems).
Second Workstation	Similar specifications to the main workstation	Used for designing and analysing the communication infrastructure alongside associated power control algorithms within the cyber layer.
Real-time Hardware Target	OPAL-RT's XG Series (e.g., OP4610XG)	Executes the power system model under real-time conditions, enabling real-time software-in-the-loop validation.
Power System Distribution Network	PV-Modified IEEE 13-Node Test Feeder	Represents the physical electrical network and allows testing under different operating scenarios and configurations.
Communication System Network	13-Node IP over WDM	Emulates the cyber layer responsible for data exchange, monitoring, and control signal transmission.
Centralised Control Scheme	Centralised Volt-VAR control	Maintains system stability by regulating feeder voltage levels within predefined operational limits.
Data Interfacing Protocol	Modbus protocol	Enables bidirectional data exchange between the physical system and the communication layer.

2.1.2. Main Components and Interfacing Connections

In this case study for the testbed, the chosen power system is a PV-modified version of the low-voltage IEEE 13 NTF, which is a well-known test feeder among researchers and engineers for its use in testing common features of distribution analysis software. The IEEE

13 NTF is relatively small and simple, and has a standard operating voltage of 4.16 kV. The feeder has unbalanced loading, contains a single voltage regulator at the substation, and is characterised by being short (low physical length) and comparatively highly loaded (demand on the feeder is high relative to its size/impedance and typical feeder ratings and under the standard IEEE 13-node benchmark loading). It also contains both overhead and underground cables, shunt capacitors, and an in-line transformer.

A corresponding 13-node communication network is designed to represent the infrastructure used for transmitting system data and control commands between the centralised controller and various power devices located at the feeder buses. The Internet protocol (IP) was chosen in conjunction with wavelength division multiplexing (WDM) because it enables high data rates by transmitting multiple wavelengths over a single fibre, making it well-suited for the demanding communication needs of modern power grids. A centralised Volt-VAR CCS is used to maintain feeder voltages within safe operating limits and to coordinate between network devices (e.g., between voltage regulation devices and the PV devices). The Modbus protocol is used over the Ethernet connection between the OPAL-RT target and two workstations, linked through a network switch. This is referred to as Modbus TCP/IP or Modbus TCP. Other Modbus transport modes exist; the other common mode is Modbus RTU, which uses a serial implementation over RS-232/RS-485. This distinction is particularly useful because two papers may both state they use "Modbus", while their performance characteristics, latency, scalability, and cybersecurity considerations are likely to differ significantly depending on the transport layer. OPAL-RT supports various communication protocols, including the modern IEC 61850 as well as traditional ones such as DNP3 and Modbus. This enables researchers to design and evaluate control and protection strategies under various communication challenges, such as latency, interruptions, or corrupted data.

2.2. Physical Layer: Power Distribution Network

2.2.1. Distribution Networks: Technical Background and Impact of DERs

Distribution networks are designed with various configurations and topologies to meet planning and operational needs. In the UK, typical distribution voltages range from 6.6 kV to 33 kV, while in the US, they span from 2.4 kV to 34.5 kV [18]. Common topologies include radial, ring/loop, and meshed systems, with variations based on local requirements. Distributed energy resources (DERs), such as photovoltaic systems, are increasingly being deployed at the network's edge. As the grid moves from transmission down to the consumer level, transmission system operators (TSOs) and distribution network operators (DNOs) experience reduced the following: 1. Visibility, including access to measurements and accurate models, 2. Controllability, such as voltage regulation and protection, 3. Flexibility and automation. This shift introduces changes in areas where utilities have limited data and control, creating significant challenges for effective distribution network planning and operation.

In traditional distribution network planning, voltage regulation assumes a unidirectional power flow from the substation to the end customers. Planners aim to keep voltage levels within acceptable ranges, often defined by standards such as ANSI C84.1 [19], by compensating for voltage drops caused by line resistance and reactance during peak load conditions. To maintain voltage within limits, capacitor banks and voltage regulators are installed along the feeder. However, the integration of DERs such as solar PV, wind, and battery storage introduces bidirectional power flow. When DERs generate excess power, especially during high production periods, reverse power flow can occur, causing voltage levels to rise above acceptable thresholds, particularly near the point of connection. This complicates planning, as voltage control must now address both voltage drops during peak

load and voltage rises during high DER output. To manage these fluctuations, planners rely on dynamic simulations that consider daily, seasonal, and weather-related variations in load and generation. Advanced solutions such as smart inverters, which can adjust reactive power output, along with real-time monitoring and automated voltage regulation systems, are increasingly used to maintain voltage stability across the network.

2.2.2. PV-Modified IEEE 13-Node Test Feeder

The modified IEEE 13 NTF is available as part of the example cases in OPAL-RT's ePHASORSIM software tool, which is a tool focused on large-scale, phasor-domain (RMS)-based simulations. The original IEEE 13 NTF was produced by the Test Feeder Working Group of the Distribution System Analysis Subcommittee (DSAS) under the Analytic Methods for Power Systems Committee (AMPS), part of Institute of Electrical and Electronics Engineers Power & Energy Society (IEEE PES) as part of a series of test feeders designed to provide standardised models allowing engineers and researchers to investigate and optimise power distribution networks under various scenarios [20].

The modified IEEE 13-NTF is based on PSS/e's photovoltaic system model and it's line diagram is shown in Figure 3. The modification includes introducing 11 single-phase PV sources, all represented by the same component models: type PVGU1 for the converter model, type PVEU1 for the controller, type PANELU1 for the solar panel, and an irradiance profile model of type IRRADU1, as shown in Table 3. Note that in ePHASORSIM's example project, these components are modelled in Modelica (an object-oriented, multi-domain modelling language for component-oriented modelling of complex systems) and interfaced with ePHASORSIM as a Functional Mock-up unit (FMU) using the Functional Mock-up Interface (FMI) standard. However, in the design of this testbed, HYPERSIM was employed to leverage its ability to incorporate models directly, instead of depending on external simulators and ad-hoc interfaces.

