Cyber-Physical Power System Modelling and Digital Co-Simulation for Grid Operation

Dongmeng Qiu

A thesis submitted in partial fulfilment of the requirements for the degree of

Doctor of Philosophy

The University of Sheffield
School of Electrical and Electronic Engineering

Principle Supervisor: Xin Zhang

April 2026

Acknowledgements

I have always believed that human beings are remarkable. We are not the fastest like cheetahs, nor do we possess the sharp vision of eagles or the strength of elephants. Yet, we stand at the top of the world. It is because we know how to use tools, how to collaborate, and how to unite for a shared purpose. This belief has accompanied me throughout my PhD journey, reminding me that no achievement is ever the result of an individual alone.

First and foremost, I would like to express my deepest gratitude to my supervisor, Professor Xin Zhang. From the very beginning, he guided me with patience, calmness, and understanding. I have never considered myself to be particularly talented, yet he has consistently supported and trained me, from someone with little knowledge of research to someone now capable of guiding junior students. His mentorship has shaped not only my academic ability but also my attitude towards research and life. I would also like to sincerely thank my second supervisor, Dr Pablo, for his valuable guidance and support. Beyond academic advice, he has shared with me many insights into life, which have broadened my perspective and influenced my personal development.

I would also like to thank Dr Mengxiang Liu, Dr Suhan Zhang, Dr Min Du and Dr Rong Zeng. As postdoctoral researchers, they have been role models to me. Their dedication, professionalism, and work ethic have set a standard that I continue to learn from.

My deepest appreciation goes to my parents. Studying in the UK has been financially demanding, and they have made great sacrifices to support me and encouraged me to pursue my dreams abroad. Their love and support are the foundation of everything I have achieved, and I will always be grateful.

I am also thankful to my friends, especially those who played football with me every Friday. Before coming here, I never imagined I would meet so many local friends. Those moments on the pitch not only kept me physically healthy but also brought balance and joy to my life during this difficult journey. A kind reminder to Luke and Yuchi: please drive safely. Moreover, thank you all from HJDC(nickname as 'Royal Casino'). I hope our friendship last forever.

Finally, I would like to thank myself. As Shakespeare wrote, "This above all: to thine own self be true." I am grateful that I pursued this degree not for external recognition or a sense of superiority, but for a deeper purpose in life. This belief has given me the strength to face obstacles with patience, and even with a smile. Compared to many people who have achieved far greater things, the challenges I've faced along the way are insignificant, but it is precisely these challenges that have shaped who I am today. This PhD journey has not always been easy, but it has given me many meaningful and beautiful memories.

Many of them are not directly related to research, but without this decision on pursuing PhD degree, they would never have happened.

Looking ahead, I hope to continue moving forward with purpose and to contribute, in my way, to making this world a better place. I also sincerely wish that all the people I have met along this journey—friends, colleagues, and teachers—will achieve their goals and find happiness in their lives.

Abstract

The rapid digitalisation of modern power systems has transformed conventional grids into cyber-physical power systems (CPPS), where physical power networks are tightly integrated with communication, computation, and control infrastructures. While this integration enables advanced monitoring, coordination, and large-scale deployment of distributed energy resources (DERs), it also introduces new vulnerabilities and uncertainties arising from complex cyber–physical interactions. In particular, the propagation of cyber contingencies and multi-source uncertainties in CPPS and their impacts on system operation remain insufficiently understood.

This thesis investigates modelling, analysis, and real-time simulation methodologies for CPPS, with a focus on distribution networks and microgrids. A general cyber-physical modelling framework is developed by coupling differential–algebraic equation (DAE)-based power system models with discrete-event communication network models. Within this framework, node-specific communication delays are used to represent cyber–physical interactions. Based on this framework, a virtual–physical power flow method is proposed to analyse CPPS contingencies and vulnerabilities under coordinated cyber and physical disturbances. A composite vulnerability index incorporating voltage deviation, communication latency, and cyber–physical node betweenness is further developed to identify critical components under cyber contingencies.

To quantify uncertainty impacts, a global sensitivity analysis method based on probabilistic modelling and Sobol' indices is introduced. Uncertainties in load demand, photovoltaic generation, and communication delays are modelled using suitable probability distributions, and a Monte Carlo-based approach is applied to evaluate their influence on system dynamics. Results show that photovoltaic uncertainty dominates bus voltage variation, while communication delays mainly produce localised effects on voltage stability and non-negligible impacts on frequency dynamics.

To validate the proposed methods, several real-time cyber-physical co-simulation platforms integrating OPAL-RT or Typhoon HIL with EXata or OMNeT++ are developed using different synchronisation schemes. These platforms enable realistic emulation of cyber attacks and demonstrate the effectiveness of the proposed methodologies for CPPS vulnerability assessment and cybersecurity analysis.

List of Publications

Journal Articles

1. **Qiu, D.**, Zhang, R., Zhou, Z., Zhang, J., and Zhang, X.: Virtual-physical power flow method for cyber-physical power system contingency and vulnerability assessment. *IET Smart Grid*, vol. 7, no. 1, pp. 13–27, 2024. doi: 10.1049/stg2.12143.

2. **Qiu, D.**, Liu, M., Zhang, R., Luo, T., Griffo, A., and Zhang, X.: Cyber-Physical Real-Time Digital Simulation for Cybersecurity Analysis in Microgrids. *IEEE Transactions on Industrial Cyber-Physical Systems*, vol. 3, pp. 429–441, 2025. doi: 10.1109/TICPS.2025.3569640.

3. **Qiu, D.**, S. Zhang, T. Luo and X. Zhang, "Global Sensitivity Analysis for Cyber-Physical Power Distribution Network," in IEEE Transactions on Industrial Cyber-Physical Systems, vol. 4, pp. 213-224, 2026, doi: 10.1109/TICPS.2026.3674974.

Conference Papers

1. **Qiu, D.**, Liu, M., and Zhang, X.: Developing Cyber-Physical Power System Co-Simulation Platform with Real-Time Digital Interface. In *Proceedings of the 2025 IEEE Kiel PowerTech*, Kiel, Germany, 2025, pp. 1–6. doi: 10.1109/PowerTech59965.2025.11180418.

2. **Qiu, D.**, Liu, M., and Zhang, X.: A Power-Communication Co-Simulation Platform for Real-Time Microgrid Cyber Security Analysis. In *Proceedings of the 2024 International Conference on Artificial Intelligence of Things and Systems (AIoTSys)*, Hangzhou, China, 2024, pp. 1–6. doi: 10.1109/AIoTSys63104.2024.10780642.

3. **Qiu, D.**, Zhang, R., Dabashi, A. H., Zhou, Z., and Zhang, X.: Cyber-physical contingency and vulnerability assessment using double power flow method. In *IET Conference Proceedings*, vol. 2022, no. 27, pp. 194–199, 2023. doi: 10.1049/icp.2023.0098.

Contents

List of Tables

List of Figures

Nomenclature

CPPS	Cyber–Physical Power Systems
CPS	Cyber–Physical Systems
GSA	Global Sensitivity Analysis
VPPF	Virtual Power–Physical Flow
HIL	Hardware-in-the-Loop
DAE	Differential–Algebraic Equation
EMT	Electromagnetic Transient
IBR	Inverter-Based Resource
PV	Photovoltaic
SCADA	Supervisory Control and Data Acquisition
PMU	Phasor Measurement Unit
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
OPAL-RT	OPAL Real-Time Simulator
RTDS	Real-Time Digital Simulator
PAI	Platform Assessment Index
FDI	False Data Injection
DoS	Denial of Service

Declaration

I, the author, confirm that the Thesis is my own work. I am aware of the University's Guidance on the Use of Unfair Means (https://www.sheffield.ac.uk/study-skills/assessment/academic-integrity/academic-integrity). This work has not previously been presented for an award at this, or any other, university.

All publications arising from the thesis are acknowledged in this section:

Qiu, D., Zhang, R., Zhou, Z., Zhang, J., and Zhang, X.: Virtual-physical power flow method for cyber-physical power system contingency and vulnerability assessment. *IET Smart Grid*, vol. 7, no. 1, pp. 13–27, 2024. doi: 10.1049/stg2.12143.

Qiu, D., Liu, M., Zhang, R., Luo, T., Griffo, A., and Zhang, X.: Cyber-Physical Real-Time Digital Simulation for Cybersecurity Analysis in Microgrids. *IEEE Transactions on Industrial Cyber-Physical Systems*, vol. 3, pp. 429–441, 2025. doi: 10.1109/TICPS.2025.3569640.

Qiu, D., S. Zhang, T. Luo and X. Zhang, "Global Sensitivity Analysis for Cyber-Physical Power Distribution Network," in IEEE Transactions on Industrial Cyber-Physical Systems, Early Access doi: 10.1109/TICPS.2026.3674974

Qiu, D., Zhang, R., Dabashi, A. H., Zhou, Z., and Zhang, X.: Cyber-physical contingency and vulnerability assessment using double power flow method. In *IET Conference Proceedings*, vol. 2022, no. 27, pp. 194–199, 2023. doi: 10.1049/icp.2023.0098.

Qiu, D., Liu, M., and Zhang, X.: A Power-Communication Co-Simulation Platform for Real-Time Microgrid Cyber Security Analysis. In *Proceedings of the 2024 International Conference on Artificial Intelligence of Things and Systems (AIoTSys)*, Hangzhou, China, 2024, pp. 1–6. doi: 10.1109/AIoTSys63104.2024.10780642.

Qiu, D., Liu, M., and Zhang, X.: Developing Cyber-Physical Power System Co-Simulation Platform with Real-Time Digital Interface. In *Proceedings of the 2025 IEEE Kiel PowerTech*, Kiel, Germany, 2025, pp. 1–6. doi: 10.1109/PowerTech59965.2025.11180418.

Chapter 1

Introduction

1.1 Background

The global energy transition towards low-carbon electricity systems has fundamentally transformed the structure and operation of modern power networks. Driven by climate commitments, electrification of transport and heating, and large-scale integration of renewable energy sources, national power systems are evolving from centrally controlled infrastructures to highly distributed, data-intensive, and dynamically interconnected networks. The National Energy System Operator (NESO) has published its "Zero Carbon Operations by 2025" roadmap, formally outlining the strategic transformation of the UK electricity system operations. The report shows an ambition to operate the Great Britain electricity system safely and securely at zero carbon whenever sufficient renewable generation is available to meet total national demand [1]. To achieve this objective requires significant improvement from traditional operation, where conventional synchronous generators historically provided essential services such as inertia, frequency response, voltage control, and short-circuit infeed.

At the global level, the scale of renewable expansion further reinforces the size of this transformation. According to the Renewables 2025 Global Status Report, cumulative global solar photovoltaic (PV) capacity exceeded 2.2 TW by the end of 2024, with a record-breaking 602 GW added within a single year, representing an annual growth rate of 37%. Solar PV generation reached approximately 2,131 TWh in 2024, accounting for 6.9% of global electricity production. Moreover, 23 countries achieved solar PV shares exceeding 10% of national electricity generation, and five countries exceeded 20%, illustrating the emergence of structurally high renewable penetration levels [2]. These developments indicate that renewable variability is no longer a marginal perturbation but a structural characteristic of modern power systems.

Therefore, future power systems will increasingly rely on digitally coordinated re-

newable resources, inverter-dominated generation, and advanced real-time control mechanisms. As renewable penetration increases and system inertia declines, uncertainty associated with renewable variability and communication-layer dynamics becomes structurally embedded within the system operation [3]. The transition toward zero-carbon operation consequently places greater emphasis on modelling approaches that can capture renewable variability, communication delays, and system-service interactions within a unified analytical environment. Such modelling requirements have become increasingly important as cyber–physical coupling increasing in modern distribution networks.

Traditionally, power systems were designed as physical infrastructures, where generation, transmission, and distribution processes were analysed through deterministic steady-state and transient models. However, the increasing reliance on communication networks for monitoring, control, and protection has fundamentally changed this operation mode. Modern power systems now operate as tightly coupled cyber-physical power systems (CPPS), where computational intelligence, communication networks, and physical electrical dynamics interact continuously [4–6]. In such systems, sensor measurements, communication delays, packet losses, and cyber events can directly influence generator outputs, inverter control actions, and network stability. The power grid is therefore no longer an isolated physical system, but a multi-layered cyber-physical system whose performance depends on both electrical and communication infrastructures.

The distribution network represents one of the most critical domains in this transformation. Unlike transmission networks, distribution systems host a high concentration of renewable distributed energy resources (DERs), particularly rooftop and utility-scale PV installations and windfarms [7]. As penetration levels increase, voltage regulation, reverse power flow, and local stability challenges become more severe. High PV penetration introduces stochastic power injection patterns that vary with irradiance, weather conditions. These characteristics significantly complicate operational planning and real-time control. In practical systems, PV inverters are typically coordinated via communication networks and supervisory control strategies, further strengthening the cyber-physical coupling.

In this context, uncertainty becomes a structural property rather than a marginal perturbation. Two dominant sources of uncertainty has added to the CPPS. The first originates from renewable generation variability. Solar irradiance exhibits both temporal and spatial randomness, and when multiple PV units are connected within a distribution network, their outputs may exhibit correlated or independent fluctuations depending on geographical and atmosphere conditions [8]. The second source arises from communication infrastructure. Communication delays, data exchange intervals, and synchronisation mechanisms influence the effectiveness of control strategies and may introduce dynamic deviations in voltage or frequency regulation [9]. Furthermore, communication delay is often node-dependent, protocol-dependent, and affected by network congestion, routing structure, and scheduling strategy. For distribution-level cyber-physical systems, where

control loops may operate at sub-second timescales, even modest latency variations can influence dynamic performance.

From a modelling perspective, differential–algebraic equation (DAE) formulations remain the standard approach for representing power system dynamics. Electrical networks are typically described through coupled differential equations to capture generator and inverter dynamics, together with algebraic equations to represent network power balance constraints [10]. Within this continuous-time framework, state variables such as bus voltages, currents, and inverter internal states are updated according to physical laws governed by electromagnetic and electromechanical interactions. When stochastic renewable inputs are introduced, additional uncertainty is embedded into the system states, increasing the analytical and computational complexity of the DAE formulation.

In contrast, communication networks are commonly modelled using graph-theoretic and complex network representations, where nodes correspond to communication devices and edges represent data transmission links [11]. Such models emphasise network topology, routing paths, connectivity, and latency characteristics rather than continuous electrical dynamics. Communication delays, packet loss, and scheduling mechanisms are often described using discrete-event or probabilistic models defined over network graphs. The combination of continuous-time DAE-based power system models and graph-based communication network models introduces new modelling structure within cyber–physical systems. Consequently, integrating multi-source uncertainty across these distinct representations introduces additional challenges and has attracted increasing attention in recent research.

Beyond modelling, quantitative evaluation of uncertainty influence is equally critical. Classical local sensitivity analysis provides limited insight when system behaviour is nonlinear and influenced by multiple interacting parameters. Global Sensitivity Analysis (GSA), particularly variance-based approaches such as Sobol' indices, offers a effective method to quantify the contribution of individual uncertain inputs and their interactions to output variability [12, 13]. By decomposing output variance into first-order and total-effect components, GSA enables identification of dominant drivers of system behaviour.

In addition, as cyber-physical systems are real-time systems in reality, simulation platforms should reflect synchronisation mechanisms and data-exchange characteristics realistically. Hardware-in-the-loop (HIL) and real-time co-simulation architectures have emerged as powerful tools to validate cyber-physical models under realistic timing constraints [14, 15]. Existing studies have explored probabilistic modelling, communication delay analysis, and real-time co-simulation techniques, often addressing these aspects separately. Their combined integration within a unified analytical and experimental environment remains an active area of research.

1.2 Motivation

The transformation towards CPPS has been widely acknowledged in both academia and industry. However, despite extensive research activities, existing studies have not formed a general framework in the domains of modelling, uncertainty analysis, and experimental validation. This constrains the capacity for systematic analysis and demonstration of how the volatility of renewable energy sources and the dynamics of the communication layer jointly influence CPPS behaviour, particularly under inverter-dominant and digitally coordinated operating conditions.

First of all, from a modelling perspective, a substantial portion of the literature represents communication effects using simplified delay assumptions [16]. While such simplifications improve mathematical tractability, they fail to capture the node-dependent and protocol-dependent latency characteristics inherent in practical communication infrastructures. In distribution networks and microgrids, where control loops operate at microsecond- and millisecond-level time scales, oversimplifying structured delay representation may lead to incomplete cyber–physical coupling models and potentially inaccurate dynamic stability assessment. A unified formulation that systematically embeds node-specific communication delay into differential–algebraic equation (DAE)-based power system models therefore remains underdeveloped.

In addition, from an uncertainty quantification perspective, most probabilistic power system studies primarily focus on physical uncertainties, such as renewable generation variability or load fluctuations, while communication-related uncertainties are often treated as deterministic or secondary parameters [17]. Although Monte Carlo simulations are widely adopted, they typically assess aggregate output variance without decomposing the relative contributions and interaction effects of multiple uncertainty sources [18]. In CPPS, renewable fluctuations and communication delays both exist and interact in nonlinear and time-varying manners. The absence of a structured variance-based global sensitivity framework capable of time-resolved decomposition limits systematic understanding of uncertainty propagation mechanisms and localisation characteristics in CPPS.

Moreover, there is a gap exists between theoretical modelling and experimental validation. Many cyber–physical modelling studies are numerical and do not explicitly consider real-time synchronisation constraints, hardware latency, or data-exchange mechanisms [19]. However, CPPS operate under real-time digital coordination, where scheduling strategies, communication protocols, and hardware-induced delays may influence dynamic behaviour. Without hardware-in-the-loop (HIL) or real-time co-simulation validation, it remains unclear whether proposed delay models and uncertainty formulations accurately reflect operational conditions.

Overall, current research efforts tend to (i) simplify communication delay representa-

tion, (ii) isolate renewable and cyber uncertainties in analysis, and (iii) lack experimentally validated integration across modelling and uncertainty quantification. These limit the development of delay-aware and uncertainty-resilient operational strategies for digitalised distribution networks.

Therefore, there is a need for a unified analytical and experimental framework that integrates DAE-based cyber–physical modelling, structured node-specific communication delay uncertainty representation, time-varying Sobol global sensitivity analysis, and real-time co-simulation validation. Establishing such a framework is essential for systematically analysing multi-source uncertainty interaction mechanisms and bridging the gap between theoretical cyber–physical modelling and practical system operation.

1.3 Aims and Objectives

1.3.1 Research Aim

The aim of this thesis is to establish a comprehensive digital co-simulation framework for cyber-physical power systems that integrates unified modelling, uncertainty quantification, and real-time validation.

Specifically, this research seeks to bridge the gap between cyber–physical modelling theory and experimentally validated system analysis by integrating differential–algebraic equation (DAE)-based systems, delay uncertainty modelling, global sensitivity analysis, and real-time co-simulation architecture into a analytical digital co-simulation platform.

1.3.2 Objectives

To achieve the above research aim, the following specific objectives are defined:

- To develop a unified cyber–physical modelling framework by integrating differential–algebraic equation (DAE)-based power system models with communication network representations, enabling explicit modelling of communication network characteristics and cyber–physical coupling mechanisms.
- To formulate a structured uncertainty representation for cyber–physical systems, incorporating stochastic renewable generation and communication delay uncertainties, and to embed these uncertainties into the unified modelling framework.
- To establish CPPS assessment such as global sensitivity analysis (GSA) approach based on Sobol' indices, enabling quantitative decomposition of the contributions

and interaction effects of multiple uncertainty sources, with time-resolved sensitivity evaluation.

- To design and implement real-time cyber–physical co-simulation platforms that integrate power system simulators and communication network emulators through efficient synchronisation and data exchange mechanisms.
- To validate the proposed modelling and analysis methodologies through hardware-in-the-loop (HIL) and real-time co-simulation experiments, and to assess platform performance under different cyber–physical scenarios.

1.4 Contributions

According to the research gaps that identified in the following Chapter 2, the main contributions of this thesis can be summarised as follows:

1. A Unified Cyber–Physical Modelling Framework

Research Gap: Existing CPPS modelling approaches lack a unified representation that can simultaneously capture detailed physical power system dynamics and communication network behaviour. Graph-theoretic and complex network models primarily focus on topological properties and neglect electrical characteristics such as power flow constraints and dynamic state evolution. Conversely, conventional power system models incorporate communication effects only in a highly simplified manner, often treating them as static or aggregated parameters. As a result, critical cyber–physical interactions, such as node-specific communication delays and their impact on system dynamics, are not explicitly represented. Furthermore, the bidirectional coupling between the cyber layer (data exchange) and the physical layer (power flow) remains inadequately modelled in existing frameworks.

To address this limitation, a unified cyber–physical modelling framework is developed based on the proposed Virtual–Physical Power Flow (VPPF) method. The framework integrates graph-theoretic representation of communication networks with differential–algebraic equation (DAE)-based power system modelling, enabling explicit characterisation of the bidirectional coupling between communication-layer dynamics and physical power flow behaviour. Within this framework, cyber-layer information exchange and physical-layer power flow are modelled to capture the impact of communication latency, network topology on system operating states. This provides a systematic foundation for vulnerability assessment in CPPS.

2. Sobol Global Sensitivity Analysis for CPPS

Research Gap: Existing CPPS assessment methodologies mainly focus on either

structural vulnerability metrics or physical-layer uncertainties, with limited consideration of cyber-induced uncertainties. Most vulnerability assessment approaches rely on static indices or deterministic scenarios, which fail to capture the stochastic and dynamic nature of cyber–physical interactions. In particular, communication uncertainties—such as stochastic delays, packet loss, and cyber disturbances—are rarely incorporated into uncertainty quantification frameworks. Moreover, existing global sensitivity analysis studies are limited to renewable generation and load variability, neglecting the interaction effects between cyber layer and physical layer uncertainties. The lack of a systematic framework to quantify both individual and coupled impacts of multi-source uncertainties limits the understanding of the impact of uncertainty in CPPS.

To address this gap, a variance-based global sensitivity analysis (GSA) framework is developed to systematically quantify the impact of multiple uncertainty sources in cyber–physical power systems, including renewable generation variability and node-specific communication delays. Based on Sobol' indices, the framework evaluates both first-order and total-effect sensitivity measures, enabling the decomposition of individual contributions and higher-order interaction effects among cyber and physical parameters. To capture the dynamic nature of cyber–physical coupling, a time-resolved sensitivity analysis approach is proposed, enabling sensitivity metrics to illustrate how sensitivity varies across different time intervals during system operation.

3. Cyber–Physical Real-Time Digital Simulation Platforms

Research Gap: Existing co-simulation and real-time digital simulation platforms for CPPS are often limited by simplified communication modelling, restricted scalability, and a lack of systematic performance evaluation. Many platforms adopt abstract or idealised representations of communication networks, which fail to capture realistic network behaviours such as protocols, packet-level interactions, and cyber attack mechanisms. In addition, existing synchronisation strategies are typically designed for specific applications and lack flexibility in handling different types of simulators with different time scales. Scalability remains a significant challenge, particularly for large-scale systems requiring high temporal resolution. Furthermore, there is a lack of standardised evaluation metrics to assess key performance aspects such as synchronisation accuracy, computational overhead, latency, and cyber attack compatibility, making it difficult to compare different co-simulation architectures and determine their suitability for cybersecurity studies.

To overcome these limitations, a set of cyber–physical real-time digital simulation platforms are designed and implemented to validate the proposed modelling and analysis methodologies under realistic operational conditions. The platforms integrate DAE-based power system simulation with discrete-event communication network emulation through multiple synchronisation mechanisms and data exchange architectures.

Three representative co-simulation architectures are developed:

- A TCP-based master-slave synchronisation platform integrating Typhoon HIL with the EXata communication network simulator, enabling coordinated microgrid-level cyber–physical simulation.
- A TCP-based time-stepped synchronisation framework coupling OPAL-RT with EXata, supporting scalable simulation with shorter time step and larger network size.
- A UDP-based and shared memory based co-simulation architecture integrating OMNeT++ with OPAL-RT, enabling low-latency data exchange and efficient real-time interaction.

In addition to platform development, an evaluation metric, termed the platform assessment index (PAI), is proposed to quantitatively assess the performance of the co-simulation platforms in terms of efficiency, cyberattacks simulation capability, and communication capability. This index provides a systematic framework for comparing different co-simulation architectures and analysing their trade-offs under varying simulation configurations.

1.5 Thesis Outline

This thesis is structured around a progressive investigation of CPPS, moving from unified modelling, to uncertainty quantification, and finally to real-time digital co-simulation platform validation.

In addition, different co-simulation platforms are used across the thesis for different purposes. These platforms are not independent repetitions, but serve different stages of the research. Chapter 4 uses an OPAL-RT and OMNeT++ digital co-simulation platform with shared-memory-based time-stepped synchronisation to generate dynamic input–output data for global sensitivity analysis. Chapter 5 develops real-time cybersecurity-oriented co-simulation platforms by integrating Typhoon HIL or OPAL-RT with EXata, enabling realistic cyberattack emulation and platform performance assessment. The use of these platforms across the thesis is summarised in Table 1.1.

Table 1.1: Use of modelling and co-simulation platforms across the thesis

Chapter	**Platform**	**Use in the thesis**
Chapter 4	OPAL-RT–OMNeT++ with shared-memory time-stepped synchronisation	Generates dynamic input–output data for Sobol-based global sensitivity analysis of the IEEE 33-bus CPPS.
Chapter 5.1	Typhoon HIL–EXata with master–slave synchronisation	Establishes the real-time microgrid cybersecurity co-simulation platform.
Chapter 5.2	OPAL-RT–EXata with time-stepped synchronisation	Improves scalability and data exchange for larger real-time CPPS co-simulation.
Chapter 5.3	Typhoon HIL–EXata and OPAL-RT–EXata platforms	Compares platform performance under FDI, DoS, packet drop, and delay attack scenarios.

Chapter 1 introduces the research background, motivation, and objectives. It outlines the challenges arising from the increasing digitalisation of modern power systems and highlights the need for integrated modelling and co-simulation frameworks to analyse cyber–physical interactions.

Chapter 2 reviews the state of the art in cyber-physical power systems, including modelling frameworks, co-simulation methodologies, uncertainty quantification, and real-time digital simulation platforms. Based on this review, key research gaps are identified in unified cyber-physical coupling representation, time-resolved sensitivity analysis, and experimentally validated co-simulation frameworks.

Chapter 3 presents a virtual–physical power flow (VPPF) framework for CPPS modelling and vulnerability analysis. The proposed approach explicitly represents cyber–physical coupling and enables systematic evaluation of coordinated cyber and physical disturbances by a vulnerability index.

Chapter 4 develops a global sensitivity analysis (GSA) framework for cyber–physical distribution networks. Sobol' first-order and total-effect indices are employed to quantify the influence of uncertain photovoltaic generation and node-specific communication delays. The results reveal the localisation characteristics and interaction mechanisms of cyber–physical uncertainties.

Chapter 5 presents the development of cyber–physical real-time digital co-simulation platforms for CPPS validation. Multiple co-simulation architectures are designed and implemented, including master–slave, time-stepped synchronisation schemes, and shared-memory based frameworks, enabling flexible and scalable integration of power system simulation and communication network emulation. The chapter consolidates a series of experimental studies and platform implementations, supporting hardware-in-the-loop validation and cybersecurity-oriented analysis of cyber–physical interactions.

Chapter 6 concludes the thesis by summarising the main findings, contribution, and outlining future research directions.

Chapter 2

Literature Review of Cyber-Physical Power System Modelling and Real-time Digital Simulation

The concept of Cyber–Physical Systems (CPS) was first introduced by the U.S. National Science Foundation (NSF) in 2008. According to the definition provided in [20],

> Cyber-physical systems are physical, biological, and engineered systems whose operations are integrated, monitored, and/or controlled by a computational core. Components are networked at every scale. Computing is deeply embedded into physical processes, possibly even into materials. The computational core is typically an embedded system that requires real-time response and is often distributed. The behaviour of a cyber-physical system emerges from the tight integration of computational (logical) processes and physical dynamics.