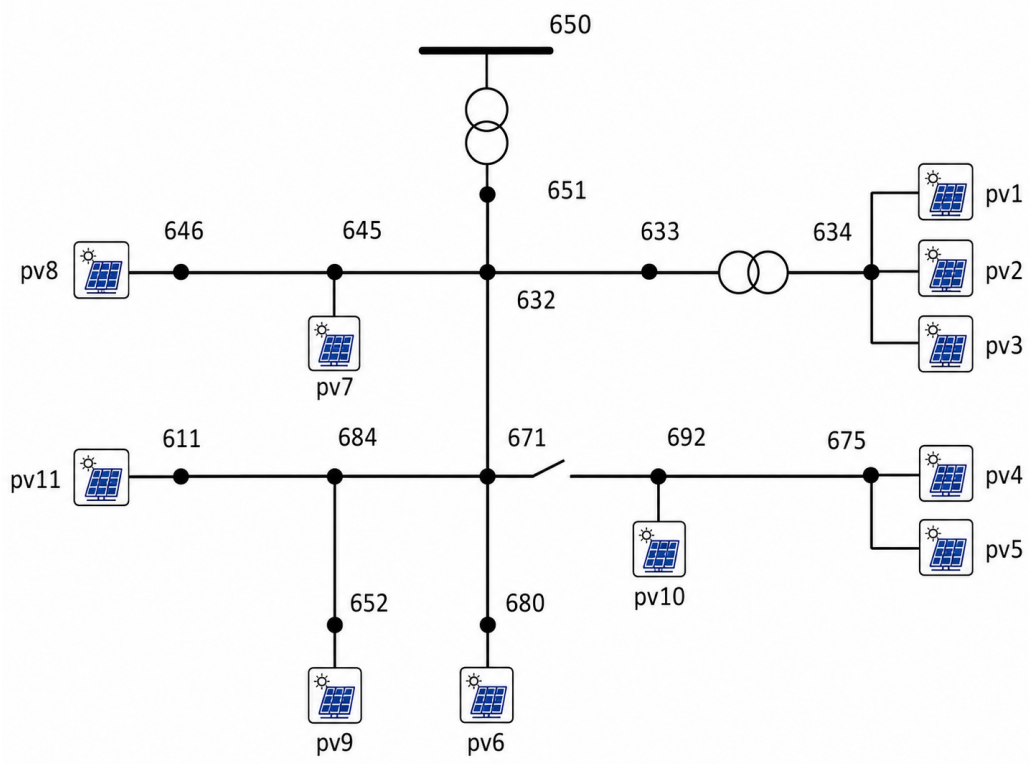

Figure 3. PV-modified IEEE 13-node test feeder used as the representative distribution network, showing the original feeder topology, transformer/regulator elements, switching point, and the placement of eleven single-phase photovoltaic units connected across selected nodes.

Table 3. Network components of the PV-modified IEEE 13-Node Test Feeder.

Network Component	Description	Specification
Nominal Voltage	Rated operating voltage of the distribution network	4.16 kV
Photovoltaic Units	Total number of integrated PV sources	11
PV Configuration	Phase connection of the PV units	Single-phase
Converter Model	Model used to represent the power electronic interface	PVGU1
Controller Model	Control scheme governing PV operation	PVEU1
Solar Panel Model	Model representing PV generation characteristics	PANELU1
Irradiance Profile Model	Input model defining solar irradiance variation	IRRADU1

2.3. Cyber Layer: IPoWDM-Based Communication Network

To transmit control commands and other critical information, a communication network has been designed that corresponds to the modified IEEE 13-NTF. This communication network also contains 13 nodes, pairing with each bus in the feeder. Further details are provided next in terms of the protocol employed and network latency information.

2.3.1. Communication Network Architecture

The selected communication architecture for the 13-node communication network is Internet Protocol over Wavelength Division Multiplexing (IPoWDM), which carries multiple wavelengths on a single fibre, enabling the support of high data rates [21]. The IPoWDM network is made up from an IP layer and an optical layer. Each IP router node serves as a hub in the IP layer, consolidating traffic from the access networks that connect end users. The optical layer supplies the high bandwidth required to support data transmission between these IP routers. A connection between the IP router and the optical layer is established through an optical switch. The optical switch is linked to the fibre connections, whilst transponders handle the conversion between optical and electronic signals (OEO). To enable transmission over long distances, erbium-doped fibre amplifiers (EDFAs) are deployed along the fibre links. In this IPoWDM network implementation, IP traffic is not only handled through optical switching and OEO conversion, but is also processed and routed by IP routers at every intermediate node along its path.

2.3.2. Communication Network Latencies

Various types of delays affect traffic as it moves through communication networks. In the IPoWDM architecture specifically, traffic experiences transmission delay, switching delays at optical switches, amplification delays at EDFAs, and processing delays at routers and transponders. Transmission delay refers to the time required to push all bits of a packet onto the transmission link, while queuing delay occurs when packets wait in buffers for processing or transmission. Propagation delay, on the other hand, describes the time it takes for data to travel through the transmission medium; in optical fibre networks, this is constrained by the speed of light. For the purposes of this work, only propagation delay and component delay are considered.

2.4. Interfacing Layer

The OPAL-RT Real-Time Hardware Target links to an external PC through Ethernet, enabling the simulation of multiple communication protocols. OPAL-RT's real-time hardware

simulator contains multi-core CPU(s) with analog/digital I/Os, connection ports and add-on modules. Through the connection ports, both modern standards such as IEC 61850 and legacy protocols such as DNP3 and Modbus can be supported, allowing researchers to design and test control and protection strategies under real-world communication challenges such as data corruption, latency, or network failures.

2.4.1. OSI and TCP/IP Model and Layers

Concerning the specific methodology used for developmental interfacing, it is essential to consider both the OSI and TCP/IP layers to understand how researchers typically connect external communication network simulators (and physical communication and IED hardware also) to communicate and transmit data with real-time power simulators. See Figure 4, which details examples of protocols, classifying them to relevant layers of the OSI Basic Reference Model to the left of the Figure, and to layers of the TCP/IP model to the right of the Figure. The primary layers of interest in the context of this study are the application, transport, and network interface layers, which correspond to the specific protocols of Modbus, TCP/IP sockets, and Ethernet, respectively, each being highlighted. Another widely adopted industrial interface is Open Platform Communications (OPC), particularly its more recent specification, OPC Unified Architecture (OPC UA). Unlike legacy OPC implementations, which relied on Microsoft COM/DCOM technologies, OPC UA is platform-independent and supports structured information modelling alongside built-in security mechanisms, including authentication, authorisation, encryption, and message-integrity protection. Within CPPS and real-time simulation environments, OPC UA can, therefore, provide an interoperable middleware layer for exchanging data among SCADA systems, PLCs, IEDs, power-system simulators, and external control or communication platforms. Although OPC UA is not employed in the testbeds presented here, its growing industrial and energy-sector adoption makes it an important alternative for secure cyber-physical interfacing.

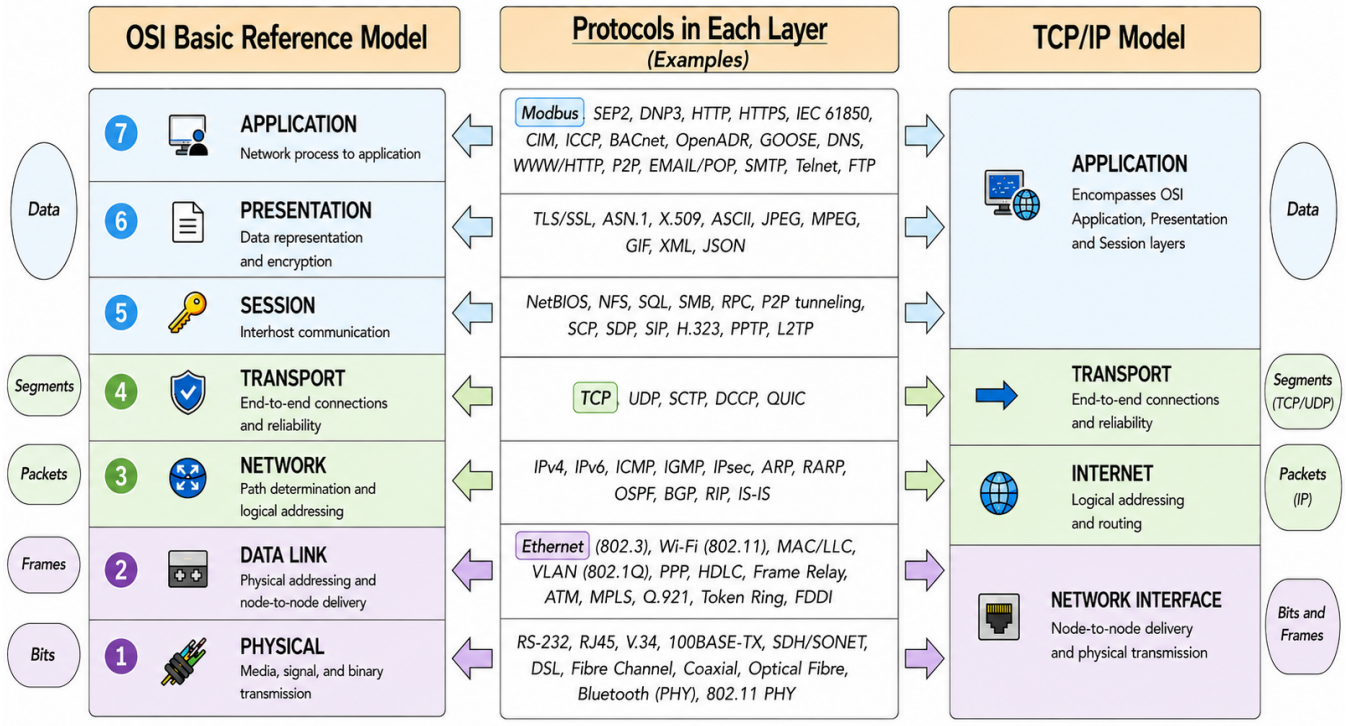

Figure 4. Mapping of protocol examples to their relevant layers in both the OSI Basic Reference Model and the TCP/IP Model, with the Modbus, TCP, and Ethernet protocols highlighted. Adapted from Sundararajan et al. 2018 [22].

2.4.2. Modelling the Communication Network: MATLAB, ns-3 or OMNeT++?

Although MATLAB was utilised in this study to simulate the communications layer, ns-3 has also been widely adopted in numerous research efforts for the same purpose. OMNeT++ has similarly been used, though less frequently than ns-3, for two primary reasons. First, ns-3 is purpose-built for communications networks and systems, while OMNeT++ is a general-purpose simulation framework that happens to be commonly applied to network simulations. Second, ns-3 offers built-in support for interfacing with external real-time simulators through its "Real-time Scheduler" module, which natively manages real-time synchronisation and simulation events. Connecting OMNeT++ with external real-time simulators, while feasible, demands considerably more time and effort, as it requires custom development of event handling procedures, software communication channels, and real-time synchronisation mechanisms.

Connecting ns-3 with OPAL-RT means linking a communication network simulator with a real-time power system simulator. The first step is to clearly define what the co-simulation aims to achieve, for example, studying how communication latency affects grid stability. Data exchange between the two platforms is typically handled through middleware or protocols such as TCP/IP sockets, allowing bidirectional real-time communication. A key challenge is synchronisation, since ns-3 uses discrete-event simulation (DES) while OPAL-RT operates in real time. This can be addressed through time-stepped coordination, where ns-3 holds its event queue until OPAL-RT finishes each time step. To meet real-time demands, ns-3's "RealtimeSimulatorImpl" scheduler must be activated. Throughout the co-simulation, ns-3 provides network-related data while OPAL-RT contributes power system state information, enabling a comprehensive integrated analysis. Thorough testing and validation are essential to confirm that data exchange, timing, and compatibility between both simulators are functioning correctly and reliably.

2.5. Control Scheme

Centralised Volt-VAR Control Scheme

The modified IEEE 13 NTF requires a centralised Volt-VAR control scheme to ensure voltages remain within set boundaries along the feeder. This control strategy will synchronise the 11 PV units, 2 transformers, 2 shunt devices, and 3 switches to work together toward achieving voltage regulation goals, with its inputs and outputs illustrated in Figure 5.

The control strategy will focus on a number of key control objectives for the various available controllable devices. Firstly, the central controller will continuously receive information about the voltages at all nodes to monitor that they remain within set boundaries so as to not violate the feeder's operational limits. This process entails continuously modifying the outputs of transformers and shunt devices in real time to address and correct any fluctuations in voltage. Secondly, the 11 nodes with PV sources will have their PV units actively integrated into the control scheme. These PV units will be directed to either inject or absorb reactive power based on the voltage conditions at neighbouring nodes, in order to help maintain voltage stability. Thirdly, the two transformers and two shunt devices in the distribution feeder will also be controlled to support voltage regulation. The central controller will instruct the transformers to adjust their tap positions, and the shunt devices (e.g., capacitor banks, reactors, etc.) will be directed to supply reactive power or absorb it as required. Finally, the three switches serve as key components of the control system, enabling network reconfiguration when needed. Their operation allows for the isolation of specific sections or the optimisation of power flows to maintain voltage stability throughout the feeder. This may involve redirecting power flow paths to achieve load balance and minimise voltage imbalances. Through these key objectives, the modified IEEE

13 NTF will uphold voltage stability and optimise reactive power management through a centralised Volt-VAR control system, enabling seamless integration of PV systems. This approach continuously fine-tunes controllable devices in response to live voltage changes, ensuring consistent power quality throughout the grid.

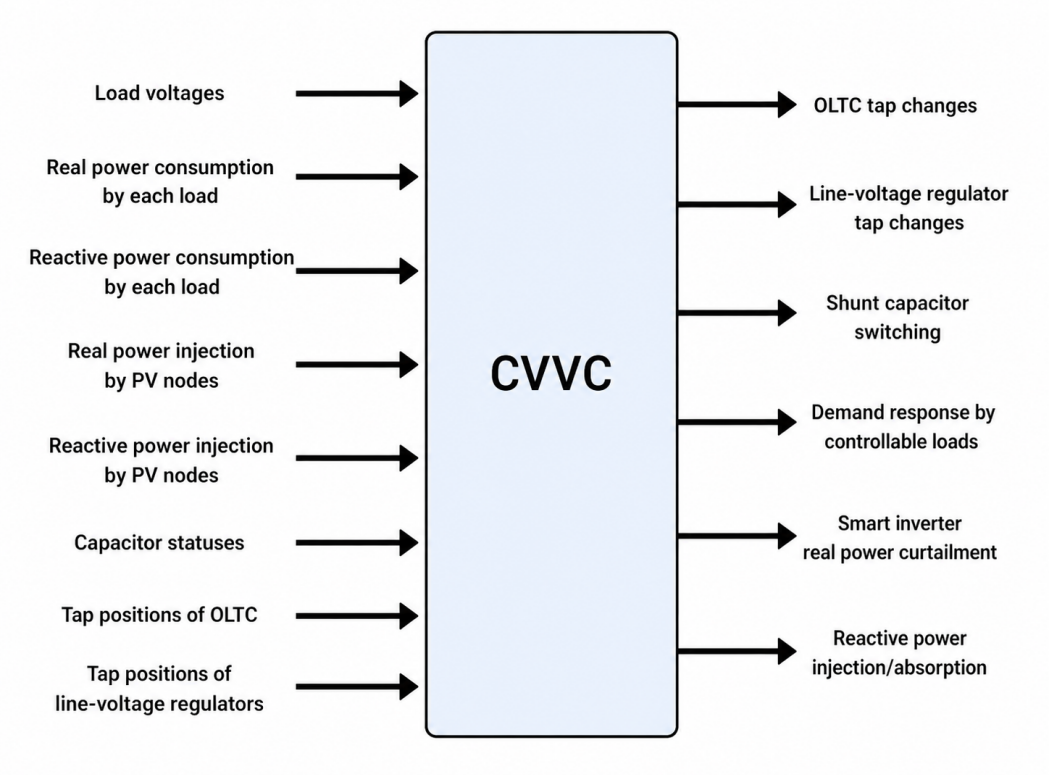

Figure 5. Centralised Volt-VAR controller illustrating inputs and outputs. Reproduced from Dabashi 2025 [2].