Modern smart grids are widely recognised as a representative application of CPS [21]. In such systems, the traditional power infrastructure is tightly coupled with communication and information technologies, forming what is commonly referred to as a cyber-physical power system (CPPS).

In CPPS, the physical layer consists of electrical components such as generators, loads, circuit breakers, transformers, and transmission or distribution lines. The cyber layer comprises communication networks, monitoring devices, control systems, data processing units, and information transmission infrastructures. Through the interaction between these two layers, system monitoring, control, and protection functions can be realised in an integrated manner.

2.1 Fundamentals of Cyber–Physical Systems and Cyber–Physical Power Systems

The basic structure and operating principle of CPS are further introduced in this section. A CPS can be understood as a closed-loop system that connects the physical world with computation and communication processes [22,23]. In a typical CPS, sensors first measure the states of the physical process, such as temperature, speed, voltage, current, or mechanical position. These measurements are transmitted through a communication network to computational units, where monitoring, decision-making, optimisation, or control algorithms are executed. The resulting control commands are then sent to actuators, which influence the physical process. Therefore, CPS operation is formed by the continuous interaction among sensing, communication, computation, control, and actuation [24].

From a modelling perspective, a CPS can be described as a closed-loop hybrid system that combines continuous physical dynamics with discrete cyber-layer computation and communication processes [22, 25, 26]. A generic CPS representation can be written as

$$\dot{x}_p(t) = f_p\left(x_p(t), u_a(t), w_p(t)\right), \tag{2.1}$$
$$y_s(t) = h_p\left(x_p(t)\right) + v_s(t), \tag{2.2}$$
$$y_c[k] = \mathcal{N}_{p\to c}\left(y_s(t_k), \tau_k^m, \ell_k^m, e_k^m\right), \tag{2.3}$$
$$x_c[k+1] = f_c\left(x_c[k], y_c[k]\right), \tag{2.4}$$
$$u_c[k] = g_c\left(x_c[k], y_c[k]\right), \tag{2.5}$$
$$u_a(t) = \mathcal{N}_{c\to p}\left(u_c[k], \tau_k^u, \ell_k^u, e_k^u\right), \quad t \in [t_k, t_{k+1}), \tag{2.6}$$

where $x_p(t)$ denotes the continuous physical state, $u_a(t)$ is the actuation input applied to the physical process, $w_p(t)$ represents physical disturbances, $y_s(t)$ is the sensor measurement, and $v_s(t)$ denotes measurement noise. The cyber-layer state is denoted by $x_c[k]$, while $y_c[k]$ and $u_c[k]$ represent the received measurement and computed control command at the discrete cyber time step k, respectively. The operators $\mathcal{N}_{p\to c}(\cdot)$ and $\mathcal{N}_{c\to p}(\cdot)$ represent the measurement and control communication channels, where τ_k, ℓ_k, and e_k denote communication delay, packet-loss status, and data distortion, respectively.

A simplified communication operator can be expressed as

$$\mathcal{N}\left(z, \tau, \ell, e\right) = \begin{cases} z(t-\tau) + e, & \ell = 0, \\ z_{\text{hold}}, & \ell = 1, \end{cases} \tag{2.7}$$

where $z(t-\tau)$ represents the delayed signal, e represents data distortion or communication error, and z_{hold} denotes the most recently available value when packet loss occurs. This formulation illustrates that CPS behaviour is determined not only by the physical

dynamics, but also by the timing, reliability, and integrity of cyber-layer information exchange.

Different from conventional computer systems, CPS are directly connected to physical processes. Therefore, cyber-layer events can influence physical behaviour, while physical-layer disturbances can also affect cyber-layer operation. For example, communication delay, packet loss, data corruption, or cyberattacks may lead to incorrect or delayed control actions. Similarly, a physical fault may affect sensors, controllers, or communication devices. This bidirectional interaction makes CPS fundamentally different from purely cyber systems or purely physical systems [22].

Cyber–physical power systems (CPPS) are a specific type of CPS in the power and energy domain. When the generic CPS formulation is specialised to CPPS, the physical process is commonly represented by differential–algebraic equations, while cyber–physical coupling is introduced through delayed measurement and control signals. A compact CPPS form can therefore be written as

$$\dot{x}_{\mathrm{ps}}(t) = f_{\mathrm{ps}}\left(x_{\mathrm{ps}}(t), V(t), u_{\mathrm{ps}}(t)\right), \tag{2.8}$$

$$0 = g_{\mathrm{ps}}\left(x_{\mathrm{ps}}(t), V(t)\right), \tag{2.9}$$

$$u_{\mathrm{ps}}(t) = \phi\left(y_{\mathrm{ps}}(t - \tau(t))\right), \tag{2.10}$$

where x_{ps} denotes power-system dynamic states, V denotes algebraic network variables such as bus voltages, and $\tau(t)$ represents the communication-induced delay in the cyber–physical feedback loop.

In CPPS, the physical process is the electrical power network, including generators, converters, loads, transformers, transmission or distribution lines, and energy storage devices. The cyber layer includes sensors, communication networks, supervisory control systems, protection devices, and control centres. Compared with general CPS, CPPS have stricter requirements on real-time operation, stability, reliability, and security, because failures in the cyber layer may directly influence voltage regulation, frequency stability, power dispatch, and system protection [6]. The relationship between general CPS and CPPS is illustrated in Fig. 2.1.

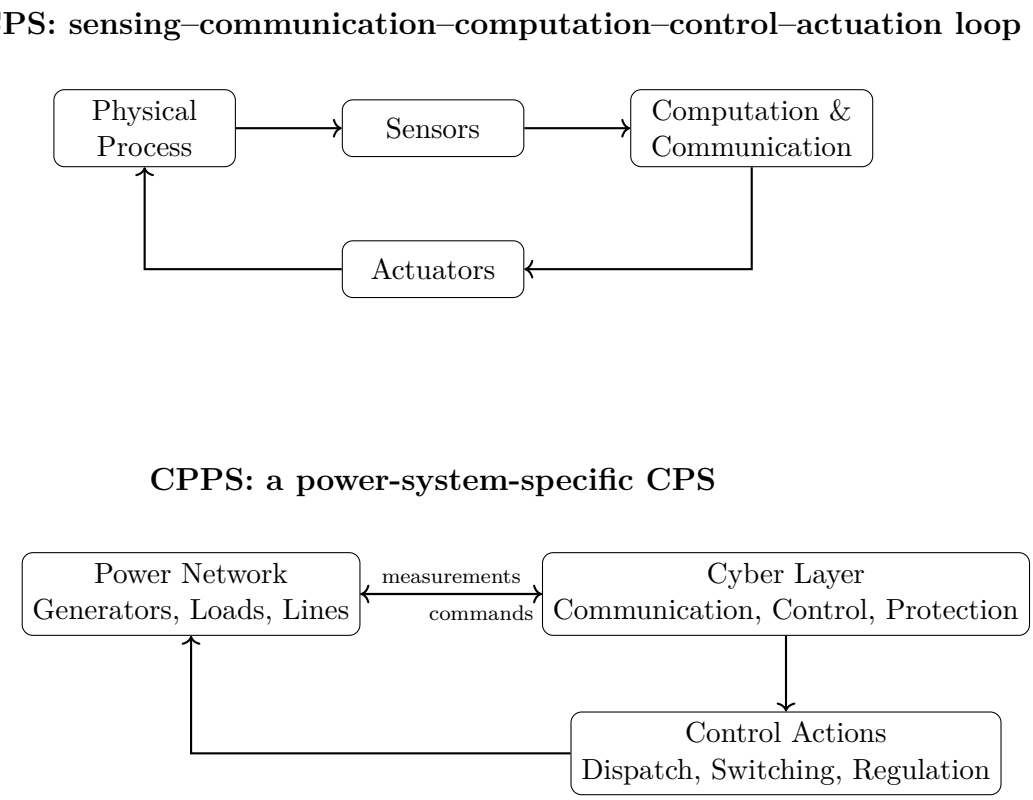


Figure 2.1: Basic structure of CPS and its specialisation into CPPS.

To improve the clarity of the literature review, the main techniques reviewed in this chapter are summarised using comparative tables. These tables provide an overview of the principles, strengths, limitations, and relevance of different CPPS modelling, assessment, and co-simulation approaches. Rather than duplicating the detailed methodological figures presented in later chapters, the tables are used to support a concise comparison of the existing techniques and to clarify the research gaps addressed in this thesis.

2.2 Cyber-Physical Power System Modelling

The smart grid represented the deep integration of power systems and communication networks. Traditional power system modelling primarily focuses on the physical dynamics of electrical networks, while the influence of communication infrastructures and cyber interactions is often neglected. However, in CPPS, disturbances or contingencies may propagate through both the physical layer and the cyber layer. Therefore, it becomes necessary to develop modelling frameworks that can capture the interactions between these two domains.

To address this challenge, extensive research has been conducted on cyber-physical power system modelling from different perspectives.

2.2.1 Modelling Method Based on Network Theory

2.2.1.1 Complex Network Modelling

Complex network-based modelling represents CPPS as unified network structures composed of nodes and edges, where both power system components and communication elements are abstracted into a common graph representation. This approach enables the analysis of large-scale system properties using tools from network science, particularly for studying structural characteristics, vulnerability, and cascading failures.

In [27], an integrated cyber–physical network was constructed by combining the electrical power system and information and communication technology (ICT) infrastructure into a single adjacency matrix representation. Network metrics, such as betweenness centrality, were introduced to identify critical nodes and edges that play important roles in both power transmission and information flow. Subsequent studies extended this framework to vulnerability assessment and cascading failure analysis [28,29], as well as stochastic modelling of failure propagation under uncertainty [30,31].

Additional developments incorporated concepts such as small-world networks [32] and community detection methods [33] to characterise network structure and identify functional clusters within CPPS. These approaches provided valuable insights into system robustness and the topological mechanisms of failure propagation.

However, by abstracting both cyber and physical components into a unified network model, these methods inherently simplified or neglected key electrical characteristics of power systems, such as dynamic behaviour, power flow constraints, and control mechanisms. As a result, while complex network-based modelling was effective for structural and vulnerability analysis, it was limited in its ability to capture detailed cyber–physical interactions and system dynamics at the operational level.

2.2.1.2 Graph-Theoretic Modelling

Graph-theoretic modelling can be viewed as a special subset of complex network approaches, where CPPS are represented using node–edge structures with an emphasis on topological relationships and computational efficiency. Unlike complex network modelling, which focuses on statistical network properties and metrics such as centrality and small-world characteristics, graph-theoretic methods primarily exploit the structural representation of nodes and edges to enable efficient analysis and algorithm implementation.

In this context, graph-based techniques have been widely applied to improve the scalability and computational performance of power system analysis. For example, [34] proposed a graph computing-based approach for real-time topology analysis, while [35]

introduced graph databases and distributed graph computing platforms, such as Giraph, GraphLab, and GraphChi, for cyber–physical power system simulation.

Furthermore, graph-theoretic formulations have been integrated into power flow analysis. In [36], it was shown that iterative methods such as the Gauss method and key steps of the Newton–Raphson algorithm can be naturally mapped onto graph processing operations, significantly improving computational efficiency for large-scale systems.

Despite their advantages in scalability and computational efficiency, graph-theoretic approaches remained largely focused on structural representations and algorithmic acceleration. As a result, they provide limited capability to capture detailed electrical dynamics and cyber–physical interactions, particularly when communication behaviours and control mechanisms need to be explicitly modelled.

2.2.2 Modelling Method Based on Power Flow Model

Power flow-based modelling represents a fundamentally different approach to CPPS modelling, where cyber-layer characteristics are embedded directly into the physical power system framework. Instead of abstracting the system into a unified network structure, this approach extends conventional power flow formulations to incorporate communication processes, enabling unified analysis within a physically interpretable modelling method.

Building upon the well-established foundation of power flow analysis governed by Kirchhoff's laws, several studies have introduced analogies between electrical power flow and information flow in communication networks. In [37], the communication network was transformed into an equivalent power network representation, where cyber links were modelled as branches with functional characteristics. This allowed information flow to be analysed using formulations analogous to the nodal admittance matrix, thereby enabling unified cyber–physical co-simulation and contingency assessment.

Further developments have incorporated dynamic behaviours in both cyber and physical domains. For instance, [38] integrated dynamic routing models for communication networks with dynamic load flow analysis, enabling the study of interactions between packet transmission processes and power system dynamics. Such approaches provided a more comprehensive framework for analysing coupled phenomena, including cascading failures triggered by both electrical disturbances and communication congestion.

In addition, advanced modelling techniques have been proposed to enhance the representation of cyber–physical interactions. The work in [39] introduced a POD-based load shedding strategy to simulate multiple failure modes, while [40] proposed a correlation matrix-based formulation to represent interdependencies among physical, communication, and control layers. These methods provided a systematic way to incorporate communica-

tion effects, such as delay, reliability, and control interactions, into power system models.

Overall, power flow-based modelling offered a natural and physically grounded framework for integrating cyber and physical domains, making it particularly suitable for unified analysis and co-simulation. However, in most existing approaches, communication processes were incorporated in a simplified or aggregated manner, with limited representation of protocol-level behaviour and node-specific delay characteristics. This limits their ability to capture detailed cyber–physical coupling and the impact of communication uncertainties on system dynamics.

Table 2.1: Comparison of CPPS modelling techniques

Technique	Main principle	Advantages	Limitations
Complex network modelling	Represents power and cyber infrastructures as interconnected nodes and edges.	Suitable for analysing topology, structural vulnerability, centrality, and cascading failure paths.	Simplifies electrical dynamics, power flow constraints, and control mechanisms.
Graph-theoretic modelling	Uses graph structures and adjacency relationships to represent CPPS topology and support computational analysis.	Efficient for topology analysis, routing representation, and large-scale structural studies.	Mainly focuses on structure and computational efficiency, with limited representation of detailed physical dynamics.
Power-flow-based modelling	Embeds cyber-layer effects into power flow or extended power system formulations.	Provides physically interpretable analysis and can link cyber contingencies with voltage, power flow, and operational impacts.	Communication processes are often simplified or aggregated, with limited protocol-level or node-specific delay modelling.
DAE-based cyber–physical modelling	Couples dynamic power system equations with communication-layer variables or delay functions.	Captures dynamic system behaviour and cyber–physical coupling more explicitly.	Requires higher computational effort and careful co-simulation or synchronisation design.

2.3 Cyber-Physical Power System Operational Assessment

While modelling frameworks provide a fundamental basis for representing the structural and dynamic behaviour of CPPS, they do not by themselves quantify how the system responds to disturbances, uncertainties, or coordinated cyber–physical disruptions. As

modern power systems become increasingly interconnected with communication networks, the propagation of disturbances is no longer confined to the physical domain but may evolve across both cyber and physical layers in a coupled and non-linear manner.

Consequently, systematic assessment methodologies are required to evaluate the performance and security of CPPS under a wide range of operating conditions. In particular, the presence of cyber-induced disturbances, communication delays, and renewable generation uncertainties introduces new dimensions of complexity that cannot be fully captured by conventional power system assessment techniques.

In this section, representative methodologies for cyber-physical systems assessment are reviewed, with particular focus on vulnerability assessment and global sensitivity analysis. These approaches provide complementary perspectives for understanding system weaknesses, identifying critical components, and analysing the propagation of uncertainties in CPPS environment.

2.3.1 Cyber-Physical Power System Vulnerability Assessment

Before reviewing specific assessment methods, it is necessary to clarify the meaning of vulnerability in the context of CPPS. In general, vulnerability refers to the susceptibility of a system, component, or function to performance degradation, instability, or failure when it is exposed to disturbances, uncertainties, or malicious attacks. In conventional power systems, vulnerability is mainly associated with physical components and operating conditions, such as transmission lines, buses, generators, loads, voltage stability, frequency stability, and cascading failures. In CPPS, however, vulnerability is extended from the physical layer to the cyber layer [6, 41].

The vulnerable components in CPPS can be broadly divided into three categories. The first category is the physical layer, including buses, transmission or distribution lines, generators, converters, transformers, loads, and distributed energy resources. These components may be vulnerable to physical faults, renewable generation variability, load fluctuations, equipment outages, and abnormal operating conditions. The second category is the cyber layer, including sensors, measurement units, communication links, routers, switches, controllers, SCADA systems, and control centres. These components may be vulnerable to communication delay, packet loss, data corruption, false data injection, denial-of-service attacks, and other cyber contingencies. The third category is the cyber–physical coupling, where cyber-layer disturbances affect physical power system operation through measurement, communication, and control loops. The examples of vulnerable components and corresponding threats are summarised in Table 2.2.

Therefore, vulnerability in CPPS does not only refer to whether a component can be attacked, but also to how seriously the system performance is affected after the distur-

bance occurs. This broader understanding provides the basis for vulnerability assessment methods that jointly consider physical impacts, cyber-layer characteristics, and cyber–physical interactions [41].

Table 2.2: Examples of vulnerable components and threats in CPPS

Layer	**Vulnerable components**	**Examples of threats or disturbances**
Physical layer	Buses, lines, generators, converters, loads, DERs	Faults, outages, renewable variability, load fluctuations, voltage or frequency instability
Cyber layer	Sensors, communication links, routers, controllers, control centres	Communication delay, packet loss, data corruption, FDI attacks, DoS attacks
Cyber–physical coupling	Measurement, communication, and control loops	Delayed feedback, incorrect control commands, cascading cyber–physical impacts

Vulnerability assessment is a fundamental approach for evaluating the resilience and security of CPPS under disturbances and cyber–physical threats. Early studies primarily focused on the impact of physical disturbances on system stability, where vulnerability was characterised by voltage deviations and the sensitivity of system states to power variations [42]. With the increasing integration of communication networks, recent research has extended vulnerability assessment to account for cyber–physical interactions.

Existing approaches can be broadly classified into index-based methods, probabilistic attack modelling, and topology-oriented resilience enhancement techniques.

Index-based methods evaluate system vulnerability using structural or operational metrics. For instance, [43] proposed a matrix-based framework to analyse cascading failures based on adjacency and dependency matrices, while [44] employed loss-of-load as an indicator to identify critical components. Similarly, graph-theoretic centrality indices were used in [45] to assess the importance of nodes and branches under contingency scenarios. Although these approaches were computationally efficient and interpretable, they were typically based on static representations and lack the ability to capture dynamic cyber–physical interactions.

Probabilistic methods model vulnerability from the perspective of attack processes and uncertainty. In [46], a Bayesian attack tree framework was developed to quantify the possibilities and impact of cyber-attacks on substations and control centres, considering the time required for attackers to compromise system components. Such approaches provide valuable insights into attack pathways and probabilistic risk, but they relied on predefined assumptions and simplified system representations, limiting their applicability to large-scale dynamic systems.

Topology-oriented approaches focus on enhancing system robustness through network design. For example, [47] investigated link addition strategies in interdependent

networks to improve system resilience, demonstrating that low-degree (LD) connection strategies can effectively enhance network robustness. However, these methods primarily address structural improvements and do not explicitly consider operational dynamics or cyber–physical coupling.

More recent studies have attempted to develop integrated vulnerability metrics that jointly consider cyber and physical domains. The Cyber-Physical Energy System Quantitative Security Metric (CPESQSM) proposed in [48] evaluates system security across electrical, cyber-risk, and network topology domains, providing a more comprehensive assessment framework. Nevertheless, such metrics were still largely based on aggregated indicators and lack the capability to capture time-varying interactions and uncertainty propagation in CPPS.

Overall, while existing vulnerability assessment methods provided valuable tools for identifying critical components and analysing system resilience, they were predominantly based on static or simplified representations. In particular, the dynamic coupling between cyber and physical layers, as well as the impact of communication uncertainties such as delay and data loss, were not explicitly modelled. This limited their ability to accurately characterise vulnerability in modern cyber–physical power systems.

2.3.2 Global Sensitivity Analysis for System Uncertainties

In addition to vulnerability assessment, uncertainty analysis has attracted increasing attention in modern power systems, particularly due to the high penetration of renewable energy sources and the increasing operational complexity. In CPPS, multiple sources of uncertainty coexist, including stochastic renewable generation, load variability, and communication-induced factors such as latency, packet loss, and data distortion. Among these factors, this thesis focuses particularly on load variation, PV generation uncertainty, and node-specific communication delay. These uncertainties interact in a coupled and non-linear manner, making it challenging to quantify their individual and joint impacts on system behaviour.

Global Sensitivity Analysis (GSA) provides a systematic framework for quantifying the influence of uncertain input parameters on system outputs over the entire input space. Compared with local sensitivity analysis, which evaluates system response around a nominal operating point, GSA captures non-linear effects and higher-order interactions among multiple inputs. Among various GSA techniques, variance-based methods, such as Sobol' indices [49–51], are widely adopted due to their ability to decompose output variance into contributions from individual parameters as well as their interactions.

Following variance-based GSA theory [52], uncertain inputs are varied probabilistically and their contributions to output variance are quantified. In this thesis, the changes

Table 2.3: Categorisation of uncertain inputs in CPPS global sensitivity analysis

Category	Variables changed in GSA	Physical interpretation
Load uncertainty	Active/reactive load demand or load multipliers	Represents stochastic demand variation in the physical distribution network.
Renewable-generation uncertainty	Solar irradiance or PV generation output	Represents renewable variability caused by changing weather and irradiance conditions.
Communication-system uncertainty	Node-specific communication delay τ_i	Represents uncertain cyber-layer latency in measurement, communication, and control loops.
Joint cyber–physical uncertainty	Simultaneous variation of PV generation and communication delay	Represents coupled uncertainty propagation between the physical and communication layers.

in sensitivity analysis refers to the probabilistic variation of uncertain input variables, rather than changes to the system topology, controller structure, or co-simulation platform. As the Table 2.3 shows, the uncertain inputs are categorised according to their physical origin, including physical-layer demand uncertainty, renewable-generation uncertainty, communication-layer uncertainty, and joint cyber–physical uncertainty. This classification provides a clear link between the general GSA concept reviewed in this chapter and the implementation presented later in Chapter 4, where load demand, PV generation, and node-specific communication delays are treated as uncertain inputs of the Sobol-based analysis.

Recent studies have applied GSA to power systems to analyse the impact of renewable generation uncertainty and load variability. For instance, [12] proposed a data-driven GSA framework for large-scale distribution systems using deep Gaussian processes, enabling scalable sensitivity analysis of voltage responses to uncertain power injections. Similarly, [13] extended GSA to integrated heat–electricity energy systems by developing a GenUT-based framework capable of efficiently handling correlated and non-Gaussian uncertainties.

More recently, advanced analytical approaches have been developed to improve the computational efficiency of GSA in power systems. In [53], an analytical probabilistic power flow (PPF) and GSA framework based on Gaussian mixture models (GMMs) was proposed, enabling direct computation of statistical characteristics and sensitivity indices without relying on large-scale Monte Carlo simulations.

In parallel, recent work has extended variance-based GSA methods to address more complex uncertainty characteristics in power systems. In [54], a framework was developed to incorporate correlated input variables into sensitivity analysis, enabling a more refined decomposition of uncertainty contributions. Such approaches improve the capability of GSA in capturing interactions and dependencies among input variables within physical

systems.

Despite these advances, existing GSA studies remained largely focused on uncertainties within the physical layer of power systems. Communication factors were typically neglected or simplified as deterministic parameters, and their interactions with physical processes were not explicitly represented. This limitation restricted the applicability of GSA in cyber–physical environments.

In CPPS, communication networks directly influence control actions and system dynamics through mechanisms such as information exchange delays, packet loss, and cyber contingencies. These effects are stochastic, time-varying, and dependent on network topology and protocols. However, such communication uncertainties have not been systematically incorporated into existing GSA frameworks.

Therefore, extending GSA to CPPS requires a unified modelling framework that explicitly integrates both physical and cyber uncertainties. By treating communication factors, such as node-specific delays and data loss, as stochastic input variables, it becomes possible to quantify their contributions to system behaviour and to analyse their interactions with physical uncertainties. This enables a more comprehensive understanding of uncertainty propagation in cyber–physical environments and forms a important contribution of this thesis.

Table 2.4: Comparison of CPPS assessment techniques

Technique	Assessment focus	Advantages	Limitations
Index-based vulnerability assessment	Evaluates critical components using indicators such as voltage deviation, latency, betweenness, or loss of load.	Simple, interpretable, and suitable for ranking vulnerable nodes or components.	Often static and may not fully capture stochastic uncertainty propagation or time-varying interactions.
Probabilistic risk or attack modelling	Represents uncertainty, attack likelihood, or failure propagation using probabilistic models.	Can capture uncertain operating conditions and attack scenarios.	Often depends on predefined assumptions and may be difficult to scale to detailed dynamic CPPS models.
Local sensitivity analysis	Evaluates output changes around a nominal operating point.	Computationally efficient and easy to implement.	Limited for nonlinear systems and does not capture global uncertainty interactions.
Global sensitivity analysis	Quantifies the contribution of uncertain inputs to output variability over the entire input space.	Captures nonlinear effects and interaction contributions among multiple uncertainties.	Requires a large number of model evaluations, especially when Monte Carlo-based Sobol' indices are used.

2.4 Cyber-Physical Co-Simulation Frameworks and Real-Time Digital Simulation Platforms

2.4.1 Co-Simulation Frameworks

Co-simulation has become a fundamental approach for analysing CPPS by enabling the integration of different simulators for power and communication networks. Comprehensive surveys, such as [55], have highlighted key challenges including time synchronisation, interoperability, and data exchange between continuous-time power system models and discrete-event communication processes. While these studies provide a systematic overview of existing architectures, most frameworks rely on simplified representations of communication dynamics, limiting their ability to capture detailed cyber–physical interactions.

To improve modelling fidelity, recent research has explored hybrid co-simulation approaches that combine different simulation methods. For example, EMT–phasor co-simulation has been widely adopted for analysing distribution networks with high penetration of inverter-based resources (IBRs). The work in [56] addressed interface inconsistency issues in unbalanced systems by introducing an improved initialisation strategy, ensuring accurate boundary conditions between EMT and phasor simulators. Such approaches enhanced numerical accuracy and computational efficiency, but primarily focussed on physical layer interactions and did not explicitly incorporate communication network dynamics.

Beyond hybrid physical-domain coupling, several studies have developed integrated cyber–physical co-simulation frameworks to enable interaction between power systems and communication networks. The framework proposed in [57] introduced a unified interface (CPPI) to coordinate heterogeneous simulators and support real-time data exchange across domains. Similarly, [58] developed a co-simulation framework for real-time reactive power control by integrating physical system simulation with cyber-layer optimisation and SCADA-based coordination. These frameworks demonstrated the feasibility of cross-domain integration; however, communication processes were typically abstracted, with limited modelling of protocol-level behaviour and network-induced delays.

Another important research direction focused on synchronisation strategies, which were critical for ensuring consistency and efficiency in co-simulation. The CoordTS method proposed in [59] improved upon conventional global event-driven approaches by introducing a hierarchical coordination mechanism, significantly reducing communication overhead between simulators. Despite these improvements, such strategies were often based on centralised coordination structures and still assumed simplified communication models, which restricted their applicability in large-scale and highly dynamic

cyber–physical systems.

In summary, existing co-simulation frameworks have made significant progress in integrating heterogeneous simulators and improving computational efficiency. However, several limitations remained. Most approaches treated communication networks in an abstract manner, without capturing node-specific and time-varying characteristics. In addition, the coupling between cyber and physical layers was often simplified, lacking explicit representation of how communication delays and network dynamics influence power system states. Furthermore, synchronisation mechanisms were typically designed for specific frameworks and may not scale efficiently for large and complex systems. These challenges highlighted the need for a unified co-simulation framework that explicitly models detailed cyber–physical coupling and communication dynamics, which is a key focus of this thesis.

2.4.2 Real-Time Digital Simulation Platforms

Building upon co-simulation frameworks, real-time digital simulation platforms extend these methodologies by incorporating hardware-in-the-loop (HIL) and experimental validation capabilities. These platforms enable high-fidelity, closed-loop analysis of CPPS under realistic operating conditions, supporting the evaluation of system dynamics, control strategies, and cyber–physical interactions.