3. CPPS Testbed for Microgrid Cyber Security Analysis

The second testbed focuses on real-time cyber-physical co-simulation for microgrid cybersecurity analysis. While many existing studies primarily assess the impact of cyber attacks, this testbed addresses the implementation side by presenting a general framework for coupling power-system and communication-network simulators. Based on Qiu et al. [23], the framework introduces two real-time synchronisation schemes, namely leader-follower and time-stepped synchronisation, and evaluates their suitability using metrics related to computational overhead, latency, scalability, and attack compatibility. This provides practical guidance for designing cyber-physical co-simulation platforms for microgrid cybersecurity studies.

3.1. Architecture of Testbed

As a framework, the real-time cyber-physical co-simulation testbed can be separated into three layers: the physical layer, the cyber layer and the interface layer. The physical layer constitutes the modelling of power systems, represented and solved using electromagnetic transient (EMT) simulation at the microsecond timescale. The cyber layer constitutes both IT and the Operational Technology (OT) systems, where both of these systems are subjected to cyber attack simulations such as FDIAs and DoS. The interface layer is responsible for managing the transmission of information between the two layers and hence propagating the effect of the simulated cyber attacks to the power system, enabling observation of the impact and subsequent analysis. Regarding implementation and the simulation tools employed, in the physical (power) layer, the transmission and distribution power networks

are modelled using OPAL-RT, whilst Typhoon HIL is employed for modelling the microgrid system. In the cyber layer, EXata Network Modelling [24], a DES and packet-level network emulation software package, is employed to model the IT system, which includes firewalls, servers and user nodes, and the OT system. In the interface layer, Python scripts are used to describe the co-simulation interfacing. These Python scripts run on several Raspberry Pi units and the Linux operating system.

3.2. Selected Power Simulation Hardware Platforms

Typhoon HIL 602+ is an FPGA-based real-time simulator designed for precise modelling of power electronics and power systems. OPAL-RT OP5600 is a hardware platform for real-time simulation that integrates a high-performance computer, a reconfigurable FPGA, and signal processing capabilities supporting up to 256 I/Os. Together, these high-performance machines can accurately replicate microgrid power electronics dynamics at the microsecond level.

3.3. Cyber Communication Layer Modelling

Communication networks for power system communications are typically simulated using DES, where specific events occur at specific points in time whereby no change in system state is assumed to occur between two events. This is different to the approach to modelling physical phenomena, such as voltage and current, which are represented by differential equations denoting continuous system behaviour [25,26]. EXata Network Modelling, by the company Keysight Technologies, Inc. [27], is the DES employed in this setup to design and model IT and OT systems with its various protocol layers, devices and components. One important benefit of EXata Network Modelling is its focus on operating in real-time, synchronising with external live networks or devices such as external hardware, particularly real-time targets, such as Typhoon HIL and OPAL-RT hardware, which is vital for this setup [24].

In EXata, each network node initialises its routing table and continuously updates routing information through an iterative relaxation process based on the Bellman-Ford routing algorithm. This enables the communication network to dynamically determine efficient packet-forwarding paths while adapting to changing network conditions, thereby supporting reliable and stable data transmission across the simulated infrastructure. As a discrete-event and packet-level communication network emulator, EXata further allows the modelling of communication behaviour, including packet delays, congestion, packet drops, and routing dynamics, which are all highly relevant within CPPS environments. Within the cyber-physical co-simulation framework proposed in the paper, this communication modelling capability is integrated with the real-time power system simulation environment to evaluate the impact of cyber contingencies on grid operation. In particular, the validation studies focus on FDI and DoS attacks targeting the OT domain.

3.4. Interfacing

In this testbed, interfacing is treated as a dedicated layer between the physical and cyber simulators, responsible for transferring measurements and control signals between the power-system and communication-network domains in real time. The interface layer enables cyber events and communication effects to propagate into the physical system, while also returning power-system data to the communication simulator for closed-loop operation. To achieve this in practice, the testbed adopts Ethernet-based communication and embedded Python scripts running on Raspberry Pis, which act as intermediary data-exchange devices between the simulators [23]. This interface layer is, therefore, also an interoperability layer, since it allows heterogeneous simulation platforms with different

execution principles, time steps, data formats, and communication behaviours to operate together within a single real-time cyber-physical co-simulation framework.

3.4.1. Synchronisation Mechanisms of the Interfacing Framework

At the theoretical level, interfacing is formulated as the synchronisation of two fundamentally different simulation processes: the power simulator, which operates continuously with fixed simulation steps, and the communication simulator, which evolves according to discrete events. In this testbed, two real-time data-exchange synchronisation schemes are adopted: leader-follower and time-stepped.

(1) Leader-Follower Synchronisation: In the leader–follower scheme, the power simulator acts as the leader and the communication simulator acts as the follower. Data exchange is not performed at every simulation instant, but only when the variation in a measured signal exceeds a predefined threshold. To realise this, the testbed employs a Quantised State System (QSS)-based event-triggering method, which converts fixed-step exchange into a dynamic event-driven process [28]. This improves computational efficiency by reducing unnecessary communication between simulators, although it introduces a bounded tracking bias between the physical measurement and the cyber-side received value.

(2) Time-Stepped Synchronisation: In the time-stepped scheme, both simulators execute simultaneously and exchange data at fixed synchronisation intervals. If an event arrives between synchronisation points, it is placed in a pending-event list until the next valid update instant. To preserve real-time behaviour, the testbed further incorporates an expired-event discarding mechanism, so that events that have become too old are removed rather than being processed late. This makes the synchronisation process more regular and ensures that outdated cyber events do not accumulate in the interface layer.

3.4.2. Practical Implementation of the Interfacing Framework

At the practical level, the interface is implemented as an Ethernet-based middleware framework using Python scripts deployed on Raspberry Pis configured in a Linux environment. These devices handle data reception, processing, conversion, synchronisation, and transmission between the power simulator and EXata. In this way, the Raspberry Pis serve as distributed interface nodes rather than relying on a direct internal software link between simulators, which improves modularity, ease of implementation, and scalability. TCP/IP is used to ensure accurate and reliable data transmission across the co-simulation platform. Both Python and Raspberry Pi software are open-source, giving the advantage of accessibility due to lower or no costs and flexibility of modifications to suit needs.

(1) Typhoon HIL and EXata Implementation: In the Typhoon HIL–EXata platform, the actual interface implementation follows the leader-follower synchronisation scheme. A 5-DER microgrid is implemented in Typhoon HIL, while EXata models the communication network using a star topology. On the interface side, the key practical modules are the Data Process Module for Typhoon, the Data Process Module for EXata, and the Event Trigger Module. The Event Trigger Module applies the QSS-based logic so that data are exchanged only when the variation in the observed value exceeds the selected quantum. As a result, Typhoon does not forward every instantaneous measurement to EXata; instead, only sufficiently significant changes are transmitted through the Raspberry Pi interface, reducing communication burden at the expense of some bounded signal bias. For visual reference, see the **1. Leader-Follower** part of the **(a) Synchronisation mechanisms** on the left side of the Figure 6, and also the **1. Typhoon HIL-EXata platform** of the **(b) Practical implementation** part on the right of the Figure.

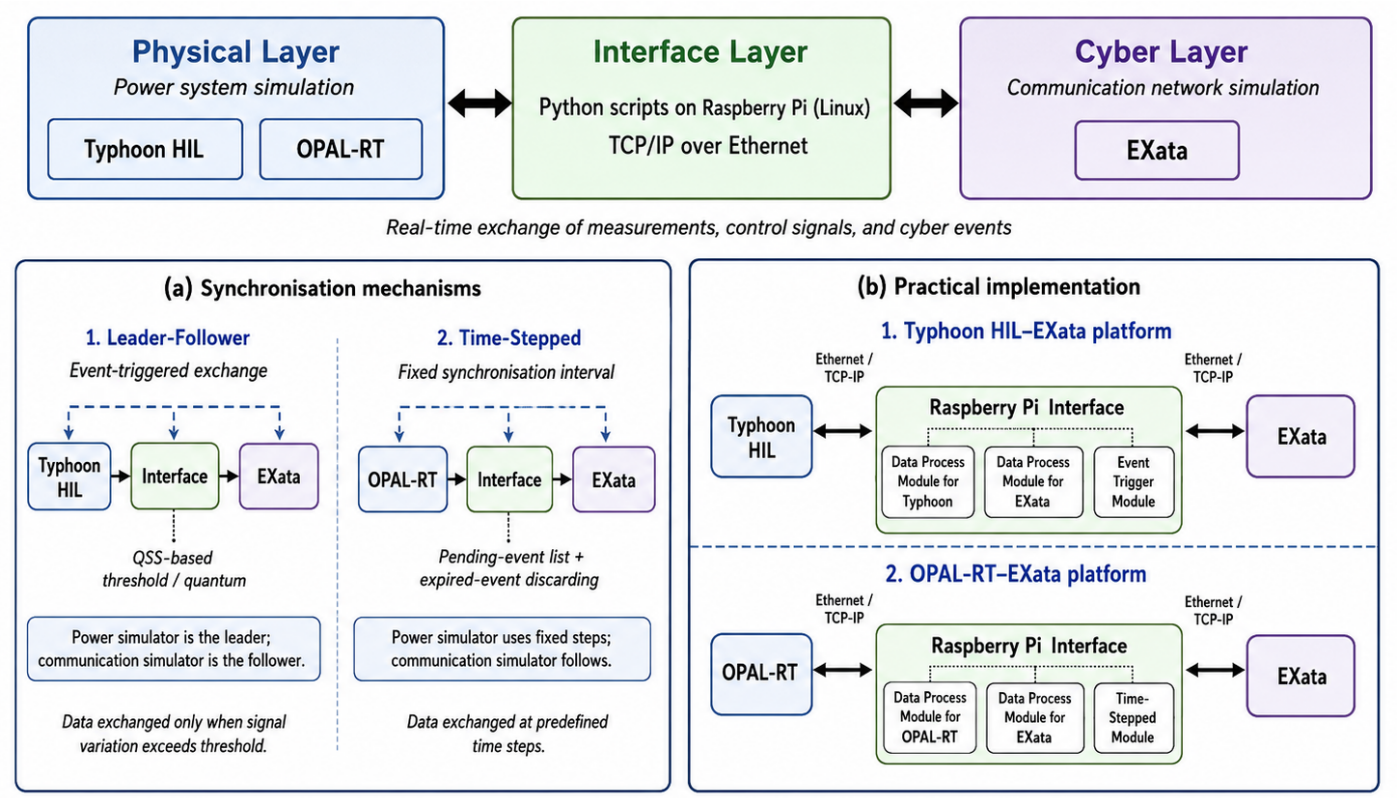

Figure 6. Illustrating connection of the interfacing layer to both the physical and cyber layer and what the interfacing layer constitutes: (**a**) Synchronisation mechanisms of data exchange and (**b**) Practical implementation of the Typhoon HIL and OPAL-RT testbeds.

(2) OPAL-RT and EXata Implementation: In the OPAL-RT and EXata platforms, the interface implementation is based on the time-stepped synchronisation scheme. A 10-DER microgrid is implemented in OPAL-RT, while EXata models the communication network using a bus topology. Here, the practical interface modules are the Data Process Module for OPAL-RT, the Data Process Module for EXata, and the Time-Stepped Module. Data are exchanged at fixed intervals, and the pending-event list together with the expired-event discarding rule ensures that stale events are removed rather than processed after excessive delay. Compared with the Typhoon-based implementation, this gives the OPAL-RT interface a more regular synchronisation pattern and allows delay effects to be represented more explicitly within the co-simulation process. For visual reference, see the **2. Time-Stepped** part of the **(a) Synchronisation mechanisms** on the left side of the Figure 6, and also the **2. OPAL-RT-EXata platform** of the **(b) Practical implementation** part on the right of the Figure.

Table 4 reports the performance indicators associated with the two synchronisation schemes on the two platforms. The synchronisation processing time constrains the minimum simulation time step, and a shorter time step allows higher synchronisation accuracy. The leader-follower scheme, used by the Typhoon testbed shown in Figure 7, has the advantage in this regard, reporting a time of 0.183 ± 0.004 ms. This is around 160 times faster than the time-stepped scheme. The RAM memory utilisation of the leader-follower and time-stepped synchronisation schemes is 1.36% and 6.85% of the total 8 GB Raspberry Pi memory, respectively. Since each Raspberry Pi currently hosts a single node (a node being one DER/control endpoint in the simulated microgrid), a single device can theoretically accommodate around 70 nodes. This architecture, therefore, supports scaling to larger cyber-physical co-simulations (1000 nodes = 15 Raspberry Pis), when based solely on the measured RAM utilisation. However, this represents a theoretical memory-based estimate

and does not account for additional processor, communication, or real-time execution constraints; large-scale experimental validation remains necessary. In addition, increasing RAM capacity and optimising the Python scripts could further improve network scalability. The script files themselves are small (only 12 KB or 28 KB) so their impact on storage is negligible. All of these scalability advantages contribute to improving CPPS testbeds' capabilities of modelling and analysing larger power system models, an important aspect of future research, as will be discussed in the next section.

Table 4. Implementation and resource requirements of the two synchronisation approaches.

Performance Indicator	Leader-Follower Scheme	Time-Stepped Scheme
Synchronisation processing time	0.183 ± 0.004 ms	30 ± 0.5 ms
RAM memory utilisation	1.36% (106 MB)	6.85% (535 MB)
Packet payload size	50 bytes	200 bytes
Interface script size	12 KB	28 KB

Adapted from Qiu et al. [23].