Some developments primarily focused on federated co-simulation architectures that combine multiple power system and communication network simulators. For instance, [60] integrated RTDS and OPAL-RT to represent transmission and distribution systems, while employing tools such as CORE, NS-3, and Mininet to emulate communication networks. Similarly, [61] utilised an OPAL-RT and SCALABLE-based platform to perform real-time HIL cybersecurity analysis, demonstrating the capability of closed-loop simulation to capture cascading effects induced by cyber incidents. These studies highlighted the feasibility of integrating different types of simulators, but mainly focus on system-level validation with limited modelling of detailed cyber–physical interactions.

Subsequent research has incorporated HIL-based platforms to enhance realism and enable direct interaction with physical devices. The framework in [62] integrated RT-LAB and OPNET with real control devices to analyse cyber-attacks such as DDoS and MITM, demonstrating how communication disturbances propagate to the physical layer. In [63], a hybrid simulation environment combining real-time simulators, industrial protection relays, and communication networks was developed for resilience assessment under cyber–physical threats. These platforms significantly improve experimental fidelity; however, they are typically designed for specific application scenarios, such as protection validation or cybersecurity testing, and often adopt simplified communication models.

More recent work has explored tightly coupled multi-simulator configurations for

specific dynamic studies. For example, [64] integrated OPAL-RT and Typhoon HIL in a closed-loop HIL framework for frequency response analysis, incorporating both analogue signals and synchrophasor-based communication. Moreover, in work [65], RTDS and OPAL-RT were connected to EXata for evaluating large-scale power grid. While such approaches demonstrate high-fidelity interaction between heterogeneous simulators, they remained constrained to particular use cases and lacked systematic evaluation of scalability and computational efficiency.

Overall, despite significant progress, existing real-time digital simulation platforms exhibited several common limitations. Most platforms were designed for specific experimental scenarios and lacked generalised and modular architectures for scalable deployment. Communication networks were often simplified in practical implementations, with limited support for detailed protocol behaviour and realistic network emulation. In addition, explicit synchronisation strategies and quantitative evaluation of simulation efficiency were rarely addressed. These limitations highlighted the need for a unified cyber–physical real-time simulation framework that incorporates detailed communication modelling, robust synchronisation mechanisms, and scalable performance evaluation, which is a central focus of this thesis.

Table 2.5: Comparison of CPPS co-simulation and real-time digital simulation techniques

Technique	Main principle	Advantages	Limitations
Offline co-simulation	Couples power and communication simulators without strict real-time constraints.	Flexible and suitable for algorithm testing and large-scale scenario studies.	Limited ability to represent real-time hardware constraints and timing behaviour.
Hardware-in-the-loop real-time simulation	Integrates real-time simulators with physical controllers, devices, or communication hardware.	Provides high experimental realism and supports validation under realistic timing constraints.	Requires specialised hardware and careful synchronisation design.
Cyber–physical real-time co-simulation	Integrates real-time power simulation with communication network emulation.	Enables realistic study of cyberattacks, communication delays, packet loss, and their impacts on power system operation.	Platform performance, data exchange latency, scalability, and synchronisation accuracy must be explicitly evaluated.

2.5 Research Gaps Identified

The comparative summaries in Tables 2.1 ,2.4 and 2.5 show that existing techniques provide useful foundations for CPPS modelling, assessment, and simulation, but they also reveal common limitations in detailed cyber–physical coupling representation, systematic uncertainty quantification, and experimentally validated real-time implementation. Based on the above review, several key research gaps in the modelling, assessment, and simulation of CPPS can be identified.

First of all, in terms of modelling, existing approaches lack a unified framework that can simultaneously capture both physical power system dynamics and communication network behaviours. Network-based methods abstract the system into graph structures, which overlook key electrical characteristics and operational constraints. Graph-theoretic approaches focus primarily on computational efficiency and topology, while power flow-based models incorporate cyber effects in a simplified manner. As a result, detailed cyber–physical coupling, particularly node-specific and time-varying communication delays, is not adequately represented in current modelling frameworks.

Moreover, from an assessment perspective, most existing methodologies focus on either structural vulnerability or physical-layer uncertainty. Vulnerability assessment methods are typically based on static indices or simplified system representations, while global sensitivity analysis (GSA) studies predominantly consider uncertainties in renewable generation and load. Communication-induced uncertainties, such as delays, packet loss, and cyber disturbances, are rarely modelled as stochastic variables, and their interactions with physical processes are not systematically quantified.

In addition, in co-simulation frameworks, although significant progress has been made in integrating heterogeneous simulators, existing approaches often rely on simplified communication models and centralised synchronisation strategies. The representation of communication protocols, network-induced delays, and dynamic cyber–physical interactions remains limited. In addition, scalability and efficiency challenges persist, particularly in large-scale and high-resolution simulations.

Last but not least, real-time digital simulation platforms are typically designed for specific applications, such as cybersecurity analysis or protection validation, and lack generalised and modular architectures. Communication network emulation is often simplified, and explicit evaluation of synchronisation performance and computational efficiency is rarely conducted. Furthermore, there is a lack of standardised evaluation metrics to quantitatively compare different co-simulation platforms, making it difficult to assess their relative performance and suitability for different application scenarios. This limits their capability to support comprehensive and scalable cyber–physical system analysis.

These limitations highlight the need for a unified cyber–physical modelling and sim-

ulation framework that explicitly incorporates communication dynamics, enables systematic uncertainty quantification, and supports scalable real-time validation. Addressing these challenges forms the central focus of this thesis.

Chapter 3

Virtual-Physical Power Flow Method for Cyber-Physical Power System Contingency and Vulnerability Assessment

Publications Related to This Chapter

This chapter includes the publications listed as follows:

Qiu, D., Zhang, R., Zhou, Z., Zhang, J., and Zhang, X.: Virtual-physical power flow method for cyber-physical power system contingency and vulnerability assessment. *IET Smart Grid*, vol. 7, no. 1, pp. 13–27, 2024. doi: 10.1049/stg2.12143.

Qiu, D., Zhang, R., Dabashi, A. H., Zhou, Z., and Zhang, X.: Cyber-physical contingency and vulnerability assessment using double power flow method. In *IET Conference Proceedings*, vol. 2022, no. 27, pp. 194–199, 2023. doi: 10.1049/icp.2023.0098.

Chapter Overview

Traditional power systems have evolved into cyber-physical power systems (CPPS) with the integration of information and communication technologies. CPPS can be considered as a typical hierarchical control system that can be divided into two parts: the power grid and the communication network. CPPS will face new vulnerabilities which can have network contingencies and cascading consequences. To address this challenge, this chapter proposes a virtual-physical power flow method for the vulnerability assessment of

CPPS. The proposed method contains dual power flows, one is to simulate a virtual power flow from decision-making units, and the other is to simulate a physical power flow. In addition, this chapter proposes a novel hierarchical control model including four layers of CPPS: the physical layer, the secondary device layer, the regional control layer, and the national control layer. The model is based on IEEE test cases using data and structures provided by MATLAB and MATPOWER. Denial-of-service and false data injection are simulated as two major cyber-attacks in CPPS. A novel vulnerability index is proposed that consists of system voltage, network latency, and node betweenness as three key indicators. It is a comprehensive and adaptive index because it encompasses both cyber and physical system characteristics and can apply several types of cyber-attacks. The results of the vulnerability assessment are compared based on the national and regional control of CPPS to evaluate the vulnerability of nodes.

It should be noted that the IEEE 39-bus and IEEE 118-bus systems used in this chapter are transmission-level benchmark systems. They are selected because this chapter focuses on system-level CPPS vulnerability assessment, hierarchical control structures, and wide-area cyber–physical interactions, while distribution-network and microgrid-level studies are addressed in Chapters 4 and 5, respectively.

3.1 Background and Motivation

Renewable energy sources (RES) such as solar power, wind power, and hydropower have become increasingly important in recent years due to global warming mitigation and the shortage of fossil fuels. Many countries have already begun to reform their traditional energy structures. For example, China added almost 117 GW of renewable power in 2020. Wind power accounted for an important portion of total electricity generation in many countries by 2020, including Denmark (over 58%), Uruguay (40.4%), Ireland (38%) and the United Kingdom (35.5%) [66]. Europe installed 17 GW of new wind energy capacity in 2021. The European Union 27 possessed 11 GW of new wind farms [67]. This will continue to increase the share of wind power in total electricity generation. RES in the power system requires a large number of sensors and actuators to monitor and control the modern power system as a smart grid. In addition, with rapid economic development and improved living conditions, electricity consumption will grow rapidly and there will be a higher demand for a stable power supply.

Therefore, a more secure information and communication system is needed to guarantee the communication security of the new power system. The inclusion of modern information and communication system and intelligent decision-making units can be seen as an example of a cyber-physical system (CPS). The concept of CPS was first introduced by the American National Science Foundation (NSF) in 2008 [20]. Based on their defi-

nition, CPS consists of physical, biological, and manufactured systems whose operations are synthetic, monitored, and controlled by a computational system. The different parts of the physical system are connected through a network system. The CPS consists of a computational control system, a communication network, and a physical environment, forming a complex system involving real-time sensing, dynamic control and information decision-making [68]. The CPPS is an extension of the CPS in the field of power systems. In order to ensure the secure and economic operation of the power system, advanced information communication and computing technologies are increasingly deployed to realize the collection, transmission and processing of massive data with the deep integration of information systems with the electric power system. CPPS, also known as "smart grid", is the future direction of power system development when there is more RES integrated to the power grid [16].

CPPS, compared with the traditional power system, will inevitably generate many new vulnerabilities across the cyber layer, making it possible to invade and attack the power infrastructure from the cyber perspective such as the Internet and digital devices. For example, on December 23rd, 2015, hackers attacked Ukraine's power grid. This attack resulted in the breakdown of control systems that were used to coordinate remote electrical substations [69]. In 2019, a series of severe blackouts happened in Venezuela; the country did not have any stable power supply for at least 10 days during the month of March [70].

In CPPS, a large number of intelligent sensing, measurement, and control devices generate a significant amount of data. In addition, the collection scope of information and communication networks is expanding [71]. Problems such as data delay, packet loss, blocking, and tampering attacks that may occur in the information and communication network will affect the power control centre's monitoring and decision-making on the current state of the power network. As a result, the integrated CPPS will enlarge the spread of the system cascading segment making it more difficult for the control centre to prevent and restore cascading failures. In September 2003, a blackout occurred in Italy which was caused by the disconnection of one power station from the power grid, which then resulted in the failure of several communication nodes. Eventually, the control centre could not monitor the power grid properly, leading to the decoupling of a larger number of power nodes [72].

To sum up, the new cyber-physical contingencies including cyber-attacks as well as cascading failures will be introduced due to the integration of the cyber and physical networks of the power grid. System vulnerability assessments are urgently required to study the modelling technology of CPPS in order to enhance the ability to analyse the propagation mechanism and the impacts of cyber-attacks.

3.2 Literature Review

CPPS modelling approaches are surveyed into two categories: complex network theories, cyber and power flow calculation.

3.2.1 Complex Network Theories

The fundamental concept of complex network theory is to simplify natural complex systems by representing them as networks composed of nodes and edges. It is mainly used to study the influence of topology on the system with applications for CPPS network topology.

In a study conducted in 2013 [72], the connectivity of CPPS structures was represented using an adjacency matrix. Moreover, it provided a concept of "Betweenness Centrality (BC)". BC is a measure used in network analysis to quantify the importance of a node within a communication network. It is based on the number of shortest paths that pass through a particular node, indicating the extent to which that node serves as a bridge or connector between other nodes within the network. Another paper [73] incorporated betweenness centrality as a factor for vulnerability assessment. A higher betweenness centrality value for a node indicates that it has a more significant role in facilitating communication or the flow of information within the network. However, a notable limitation of this article is the omission of the latency metric, which plays a crucial role in data transmission within communication systems. Considering different loading conditions, another study [74] introduced the "Vulnerability-weighted Node Degree (VWND)" index. It indicated the importance of a node is related to its incident edges' vulnerabilities. However, the model used in the study did not take into account RES.

Two stochastic models based on complex network theory were presented in papers [71] and [75]. The former presented normal distribution probability density function curves for power flow in different lines, while the latter proposed random cyber-attacks under centralized and decentralized multi-agent control modes. Small-worldness was first defined by Watt and Strogatz [76]. It was a network topology property characterized by short average path lengths between nodes and high clustering coefficients. In paper [77], a dynamic small-worldness index was proposed to assess the robustness of the CPPS. It was used to evaluate the robustness of a realistic 1326-bus transmission network. Because the distributed structure of small-world networks makes it difficult for an attacker to destroy the entire system by targeting a single node or connection, it can improve the system's resilience and adaptability.

3.2.2 Cyber and Power Flow Calculation

Power flow calculation is a standard method for steady-state analysis of power systems. It calculates the steady-state operating state of a complex power system under normal and fault conditions [78]. The purpose of the calculation is to find out the overload and overvoltage components, optimise the power distribution and minimise power losses. The power flow calculation can adequately represent the change in the steady-state characteristics of the power system according to the topology, generation, and load variations, which is essentially based on Kirchhoff's voltage and current laws [79]. Some structures in the communication system are similar to those in the power system, for example, there is a directed current in the power system, and it consists of nodes and cables, while there is a directed information flow in the communication system, and it consists of nodes and links. By simplifying the features of the communication system, the information system can be simulated with the power system using the traditional power flow calculation. The obtained results can be used to analyse the node congestion and the flow of data streams. This approach which is called Cyber and Power Flow Calculation is applicable to CPPS with relatively simple cyber network structures.

In the paper [80], the CPPS network topology was presented in terms of a sparse matrix. The information flow in the communication system can be treated as the same pattern as the power flow in the power system. Conversion between the two flows is available via data process branch. As a result, two systems can conduct co-simulation in one environment with cyber-contingency assessments. Paper [37] developed a model using a dynamic routing algorithm [38] to describe the information packet transmission in the cyber network as well as to apply the dynamic load flow model to describe the power grid. Paper [81] provided a mode based on an optimized load-shedding policy to simulate the power-loss failures, out-of-control failures, and data-blocking (POD) failures in the process of cascade events. The research of [39] provided a concept of 'Cyber Ground'. The concept means that all the redundant nodes in the network layer are integrated into a cyber ground node through a data-pool branch. The advantage of this is that by integrating the redundant nodes, the computational pressure on the system is reduced and the computational efficiency is improved.

3.2.3 Contribution

To summarise, the contributions of the paper are listed as follows:

1. A virtual-physical power flow model is created based on graph theory. The model has four layers, physical layer, secondary device layer, regional control centre layer and national control centre layer.

2. A constrained false data injection (FDI) attack model and a denial of service (DoS) attack model are used in the CPPS system to test the vulnerability of the CPPS.

3. A novel vulnerability index including system voltage variation, network latency, and node betweenness is proposed in the paper. This is a more comprehensive assessment index, as it contains parameters for evaluating physical network and cyber network, before and after the CPPS is attacked, and includes parameters for the whole system as well as the single nodes.

The remainder of this paper is organised as follows: Section 3.3 introduces the cyber contingencies modelling, the virtual-physical power flow method as well as the novel vulnerability index. Section 3.4 includes the IEEE models for the case study. Section 3.5 provides the results of the simulation and vulnerability index, while Section 3.6 concludes the paper.

3.3 Cyber Contingency Modelling

In this section, a preliminary introduction of the two types of cyber-attacks implemented in this study is provided, followed by the introduction of the virtual-physical power flow method employed for simulation. This culminates with the presentation of a novel vulnerability index.

3.3.1 Cyber Contingencies Classification

To test the vulnerability in the CPPS, some contingencies should be made. Cyber-attacks can be categorized into four types [39].

1) Data Error:

Data error represents false data injection into the system, which is simulated as artificial value addition or reduction of the original data.

$$X_{N_E} = X_N + \Delta X_N \tag{3.1}$$

Where

X_N: B_N or L_N in (1)

ΔX_N: error data in node N

2) Data delay:

Data delay represents a latency which adds a time constant to the original transmis-

sion time as follows:

$$D_{N_E} = D_N + \Delta D_N \tag{3.2}$$

Where

D_{N_E}:delayed latency at node N

ΔD_N:delayed transmission time

3) Data Termination Loss:

Data termination means the data package is terminated or lost as follows:

$$Pack_{N_E} = \{\emptyset\} \tag{3.3}$$

where

$Pack_{N_E}$:terminated data at node N

$\emptyset$:empty set

4) Data malposition:

$$Pack_{N_E} = \{B_{N+n}, L_{N+n}, D_{N+n}\} \tag{3.4}$$

where

$Pack_{N_E}$:error data at node N

n: an integer representing another bus

In these four contingencies, the first three occur most often, and since data termination loss can be seen as a case of infinite data delay, the first and third cases are chosen for simulation in this paper.

3.3.1.1 Constrained False Data Injection Modelling

Data errors can be caused by human or environmental factors. It can be called a false data injection attack when the contingency is human-caused [37].

In a standard AC power system, the active power flow under non-linear expression is defined by

$$P_i = V_i^2 g_{ij} - V_i V_j g_{ij} cos\Delta\theta_{ij} - V_i V_j b_{ij} sin\Delta\theta_{ij} \tag{3.5}$$

and reactive power flow by

$$Q_i = -V_i^2 b_{ij} + V_i V_j g_{ij} cos\Delta\theta_{ij} - V_i V_j b_{ij} sin\Delta\theta_{ij} \tag{3.6}$$

$i = 1, 2, ..., N$ which stands for the node name and $j \in i$. Voltage V and phase angle θ are the system states, while active power P and reactive power Q are the parameters measured by the digital sensors in each physical node [82]. In the paper [83], Gu et al attack the system by adjusting the state variables. Notably, when the manipulated state variable is close to 90% of its original size, their proposed method identified most of the attack instances without any undetected cases. However, if the adjusted state variable is close to 95% of its original value, more instances escape detection. This observation is because 95% of the manipulations were closer to the original value than 90% of the manipulations, thus resulting in a smaller impact on the observed metrics. Therefore, in this study, the constrained False Data Injection (FDI) model also keep the adjustment in the range of 5% to 10%. Certain nodes exhibit greater underlying active and reactive power and therefore they exhibit greater magnitudes that can be manipulated and vice versa. This paper aims to further investigate these intricacies.

Should the injected data exceed a given threshold, the execution of the Optimal Power Flow (OPF) within the control centre may become unfeasible. The System Operator (SO), leveraging sophisticated algorithms, is promptly alerted of any abnormalities or contingencies within the system. Meanwhile, cyber attackers, exploiting advanced strategies, could design their attacks such that they disrupt the system to a certain extent whilst evading immediate detection by the SO [84]. This paper revises the threshold in consideration to the equality and inequality constraints of power systems of the power system. If the erroneous data doesn't breach these thermal constraints, implying the control centre's ability to perform an OPF calculation, then the situation is classified as a constrained FDI attack. These observations are essential for power system state estimation and understanding the nature of stealth attacks. This manuscript aims to investigate these facets.

A criticality-based perturbation model is used as the FDI attack model in this paper according to the paper [85]. The main tampered data $s'_t = [P, Q]$ of the proposed FDI model need to satisfy physical equality and inequality constraints of power systems as following:

$$\min \quad \|s'_t - s_t\|_N \tag{3.7}$$
$$\text{s.t.} \quad f_{FDI}(s'_t) = f'_{FDI} \tag{3.8}$$
$$f_{gs}(s'_t) = 0 \tag{3.9}$$
$$f_{hs}(s'_t) = 0 \tag{3.10}$$

where f'_{FDI} represents the output manipulated by the attacker; $f_{gs}(\cdot)$ includes AC power flow equations (3.5), (3.6). Moreover, $f_{hs}(\cdot)$ consists of physical capacity limits, such as line thermal limits (3.11), (3.13), generation active power flow limits (3.13) and bus

voltage limits (3.14).

$$p_{ij}^{min} \leq p_{ij} \leq p_{ij}^{max} \tag{3.11}$$

$$q_{ij}^{min} \leq q_{ij} \leq q_{ij}^{max} \tag{3.12}$$

$$p_{i}^{Gmin} \leq p_{i} \leq p_{ij}^{Gmax} \tag{3.13}$$

$$v_{i}^{min} \leq v_{i} \leq v_{i}^{max} \tag{3.14}$$

In such an attack, when the data of FDI meets the above requirements, the attacker can utilize the data typically tolerated by OPF calculation so that he can further increase the impact of false data injection attacks without being detected [86]. In the power grid, the load capacity in every node has its limitations. P, Q limitation of node N is $[X_{minN}, X_{maxN}], X = P, Q$ which is calculated based on equation (3.7).

The constrained false data P_{fN}, Q_{fN} are in Gaussain distribution [87] as follows:

$$P_{fN}, Q_{fN} \sim N(\mu, \sigma^2) \tag{3.15}$$

$$\mu = \frac{X_{minN} + X_{maxN}}{2} \tag{3.16}$$

$$\sigma = \frac{X_{minN} - X_{maxN}}{6} \tag{3.17}$$

3.3.1.2 Denial of Service Modelling

DoS attacks refers to an attacker interrupting the normal operation of the power grid by interfering with communication channels, attacking network protocols, etc. Such attacks can cause communication link failures and message delays, resulting in the failure to transfer information between sensors, actuators, and control systems in a timely manner. In severe cases it can bring down the entire system [88, 89].

There are three types of DoS attack: random DoS [90], Periodic DoS and Non-periodic DoS. In this paper, only Non-periodic DoS is under consideration.

DoS attack in node N in time k is presented in (3.18).

$$Pack_N = \emptyset, wheret = k. \tag{3.18}$$

The detailed description of $Pack_N$ is presented in (3.18). When facing a DoS attack, the control centre cannot obtain the data of all nodes at the same time. To deal with the DoS attack, the control centre keeps the system in operation through resilience control [91, 92]. the system operator can use the most recent transmitted data for power flow calculation for the data of nodes that have been attacked by DoS. The mechanism of resilience control

is presented in the following equation: when a node is in DoS in time k, the data collected by the control centre is represented by

$$PF = \begin{cases} Data_N(t),\ when\ node\ N\ is\ normal, \\ Data_N(t-k),\ when\ node\ N\ is\ in\ DoS\,, \end{cases} \tag{3.19}$$

In this paper, the simulation of a DoS attack is performed in a dynamic system, demands in the CPPS are set to satisfy the uniform distribution.

$$P_N, Q_N \sim N(0.95, 1.05), \tag{3.20}$$

where in equation (3.21), P_N,Q_N are in form of per unit.

3.3.2 Virtual-Physical Power Flow Method

This paper proposes a Virtual-Physical Power Flow method (VPPF) to simulate how CPPS operates in an ideal situation. The mechanism of the model uses MATPOWER 7.1 Toolbox in MATLAB to calculate power flow in two stages in one loop of simulation. As shown in Figure 3.1 of the VPPF method procedure, during the first stage, the secondary devices generate digital signals which carry the physical parameters, such as the voltage and the active and reactive power of nodes in the power grid. Then, the physical system's information is transformed into information packages in the secondary device layer. The structure of the information package is shown below:

$$Pack_N = \{P_N,\ Q_N,\ v_N,\ R_{N1},\ X_{N1},\ X_{N2}, ...,\ D_N\}, \tag{3.21}$$

where

$$\begin{aligned} N &: Node\ Name \\ Pack_N &: Information\ package\ in\ node\ N \\ P_N &: Active\ power\ of\ node\ N \\ Q_N &: Reactive\ power\ of\ node\ N \\ v_N &: Voltage\ of\ bus\ N \\ R_N &: Resistance\ of\ a\ line\ connected\ to\ node\ N \\ X_N &: Reactance\ of\ a\ line\ connected\ to\ node\ N \\ D_N &: Latency\ in\ node\ N \end{aligned}$$

After the secondary device layer of each bus changes the physical status into information packages, the data is sent to each regional control centre. After that, every regional control centre collects all information in its area and sends it to the top layer of CPPS,

which is the control centre. The control centre then uses this information to perform an OPF.

The OPF operated in the national control centre is so-called 'Virtual Power Flow'. The outcome of the OPF contains information orders to dispatch the generators. The orders are then sent from the top control centre to the regional control centres. Eventually, the orders are sent to the buses, where generators are deployed to change the power outputs, including active and reactive power. During the second stage of VPPF, the power grids run another power flow (Physical Power Flow) using the new generation data. If the power flow in the physical layer is not the same as that in the control centre, it proves that there is contingency during the transmission period. This difference will be reflected in the active and reactive power in the lines or the voltage at the nodes.

In this paper, system voltage variation is chosen as one of the criteria to quantify the impact of a contingency on the CPPS. The procedure of the whole VPPF method is represented in the flow chart, as shown in Figure 3.1.

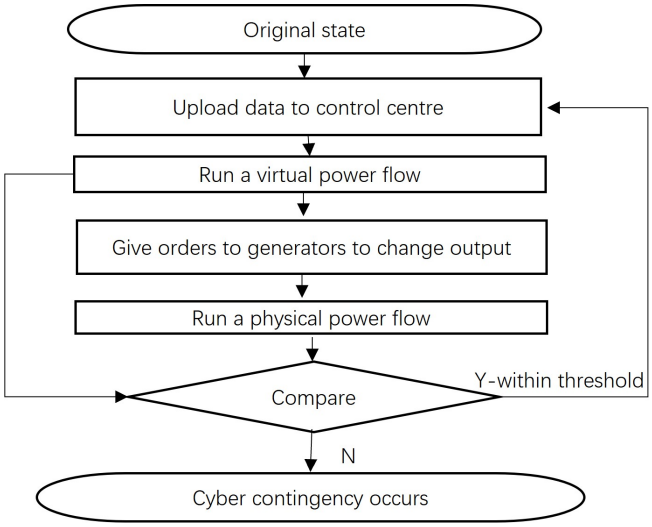


Figure 3.1: VPPF Method Procedure

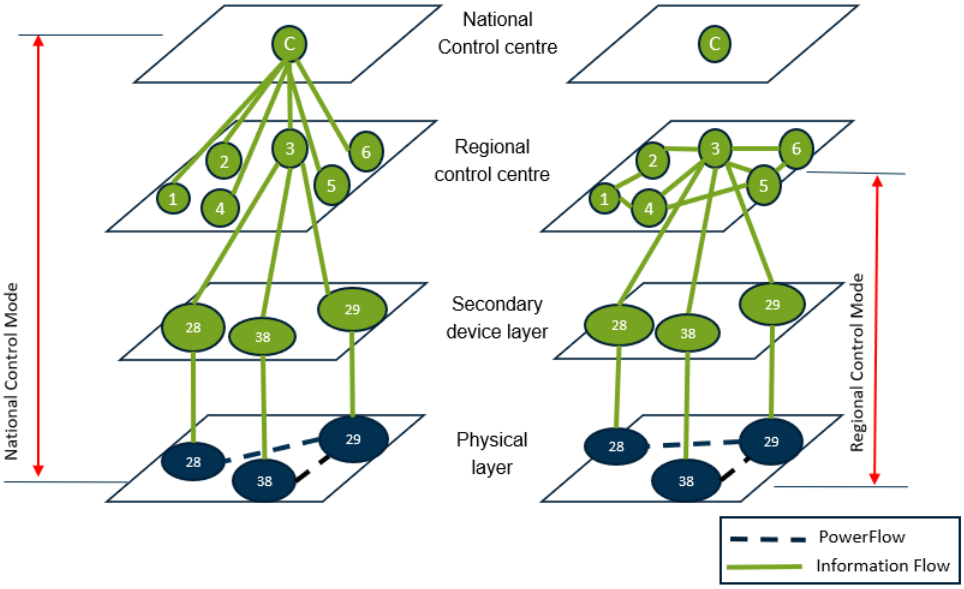


Figure 3.2: Cyber-Physical Power System Structure

Figure 3.2 shows the basic hierarchical structure of the CPPS considered in this chapter. The two control layers are introduced to represent two levels of decision-making in the proposed VPPF framework, rather than duplicated communication networks. The lower control level is the regional control centre, where field measurements collected from the physical layer through secondary devices are processed within each local zone. The upper control level is the national control centre, where information from different regional control centres is further aggregated and processed for centralised generation dispatch.