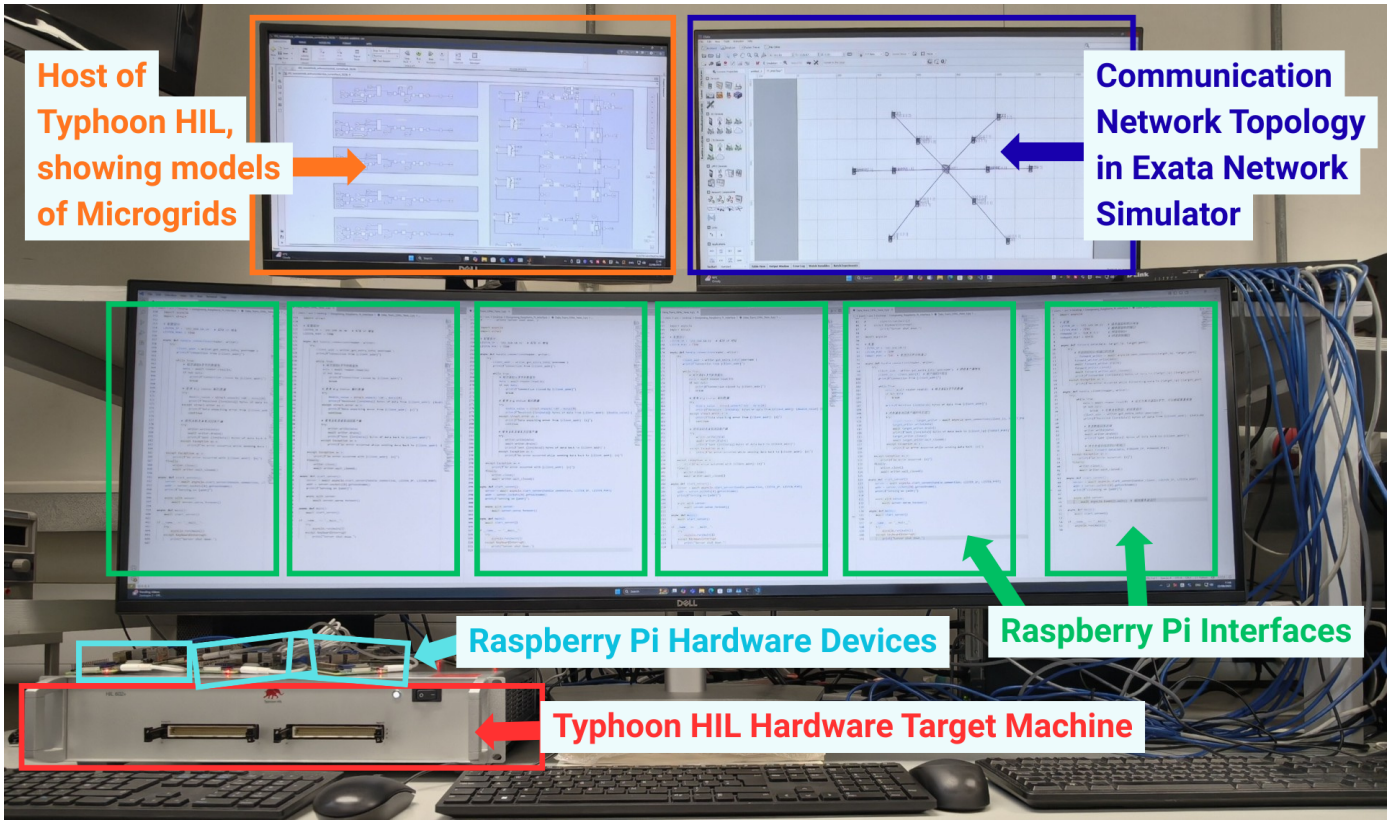

Figure 7. The setup of the Typhoon CPPS based platform with the Raspberry Pis hardware and software interfaces, showing also the screenshots of the Typhoon HIL host and the Exata Network Simulator.

4. Discussion and Future Research

Relative to the CPPS testbeds reviewed in Section 1.2, two main implementation-oriented contributions can be identified from the testbeds presented in this paper. The first testbed, presented in Section 2, demonstrates an accessible configuration for SIL CPPS studies by using MATLAB to model both the communication network and the power-system control scheme. This is significant because many CPPS testbeds rely on specialised network simulators, whether commercial or research-grade, which may limit reproducibility and accessibility for researchers without access to such tools. By contrast, MATLAB is widely available across universities, research laboratories, and engineering programmes, and is

already familiar to many power system researchers and students. Its use, therefore, reduces the technical learning barrier associated with constructing communication-aware CPPS studies, particularly for researchers whose primary expertise lies in power systems rather than communication-network simulation. This makes the testbed valuable not only as a research platform for investigating communication delays, cyber-contingencies, and control resilience, but also as an educational and developmental framework for introducing postgraduate and advanced undergraduate students to cross-domain CPPS analysis. In this sense, the contribution of the first testbed lies not only in its technical configuration, but also in its potential to broaden participation in CPPS research by lowering the entry barrier to cyber-physical simulation.

This emphasis on accessibility is also reflected in the second testbed, presented in Section 3, although in a different part of the cyber-physical simulation workflow. Whereas the first testbed lowers the entry barrier by using MATLAB as a familiar environment for communication-network and control modelling, the second testbed contributes accessibility at the interfacing level by providing a more generalisable implementation framework for real-time cyber-physical co-simulation. Its contribution, therefore, lies not only in connecting power-system and communication-network simulators, but in making the coupling process more explicit, modular, and reproducible. The leader-follower and time-stepped synchronisation schemes provide two distinct mechanisms for coordinating data exchange between fixed-step power system simulation and event-driven communication network simulation. This is important because the fidelity of CPPS studies depends not only on the accuracy of the power and cyber simulations individually, but also on how reliably measurements, control signals, delays, and communication events are exchanged between them in real time. A further contribution is the practical realisation of this interface through Python-based data-exchange scripts deployed on Raspberry Pi devices. This provides a relatively accessible and adaptable middleware layer, reducing dependence on direct simulator-to-simulator links or highly specialised integration methods. By distributing data processing, conversion, synchronisation, and transmission tasks across intermediary interface nodes, the framework supports scalability while preserving implementation clarity. In this sense, the second testbed complements the first: together, they demonstrate that accessibility in CPPS testbed development can be improved both at the modelling layer, through familiar software environments, and at the interfacing layer, through modular and low-cost implementation approaches. This common emphasis is significant because wider participation in CPPS research depends not only on high-fidelity simulation tools, but also on testbed architectures that can be understood, reproduced, adapted, and extended by researchers across different levels of expertise and institutional resources. Taken together, the two testbeds show that innovation in real-time CPPS simulation can extend to the accessibility, modularity, and reproducibility of the interfacing layer between power-system, communication-network, and control-domain models.

4.1. Scalable and Representative Power and Cyber Models

Scalability remains a key focus for future research. Much of the existing work in CPPS relies on test systems, such as IEEE PES Test Feeders [29] for distribution feeders, which serve as smaller-scale representations of more complex, real-world systems. This does not diminish their value; conceptual models are essential for initial validation and offer several practical advantages. However, to generate insights that are more realistic, applicable, and ultimately more meaningful, studies must increasingly incorporate more representative models and network configurations, which are typically larger. For this reason, scalability continues to be a critical consideration in advancing CPPS research.

In addition, scalability is not limited to the power system domain alone; the cyber domain must also incorporate more advanced and representative models. Traditionally, much of the literature has focused on cyber infrastructure at the transmission level, particularly in relation to communication between control centres and substations. While there is a growing body of work addressing cyber models at the distribution level, such as in networked microgrids [30], Internet of Energy applications in microgrids [31], and IoT-based local energy market designs [32], important components such as edge communication nodes remain under-represented. This is increasingly significant given the expanding role of prosumers and smart inverters equipped with embedded communication capabilities. As cyber technologies continue to evolve and become more widely deployed at the edge of CPPS, future research must capture this shift. This highlights the importance of scalability not only in the power domain but also across the cyber layer.

4.2. Cybersecurity Threats, Validation, and Resilience in CPPS

Cybersecurity will remain a central research priority in CPPS, particularly as power systems become increasingly digitalised, distributed, and communication-dependent. This is reinforced by the World Economic Forum Global Risks Perception Survey 2025-2026, which ranks cyber insecurity among the ten most significant global risks in both the short and long term [33]. Within CPPS research, cybersecurity studies have traditionally focused on the design and simulation of common attack classes, including FDI, DoS, and MITM attacks, in order to assess their impact on power system monitoring, control, and operation [34]. While such work has historically centred on transmission-level infrastructures, the research emphasis is clearly shifting towards distribution networks, driven by the growth of RES, smart monitoring and control devices, EV and charging infrastructure, and broader DSO digitalisation pressures [35,36].