This hierarchical structure is used to distinguish two operating modes in the proposed vulnerability assessment. In the regional control mode, the information detected in the physical layer is collected and processed within the corresponding regional control

centre, and the control or dispatch decision is sent back to the physical nodes through the regional communication path. In the national control mode, the information is first collected by regional control centres and then transmitted to the national control centre for centralised processing. The resulting dispatch instructions are then sent back through the same hierarchical communication path. Therefore, the two communication/control layers allow the difference between regional and national dispatch to be represented explicitly, especially in terms of information-routing distance, accumulated communication latency, and cyber–physical vulnerability.

3.3.3 Defining Vulnerability Index

There are several indexes for evaluating vulnerability in CPPS, considering the loss of load and robustness [93–95]. In this paper, the vulnerability index is different. The majority of grid models employed in the current indices do not incorporate RES, which is an oversight given the vigorous development and implementation of RES in the contemporary energy landscape. Moreover, these existing indices don't have latency metric which would significantly enrich their evaluative capabilities. In this manuscript, both these factors are concurrently considered. The communication network is segmented, and two operational modes of generation dispatch are integrated into the index, rendering it more comprehensive and pertinent to the present-day grid systems. The advantage of this approach is the scalability of the index, allowing for the future integration of new models of cyber-attack, thus enhancing its predictive and preventative capacity for potential threats in power system operation.

In order to assess and give an outcome for the vulnerability of the CPPS due to a cyber contingency, a vulnerability index is developed, which is calculated as follows:

$$I(N) = [L_R(N) + L_N(N)] \times \Delta v(N) \times C_B(N). \tag{3.22}$$

In equation 3.22, $L_R(N)$ is the re-routed network latency with DoS of node N. $L_N(N)$ is the normal network latency without DoS of the node N. $C_B(N)$ represents the betweenness of the node N, that is, the number of shortest paths that include the node N. Betweenness is different when the system topology is different. In this paper, cyber network betweenness and physical network betweenness are considered. $\Delta v(N)$ represents the system voltage variation of node N when a contingency has occurred in node N.

Calculation of $\Delta v(N)$ is as follows:

$$\Delta v(N) = \sum_{i=1}^{N_{\max}} \left| V_F(i) - V_N(i) \right|, \tag{3.23}$$

where V_F represents fault voltage, and V_N represents normal voltage. In this paper, the

occurrence of V_F is caused by two factors. One is an FDI attack that happens in node N. The other is a DoS attack that happens in node N. The mechanism of two types of attack is explained in Section 3.3.1. For each test case of data error for one node, by summing the voltage results on every bus, the total system voltage variation for the data error of the node can be obtained.

Calculation of betweenness $C_B(N)$ is as follows:

$$C_B(N) = \sum_{s \neq N \neq t} \frac{\delta_{st}(N)}{\delta_{st}}, \tag{3.24}$$

where $C_B(N)$ represents the value of the betweenness of node N. $\delta_{st}(N)$ denotes the number of shortest paths from node s to node t via node N. δ_{st} denotes the number of all shortest paths between node s and node t.

3.4 Case Study

In this section, the power system is initially presented, followed by an introduction of the communication system, culminating with an articulation of the integration methodology employed between the two systems.

3.4.1 Power System Model

The IEEE 39-bus test system, also known as the 10-machine New England power system, and the IEEE 118-bus test system, which represents a simplified transmission network approximation of the American electric power system, are selected as the physical power network models in this chapter. It should be noted that both test systems are transmission benchmark systems rather than distribution networks or microgrids. They are adopted in this chapter because the proposed VPPF method focuses on system-level CPPS contingency and vulnerability assessment. In particular, the hierarchical communication structure, regional and national control modes, wide-area information routing, network latency, and cyber–physical node betweenness considered in this chapter are more naturally represented using transmission-level systems with multiple buses, generators, and inter-area connections.

The use of transmission-level benchmark systems in this chapter is therefore intended to validate the proposed VPPF method and vulnerability index under a system-level CPPS structure. The detailed data of the IEEE 39-bus and IEEE 118-bus systems are obtained from the MATPOWER 7.1 toolbox in MATLAB. To enable regional control mode and information flow across different zones, the IEEE 39-bus system is divided into

6 zones, while the IEEE 118-bus system is divided into 12 zones.

In order to simulate the RES penetration and their impacts on the cyber-physical power systems, within the IEEE-39 test case, each zone is integrated with certain number of 2 MW wind turbines. The total wind generation capacity is 3000 MW. A number of 1500 wind turbines are integrated to 17 nodes. Each wind turbine's power output follows a Weibull distribution [96], characterised by a scale parameter of 11.1 and a shape parameter of 2.2, simulating the hourly power output across a 24-hour cycle. By modulating the quantity of wind turbines, wind power generation is manipulated to comprise approximately 50% of the overall system's power generation. For the IEEE-118 test case, the number of wind power turbines is 2500. A total of 5000 MW wind generation capacity, ensuring a comparable contribution of wind power, approximately 50% to the total power generation within the system.

3.4.2 Communication System Model

The communication systems associated with the IEEE-39 test case and IEEE-118 test case have four layers. The bottom layer, called the secondary device layer, has sensors to detect data from the power network and transform it from physical value to digital signal. Accordingly, each node within the power system is outfitted with a secondary side device. Nonetheless, the configuration of the communication network is built by using star-structure with each node directly connected to the regional control centre of the respective zone. The line parameter in the information network is defined as "latency". Given that each device within the zone varies in its distance from the regional control centre, the calculation of latency utilises the power system topology as a reference, and Dijkstra's algorithm is used to determine the shortest communication path. Dijkstra's algorithm is employed to identify the shortest path between nodes, and the calculation defines the latency for each secondary device to its directly connected regional control centre. This method can also be utilised to calculate the latency from the regional control centres to the national control centre.

In this chapter, a representative link latency of 100 ms and a representative node latency of 200 ms are adopted for the communication network. They are used as aggregated modelling parameters to represent link transmission delay and node-level processing, forwarding, queuing, and routing delay in a hierarchical CPPS communication network. This assumption is consistent with the fact that communication delay requirements in smart-grid applications vary significantly with the application type. For example, wide-area protection and control applications may require response times from below 0.1 s to minutes, while distribution automation applications may tolerate delays of several seconds [97].

All 39 buses in the power system are divided into six zones, while in the IEEE-118 test case, there are 12 zones. Each zone has its regional control centre, which should be powered by the power network. Therefore, they are located in certain nodes in the power grid. For each zone, the location of regional control centres is determined where the average transit time from other buses in the zone is minimal. As a result, Dijkstra's algorithm is utilised to locate the node with the shortest average transit time to other nodes within the zone, utilising the power system topology as a reference.

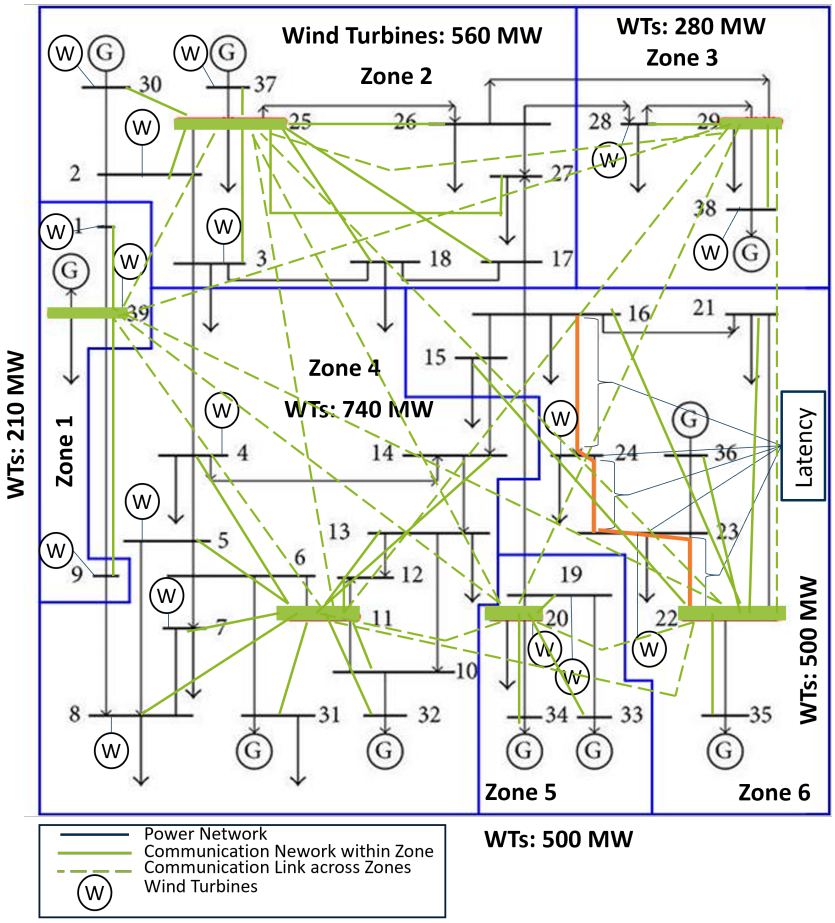


Figure 3.3: IEEE-39 Test Case of CPPS with Communication Networks

The zones and the regional control centres' locations of the IEEE-39 test case are shown with green colour in Figure 3.3. The nodes with wind power turbines are shown in the figure as well. An example of latency calculation is presented with orange line, which represents the latency from node 16 to regional control centre node 22. The latency from the regional control centre to the national control centre in IEEE-39 test case is shown in Table 3.1. For the IEEE-39 test case, Bus 16 is selected as the physical reference bus and electrical supply point associated with the cyber-layer national control centre. The national control centre itself is modelled as a communication node, rather than as a physical power-system bus.

Table 3.1: Regional Control Centres Location for IEEE-39 system

Zone Name	Regional Control Centre	Latency to National Control Centre
1	Node 39	1800 ms
2	Node 25	1200 ms
3	Node 29	1200 ms
4	Node 11	1500 ms
5	Node 20	600 ms
6	Node 22	600 ms

The locations of regional control centres in IEEE-118 test case with wind turbines number in each zone is shown in Figure 3.4. Table 3.2 shows the latency from regional control centres to national control centre. For the IEEE-118 test case, Bus 69 is selected as the physical reference bus and electrical supply point associated with the cyber-layer national control centre.

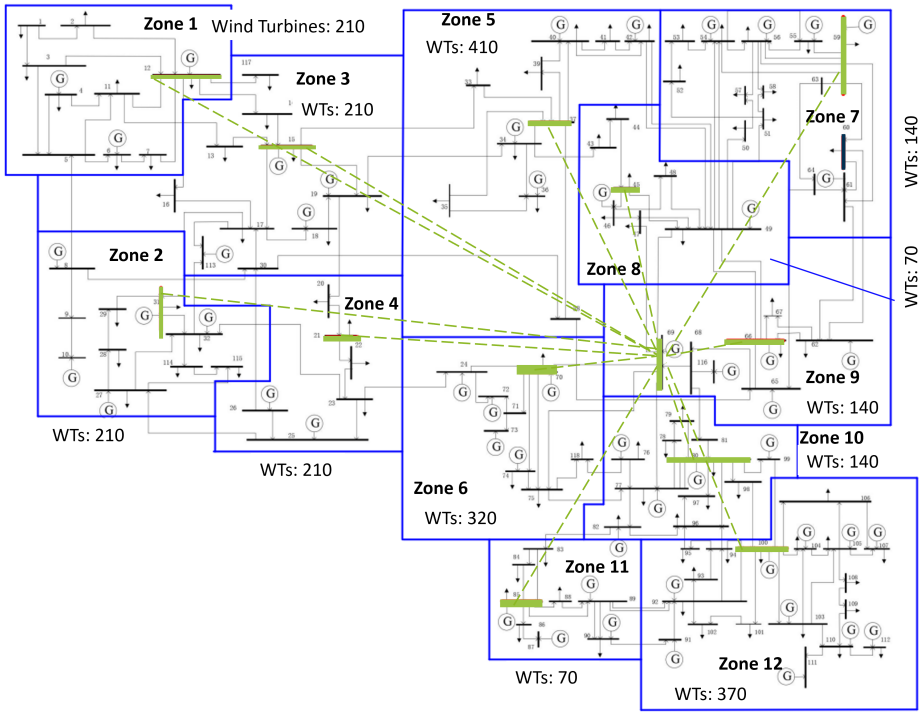


Figure 3.4: IEEE-118 Test Case of CPPS with Communication Network Zones in National Control Mode

Table 3.2: Regional Control Centres Location for IEEE-118 system

Zone Name	Regional Control Centre	Latency to National Control Centre
1	Node 12	2100 ms
2	Node 31	1500 ms
3	Node 15	1800 ms
4	Node 21	1500 ms
5	Node 37	1200 ms
6	Node 70	300 ms
7	Node 59	900 ms
8	Node 45	600 ms
9	Node 66	600 ms
10	Node 80	600 ms
11	Node 85	1200 ms
12	Node 100	1200 ms

3.4.3 CPPS Model Construction

To build a model that MATLAB can operate, a graph-based model is presented in this paper. The model combines a physical power system with a communication network to accomplish cross-domain simulation. A logical adjacency matrix M_P is produced for the graph-based power grid. Because the physical layer and the secondary device layer have the same topology structure, in the matrix, these two layers are represented by the same variable M_P. M_C stands for the control centre in the communication system and M_{ZC} represents zone control centres. Each layer is composed of a logical adjacency matrix as follows:

$$M_\omega = \begin{bmatrix} M_{1,1} & \cdots & M_{1,n} \\ \vdots & \ddots & \vdots \\ M_{m,1} & \cdots & M_{m,n} \end{bmatrix} \tag{3.25}$$

where $M_{m,n} = 0$ (no direct link), 1 (link exists), and ω denotes the type of matrix (P, C, ZC, etc.).

Next, the whole CPPS network is the combination of adjacency matrices of the four layers. Combining different layers will create four new sub-matrices describing the links between layers, M_{PZC}, M_{ZCP}, M_{ZCC} and M_{CZC} represent links between physical layer to zone control centre, zone control centre to control centre according to the subscript, as shown below.

$$M_{CPPS} = \begin{bmatrix} M_P & M_{ZCP} & 0 \\ M_{PZC} & M_{ZC} & M_{ZCC} \\ 0 & M_{CZC} & M_C \end{bmatrix} \tag{3.26}$$

where

M_P: physical layer and secondary device layer,

M_{ZC}: zone control centre layer,

M_C: control centre layer,

M_{PZC}: links from physical layer to zone control centres,

M_{ZCP}: links from zone control centres to physical grid,

M_{ZCC}: links from zone control centres to control centre,

M_{CZC}: links from control centre to zone control centres.

3.5 Results and Discussion

All simulations are conducted using MATLAB for the IEEE-39 test case and IEEE-118 test case. This section will simulate the cyber-attack models and discuss the contingency assessment outcomes of adjacency matrix, system voltage, network latency and node betweenness of CPPS. Vulnerability index is presented at the end of this section.

3.5.1 Adjacency Matrix

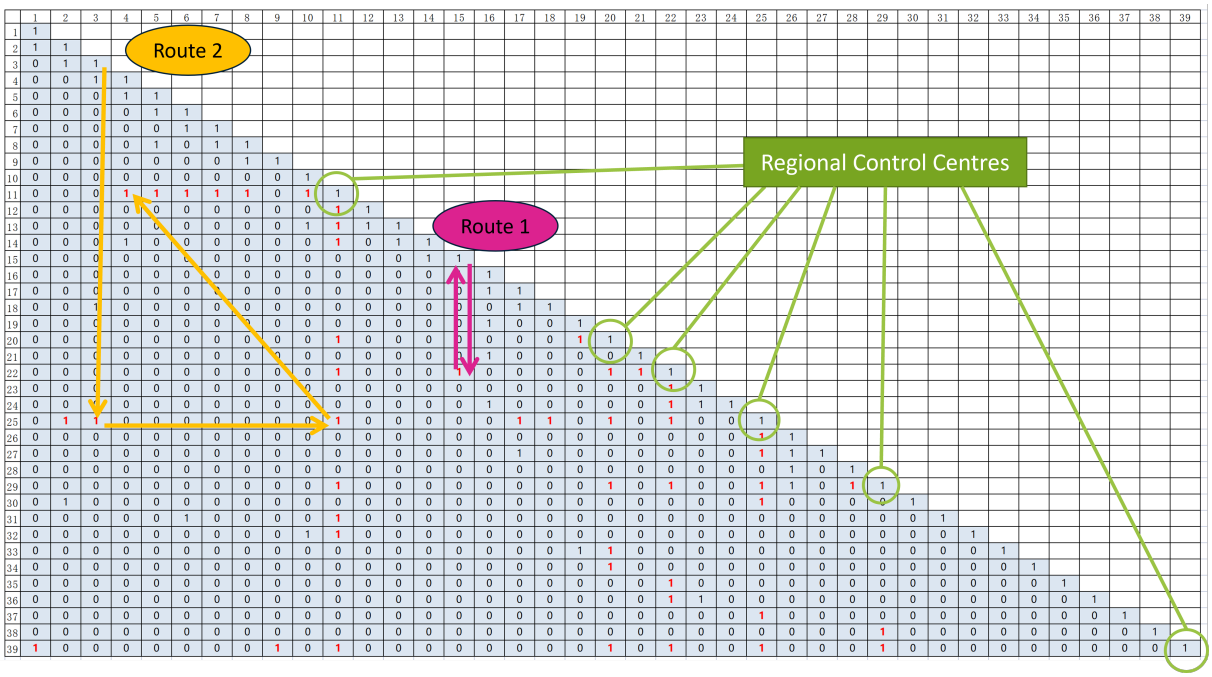


Figure 3.5: IEEE-39 test case adjacency matrix under regional generation dispatch. Grey entries denote physical power-network connections, red entries denote cyber-layer communication links, Route 1 illustrates local bidirectional communication within one zone, and Route 2 illustrates inter-zone information routing.

Figure 3.5 illustrates the adjacency matrix of the IEEE-39 test case under the regional generation dispatch mode. The matrix is a binary connectivity representation of the constructed CPPS, where the row and column indices correspond to the buses or cyber–physical nodes in the IEEE-39 system. A value of "0" denotes that there is no direct connection between two nodes. A grey "1" denotes a physical connection in the power network, while a red "1" denotes a cyber-layer communication link or information route. The red entries associated with the regional control centres are highlighted to show the communication structure used for regional information exchange. This adjacency matrix is generated according to the combined CPPS connectivity matrix in Eq. 3.26.

It should be noted that the arrows in Fig. 3.5 are visual annotations used to explain representative information-routing paths, rather than additional elements of the adjacency matrix. Route 1, shown by the up–down arrow, represents a local bidirectional communication process within a single communication zone. For example, information from node 15 is uploaded to its associated regional control centre, node 22, through the route $(15, 22)$. After the regional control centre processes the received information, the corresponding dispatch or control instruction is sent back to node 15 through the same regional communication path. Therefore, Route 1 illustrates the basic measurement-upload and command-return process in regional generation dispatch.

Route 2, shown by the triangular arrow, represents an inter-zone communication process. When information needs to be exchanged between nodes located in different communication zones, the message is first sent from the source node to its own regional control centre, then forwarded to the regional control centre of the destination zone, and finally delivered to the destination node. For example, when information is transmitted from node 3 to node 4, it is first sent from node 3 to the regional control centre of zone 2, node 25, through the route $(3, 25)$. It is then forwarded from node 25 to the regional control centre of zone 4, node 11, through the route $(25, 11)$. Finally, the information is delivered from node 11 to node 4 through the route $(11, 4)$. The triangular arrow is therefore used only to visualise this multi-hop cross-zone information route; it does not represent a physical triangular connection in the power network.

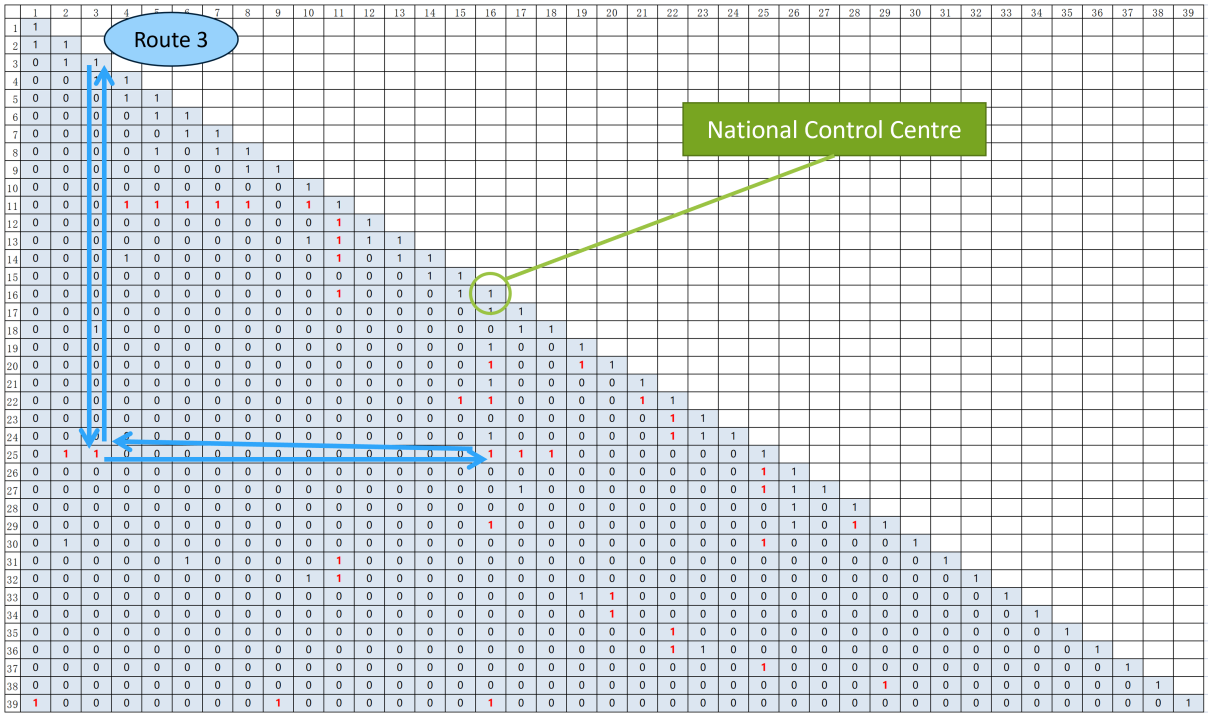


Figure 3.6: IEEE-39 test case adjacency matrix under national control mode. Grey entries denote physical power-network connections, red entries denote cyber-layer communication links, and Route 3 illustrates an information route through the cyber-layer national control centre.

Figure 3.6 presents an example of information routing under the national generation dispatch mode in the IEEE-39 test case. Compared with the regional dispatch mode, information in the national control mode is further transmitted from the regional control centre to the cyber-layer national control centre before the dispatch decision is made. Route 3 starts from node 3 and first passes through the route $(3, 25)$ to reach node 25, which is the regional control centre associated with zone 2. The information is then forwarded through the route $(25, 16)$ to the cyber-layer national control centre. In this model, bus 16 is selected as the physical reference bus associated with the national control

centre; the national control centre itself is modelled as a cyber/control-layer node rather than as a physical power-system bus. After the information is centrally processed, the generation dispatch instruction is sent back to node 3 through the same communication path.

For the IEEE-118 test case, the adjacency matrix follows a similar information-routing structure and generation-dispatch logic. However, because the IEEE-118 test case contains a much larger number of buses and cyber–physical connections, the corresponding adjacency matrix is too large to be clearly displayed in this section.

3.5.2 System Voltage

The system voltage variation discussed in this section is evaluated under two types of cyber contingencies: constrained false data injection attacks and denial-of-service attacks. The purpose of these scenarios is to examine how cyber-layer disturbances propagate to the physical power network and cause bus voltage deviations. The system voltage variation is represented as a percentage of the highest variation case, so that the results can be compared across CPPS test systems with different sizes and structures.

To clarify the case-study design, the voltage variation scenarios investigated in this section are summarised in Table 3.3. In the FDI scenarios, each bus is attacked individually and the resulting system-wide voltage deviation is calculated. In the DoS scenarios, each communication node is interrupted individually and the corresponding physical voltage impact is evaluated. Both attack types are studied in the IEEE-39 and IEEE-118 CPPS test cases.

Table 3.3: Voltage variation scenarios studied in Section 3.5.2

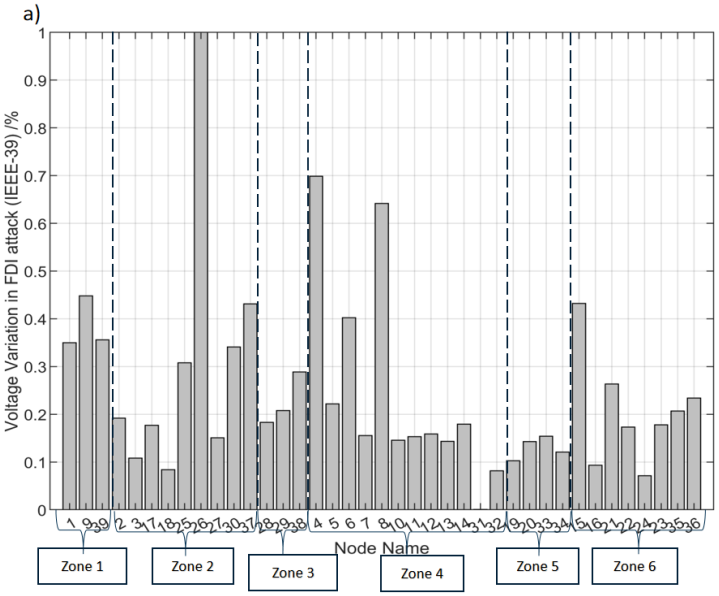
Scenario	Test system	Attack type	Studied condition	Output metric
S1	IEEE-39	Constrained FDI attack	Each bus is attacked individually. Wind generation varies over a 24-hour cycle.	System voltage variation $\Delta v(N)$
S2	IEEE-118	Constrained FDI attack	Each bus is attacked individually. Wind generation varies over a 24-hour cycle.	System voltage variation $\Delta v(N)$
S3	IEEE-39	DoS attack	Each communication node is interrupted individually, and the resulting physical voltage impact is evaluated.	System voltage variation $\Delta v(N)$
S4	IEEE-118	DoS attack	Each communication node is interrupted individually, and the resulting physical voltage impact is evaluated.	System voltage variation $\Delta v(N)$

3.5.2.1 System Voltage Variation made by FDI Attack

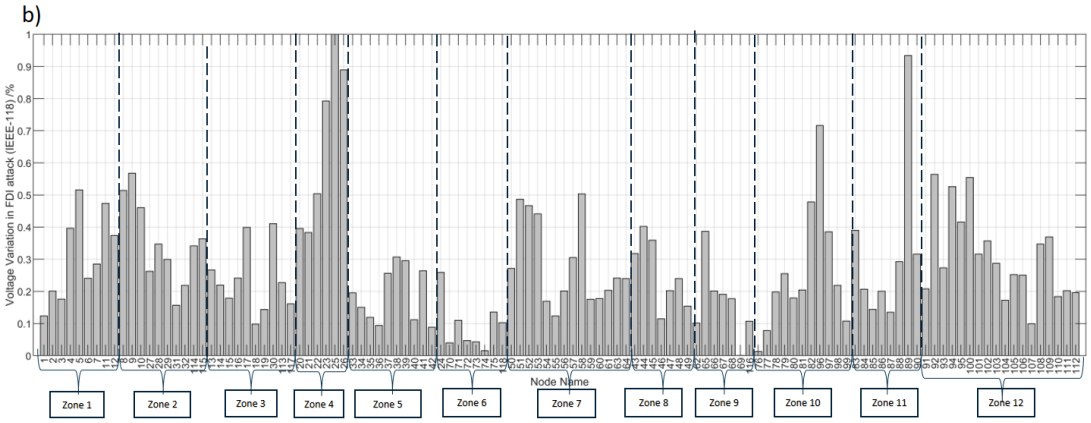
In this case, the FDI attack modelling in equation 3.15, is applied to each node respectively. After that, the system voltage variation in the CPPS due to FDI will be calculated in equation 3.23 respectively. The system voltage variation also considers the volatility of wind power output which is modelled by Weibull distribution on a 24-hour cycle. Therefore, for FDI attacks on each node, the test case simulates 24 attacks, corresponding to one attack per hour. Then, the system voltage variations which are generated by these 24 FDI attacks are summed as a final system voltage variation for this specific node over 24 hours. The test case will then be continued to the next node so that the system voltage variation of all nodes can be obtained.

Figures 3.7 presents the results of the system voltage variation under FDI attack of each node respectively in the IEEE-39 test case. The results are arranged according to each communication network zone in order to compare the results across different zones.

In Figure 3.7a, system voltage variation is ranked in percentage for each bus in the IEEE-39 test case. The results are analysed against each individual node as well as for each communication network zone. For each individual node under the FDI attack, it is found that nodes 26, 4, and 8 represent the highest system voltage variation, while the nodes 3, 14, 24 and 32 show the relatively low variation in the system voltage. This is primarily due to the different locations of node which are subject to different physical properties across CPPS. For example, the nodes 26 and 4 are both located at the edge of the physical network of CPPS (as shown in Figure 3), so that the higher system voltage variations are observed due to the weaker reactive power control on the edge and remote locations of the power network. In contrast, the nodes which are located in the central parts of the power network or with generators will both receive stronger support in terms of voltage regulation, therefore the nodes 3, 14, 24 and 32 have the lower system voltage variation. For each different zone, the higher system voltage variations are observed in zones 2, 4 and 6 respectively, because these zones have larger physical networks in their regions but less generators to regulate the voltage. In addition, a large amount of wind power generation is integrated in these zones to make voltage regulation more challenging. For zones 1, 3 and 5, there are smaller physical power networks but relatively more generators in order to control the voltage. Therefore, the system voltage variations are minimised in these zones. Figure 3.7b shows the system voltage variations caused by FDI in IEEE-118 test case. The similar results are observed that the system voltage variations are highly related to the physical power networks. In summary, the system voltage variation is highly dependent on the physical network topology as well as the distribution of generation. This system voltage variation index is capable of assessing the vulnerability on the physical aspects of CPPS.



(a) System Voltage Variation of IEEE-39 Test Case under FDI



(b) System Voltage Variation of IEEE-118 Test Case under FDI

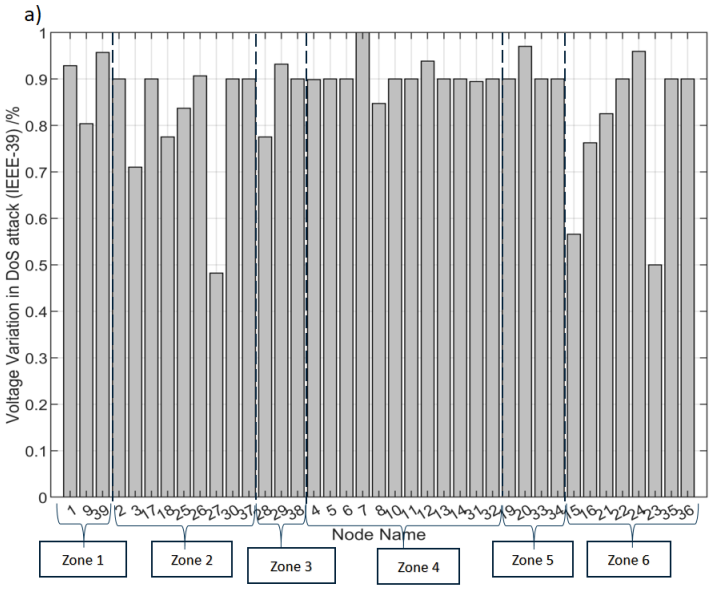
Figure 3.7: Results of System Voltage Variation under FDI

A comparison of Figure 3.7a and 3.7b provides an understanding of how the system voltage variations behave in two CPPS with different sizes and structure. This is attributed to the fact that the manipulated data from the constrained FDI attack is impacted by the active and reactive power of each node, coupled with the wind power generation which introduces further volatility into the system. In the IEEE-39 system, zone 2 includes the nodes with the minimum and maximum system voltage variations respectively. On the other hand, the IEEE-118 test case with increased number of nodes, presents a widely spread-out voltage variations across different zones. However, the system voltage variation results appear independent of each communication network zone in the cyber aspects of CPPS. As a result, for FDI attacks, knowing the topology of the power network allows the attacker to analyse the best location for an FDI attack in terms of voltage variation. Therefore, the defence of FDI can focus mainly on the change in the

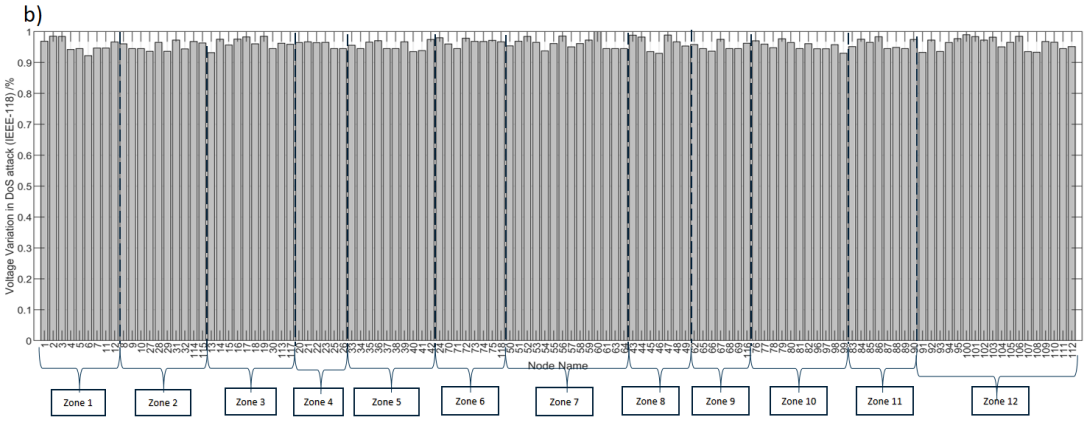
topology, such as moving target defence [98].

3.5.2.2 System Voltage Variation made by DoS attack

From the mechanism of DoS modelled in equation 3.18, DoS is applied to only affect one specific communication node of CPPS. However, the system voltage variation is across the whole CPPS can be influenced as well. Figure 3.8, which presents the results of the system voltage variation of buses in the IEEE-39 test case. The result shows the more uniformly distributed of system voltage variation across all the nodes under the DoS, with a variance of 13.4 in system voltage variation of the IEEE-39 test case. However, in FDI, the variance of system voltage variation can reach as high as 37.5, indicating the locational impacts of FDI are much greater than the DoS attack.



(a) System Voltage Variation of IEEE-39 Test Case under DoS



(b) System Voltage Variation of IEEE-118 Test Case under DoS

Figure 3.8: Results of System Voltage Variation under DoS

By comparing Figure 3.8a and 3.8b, it can be seen that DoS causes a different impact across different sizes of CPPS, with the variance of system voltage becoming more uniform in the larger-scale systems. By comparing the IEEE-39 test case and IEEE-118 test case, the variance of system voltage variation in IEEE-118 test case is greatly reduced to 0.274. This suggests that in larger CPPS, the individual voltage impact caused by DoS attacks on different nodes become similar and more uniformly distributed. When a DoS attack occurs, it is difficult to determine the exact location of the attack by the system voltage variation, as each node has a similar performance of system voltage impact. In summary, the system voltage variation is less effective indicator to assess the DoS attack in CPPS.

3.5.3 Network Latency

Latency of communication networks of CPPS is investigated for DoS attack of CPPS. The initial study found that the DoS attack on individual node has minimal impacts comparing with DoS attack on the regional control centres. Therefore, the DoS attack on each regional control centre is investigated respectively.

3.5.3.1 Latency in IEEE-39 Test Case

Figure 3.9 shows the network latency before and after the DoS attack for each node on the regional control centre in the CPPS. Shortest path of communication network is re-routed when the original communication link is interrupted, which is caused by a DoS attack in this paper. When a regional control centre is attacked by a DoS, the communication links that between this regional control centre and connected nodes are all interrupted within this zone. As a result, the nodes in the DoS attacked zone will reroute to a nearest neighbouring zone where another regional control centre is still in service, which results in an increase in network latency of each node after the communication link reroute. The normal network latency as well as the re-routed network latency are compared in the form of network latency. Results that in dark red represents normal network latency in each region, while bars in light red represent the re-route network latency under DoS attack.

In the normal network latency without cyberattack, nodes 17, 18, 4, 8, 14, 15 have higher values of network latency, while nodes 39, 25, 29, 11, 20, 22 have the lowest network latency in each zone. This is because these nodes have to pass through multiple intermediate nodes to reach the regional control centre, and the latency in the communication network is calculated on the shortest path of the physical network topology as an assumption. As a result, the shortest path in communication networks of CPPS is the key factor that influences the network latency without DoS attack.

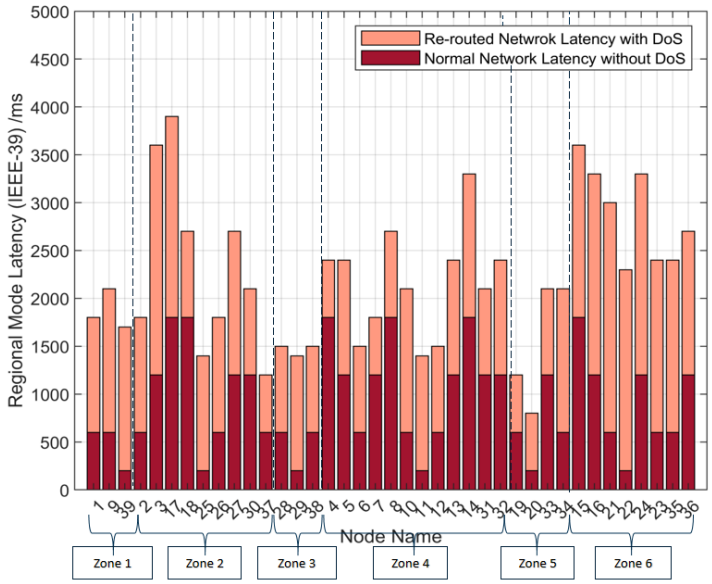


Figure 3.9: Network Latency of IEEE-39 Test Case

However, after the DoS attack with the re-routed communication networks, re-routed network latency of regional control centre nodes has the significant increase comparing with the normal operating condition. This is because the regional control centres are usually directly connected with other control centres. When DoS attack occurs, the direct communication links become interrupted, so that the DoS attacked regional control centres which are located at the centre of each zone need a longer latency to reach the neighbouring zone via the re-routed communication links. For other nodes that are located at the edge of each zone, there are two types of results: 1) nodes such as 16, 17, 32 that are located at the edge of the zone as well as at the edge of the CPPS, their re-routed network latency become relatively high. 2) nodes that are located at the edge of their own zone but close to the neighbouring zones, their re-routed network latency has minimal increase under DoS attacks, because their re-routed communication links are closer to the regional control centre of the nearest zone, such as nodes 4, 7, 19. Moreover, for different zones, the more interconnected zone 4 has the relatively less network latency increase than the more isolated zone 6. This shows that the zone with more interconnected communication links become more resilient to the DoS attacks.

It is also found that FDI attack has minimal impacts on the latency of communication networks, the network latency is mainly impacted by the DoS attacks.

3.5.3.2 Latency in IEEE-118 Test Case

Figure 3.10 shows the network latency of IEEE-118 test case in normal and re-routed network latency under the DoS attacks. Nodes 9, 10 and 26 have the highest value of network latency in the normal operating conditions, while nodes 12, 31, 15 have the lowest

normal network latency. These are due to the locations of the nodes with different length of communication links as shown in Figure 3.4. The nodes which are further away from the regional control centre have a longer network latency. These results are similar to the IEEE-39 test case.

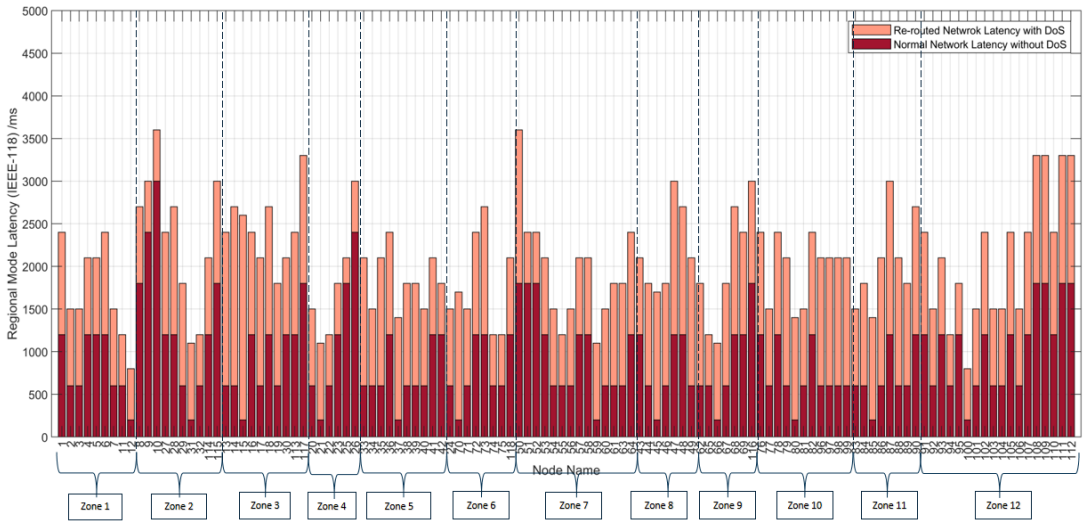


Figure 3.10: Network Latency of IEEE-118 Test Case

The results also show that the larger CPPS such as IEEE-118 test case in Figure 10 has the higher average network latency of 2,000 ms across all nodes, which is compared with the average network latency of 1,500 ms in the IEEE-39 test case. This is due to the larger size of the CPPS with communication networks that are distributed across longer distance. However, such larger CPPS has the lower network latency increase under the DoS attacks. This is due to the more interconnected zones of IEEE-118 test case that can provide more resilience in response to the DoS attacks.

The results show that the network latency is a feasible indicator to identify the impacts of DoS attacks on the different nodes of CPPS with various size and locations.

3.5.4 Node Betweenness

Node betweenness is calculated based on both the power network and the communication network, respectively. In this chapter, betweenness is used as a topology-dependent shortest-path centrality metric, rather than a time-varying dynamic betweenness metric. It quantifies the structural importance of a node within a given CPPS topology and control mode.

The physical-network betweenness reflects the importance of a bus in the power-network topology, while the cyber-network betweenness reflects the importance of a communication node in the information-routing structure. The results of both physical-node

betweenness and cyber-node betweenness are added together to form the cyber–physical node betweenness used in the vulnerability index. The node betweenness is calculated according to Eq. 3.24.

3.5.4.1 Node Betweenness in IEEE-39 Test Case

The results of the cyber-physical node betweenness in the IEEE-39 test case of CPPS is presented in Figure 3.11. Nodes 16, 14 and 4 have the highest value of betweenness in physical network. These are due to the power network topology. Nodes with higher betweenness in physical network demonstrates that they are more interconnected with other nodes, therefore they become one of the intermediate nodes in these shortest paths between other nodes. While nodes with less connectivity, they have lower values of node betweenness, because there are a smaller number of shortest paths go through these nodes. There are some nodes which have no betweenness in the physical network, for example, nodes 30, 37 and 28. Because they are not the intermediate node of any shortest path, due to their locations are at the edge of the physical network.

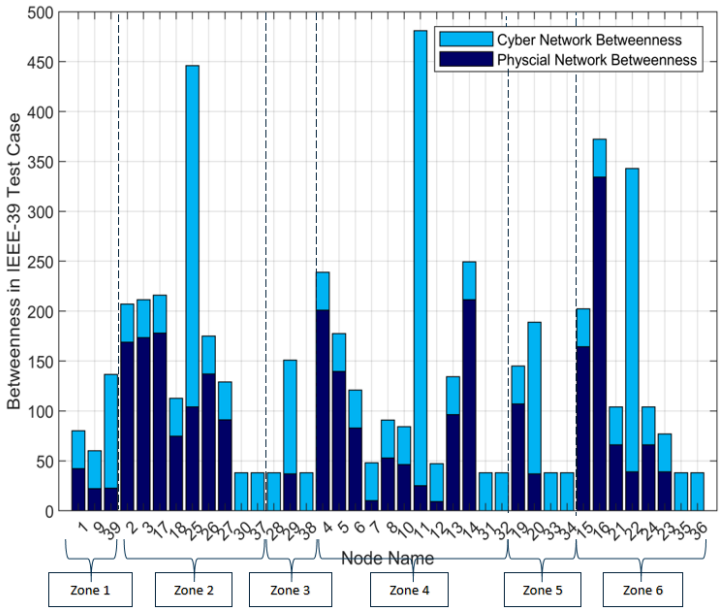


Figure 3.11: Cyber-physical Node betweenness of IEEE-39 Test Case

In communication network, nodes 39, 25, 29, 11, 20 and 22 have the highest value of betweenness in cyber network, as they are all regional control centre which are centralised in their own communication zones. In these regional control centres, nodes 39 and 29 have the lowest cyber network betweenness among regional control centres, because zone 1 and zone 3 only have three cyber nodes with less communication links. While node 11 owns the highest cyber network betweenness since zone 4 have the most cyber nodes and communication links in the IEEE-39 test case.

The distribution of cyber-physical node betweenness is different due to the different topology of power and communication networks. The power network is a more distributed network with power flow being distributed across the whole system, while the communication network is more centralised network with information flows that require to be connected via certain nodes, such as regional control centre in each zone. For example, node 11 has a low physical network betweenness which has minimal impacts on the power network, but it has very high cyber network betweenness indicating the cyber importance of node 11 as its role of regional control centre. In contrast, node 16 has a very high physical network betweenness, as it is located in the centre of power networks, but it has very low cyber network betweenness in the communication network. The cyber-physical node betweenness is added together to better reflect the cyber-physical nodal importance of CPPS.

3.5.4.2 Node Betweenness in IEEE-118 Test Case

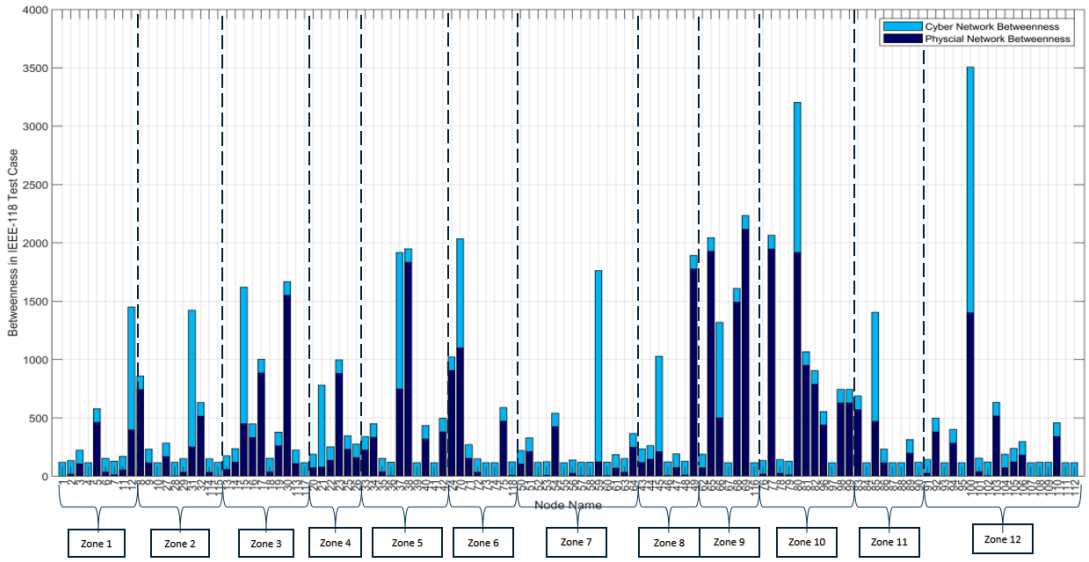


Figure 3.12: Cyber-physical Node betweenness of IEEE-118 Test Case

Figure 3.12 represents the results of cyber-physical node betweenness in IEEE-118 test case. Similar to the results of the IEEE-39 test case, nodes 12, 31, 15, 21, 37, 70, 59, 45, 66, 80, 85, 100 in IEEE-118 test case have high cyber network betweenness compared to other nodes. Each of these nodes is a regional control centre in each zone. In the physical network, nodes with high values of physical network betweenness are not evenly distributed in each zone, for example, nodes in zone 1 and zone 7 all have relatively lower physical network betweenness due to their remote locations in power networks, while most of nodes in zone 9 and zone 10 have higher physical network betweenness due to their central locations of power networks.

By comparing Figure 3.11 with Figure 3.12, it can be seen that the range of node betweenness in the IEEE-39 test case is from 50 to 500, while in the IEEE-118 test case the range of node betweenness is from 100 to 3,500. The average value of node betweenness in IEEE-118 test case is much higher than that in IEEE-39 test case. This is due to the fact that in the larger CPPS there are more nodes and associated shortest paths in both physical and cyber networks.

The cyber-physical node betweenness can be considered as an indicator to assess the impacts of various cyberattacks on CPPS. For example, FDI attack may become more effective on the node with higher physical network betweenness, as it is more interconnected with other power nodes that may have higher impacts on VPPF. In the cyber network, the higher the cyber network betweenness, the more likely the node will encounter cyber contingencies such as DoS attack, due to the centralised communication network structure used in this test cases. Therefore, the higher the cyber-physical node betweenness, the higher the vulnerability of the node under cyberattacks.

3.5.5 Vulnerability Index Assessment

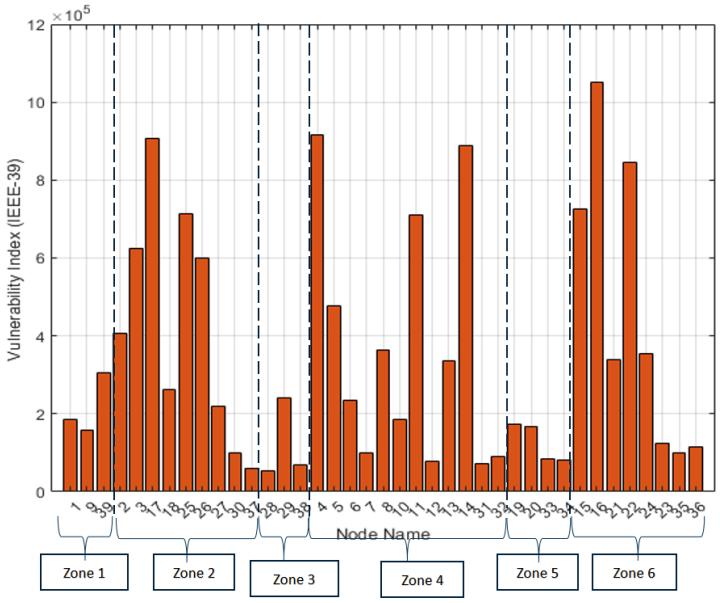


Figure 3.13: Vulnerability Index in IEEE-39 Test Case

Figure 3.13 and 3.14 presents the vulnerability index of each node in IEEE-39 test case and IEEE-118 test case respectively. The results of vulnerability index are calculated in equation 3.22, which consists of three indicators: system voltage variation, network latency, and node betweenness. As shown in Figure 3.13, nodes 17, 4, 14, 16 have the highest values of the vulnerability, which means they are the most vulnerable nodes of CPPS subject to cyber contingencies. This is due to the nodes 17, 14 and 16 which have

very high re-routed network latency after the DoS attacks, as well as the high physical network betweenness. The high vulnerability of node 4 is due to the high voltage variation after FDI attack. The vulnerability index of nodes 28, 38 and 12 is relatively low, because they are all located at the edge of the networks with low level of node betweenness, closed to a synchronous generator that are less affected by voltage variations, as well as low re-routed latency of communication networks.

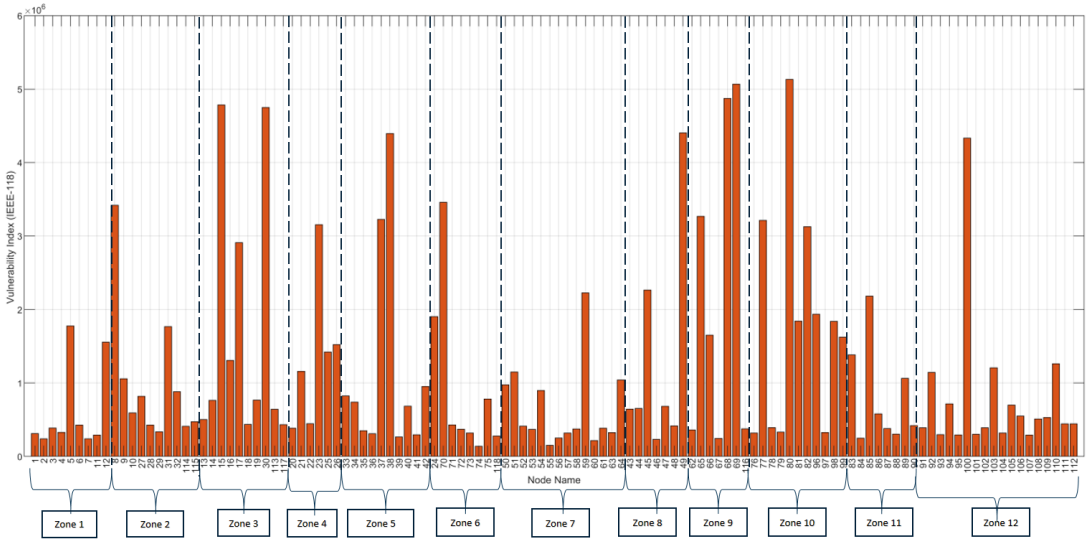


Figure 3.14: Vulnerability Index in IEEE-118 Test Case

In Figure 3.14, nodes 80, 69, 68, 100 have high value of the vulnerability index, which means they are expected to be the most vulnerable nodes in this CPPS. Nodes 80, 68 and 100 are regional control centres, while 69 is the national control centre. This simulation results illustrate that control centres are more vulnerable than normal nodes, and they can have higher impacts on the CPPS when under a cyberattack. However, there are some exceptions, in zone 4 where node 21 is the regional control centre, but node 23 has a much higher vulnerability index than node 21. This is due to the higher physical network betweenness as well as higher voltage variation of node 23, so that its physical vulnerability is outweighed over the cyber vulnerability. It is found that not only the regional control centre of communication network that needs to pay attention to cybersecurity, but also the physical vulnerability of the power network needs to take into consideration, as the cyberattacks will impact the power networks such as voltage variations.

3.6 Conclusion

This article proposes a VPPF method to detect cyber contingencies in the CPPS. A hierarchical system with four layers is proposed with national and regional control structure of

CPPS. In order to build communication networks for the analysis of cyber contingencies, a 6 and 12 communication zones are designed by using star-structured communication network with various network latencies, which are developed based on the topology of IEEE-39 and IEEE-118 test cases. Constrained FDI attack and DoS attack are simulated to evaluate vulnerability of cyber and physical nodes in CPPS. The proposed novel vulnerability index includes system voltage variation, network latency and node betweenness as the three indicators. It is found that system voltage indicator is more effective in detecting the FDI attack, as such attack can be identified by the impacts on the physical network such as topology and generation distribution. As for network latency indicator, the results show that the zone with interconnected communication links become more resilient to the DoS attacks. The node betweenness indicator provides an effective way to address 'cyber-physical node betweenness' in the CPPS due to the different topology of power and communication networks. The results show that the higher the cyber-physical node betweenness, the higher the vulnerability of the node under cyberattacks.

The overall vulnerability index ranks the low vulnerability of nodes with the following three types: nodes at the edge of the networks with fewer betweenness, nodes near a synchronous generator that are less affected by voltage variations, and nodes with low re-routed latency of communication networks. The vulnerability index also identifies that control centres have the highest vulnerability, so that they are more vulnerable to cyberattacks.