The vast majority of existing studies focus on capturing the impact of cyber-attacks on CPPS operation, rather than engineering the attacks themselves within the cyber-physical testbed. Future research should, therefore, advance towards more integrated control-cyber-communication-power environments, in which attacks can be systematically designed, injected, and validated as part of the experimental framework. Such an evolution would support the development of 'smart grid cyber ranges' capable of enabling realistic attack emulation, alongside detection, mitigation, recovery, and resilience assessment. Their practical value is clear: unlike real power infrastructure, which cannot be subjected to continual cyber experimentation, cyber ranges provide a safe environment for red and blue teams to uncover vulnerabilities, validate defences, and transfer improved protections into operational systems, among other benefits.

4.3. Cyber-Physical Validation of Cryptography and Secure Encoding

As distribution networks continue to evolve through the rapid deployment of smart inverters, DER controllers, grid-edge devices, and other digitally connected assets, future research must address not only their control and operational functionality, but also the communication, encoding, and security mechanisms that underpin their cyber-physical integration. New communication standards and message structures introduced for modern distribution applications cannot be assumed to be secure or operationally suitable by design; rather, they must be validated under realistic cyber-physical conditions to ensure that confidentiality, integrity, authentication, and timing requirements are all preserved. This is particularly important because widely adopted protocols in these environments, such as SunSpec Modbus, may lack native security provisions, thereby increasing the attack surface of distribution systems. In this context, cryptographic and secure encoding schemes should be treated as a core future research area, especially for resource-constrained field

devices where conventional security mechanisms may impose unacceptable overheads. As highlighted by Haseeb et al. [4], current research still lacks sufficient real-time validation of cryptographic countermeasures against common attacks in experimental smart grid testbeds. Similarly, Aftab et al. [37] emphasised that assessing the impact of cyber-attacks and validating mitigation schemes requires a real-time testbed integrating both power system and communication network simulation. Future work should, therefore, prioritise the cyber-physical validation of lightweight cryptographic and secure encoding approaches across emerging distribution protocols, with particular emphasis on their latency, computational burden, interoperability, and effectiveness under realistic attack scenarios.

Author Contributions: Conceptualization, writing—original draft preparation, A.H.D.; methodology, software, formal analysis, investigation, A.H.D. and D.Q.; writing—review and editing, A.H.D., D.Q., X.Z. and G.T.; supervision, project administration, funding acquisition X.Z. and G.T. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the Engineering and Physical Sciences Research Council Doctoral Training Partnership with High Voltage Substation Services Ltd. "Smart Energy Infrastructure for Future Power Networks" grant number 2719714 and by the UK Research and Innovation Future Leaders Fellowship "Digitalisation of Electrical Power and Energy Systems Operation" grant number MR/W011360/2.

Data Availability Statement: The original contributions presented in this study are included in the article. Further inquiries can be directed to the corresponding author.

Acknowledgments: During the preparation of this manuscript, the authors used ChatGPT Images 2.0 (OpenAI) for assistance with the graphical design and visual refinement of selected illustrative figures. The authors reviewed and edited all generated outputs and take full responsibility for the content of this publication.

Conflicts of Interest: The authors declare no conflicts of interest. The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript; or in the decision to publish the results.

Abbreviations

The following abbreviations are used in this manuscript:

AGC	Automatic Generation Control
ANSI	American National Standards Institute
CCS	Centralised Control Scheme
CPPS	Cyber-Physical Power Systems
CPS	Cyber-Physical Systems
DER	Distributed Energy Resource
DERMS	Distributed Energy Resource Management System
DES	Discrete-Event Simulation
DNP3	Distributed Network Protocol 3
DoS	Denial of Service
EDFA	Erbium-Doped Fibre Amplifier
EMT	Electromagnetic Transient
FDIA	False Data Injection Attack
FPGA	Field-Programmable Gate Array
HELICS	Hierarchical Engine for Large-scale Infrastructure Co-Simulation

HIL	Hardware-in-the-Loop
IEC	International Electrotechnical Commission
IED	Intelligent Electronic Device
I/O	Input(s)/Output(s)
IoT	Internet of Things
IP	Internet Protocol
IPoWDM	Internet Protocol over Wavelength Division Multiplexing
IT	Information Technology
LFC	Load Frequency Control
MITM	Man-in-the-Middle
NIST	National Institute of Standards and Technology
NTF	Node Test Feeder
OEO	Optical-Electrical-Optical
OPC	Open Platform Communications
OPC UA	Open Platform Communications Unified Architecture
OSI	Open Systems Interconnection
OT	Operational Technology
PES	Power and Energy Society
PLC	Programmable Logic Controller
PMU	Phasor Measurement Unit
PV	Photovoltaic
QSS	Quantised State System
RES	Renewable Energy Sources
RMS	Root Mean Square
RTAC	Real-Time Automation Controller
RTDS	Real-Time Digital Simulator
RTU	Remote Terminal Unit
SCADA	Supervisory Control and Data Acquisition
SDN	Software-Defined Networking
SIL	Software-in-the-Loop
TCP/IP	Transmission Control Protocol/Internet Protocol
UDP	User Datagram Protocol
VVC	Volt-VAR Control
WADC	Wide-Area Damping Control
WAMC	Wide-Area Monitoring and Control
WDM	Wavelength Division Multiplexing

References

1. Yohanandhan, R.V.; Elavarasan, R.M.; Manoharan, P.; Mihet-Popa, L. Cyber-Physical Power System (CPPS): A Review on Modeling, Simulation, and Analysis with Cyber Security Applications. *IEEE Access* **2020**, *8*, 151019–151064. [CrossRef]
2. Dabashi, A.H. Novel Cross-Domain Analysis of Cyber-Physical Power Systems Using Enhanced Modelling and Simulation Techniques. Doctoral Dissertation, Brunel University of London, Uxbridge, UK, 2025. [CrossRef]
3. Acharya, A.; Bhalja, B.R. Novel Deep Learning-Based Approach for Detection, Classification, and Mitigation of Cyber Attacks in Power Distribution Systems. *IEEE Trans. Ind. Appl.* 2026, *early access*. [CrossRef]
4. Haseeb, A.; Shahid, A.; Dordoni, T.; AhmadiAhangar, R.; Rosin, A.; Kilter, J.; Aksoy, L.; Ghasempouri, T. Secure Communication in Smart Grid Systems Against MITM Attacks Using Lightweight Cryptography. In *2026 IEEE 23rd Mediterranean Electrotechnical Conference (MELECON)*; IEEE: New York, NY, USA, 2026; pp. 1–6.
5. Masood, M.Y.; Rifà-Pous, H.; Awais, M.; Khawar, A.; Muzaffar, M. Co-Simulation of FDI and DOS Attacks in IoT-Enabled Next-Generation Smart Grids: A Framework for Resilience. In *2026 7th International Conference on Advancements in Computational Sciences (ICACS)*; IEEE: New York, NY, USA, 2026; pp. 1–7.
6. GridLAB-D. Available online: https://www.gridlabd.org/ (accessed on 24 March 2026).
7. Hardy, T.D.; Palmintier, B.; Top, P.L.; Krishnamurthy, D.; Fuller, J.C. HELICS: A Co-Simulation Framework for Scalable Multi-Domain Modeling and Analysis. *IEEE Access* **2024**, *12*, 24325–24347. [CrossRef]