Chapter 4

Global Sensitivity Analysis for Cyber-Physical Power Distribution Networks

Publication Related to This Chapter

This chapter includes the publication listed as follows:

Qiu, D., S. Zhang, T. Luo and X. Zhang, "Global Sensitivity Analysis for Cyber-Physical Power Distribution Network," in IEEE Transactions on Industrial Cyber-Physical Systems, vol. 4, pp. 213-224, 2026, doi: 10.1109/TICPS.2026.3674974.

Chapter Overview

Cyber-physical power systems (CPPS) operate under uncertainties from both the power and communication layers, yet there are limited systematic methods to evaluate uncertain cyber-physical impacts. To address this gap, we build a CPPS model by coupling a power distribution network represented by differential–algebraic equations (DAEs) and a discrete-event communication network with node-specific communication delays. On this basis, global sensitivity analysis (GSA) is introduced to quantify the impact of cyber-physical uncertainties on the power distribution network, thereby identifying the most critical factors that affect CPPS operation. Probabilistic models are used to simulate load, photovoltaic (PV) generation, and communication delays, and a Monte Carlo framework is built to estimate Sobol' sensitivity indices. Finally, a CPPS digital co-simulation platform is developed which integrates OPAL-RT power system simulator and OMNeT++ communication network simulator via shared memory mechanism to validate the CPPS

framework. Case studies demonstrate the quantitative relationship between the sources of uncertainty and their impacts within the CPPS, indicating that PV generation dominates the variance of bus voltages, whereas communication node delays mainly affect local voltage stability in the test system.

4.1 Introduction

The increasing integration of advanced information and communication technologies (ICTs) into modern power grids has evolved into cyber-physical power systems. This integration brings significant benefits, including real-time monitoring, wide-area control, demand-side participation, and promoting renewable energy sources (RES) integration, all of which are critical to achieving the Net Zero target in the United Kingdom [99]. However, new vulnerabilities of the coupling CPPS structure have been created. For example, cyberattacks such as false data injection [100], denial-of-service attacks [101], or cross-layer hybrid attacks [102] can bypass traditional defense mechanisms, directly disrupting measurement and control processes between physical and cyber layers and triggering large-scale disturbance. In 2023, a hacker accessed power grid control systems and cut off power supply in Russia. In 2022, Sandworm caused an unplanned power outage in Ukraine. As a result, the cybersecurity and resilience of CPPS have become an urgent challenge that requires more attention.

The power distribution networks play an important role in CPPS, since they are developing towards active distribution networks that integrate active RES such as photovoltaics (PVs). Distribution networks are characterised by dispersed structures, bidirectional power flows, and high uncertainties due to stochastic demand and renewable generation [7]. In addition, power distribution networks connect directly to end users, where flexible resources are deployed, including electric vehicles, energy storage, and demand-side management. These unique features make distribution networks more sensitive to communication quality, providing significant challenges to the stability, security, and resilience of CPPS.

In recent years, significant progress has been made in analysing the uncertainties in the distribution network. Reference [103] identified several causes of uncertainty within communication networks, including both technical and economic factors. In [104], the uncertainties in communication performance (e.g., communication delay) can affect the reliability and operational quality of distribution. Reference [105] took the operator performance into account to present a human-in-the-loop uncertainty analysis. However, both [104, 105] have limited investigation on uncertainties in coupling systems. Reference [106] proposed quantitative indices with 5G-based recovery strategies to mitigate the effect of communication uncertainties. However, it lacked the validation provided by

the CPPS digital co-simulation platform.

Despite these advancements, some limitations remain to be resolved. Many studies were still based on static or simplified models [107, 108], which lacked insight into power system dynamics and multi-source uncertainties. Communication delay analysis often relied on fixed or simple stochastic models [109, 110], failing to capture real network congestion, packet loss, and dynamic variations. Furthermore, most studies did not systematically quantify uncertainties or provide holistic assessments of CPPS resilience. Some studies relied on Monte Carlo simulations for security assessment or critical-component identification; however, high computational cost and data-quality limitations constrained their practical applicability, given the fact that these methods were purely theoretical [111].

To fill these research gaps, this paper proposes a global sensitivity analysis (GSA) method for CPPS based on a real-time digital co-simulation framework, which offers a systematic and quantitative approach to assess the influence of various uncertainties in the CPPS model. The main contributions are as follows:

- A probabilistic CPPS modelling framework is developed to establish coupling between a DAE-based power distribution network model and a discrete-event communication network, incorporating both physical and functional coupling. This enables bidirectional interaction and accurately captures cross-domain dependencies in CPPS.
- The GSA method is applied for the first time to CPPS to quantitatively assess the impact of system states and cyber variables on overall system performance. Both first-order and total-effect Sobol' indices are employed to distinguish the main effects from interaction effects of uncertainty, allowing a systematic ranking of uncertain inputs, and providing valuable information for uncertainty quantification.
- A digital co-simulation platform is proposed that employs a shared memory mechanism for efficient data exchange between the OPAL-RT power system simulator and the OMNeT++ communication network simulator. The real-time digital co-simulation platform is implemented to demonstrate the capability for CPPS digital co-simulation and validate the effectiveness of the proposed GSA method.

The rest of this paper is organised as follows: Section 4.2 presents the probabilistic modelling of CPPS; Section 4.3 presents the GSA method with independent random inputs; Section 4.4 describes the proposed real-time digital co-simulation platform; Section 4.5 reports simulation results on the IEEE 33-bus system; Section 4.6 concludes the paper.

4.2 Probabilistic Modelling of Cyber-Physical Power Systems

4.2.1 Formulations of Power and Communication Systems

4.2.1.1 Power System Model

The power distribution network includes both physical and cyber components, such as a main grid feeder, control centre, radial distribution lines, information flow, synchronous machines, distributed RES such as PV generation, and various loads connected at the buses. The physical components are typically modelled by DAEs,

$$\dot{\boldsymbol{x}} = f(\boldsymbol{x}, \boldsymbol{V}), \tag{4.1}$$

$$\mathbf{0} = \boldsymbol{I}(\boldsymbol{x}, \boldsymbol{V}) \; - \; Y_N \, \boldsymbol{V}, \tag{4.2}$$

where x collects the dynamic states of the power-system devices, including synchronous machine states, PV inverter states, and controller states. V denotes the algebraic bus voltage vector, I denotes the injected current vector from generators, PV units, and loads, and Y_N is the network admittance matrix. The DAE formulation in 4.1–4.2 is a compact representation of the dynamic device equations and algebraic network constraints commonly used in power-system dynamic modelling [112].

To make the physical meaning of 4.1–4.2 explicit, the algebraic network equation can be written in rectangular coordinates as

$$0 = \begin{bmatrix} I_x(x,V) \\ I_y(x,V) \end{bmatrix} - \begin{bmatrix} G & -B \\ B & G \end{bmatrix} \begin{bmatrix} U_x \\ U_y \end{bmatrix}, \tag{4.3}$$

where $V = U_x + jU_y$ and $Y_N = G + jB$. The injected current vector can be decomposed as

$$I(x,V) = I_{\mathrm{SG}}(x,V) + I_{\mathrm{PV}}(x,V) - I_{\mathrm{L}}(V), \tag{4.4}$$

where I_{SG}, I_{PV}, and I_{L} represent the current contributions from synchronous machines, PV inverters, and loads, respectively. For a constant-power load connected at bus i, the load current can be expressed as

$$I_{\mathrm{L},i} = \frac{P_{\mathrm{L},i} - jQ_{\mathrm{L},i}}{V_i^*}, \tag{4.5}$$

where $P_{\mathrm{L},i}$ and $Q_{\mathrm{L},i}$ are the active and reactive load demand at bus i.

For example, a synchronous machine connected at bus i can be represented by the

classical rotor equations

$$\dot{\delta}_i = \omega_b(\omega_i - \omega_s), \tag{4.6}$$

$$M_i\dot{\omega}_i = P_{m,i} - P_{e,i} - D_i(\omega_i - \omega_s), \tag{4.7}$$

where δ_i is the rotor angle, ω_i is the rotor speed, M_i is the inertia constant, D_i is the damping coefficient, $P_{m,i}$ is the mechanical input power, and $P_{e,i}$ is the electrical output power. The electrical power is obtained from the terminal voltage and stator current, e.g.

$$P_{e,i} = \mathrm{Re}\left\{V_i I^*_{\mathrm{SG},i}\right\}. \tag{4.8}$$

Similarly, the PV unit is represented as a grid-connected voltage-source converter with a DC-link and an L_f filter. A representative inverter current model in the dq reference frame can be written as [113]

$$L_f\dot{i}_d = v_{inv,d} - v_d + \omega L_f i_q - R_f i_d, \tag{4.9}$$

$$L_f\dot{i}_q = v_{inv,q} - v_q - \omega L_f i_d - R_f i_q, \tag{4.10}$$

where i_d and i_q are the inverter output currents, $v_{inv,d}$ and $v_{inv,q}$ are the converter-side voltages, v_d and v_q are the grid-side voltages, and R_f and L_f are the filter resistance and inductance. These device-level dynamic equations are assembled into the compact state equation 4.1, while their current injections are coupled to the network equation 4.2. Detailed formulations of the full two-stage model can be found in [114].

4.2.1.2 Communication Network Model

Communication networks, including TCP/IP, VoIP and cellular technologies, are packet-switched systems and are commonly simulated as discrete-event systems [115]. The state variables of communication components are updated according to discrete-events and are defined over discrete sets, rather than being derived from continuous dynamics. Mathematically, the communication system is formulated as follows: let $\eta \in \Upsilon$ represent the communication network state, where $\Upsilon \subset \mathbb{R}^{n_c}$ denotes the corresponding Euclidean state space. The condition of η is governed by a difference inclusion, with its right-hand side characterised by a set-valued communication state update map G_C. The system receives a system input signal $\nu \in \mathcal{V} \subset \mathbb{R}^{m_c}$, and the system output signal $\zeta \in \mathbb{R}^{r_c}$ is determined by a communication output map K that depends on both the state and the input:

$$\eta^+ \in G_C(\nu, \eta), \quad \zeta = K(\nu, \eta). \tag{4.11}$$

In Eq.4.11, the communication state η can be interpreted as a collection of practical

network variables, such as queue lengths, link states, packet-loss states, and time stamps of transmitted messages. The input ν represents the data packet or measurement/control message injected into the communication network, while the output ζ represents the delivered message after transmission delay, queueing, processing, and possible packet loss. Although OMNeT++ calculates these quantities through an event-driven simulation mechanism, their physical meanings can be explained using standard communication-network delay models [116]. For a packet transmitted through link (i, j) at time step k, the end-to-end link delay can be decomposed as

$$d_{ij}[k] = d_{ij}^{\text{proc}}[k] + d_{ij}^{\text{queue}}[k] + d_{ij}^{\text{trans}}[k] + d_{ij}^{\text{prop}}[k], \tag{4.12}$$

where d_{ij}^{proc} is the processing delay, d_{ij}^{queue} is the queueing delay, d_{ij}^{trans} is the transmission delay, and d_{ij}^{prop} is the propagation delay. These terms can be further approximated as

$$d_{ij}^{\text{trans}}[k] = \frac{L_{ij}[k]}{R_{ij}}, \tag{4.13}$$

$$d_{ij}^{\text{prop}}[k] = \frac{l_{ij}}{v_{\text{prop}}}, \tag{4.14}$$

$$d_{ij}^{\text{queue}}[k] \approx \frac{q_{ij}[k]}{R_{ij}}, \tag{4.15}$$

where $L_{ij}[k]$ is the packet length in bits, R_{ij} is the link data rate, l_{ij} is the physical or logical link distance, v_{prop} is the signal propagation speed, and $q_{ij}[k]$ is the queue backlog in bits.

The queue state can be updated in discrete time as

$$q_{ij}[k+1] = \min\left\{Q_{ij}^{\max}, [q_{ij}[k] + a_{ij}[k] - R_{ij}T_s]^+\right\}, \tag{4.16}$$

where $Q_{ij}^{\max}$ is the maximum queue capacity, $a_{ij}[k]$ denotes the amount of newly arrived data, T_s is the communication update interval, and $[\cdot]^+ = \max(\cdot, 0)$. Packet loss can be represented by the binary variable

$$\ell_{ij}[k] = \begin{cases} 0, & q_{ij}[k] + a_{ij}[k] \le Q_{ij}^{\max}, \\ 1, & q_{ij}[k] + a_{ij}[k] > Q_{ij}^{\max}, \end{cases} \tag{4.17}$$

where $\ell_{ij}[k] = 1$ indicates packet loss due to queue overflow or communication failure.

Based on these quantities, a practical form of the communication output map in (4.3) can be written as

$$\zeta_j[k] = \begin{cases} \nu_i[k - d_{ij}[k]], & \ell_{ij}[k] = 0, \\ \zeta_j[k-1], & \ell_{ij}[k] = 1, \end{cases} \tag{4.18}$$

where the first case represents successful delivery of a delayed packet, and the second

case represents a hold-last-value strategy when the packet is lost. Therefore, the abstract communication state in (4.3) can be understood as

$$\eta[k] = \{q_{ij}[k], d_{ij}[k], \ell_{ij}[k]\}_{(i,j)\in\mathcal{E}_c}\,, \tag{4.19}$$

where $\mathcal{E}_c$ denotes the set of communication links.

4.2.2 The Coupling Mechanism of Cyber-Physical Power Systems

In the proposed CPPS framework, the interaction between the power system and the communication network is represented by node-specific communication delays. These node-specific communication delays model the effective time shift between measurements, communication, and control actions at the system level, while the physical data-transfer delay of the digital co-simulation platform is assumed to be negligible and handled separately by the synchronisation mechanism [6].

Let $\mathbf{u}^{\mathrm{ps}}(t)$ denote the coupling inputs to the power system vector and $\mathbf{u}^{\mathrm{cn}}(t)$ denote the coupling inputs to the communication network vector, respectively. The coupling between the cyber and physical layers is formulated as

$$\mathbf{u}^{\mathrm{ps}}(t) = f_{\mathrm{cn}\to\mathrm{ps}}(\mathbf{y}^{\mathrm{cn}}(t-\boldsymbol{\tau}))\,, \tag{4.20}$$

$$\mathbf{u}^{\mathrm{cn}}(t) = f_{\mathrm{ps}\to\mathrm{cn}}(\mathbf{y}^{\mathrm{ps}}(t-\boldsymbol{\tau}))\,, \tag{4.21}$$

where $\mathbf{y}^{\mathrm{ps}}(t)$ and $\mathbf{y}^{\mathrm{cn}}(t)$ denote the measurement outputs and control signals, respectively. $\boldsymbol{\tau}$ denotes communication delay vector and $\boldsymbol{\tau} = [\tau_1, \ldots, \tau_N]^\top$ represents the vector of node-specific communication delays.

More explicitly, the physical-to-cyber coupling can be described by the sampling and transmission of power-system measurements. For node i, the sampled measurement sent to the communication network at time t_k is

$$\nu_i^{ps\to cn}[k] = h_i\left(x(t_k), V(t_k)\right), \tag{4.22}$$

where $h_i(\cdot)$ extracts the local physical measurements, such as bus voltage, current, or converter state. After passing through the communication network, the received measurement is

$$\tilde{y}_i^{ps}[k] = \begin{cases} \nu_i^{ps\to cn}[k-\kappa_i], & \ell_i[k]=0, \\ \tilde{y}_i^{ps}[k-1], & \ell_i[k]=1, \end{cases} \tag{4.23}$$

where $\kappa_i = \lceil \tau_i/T_s \rceil$ is the discrete delay step corresponding to the node-specific delay τ_i, and $\ell_i[k]$ is the packet-loss state. The cyber-layer controller or communication process

then generates the control signal

$$u_i^{cn}[k] = \psi_i\left(\tilde{y}_i^{ps}[k]\right), \tag{4.24}$$

where $\psi_i(\cdot)$ denotes the control, monitoring, or data-processing function in the cyber layer.

Similarly, the cyber-to-physical coupling is represented by applying the delayed cyber-layer signal to the power-system model:

$$u_i^{ps}(t_k) = \begin{cases} u_i^{cn}[k-\kappa_i], & \ell_i[k] = 0, \\ u_i^{ps}(t_{k-1}), & \ell_i[k] = 1. \end{cases} \tag{4.25}$$

This formulation shows that communication delay and packet loss modify the timing and availability of measurement and control signals, thereby affecting the dynamic power-system equations in 4.1 and the algebraic network constraints in 4.2.

The communication delay τ_i characterises the effective delay of the closed-loop information exchange associated with node i, including communication, scheduling, and control execution within the CPPS. It represents a model-level delay of the cyber-physical interaction, rather than the physical transmission or synchronisation latency of the HIL or digital co-simulation platform.

In this work, each node-specific communication delay is modelled as

$$\tau_i = t_{0,i} + \delta_i, \tag{4.26}$$

where $t_{0,i}$ denotes the nominal communication delay at node i, and δ_i is a stochastic delay deviation capturing the uncertainty in the cyber-physical coupling at that node.

4.2.3 Uncertainties in Cyber-Physical Power System

The uncertainties in CPPS arise from two main aspects: power system and communication network. In this paper, we focus on three types of uncertainties during the CPPS normal operation: load, PV generation and communication delay.

4.2.3.1 Load Uncertainty

In CPPS, we assume loads have constant power factors and the active power of loads follows a Gaussian distribution as [117]. This assumption is commonly adopted in probabilistic load flow studies to represent stochastic load demand. It is also reasonable for aggregated distribution-network loads, since the total load at a bus can be regarded as the combined effect of many individual demand variations.

$$p(\psi^{\mathrm{lp}}) = \frac{1}{\sqrt{2\pi}\sigma_{\psi^{\mathrm{lp}}}} \exp\left[-\frac{\left(\psi^{\mathrm{lp}} - \mu_{\psi^{\mathrm{lp}}}\right)^2}{2\sigma^2_{\psi^{\mathrm{lp}}}}\right], \tag{4.27}$$

where p denotes the probability density function; ψ^{lp} represents the active power of loads; $\mu_{\psi^{\mathrm{lp}}}$ and $\sigma_{\psi^{\mathrm{lp}}}$ denote the mean and standard deviation of load active power. Although the stochastic loads enter the power system model as algebraic parameters, the system states remain continuous due to network dynamics and inverter-based generation control.

4.2.3.2 Solar Generation Uncertainty

In this paper, PV generation uncertainty is represented through uncertain solar radiation, modelled by a Beta distribution [118].

$$p(SR) = \frac{\Gamma(\kappa+\varepsilon)}{\Gamma(\kappa)\Gamma(\varepsilon)} \left(\frac{SR}{SR_{\max}}\right)^{\kappa-1} \left(1 - \frac{SR}{SR_{\max}}\right)^{\varepsilon-1}, \tag{4.28}$$

where Γ is the gamma function, κ and ε are Beta distribution shape parameters, SR and $SR_{\max}$ are the actual and maximum solar radiation, respectively.

4.2.3.3 Time Delay Uncertainty

The uncertainty of the node-specific communication delay is modelled by a uniform distribution centred on its nominal value $t_{0,i}$ [119]. The uniform distribution is adopted as a bounded-uncertainty model rather than an empirically fitted delay distribution. This assumption is commonly used when detailed traffic traces are unavailable but the possible delay range can be specified; similar bounded uniform delay assumptions have been used in networked control systems and smart-grid communication simulations [120, 121].

$$p(\tau_i) = \begin{cases} \dfrac{1}{2\lambda_i}, & t_{0,i} - \lambda_i \le \tau_i \le t_{0,i} + \lambda_i, \\ 0, & \text{otherwise}, \end{cases} \tag{4.29}$$

where τ_i denotes the communication delay associated with node i, and λ_i denotes the delay uncertainty bound at node i, in other words, it specifies the maximum deviation that captures the uncertainty of the cyber-physical information exchange at that node.

For each Monte Carlo realisation, τ_i is sampled once from the above distribution and kept constant during the entire transient simulation, representing a quasi-static but uncertain communication condition in the CPPS. Moreover, τ_i is different in different Monte Carlo realisations.

4.3 Global Sensitivity Analysis with Independent Random Inputs

4.3.1 Variance Decomposition

A deterministic model whose outputs depend on an uncertain input vector $\mathbf{X} \in \mathbb{R}^{N_x}$ is considered in this paper, where $\mathbf{X}$ collects all uncertain parameters from both the power and communication layers, and the inputs are assumed to be independent and N_x represents the dimension of the uncertain inputs. Furthermore, an isoprobabilistic transform is applied to map the marginal distributions to make the analysis performed on $[0,1]^{N_x}$.

This independence assumption is adopted as a baseline modelling simplification for the proposed Sobol-based GSA. The load demand, PV generation, and node-specific communication delays are treated as independent uncertainty sources because they originate from different physical and cyber-layer mechanisms and only their marginal probability distributions are considered in this study. In practical CPPS applications, uncertainties may be correlated, for example due to spatially correlated solar irradiance, correlated load profiles, or network-wide congestion. In such cases, dependent-input GSA methods, such as copula-based or correlation-aware Sobol' indices, should be adopted [122, 123].

4.3.1.1 Uncertain Input Variables X

The input vector can be written as

$$\mathbf{X} = (X_1, \ldots, X_{N_x}), \qquad N_x \in \mathbb{N}. \tag{4.30}$$

The components X_i represent the model parameters, initial or boundary conditions, and external parameters. In this paper, the uncertain inputs, including load, PV generation, and node-specific communication delay, are treated as statistically independent random variables. Only marginal probability distributions are considered. The uncertain inputs X_i include: load of each bus, which is represented by the operation of injected current and voltage at each bus; communication delay (τ_i) on each bus i; stochastic fluctuation of solar radiation.

4.3.1.2 Model Output Observables Y_ℓ

Let $M(X)$ denote the model output generated by the CPPS digital co-simulation platform, where X is the uncertain input vector. In this work, the complete output set considered for GSA consists of the dynamic, control, voltage, and current states of the

cyber–physical power distribution network. These output variables can be grouped as follows: synchronous machine states, including rotor angles and angular speeds; PV unit and inverter states, including inverter currents, terminal voltages, DC-link voltages, controller reference signals, and PWM duty ratios; bus voltage states, including the real and imaginary components of bus voltages, U_x and U_y; bus current states, including the real and imaginary components of injected currents, I_x and I_y.

For clarity, the output vector can be written in a grouped form as

$$Y = [Y_{\mathrm{SG}}, Y_{\mathrm{PV}}, Y_{\mathrm{V}}, Y_{\mathrm{I}}], \tag{4.31}$$

where Y_{SG} denotes synchronous machine states, Y_{PV} denotes PV inverter and controller states, Y_{V} denotes bus voltage states, and Y_{I} denotes bus current states.

For the sensitivity analysis, each scalar output is extracted from the complete output vector using an output extraction function q_ℓ:

$$Y_\ell = q_\ell\Big(M(X)\Big), \tag{4.32}$$

where ℓ denotes the index of a selected scalar output. Therefore, the Sobol indices are computed for each output state individually. Since the complete output vector contains multiple state categories, only representative outputs and the most or least sensitive states are selected for detailed discussion in the results section.

4.3.1.3 Hoeffding–Sobol' Functional Decomposition

The terms in the Hoeffding–Sobol' decomposition do not have manually assigned weights. Instead, each term is associated with a variance contribution. After normalisation by the total output variance, these contributions form Sobol' indices, which can be interpreted as the relative contribution weights of individual inputs and their interactions. Therefore, the importance of each uncertainty source is determined by the model response rather than by a pre-defined weighting factor.

To quantify how individual uncertainties contribute to the variability of Y_ℓ, a variance-based decomposition is adopted. For a fixed ℓ and square-integrable Y_ℓ on $[0,1]^{N_x}$ with independent inputs,

$$Y_\ell = f_0^{(\ell)} + \sum_{i=1}^{N_x} f_i^{(\ell)}(X_i) + \sum_{i<j} f_{ij}^{(\ell)}(X_i, X_j) + \cdots + f_{1\ldots N_x}^{(\ell)}(\mathbf{X}), \tag{4.33}$$

where the component functions are mutually orthogonal (zero mean with respect to each

of their arguments). They are identified via

$$\begin{aligned} f_0^{(\ell)} &= \mathbb{E}[Y_\ell], \\ f_i^{(\ell)}(X_i) &= \mathbb{E}[Y_\ell \mid X_i] - f_0^{(\ell)}, \\ f_{ij}^{(\ell)}(X_i, X_j) &= \mathbb{E}[Y_\ell \mid X_i, X_j] - f_0^{(\ell)} - f_i^{(\ell)} - f_j^{(\ell)}, \end{aligned} \tag{4.34}$$

with analogous expressions for higher orders.

According to Eqs. **??**, 4.33 and 4.34, the variance decomposes as

$$\mathrm{Var}(Y_\ell) = \sum_{i=1}^{N_x} V_i^{(\ell)} + \sum_{i<j} V_{ij}^{(\ell)} + \cdots + V_{1\ldots N_x}^{(\ell)}, \tag{4.35}$$

with

$$\begin{aligned} V_i^{(\ell)} &= \mathrm{Var}_{X_i}\Big(\mathbb{E}[Y_\ell \mid X_i]\Big), \\ V_{ij}^{(\ell)} &= \mathrm{Var}_{X_i,X_j}\Big(\mathbb{E}[Y_\ell \mid X_i, X_j]\Big) - V_i^{(\ell)} - V_j^{(\ell)}. \end{aligned} \tag{4.36}$$

Here, each term $V_i^{(\ell)}$ represents the variance contribution caused solely by the uncertainty of input X_i, while higher-order terms capture interaction effects among multiple uncertain inputs. Repeating the analysis with different indices ℓ yields sensitivity profiles by spatial, temporal, or component sensitivity in a model-agnostic manner.

From a physical perspective, the variance terms $V_i^{(\ell)}$ quantify the extent to which the uncertainty of input X_i alone contributes to the variability of the output Y_ℓ, while higher-order terms represent interaction effects among multiple inputs. This interpretation is particularly relevant for CPPS, where uncertainties from the power and communication layers may interact in complex ways.

4.3.2 First-order and Total-Effect Sobol' Indices

In this work, first-order and total-effect Sobol' indices are adopted to achieve a practical and physically balance between computational feasibility and sensitivity interpretability in CPPS. From a computational perspective, the proposed CPPS framework involves more than one hundred uncertain inputs (including stochastic loads, solar radiation, and node-specific communication delay), for which the explicit computation of higher-order indices can result in a high computational cost in the digital co-simulation procedure.

From a physical perspective, first-order indices capture the dominant contributions of individual uncertainty states, while the difference between total-effect and first-order indices reflects aggregated interaction effects. In the investigated scenarios, output uncertainties are primarily dominated by first-order contributions, indicating limited multi-way coupling. Therefore, first-order and total-effect indices provide effective sensitivity char-

acterisation with significantly reduced computational burden.

Given the input vector $\mathbf{X}$ in Eq. 4.30 and the scalar observable Y_ℓ in Eq. **??**, and using the functional decomposition in Eq. 4.33, the first-order Sobol' index $S_i^{(\ell)}$ quantifies the main (additive) contribution of the uncertain input X_i to the variance of Y_ℓ. The total-effect Sobol' index $S_{T_i}^{(\ell)}$ measures the overall influence of X_i, including both its direct effect and all interaction effects with the remaining inputs.

4.3.2.1 First-order index

$$S_i^{(\ell)} \;=\; \frac{V_i^{(\ell)}}{\mathrm{Var}\Big(Y_\ell\Big)}, \tag{4.37}$$

where $V_i^{(\ell)} = \mathrm{Var}_{X_i}\Big(\mathbb{E}[\,Y_\ell \mid X_i]\Big)$. This measures the fraction of the variance of Y_ℓ attributable solely to the variability of X_i, with the remaining inputs $\mathbf{X}_{\sim i}$ averaged out.

4.3.2.2 Total-effect index

$$\begin{aligned} S_{T_i}^{(\ell)} &= \frac{\mathbb{E}_{\mathbf{X}_{\sim i}}\Big[\mathrm{Var}_{X_i}\Big(Y_\ell \mid \mathbf{X}_{\sim i}\Big)\Big]}{\mathrm{Var}\Big(Y_\ell\Big)} \\ &= 1 - \frac{\mathrm{Var}_{\mathbf{X}_{\sim i}}\Big(\mathbb{E}_{X_i}\Big[Y_\ell \mid \mathbf{X}_{\sim i}\Big]\Big)}{\mathrm{Var}\Big(Y_\ell\Big)}. \end{aligned} \tag{4.38}$$

Here, $\mathbf{X}_{\sim i}$ denotes all inputs except X_i; therefore, $S_{T_i}^{(\ell)}$ accounts for both the main effect of X_i and all its interaction effects. The use of the first-order and total-effect indices allows dominant uncertainty sources and interaction effects in CPPS to be systematically distinguished without computing higher-order Sobol' indices.

The difference between the first-order and total-effect indices can be interpreted as follows. The first-order index $S_i^{(\ell)}$ measures the direct or main effect of the uncertain input X_i on the output Y_ℓ, while the influence of all other inputs is averaged out. Therefore, it answers the question: how much of the output variance can be explained by varying X_i alone? In contrast, the total-effect index $S_{T_i}^{(\ell)}$ measures the overall effect of X_i, including both its direct effect and all interaction effects involving X_i and the remaining inputs $X_{\sim i}$. Therefore, it answers the question: how much output variance would remain unexplained if the uncertainty of X_i were removed?

For independent inputs, the total-effect index is always greater than or equal to the first-order index,

$$S_{T_i}^{(\ell)} \geq S_i^{(\ell)}. \tag{4.39}$$

The difference between them,

$$S_{T_i}^{(\ell)} - S_i^{(\ell)}, \tag{4.40}$$

indicates the aggregated interaction contribution between X_i and other uncertain inputs. If $S_i^{(\ell)}$ is close to $S_{T_i}^{(\ell)}$, the input mainly affects the output independently. If $S_i^{(\ell)}$ is small but $S_{T_i}^{(\ell)}$ is large, the input mainly affects the output through interactions with other variables.

4.3.3 Indices Calculation

For analytically tractable models, Sobol' indices can be obtained in closed form by evaluating the integrals implied by the Hoeffding–Sobol' decomposition. In most practical sensitivity analysis cases, these integrals are intractable and the indices are estimated numerically via Monte Carlo sampling over the unit hypercube. The Monte Carlo method draws random points uniformly in $[0,1]^{N_x}$ and evaluates the model at these points to construct variance-based estimators.

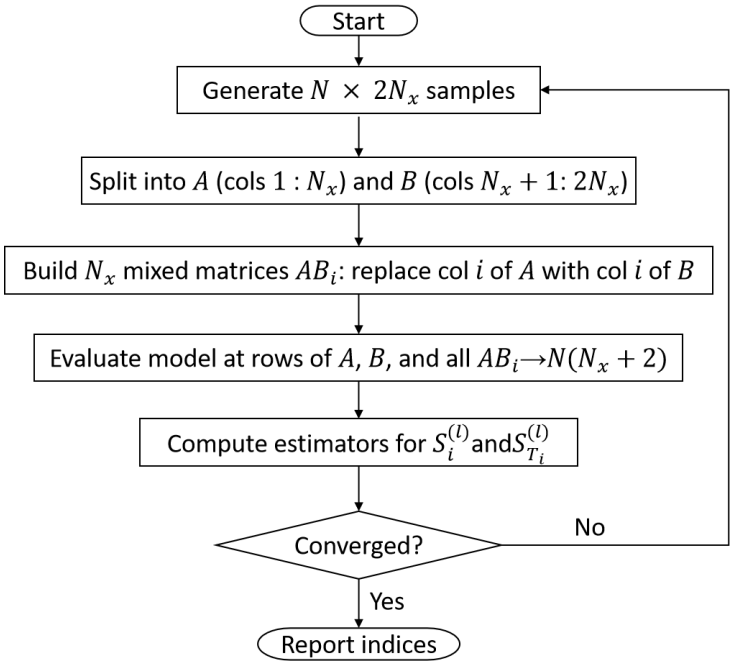


Figure 4.1: Process of Sobol' indices computation using Monte Carlo sampling.

The iterative process for computing Sobol's indices using the Monte Carlo sampling method is presented in Fig. 4.1. To estimate the Sobol' indices, two independent base sample matrices, denoted by A and B, are first generated from the uncertain input space:

$$A, B \in \mathbb{R}^{N \times N_x}, \tag{4.41}$$

where N is the Monte Carlo sample size and N_x is the number of uncertain input variables.

Each row of A or B represents one realisation of all uncertain inputs, including load uncertainty, PV generation uncertainty, and node-specific communication delay.

Equivalently, the two matrices can be obtained by generating an $N \times 2N_x$ sample matrix and splitting its columns into two base designs A and B. For each input variable X_i, a mixed matrix AB_i is formed by replacing the i-th column of A with the i-th column of B:

$$AB_i = [A_1, \ldots, A_{i-1}, B_i, A_{i+1}, \ldots, A_{N_x}]\,. \tag{4.42}$$

The model is then evaluated at all rows of the A, B, and AB_i matrices. This requires $N(N_x + 2)$ model evaluations, including N evaluations for A, N evaluations for B, and N evaluations for each mixed matrix AB_i. The resulting model outputs are used to estimate the first-order Sobol' index $S_i^{(\ell)}$ and the total-effect Sobol' index $S_{T_i}^{(\ell)}$ according to Eqs. 4.37 and 4.38. Finally, the sample size N is increased until the estimated indices stabilise.

There are several Monte Carlo estimators available for both indices. The approaches used in this paper are inspired by the following indices estimation method in [49]:

$$\mathrm{Var}_{X_{\sim i}}\Big(\mathbb{E}_{X_i}(Y|X_{\sim i})\Big) \approx \frac{1}{N}\sum_{j=1}^{N} \mathcal{M}(\mathbf{B}_j)\Big(\mathcal{M}(\mathbf{A}_{B,j}^{(i)}) - \mathcal{M}(\mathbf{A}_j)\Big), \tag{4.43}$$

and

$$\mathbb{E}_{X_i}\Big(\mathrm{Var}_{X_{\sim i}}(Y|X_i)\Big) \approx \frac{1}{2N}\sum_{j=1}^{N} \Big(\mathcal{M}(\mathbf{A}_j) - \mathcal{M}(\mathbf{A}_{B,j}^{(i)})\Big)^2, \tag{4.44}$$

for the estimation of the S_i and the S_{Ti} indices, respectively.

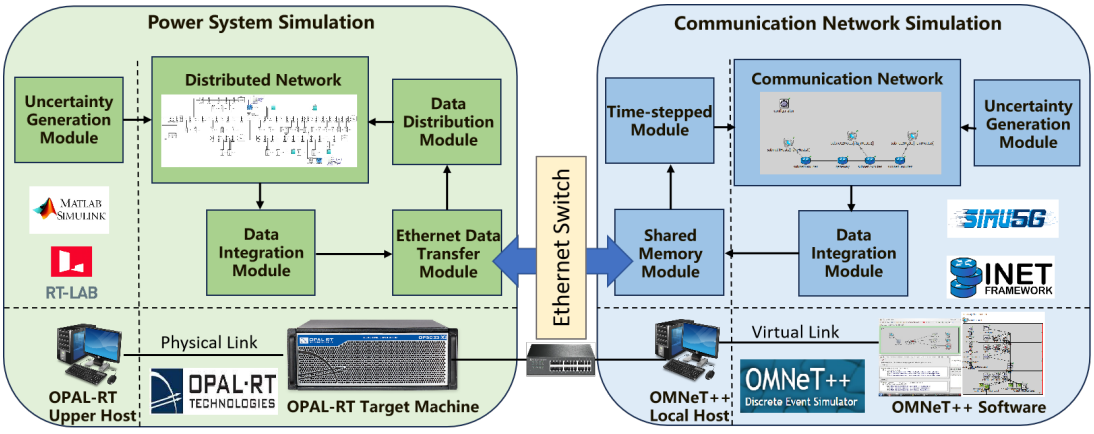


Figure 4.2: Cyber-physical co-simulation structure for distribution-network GSA using OPAL-RT and OMNeT++.

4.4 Cyber-physical Power System Digital Co-simulation Platform

As mentioned in Section 4.1, the Monte Carlo method requires substantial data of the input and output state vectors, and previous research mainly focused on the theory and had limited insight in realistic scenarios. Therefore, it is essential to establish a CPPS digital co-simulation platform and use it to generate large-scale, high-fidelity input–output datasets under realistic cyber–physical operating conditions, which are subsequently used in the Monte Carlo framework to estimate Sobol' sensitivity indices. As shown in Fig. 4.3, the proposed platform acts as the data-generation engine that connects probabilistic uncertainty modelling, digital co-simulation, and Sobol-based global sensitivity analysis.

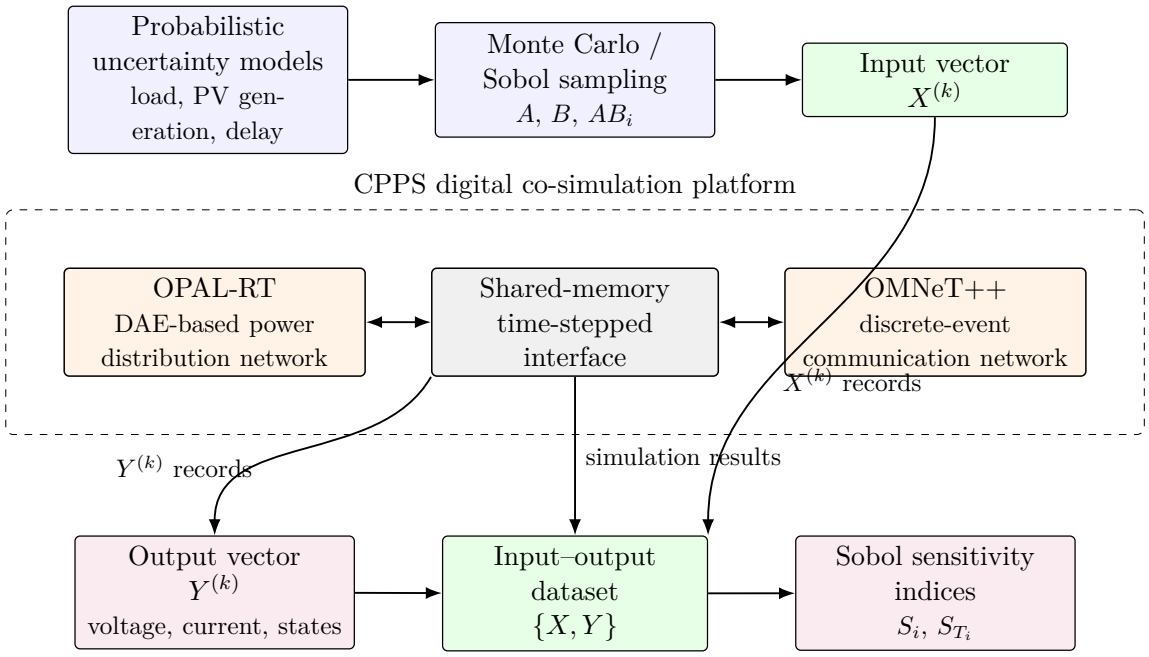


Figure 4.3: Workflow linking uncertainty sampling, CPPS digital co-simulation, and Sobol-based global sensitivity analysis.

This paper provides the Ethernet-based implementation framework for cyber-physical digital co-simulation, thereby providing essential data for GSA. As shown in Fig. 4.2, the CPPS digital co-simulation platform consists of an OPAL-RT power system simulator and an OMNeT++ communication network simulator, and a time-stepped digital co-simulation scheme is used to exchange data.

It should be noted that the co-simulation platform in Fig. 4.2 differs from the platforms presented in Chapter 5 not in terms of application scenario, but in terms of development stage and functional maturity. The platforms in Chapter 5 represent earlier stages of the co-simulation platform development, where Typhoon HIL or OPAL-RT is coupled with EXata to demonstrate real-time cyber–physical interaction and to validate

representative cybersecurity scenarios, including false data injection, packet drop, denial-of-service, and delay attacks. These platforms provide the basis for establishing real-time power–communication co-simulation capability.

By contrast, the platform developed in this chapter is a more comprehensive co-simulation framework. Although it is applied here to the IEEE 33-bus cyber–physical power distribution network for global sensitivity analysis, the architecture itself is not restricted to distribution networks. By replacing the physical power system model and communication topology, the same framework can be extended to other CPPS scenarios, including microgrids. Compared with the earlier platforms in Chapter 5, this platform places greater emphasis on deterministic synchronisation, efficient data exchange, and repeatable large-scale simulation. The shared-memory-based time-stepped interface between OPAL-RT and OMNeT++ is therefore adopted to support Monte Carlo sampling, uncertainty propagation analysis, and Sobol-index-based global sensitivity analysis. In this sense, Fig. 4.2 represents an improved and more general platform architecture built upon the experience gained from the previous co-simulation platforms.

4.4.1 Power Distribution Network Simulation in OPAL-RT

The OPAL-RT is a powerful simulator for real-time digital power system simulation. Featuring an Intel Xeon processor with a maximum of 44 cores, the OP 5033XG simulator is a powerful master system for setups that expanded with FPGA and I/O expansion modules. In addition, it offers a suitable platform for real-time cybersecurity applications, where hardware integration supports network protocols such as C37.118 and IEC61850.

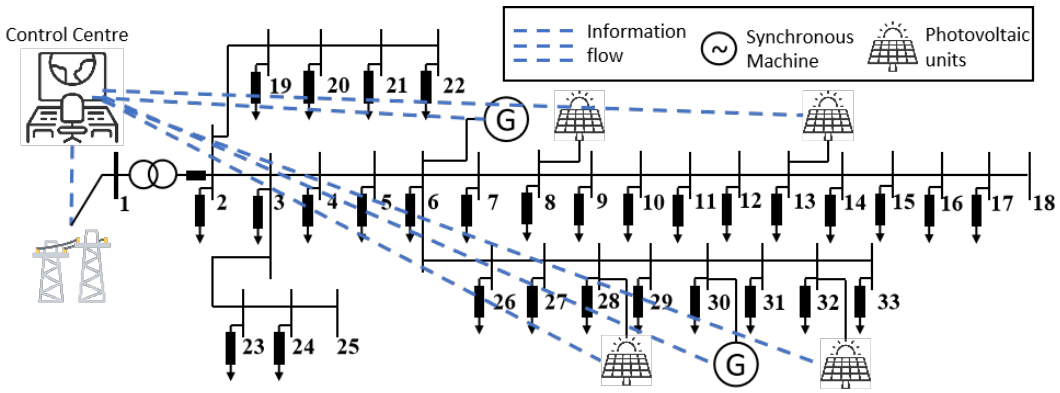


Figure 4.4: IEEE 33-bus power distribution network with communication structure.

This study develops a power system digital simulation model based on the IEEE 33-bus power distribution network implemented on the proposed simulation platform. The power distribution system topology is presented in Fig. 4.4. The original 12.66 kV and 60 Hz IEEE 33-bus system is modified by integrating four distributed PV units at buses

8, 13, 28, and 32, operating in parallel with existing loads, and two distributed machines based on synchronous machines at buses 6 and 30. The main grid is represented by a slack bus with a fixed voltage magnitude of 1 p.u. and a phase angle of 0°, which provides the reference operating point during the simulation.

The PV units are modelled using a detailed PV array model with double-loop vector control and DC link voltage regulation, while the synchronous machine-based distributed generators are represented by a classical generator model with rotor angle and speed dynamics, augmented with transient EMF states. The system load is represented as a stochastic, time-varying demand following a Gaussian distribution and centres at 5084.26 + j2547.32 kVA, with active and reactive power updated at each simulation step to emulate realistic load fluctuations ($\mu = 1, \sigma = 0.05$ in p.u.). The installed rated PV power corresponds to 40% of the nominal system load under baseline operating conditions. During simulation, stochastic load variations are introduced independently, and the instantaneous PV penetration is allowed to vary naturally without dynamic rescaling. To ensure numerical stability during real-time execution, the detailed PV and synchronous machine models are executed within the OPAL-RT real-time simulation environment, which is designed to handle stiff DAE-based power system models under fixed-step real-time constraints. The main dynamic parameters of PVs and synchronous machines are provided in Tables 4.1 and 4.2.

Table 4.1: Main Dynamic and Parameters of PV Units

C_{pv} (F)	L_{dc} (H)	C_{dc} (F)	L_f (H)	$u_{\text{dc,ref}}$ (V)	T (°C)
1.0×10^{-4}	5.0×10^{-2}	5.0×10^{-3}	5.0×10^{-3}	800	25
k_p (DCV)	k_i (DCV)	k_{op} –	k_{oi} –	k_{ip} –	k_{ii} –
−0.1	−0.01	−0.05	10	2	9

In the PV model, C_{pv} denotes the equivalent capacitance of the PV array, L_{dc} and C_{dc} represent the inductance and capacitance of the DC-link circuit, respectively, and L_f is the inverter filter inductance. $u_{\text{dc,ref}}$ denotes the reference DC-link voltage, and T represents the operating temperature of the PV units. The parameters k_p and k_i correspond to the proportional and integral gains of the DC-voltage control loop, while k_{op} and k_{oi} denote the proportional and integral gains of the outer control loop. The parameters k_{ip} and k_{ii} represent the proportional and integral gains of the inner current control loop. All PV units are the same parameters in this chapter.

Table 4.2: Main Dynamic Parameters of Synchronous Machines

P_m (p.u.)	T_j (s)	D_{sg} –	r_a (p.u.)	x'_d (p.u.)	x'_q (p.u.)	f (Hz)
0.58665	47.28	100	0	0.0608	0.0969	60
0.37923	47.28	100	0	0.0608	0.0969	60

In the synchronous machine model, P_m denotes the mechanical input power, T_j is the inertia time constant, and D_{sg} represents the damping coefficient of the machine. The parameter r_a denotes the armature resistance, while x'_d and x'_q represent the transient reactances along the d-axis and q-axis, respectively. Finally, f denotes the nominal operating frequency of the synchronous machine.

4.4.2 Communication Network Simulation in OMNeT++

OMNeT++ is an open source discrete-event simulator, which provides a modular simulation framework written in C++, along with various extensions that support the development of network simulation models based on a component-based architecture.

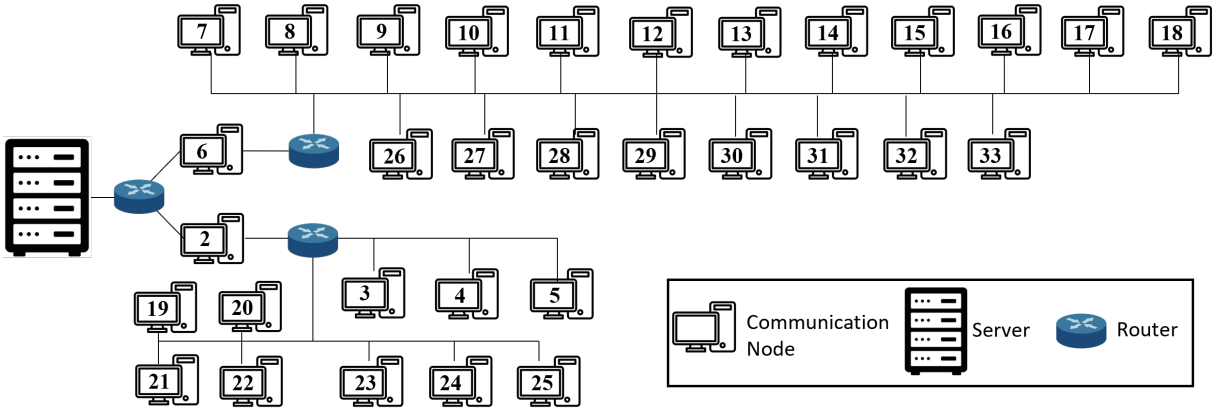


Figure 4.5: The OMNeT++ model of the IEEE 33-bus communication network.

As shown in Fig. 4.5, each bus in the power distribution system and each distributed power source corresponds to a communication node in the communication network, which is modelled by the INET model StandardHost. Since OMNeT++ is a discrete-event simulator, most of the simulation is non-real-time. To implement OMNeT++ with OPAL-RT to conduct CPPS digital co-simulation, the OMNeT++ model should not only communicate with the OPAL-RT target machine, but also operate in a real-time manner. The communication network adopts a double-star topology, where node 2 and node 6 are two data transfer nodes, and node 1 acts as the server. The node-specific communication delay τ_i in the CPPS model follows a uniform distribution as shown in Eq. 4.29.

There are multiple methods to implement the data transfer interface for digital co-simulation between OPAL-RT and OMNeT++, such as virtual Ethernet(veth) pairs and shared memory. The veth method can better simulate Internet protocols, since it creates virtual Ethernet peers to transfer data from the OMNeT++ host machine to the OMNeT++ model. Compared with the veth method, the shared memory method does not rely on virtual links. Instead, external input data are assigned to the corresponding memory space using the Boost::interprocess library from which the OMNeT++ model can directly access and process the data. In OMNeT++, the network configuration in the omnetpp.ini file should be configured with the RealTimeScheduler to ensure that the simulated time is consistent with real time. This method enhances execution speed and improves data processing efficiency, thus reducing transmission delays in real-time simulation and increasing the overall accuracy of CPPS digital co-simulation.

4.4.3 Time-Stepped Synchronisation Scheme Using Shared Memory

The digital co-simulation mechanism between the power distribution network in the OPAL-RT and communication network in the OMNeT++ is carried out using a time-stepped synchronisation scheme. In this approach, both simulators are simulated in discrete time steps to improve the data consistency between the physical and cyber dynamics and to ensure accurate temporal alignment between the continuous-time DAE-based power system model and the discrete-event communication network.

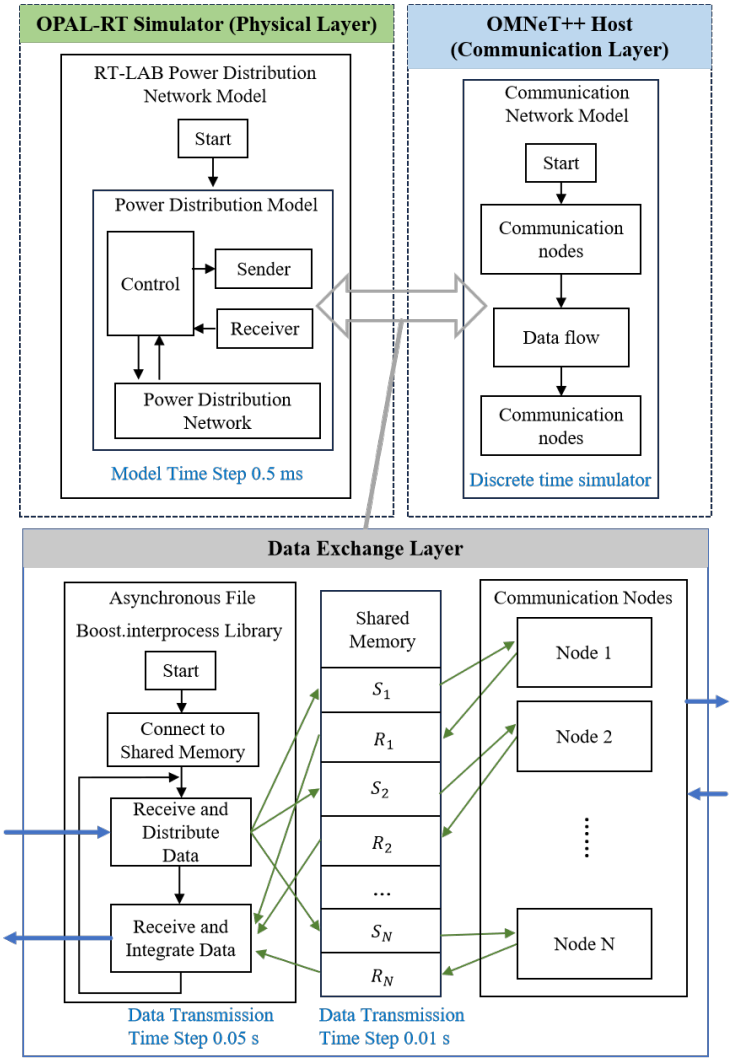


Figure 4.6: Mechanism of shared memory time-stepped synchronisation scheme.

Compared to the conventional time-stepped method [124] and existing shared-memory-based implementations [125], the proposed scheme provides an improved experimental integration framework for cyber–physical digital co-simulation. As shown in Fig. 4.6, at the beginning of each digital co-simulation step, the power distribution network model running in OPAL-RT's RT-LAB computes the electrical states (e.g., bus voltages, branch currents, generator outputs) based on the most recent control and measurement data received from the communication network. These outputs are exchanged with OMNeT++ via the UDP protocol using the sender and receiver in the Ethernet communication interface. The *Boost.Interprocess* function is used in the Asynchronous File in OMNeT++ host to ensure data is received and distributed to the shared memory. The communication network simulation delivers the updated control messages or network status information between nodes and sends back to the power distribution network simulation at the end of the simulation loop. This synchronisation scheme ensures deterministic data exchange and mitigates errors caused by asynchronous event scheduling.

To characterise the timing behaviour of the proposed digital co-simulation platform, key synchronisation and data-exchange metrics are summarised in Table 4.3. Furthermore, cycle-to-cycle synchronisation skew and scheduler-induced jitter are negligible under the fixed-step RealTimeScheduler configuration and are therefore omitted.

Table 4.3: Timing Metrics of the Proposed CPPS Digital Co-Simulation Platform

Metrics	**Value**
Synchronisation step T_s	0.5 s
Data-exchange latency (RTT)	0.156/0.234/0.257 ms (min/avg/max)
Latency jitter (mdev)	0.018 ms
Packet loss rate	0 %
Node-specific communication delay τ_i^{cn}	[0.3, 0.5] s

Monte Carlo samples are generated offline prior to the CPPS digital co-simulation, and each Monte Carlo realisation is executed as an independent digital co-simulation loop. This execution strategy prevents platform-level nondeterministic latency and jitter from accumulating across runs, while time synchronisation within each loop is preserved by the fixed-step synchronisation scheme.

Moreover, fast PV dynamics and physical transients are resolved within the DAE solver of the OPAL-RT power system simulator. Node-specific communication delay and packet losses are handled exclusively at the digital co-simulation boundary as delayed or held inputs applied at fixed synchronisation time-step. As a result, time-step violations between continuous-time and discrete-event simulations can be prevented.

4.5 Co-simulation-based Global Sensitivity Analysis Results

As shown in Fig. 4.7, the proposed CPPS digital co-simulation platform is constructed based on the facilities in the Control and Power Systems laboratory at the University of Sheffield.

In this paper, as mentioned in Section 4.3.1, a total of 119 parameters are considered in the input X, mainly including the voltage and current of the PV units, the load on each bus, and node-specific communication delay. The output Y consists of several system states of the power distribution network. The GSA is conducted using the output Y, and the following section presents key simulation results.