8. Hueros-Barrios, P.J.; Espolio-Maestro, J.; Rodríguez-Carrasco, S.; Santos-Pérez, C.; Rodríguez-Sánchez, F.J.; Sánchez, P.M.; Tradacete-Ágreda, M.; Blaabjerg, F. Real-time digital twin prototype for cyber-physical analysis of anomalies in PV–PEM–BESS systems for green hydrogen production. *Sustain. Energy Grids Netw.* **2026**, *45*, 102152. [CrossRef]
9. InfluxDB. Available online: https://www.influxdata.com/ (accessed on 26 March 2026).
10. Grafana. Available online: https://grafana.com/ (accessed on 26 March 2026).
11. McCornack, B.; Hyder, B.; Mahapatra, K. Impact Characterization of PMU Network Anomalies on Wide-Area Voltage Control using Cyber-Hardware-In-the-Loop Co-simulation. In *2025 Resilience Week (RWS)*; IEEE: New York, NY, USA, 2025; pp. 1–6.
12. Girdhar, M.; Park, K.; Su, W.; Hong, J.; Liu, C.C. Cybersecurity Enhancement in Digital Substations: Hidden Markov Model-Based Smart Cyber Switching and Threat Response. *IEEE Access* **2025**, *13*, 217022–217037. [CrossRef]
13. Seshasai, B.; Ghosh, S.; Koley, E.; Jena, P.K. Real-Time Impact Assessment of Sensor Measurement Falsification on Smart Grid Operations. *IEEE Trans. Instrum. Meas.* **2025**, *74*, 9009714. [CrossRef]
14. Saini, A.; Bhui, P. Securing wide-area damping controller against cyber attacks using semi-supervised generative adversarial network and support vector machine-based synthetic minority oversampling technique. *J. Mod. Power Syst. Clean Energy* **2025**, *14*, 145–157. [CrossRef]
15. Kondu, S.C.V.; Ravikumar, G.; Mohan, S.N. Cps-derms: Cyber-physical security and impact analysis of derms against mitm attacks. In *2025 IEEE Green Technologies Conference (GreenTech)*; IEEE: New York, NY, USA, 2025; pp. 1–5.
16. Srivastava, A.; Zhao, J.; Moore, K.; Anagnostou, E. Development of cyber-physical security simulation testbed in RTDS using Modbus communication. In *2024 IEEE Power & Energy Society General Meeting (PESGM)*; IEEE: New York, NY, USA, 2024; pp. 1–5.
17. Ali, O.; Mohammed, O.A. Cyber-HIL Autonomous Inverter-Based Microgrid Framework: Control System Performance and Communication Network Quality of Service. In *2024 IEEE Industry Applications Society Annual Meeting (IAS)*; IEEE: New York, NY, USA, 2024; pp. 1–8.
18. Glover, J.D.; Overbye, T.J.; Sarma, M.S. *Power System Analysis and Design*, 6th ed.; Cengage Learning: Boston, MA, USA, 2017.
19. *ANSI C84.1-2020*; Electric Power Systems and Equipment—Voltage Ratings (60 Hertz). American National Standards Institute: Washington, DC, USA, 2020.
20. Schneider, K.P.; Mather, B.A.; Pal, B.C.; Ten, C.W.; Shirek, G.J.; Zhu, H.; Fuller, J.C.; Pereira, J.L.R.; Ochoa, L.F.; de Araujo, L.R.; et al. Analytic Considerations and Design Basis for the IEEE Distribution Test Feeders. *IEEE Trans. Power Syst.* **2018**, *33*, 3181–3188. [CrossRef]
21. Shen, G.; Tucker, R.S. Energy-minimized design for IP over WDM networks. *J. Opt. Commun. Netw.* **2009**, *1*, 176–186. [CrossRef]
22. Sundararajan, A.; Chavan, A.; Saleem, D.; Sarwat, A.I. A Survey of Protocol-Level Challenges and Solutions for Distributed Energy Resource Cyber-Physical Security. *Energies* **2018**, *11*, 2360. [CrossRef]
23. Qiu, D.; Liu, M.; Zhang, R.; Luo, T.; Griffo, A.; Zhang, X. Cyber-Physical Real-Time Digital Simulation for Cybersecurity Analysis in Microgrids. *IEEE Trans. Ind. Cyber-Phys. Syst.* **2025**, *3*, 429–441. [CrossRef]
24. Exata Network Modeling. Available online: https://www.keysight.com/us/en/product/SN100EXBA/exata-network-modeling.html (accessed on 16 April 2026).
25. Varga, A. Discrete event simulation system. In Proceedings of the European Simulation Multiconference (ESM'2001), Prague, Czech Republic, 6–9 June 2001; Volume 17, p. 7.
26. Cassandras, C.G. Discrete-event systems. In *Handbook of Networked and Embedded Control Systems*; Springer: Cham, Switzerland, 2005; pp. 71–89.
27. Keysight. Available online: https://www.keysight.com/ (accessed on 16 April 2026).
28. Migoni, G.; Kofman, E.; Cellier, F. Quantization-based new integration methods for stiff ordinary differential equations. *Simulation* **2012**, *88*, 387–407. [CrossRef]
29. IEEE PES Test Feeder. Available online: https://cmte.ieee.org/pes-testfeeders/resources/ (accessed on 2 April 2026).
30. Ali, O.; Aghmadi, A.; Mohammed, O.A. Performance evaluation of communication networks for networked microgrids. *e-Prime-Adv. Electr. Eng. Electron. Energy* **2024**, *8*, 100521. [CrossRef]
31. Ali, O.; Mohammed, O.A. A Network-Aware Cyber-Physical Testbed for Internet of Energy Systems: Communication-Centric Control and Cyber Vulnerability Analysis. *IEEE Netw.* **2025**, *40*, 272–280. [CrossRef]
32. Dabashi, A.H.; Maleki, S.; Mukherjee, B.; Epiphaniou, G.; Maple, C.; Konstantinou, C.; Lakshminarayana, S. Cybersecurity Issues in Local Energy Markets. *arXiv* **2025**, arXiv:2507.01536.
33. World Economic Forum. *The Global Risks Report 2026*; Technical report; World Economic Forum: Geneva, Switzerland, 2026.
34. Krkoleva Mateska, A.; Krstevski, P.; Borozan, S. Overview and improvement of procedures and practices of electricity transmission system operators in south east europe to mitigate cybersecurity threats. *Systems* **2021**, *9*, 39. [CrossRef]
35. Hijgenaar, S.; Ștefanov, A.; Van Voorden, A.M.; Palensky, P. Cyber Resilience of Electric Vehicle Charging in Smart Grids: The Dutch Case. *IEEE Access* **2025**, *13*, 111454–111483. [CrossRef]

36. Musleh, A.S.; Chen, G.; Liu, B.; Fan, S.; Al-Durra, A.; Muyeen, S.; Dong, Z.Y.; Ambia, M.N.; Gjorgiev, B.; Tao, S.; et al. Cybersecurity challenges in renewable-dominated power grids addressing vulnerabilities and resilience strategies. *Cell Rep. Phys. Sci.* **2026**, *7*, 103261. [CrossRef]
37. Aftab, M.A.; Hussain, S.S.; Farooq, S.M.; Venkatraman, M.S.; Ahmed, S.; Konstantinou, C. Sunspec Modbus Based Smart Inverter Cyber-Attack Modeling and Mitigation Scheme. *IEEE Trans. Ind. Inform.* **2025**, *22*, 486–497. [CrossRef]