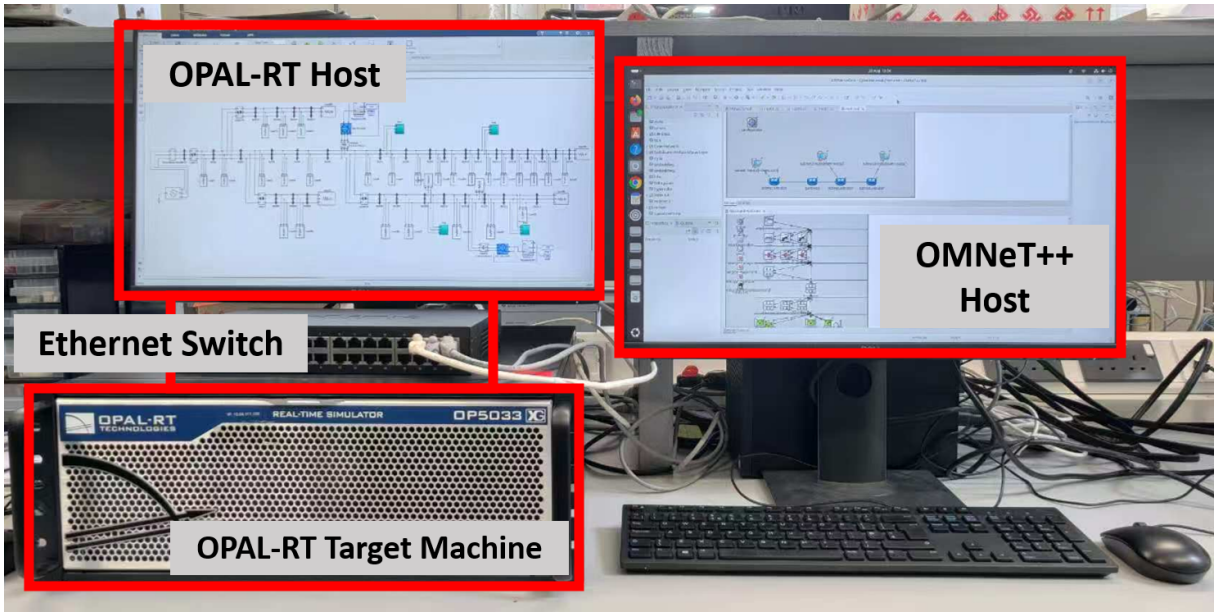
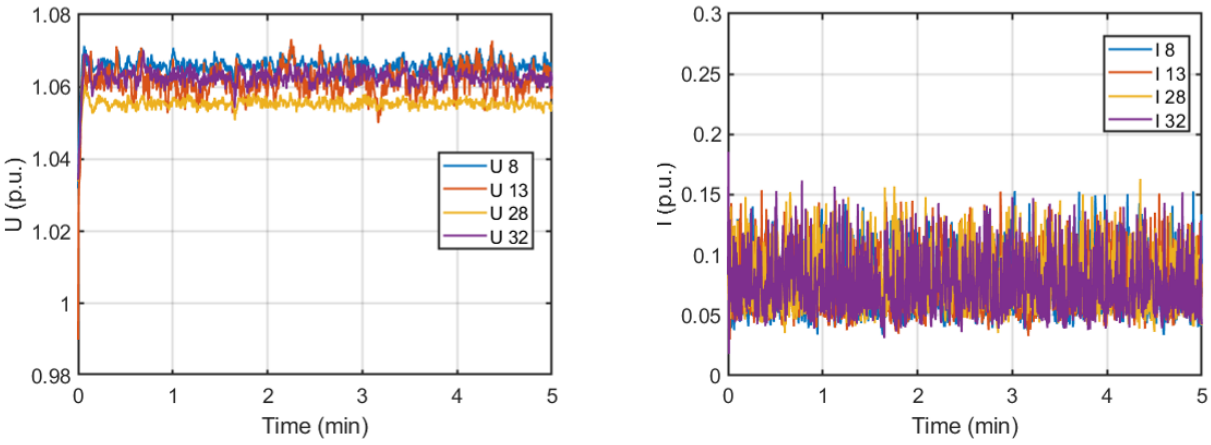


Figure 4.7: Implementation of cyber-physical power systems digital co-simulation platform.

4.5.1 IEEE 33-bus System Normal Operation Results

The CPPS digital co-simulation results of four buses in the IEEE 33-bus power distribution network are presented in Fig. 4.8. The voltage and current of the buses are shown in Fig. 4.8a and Fig. 4.8b, respectively.



(a) Voltage in buses

(b) Current in buses

Figure 4.8: CPPS digital co-simulation results of voltage and current in buses 8, 13, 28 and 32.

The results show that both voltage and current responses of the buses exhibit noticeable fluctuations when the uncertainties are considered in the system. As shown in Fig. 4.8a, the bus voltages stabilise around their nominal values but present continuous oscillations. These oscillations are mainly due to three sources: (i) PV generation variations

due to solar radiation dynamics, (ii) load fluctuations in the power distribution network, and (iii) the effect of node-specific communication delay. The currents in Fig. 4.8b also display noticeable fluctuations under input uncertainties and follow very similar patterns across all four units. The quantified analysis of the sensitivity to the three sources of uncertainties is discussed in the following sections.

4.5.2 Global Sensitivity Analysis Results on Node-specific Communication Delays

The sensitivity of system outputs to node-specific communication delay is analysed in this section, since communication delay is one of the key parameters characterising cyber–physical coupling. The data used for GSA are obtained from the proposed CPPS digital co-simulation platform, including both the sampled input vector and the corresponding output state vector generated from each co-simulation run.

Table 4.4 lists the most and least sensitive output states with respect to node-specific communication delay uncertainties. The purpose of this comparison is to identify which dynamic states are strongly affected by cyber-layer delay uncertainty and which states are mainly governed by local physical dynamics or local control loops.

Table 4.4: Most and Least Sensitive Output States to Node-Specific Communication Delays

Most sensitive output states			
Output Index	Group	Parameter	Sensitivity
3	SG state	Generator speed ω_1	0.862
4	SG state	Generator speed ω_2	0.534
40	PV inverter control	PV4 PWM duty ratio d	0.378
79	Bus voltage U_y	Bus 6 U_y	0.213
72	Bus voltage U_x	Bus 32 U_x	0.210
Least sensitive output states			
Output Index	Group	Parameter	Sensitivity
1	SG state	Generator rotor angle δ_1	0.00000
18	Controller	PV2 reference voltage u_{rd1}	0.00001
11	PV grid current	PV3 grid current i_y	0.00037
20	Controller	PV4 reference voltage u_{rd1}	0.00052
13	Controller	PV1 reference current $i_{d,ref1}$	0.00053

The results in Table 4.4 provide three main insights. First, the synchronous machine

speed states ω_1 and ω_2 present the highest sensitivity values, indicating that node-specific communication delays can significantly influence frequency-related dynamics and electromechanical responses. This suggests that frequency-related states should be prioritised in delay-aware monitoring and cyber–physical control design. Second, selected voltage-related states, such as Bus 6 U_y and Bus 32 U_x, also appear among the most sensitive outputs, showing that communication delay uncertainty can propagate to voltage dynamics through delayed measurement and control interactions. Third, the rotor angle, PV grid currents, and several controller reference signals exhibit very low sensitivity values. This indicates that these states are mainly dominated by local electrical dynamics, fast inverter control loops, and algebraic network constraints rather than delayed communication signals.

Therefore, the sensitivity analysis demonstrates that communication delay uncertainty does not affect all CPPS states uniformly. Instead, its impact is concentrated on frequency-related and selected voltage-related states. This provides a practical basis for identifying communication-sensitive states and for prioritising delay mitigation, communication network design, and cyber–physical control improvement.

Before presenting the cross-scenario comparison, the two scenarios used in Table 4.5 are defined as follows. Scenario A represents the baseline communication-delay uncertainty case. In this scenario, the IEEE 33-bus CPPS model, PV generation condition, load uncertainty setting, communication topology, and Sobol sampling procedure are kept consistent with the previous delay-sensitivity analysis. The node-specific communication delays follow the baseline uncertainty setting defined in Eq. 4.29. Scenario B represents a targeted delay-perturbation case. It uses the same power system model, communication topology, load and PV uncertainty settings, and GSA procedure as Scenario A, but introduces additional communication delays of 0.5 s and 1 s at node 10 and node 24, respectively. This setting is used to emulate local cyber-layer congestion or intentional delay disturbance at selected communication nodes. Therefore, the comparison between Scenario A and Scenario B isolates the impact of targeted communication-delay perturbations on the spatial distribution and robustness of sensitivity characteristics.

To facilitate physical interpretation of the Sobol' sensitivity results, a set of aggregated metrics is introduced to characterise (i) the robustness of dominant delay locations, (ii) the spatial locality of delay impacts, (iii) the relative contribution of delays to different state groups. These metrics are derived directly from the Sobol' indices.

Table 4.5: Cross-scenario comparison of communication-delay sensitivity characteristics

Metric	**Scenario A**	**Scenario B**
Cross-scenario consistency metrics		
Mean Top-5 delay-node overlap	2.19 (maximum = 5)	
Jaccard similarity of Top-5 delay nodes	0.419	
Scenario-specific sensitivity metrics		
Mean voltage locality ratio (U_x)	0.38	6.11
Mean voltage locality ratio (U_y)	0.11	1.99
Delay-energy ratio (current/voltage)	0.014	0.366

Table 4.5 summarises a comparison between two scenarios. The Top-5 delay overlap and the corresponding Jaccard similarity quantify the consistency of the most influential delay nodes across scenarios. The Jaccard similarity measures the degree of overlap between the sets of dominant delay nodes identified under different scenarios, with values closer to one indicating higher consistency. An average overlap of 2.19 and a Jaccard similarity of 0.419 indicate a moderate but non-random robustness of the dominant delay structure under perturbation.

For voltage-related states, the locality ratio provides a direct measure of spatial dominance, where values exceeding unity indicate local influence and values above three imply strong locality. The markedly increased locality ratios observed in Scenario B therefore demonstrate that delay-induced voltage sensitivities become strongly localised when targeted perturbations are applied. By contrast, the delay-energy ratio between current and voltage states remains below 1, confirming that communication delays predominantly affect algebraic voltage states through local measurement and control paths, while current sharing is largely preserved by network impedance constraints and inverter inner-loop regulation.

4.5.3 Global Sensitivity Analysis Results on Solar Radiation

The GSA results in Table 4.6 compare the input sensitivity rankings under two operating scenarios. It should be noted that the ranking principle is identical in both scenarios. For each scenario, the input states are ranked in descending order according to the magnitude of their Sobol sensitivity indices. Therefore, Rank 1 denotes the most influential input state under the corresponding scenario, and a smaller rank value indicates a higher sensitivity contribution. The rank shift is calculated as

$$\Delta\text{Rank} = \text{Rank}_2 - \text{Rank}_1, \tag{4.45}$$

where a negative value means that the input becomes more influential in Scenario 2.

The two scenarios are defined as follows:

- **Scenario 1: Baseline PV and communication-delay condition.** All PV units operate under the baseline solar radiation condition corresponding to 40% solar radiation. The node-specific communication delays are kept at their baseline values without additional delay perturbation.
- **Scenario 2: High-PV and targeted delay-perturbation condition.** The solar radiation level of the PV units is increased from 40% to 90%. In addition, extra communication delays are introduced at selected nodes, with an additional 1 s delay at Bus 24 and an additional 0.5 s delay at Bus 10. This scenario represents a stressed cyber–physical operating condition that combines high PV generation with local cyber-layer congestion or delay disturbance.

Table 4.6: Top-Ranked Input States and Their Rank Shifts Between Different Scenarios

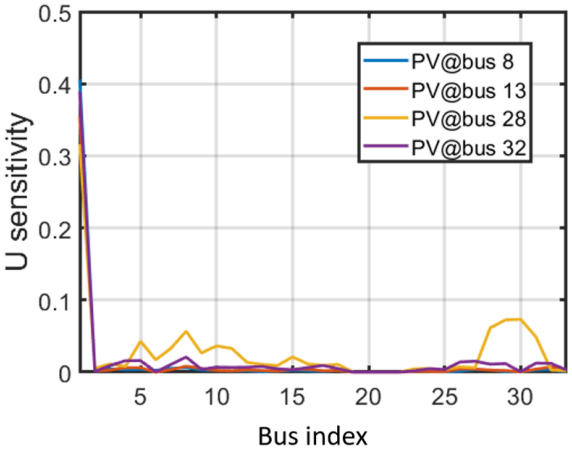
Index	**Type**	**Rank$_1$**	**Rank$_2$**	$\Delta Rank$
9	PV terminal voltage (PV state)	8	1	-7
72	Bus 32 U_x	5	2	-3
13	Controller $i_{d,ref1}$ (PV1)	116	3	-113
15	Controller $i_{d,ref3}$ (PV3)	86	4	-82
14	Controller $i_{d,ref2}$ (PV2)	94	5	-89
16	Controller $i_{d,ref4}$ (PV4)	107	6	-101
90	Communication delay at node 8	17	7	-10

It can be seen that the uncertainty ranking in scenario 1, sensitivity ranking is dominated by electrical and control states on PV units, reflecting the prevalence of local inverter dynamics under moderate and simultaneous penetration. In contrast, the stressed scenario ($Rank_2$) leads to substantial rank shifts, with several less sensitive inputs becoming dominant. In particular, the PV terminal voltage becomes one of the most sensitive variables, indicating heightened sensitivity to local voltage regulation under higher PV generation output. In the power distribution network layer, the voltage component U_x at Bus 32 also becomes highly sensitive, indicating the remote buses are sensitive to the asymmetric power injections. In addition, multiple inverter current reference signals $i_{d,\mathrm{ref}}$ exhibit rank increases, reflecting the increased sensitivities on converter control actions to maintain power balance. Moreover, the rank of communication delay at node 8 rises as well, demonstrating that communication network layer disturbances can significantly affect system dynamics under high PV penetration.

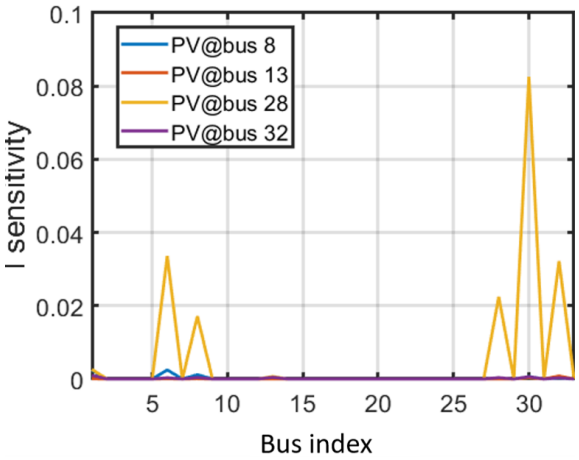
Overall, the results show that sensitivity rankings depend on the system operation conditions. The proposed GSA-based comparison between nominal and stressed scenarios therefore provides an effective assessment of external validity beyond fixed penetration and normal cyber conditions.

4.5.4 Global Sensitivity Analysis Results on Fixed-Time Uncertainties

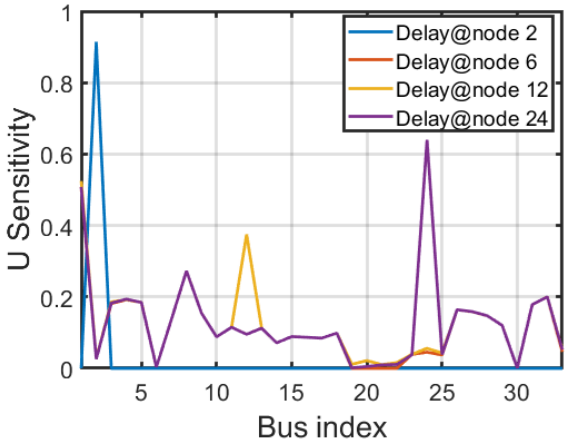
In the following section, typical results of the GSA according to Section 4.3 are reported to quantify the sensitivity contribution of uncertain inputs to the system states of the CPPS.



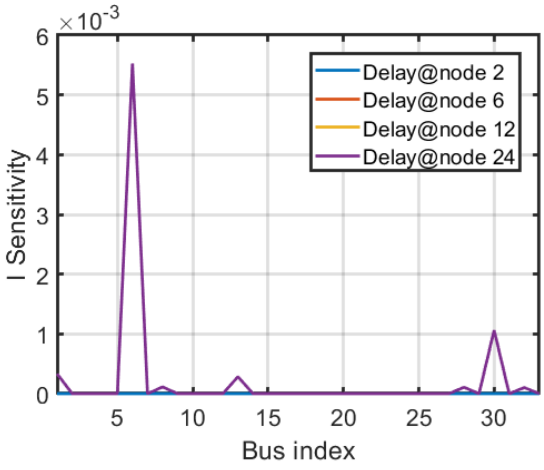
(a) Voltage sensitivity in response to fixed-time PV uncertainty.



(b) Current sensitivity in response to fixed-time PV uncertainty.



(c) Voltage sensitivity in response to fixed-time uncertainty in communication node delays.



(d) Current sensitivity in response to fixed-time uncertainty in communication node delays.

Figure 4.9: Sensitivity analysis on fixed-time uncertainties at the 10th minute of CPPS simulation.

4.5.4.1 Sensitivity Contribution of Uncertain PV Generation

Fig. 4.9a shows that the voltage sensitivity at bus 1 (slack bus) is relatively high (ranging from 0.3 to 0.4) in response to all four uncertain PV units, while the sensitivities at most other buses remain close to zero. This can be explained by the role of the slack bus, which serves as the system reference and balances active and reactive power. Therefore, any uncertainty that leads to PV output variation will be reflected in the voltage sensitivity of the slack bus. In addition, Bus 28 exhibits higher voltage sensitivity because it is a PV connection point and is located at the end of the power distribution network, making its voltage more sensitive to variations in PV generation. These results verify that PV output influences bus voltages both globally, through the slack bus, and locally, near the PV connection points.

Fig. 4.9b illustrates that only the uncertain PV unit located at bus 28 exhibits noticeable contributions to the current sensitivity, particularly at buses 6, 8, 28, 30, and 32, whereas the other PV units show little influence. This is mainly attributed to the control characteristics of the PV inverters. PV units typically operate in a current-controlled mode, directly modulating current injection to track active power references. Since PV unit at bus 28 contributes more significantly to generation at this time (10th minute), its uncertain variations affect the current distribution, and subsequently affect neighbouring generation nodes. This phenomenon indicates that the sensitivity of PV current states is primarily governed by the employed PV control mode, in which active power regulation is achieved through direct current control, rather than by any global reference effect.

The sensitivity of voltages is higher than that of currents. This indicates that the uncertainties of PV generation have a greater impact on bus voltages, while their influence on current distribution is relatively limited. As a result, in the CPPS framework, PV-related uncertainties are expected to play a more critical role in voltage dynamics than in current sensitivity.

4.5.4.2 Sensitivity Contribution of Uncertain Node-Specific Communication Delays

In Fig. 4.9c, at the 10th minute, the communication delay at each node mainly affects the voltage sensitivity of its own bus, while its influence on other buses is limited. For example, the communication delays at nodes 2 and 6, which serve as data transfer nodes in the communication network as shown in Fig. 4.5, do not significantly affect the voltage sensitivities at nodes 12 and 24, even though the latter rely on them to reach the data centre. Similarly, communication delays at nodes 12 and 24 do not affect neighbouring buses through the communication paths. This is because communication delays enter the

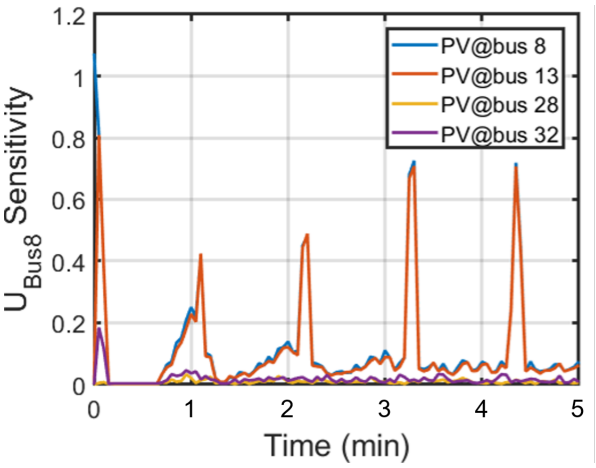
control loop as node-specific measurement or actuation delays, rather than as cumulative hop-by-hop delays along the communication routes. This indicates that the effect of the uncertainty in communication delays on bus voltages is highly localised and is not influenced by the topology of the communication network.

As shown in Fig. 4.9d, the sensitivities of bus currents with respect to communication delays are extremely low, with the maximum value below 5×10^{-3}. This is because PV-injected currents are primarily determined by local measurements and control, such as solar radiation and local voltage feedback in droop or *dq* control. This suggests that communication delays have almost no observable impact on current distribution, while their effects tend to be highly localised at their own delayed nodes. The results highlight that communication delay uncertainties play a more critical role in shaping voltage dynamics than in affecting current flows in the CPPS framework.

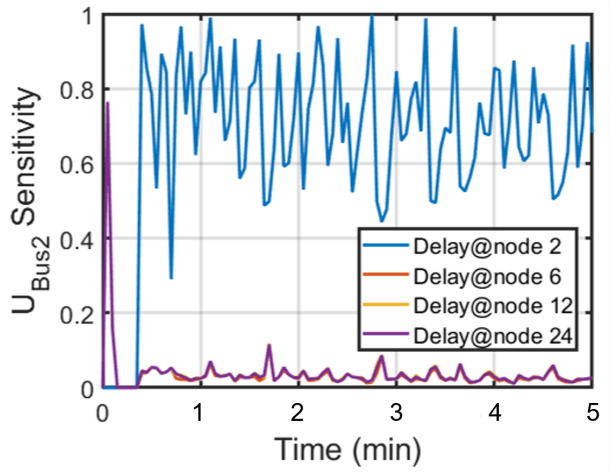
4.5.5 Global Sensitivity Analysis Results on Time-Varying Uncertainties

4.5.5.1 Voltage Sensitivity in Response to Time-Varying Uncertainties of PV Generation

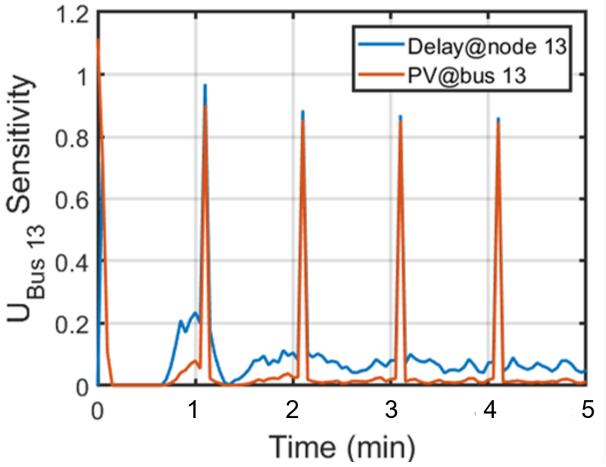
Fig. 4.10a shows the time-varying sensitivity of bus 8 voltage with respect to the four uncertain PV units. It can be observed that PV units at buses 8 and 13 exhibit similar sensitivity variations, while PV units at buses 28 and 32 have negligible impact on bus 8 voltage. This corresponds to the network topology as in Fig. 4.4, since buses 8 and 13 are located on the same power distribution line, resulting in a stronger correlation between their outputs. These results indicate that voltage fluctuations are strongly related to time-varying uncertainties of PV generation outputs only on the same power distribution line, verifying the influences of both local PV units and network topology on voltage control in the power distribution network.



(a) Bus 8 voltage sensitivity in response to time-varying PV generation uncertainties.



(b) Bus 2 voltage sensitivity in response to node-specific communication delay uncertainties.



(c) Joint time-varying uncertainties of PV generation and communication delays.

Figure 4.10: Sensitivity analysis of bus voltages in response to time-varying uncertainties.

4.5.5.2 Voltage Sensitivity in Response to Time-Varying Uncertainties of Communication Delays

Fig. 4.10b illustrates the sensitivity of bus 2 voltage with respect to the communication delays at nodes 2, 6, 12, and 24. The results show that only the delay at node 2 maintains a consistently high influence on the voltage of its own bus, while the other three nodes exhibit little contribution. This indicates that the impact of communication delay is highly localised: the delay of a communication node primarily affects its corresponding power bus.

4.5.5.3 PV Inverter Current Dynamics in Response to Time-Varying Uncertainties of Communication Delays

Fig. 4.11 shows the time-varying sensitivity of PV inverter currents in response to communication delays. For each PV unit, the delay at its locally connected communication node consistently exhibits the highest sensitivity, indicating that inverter current dynamics are most affected by local measurement and communication delays. Moreover, communication delays associated with other PV buses also appear in the dominant delays in the figure. Delays at nodes 8 and 13 are also among the most sensitive variables in inverter currents of PV unit on bus 32. These effects are because delay-induced voltage and current perturbations propagate through network impedances and influence neighbouring inverter operating points. Overall, the results demonstrate that communication delays impact PV inverter current dynamics through a combination of local control-loop variation and network interactions among multiple power system devices.

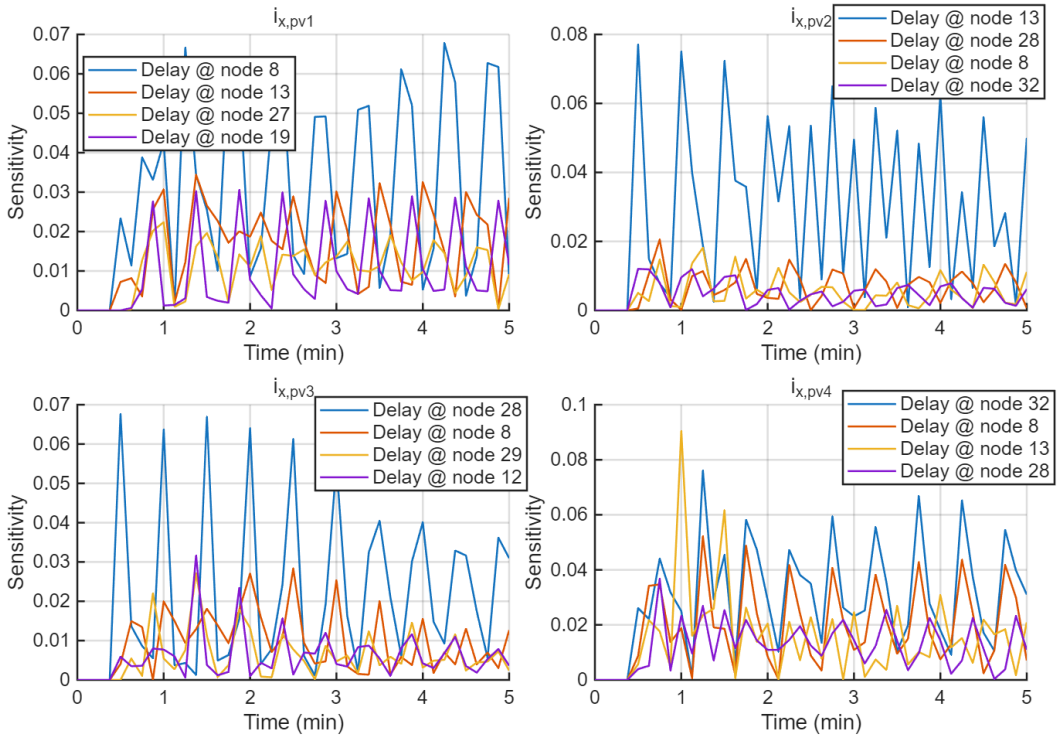


Figure 4.11: Sensitivity analysis of PV inverter currents in response to communication delays.

4.5.5.4 Joint Time-Varying Uncertainties of PV Generation and Communication Delays

Fig. 4.10c compares the sensitivity of bus 13 voltage with respect to the joint uncertainties of PV generation and communication delay located at both bus 13 and node 13. It can be

seen that the effect of communication delay remains higher than that of PV generation throughout the entire CPPS simulation time steps, indicating that communication delay uncertainty plays a more dominant role than local PV uncertainty at the same bus. However, at the time of data exchange in the CPPS synchronisation scheme, the sensitivity contribution of PV generation increases significantly and combines with the effect of communication delay, so that the voltage fluctuations in bus 13 are more determined by the joint influence of local PV generation and communication delay. This demonstrates a significant coupling effect between power and communication uncertainties in the CPPS framework.

4.6 Conclusion

In this paper, a GSA-based method is proposed to investigate the impacts of multiple uncertainties in CPPS with respect to the power distribution network. The uncertainties of load, PV generation, and node-specific communication delays in the CPPS framework are quantified using probabilistic models, and Monte Carlo-based Sobol' indices are used to quantify the sensitivity. A CPPS digital co-simulation platform integrating an OPAL-RT power system simulator and an OMNeT++ communication network simulator is developed using shared memory and a time-stepped synchronisation scheme. The global sensitivity indices on the IEEE 33-bus system show that PV generation has a dominant effect on bus voltages, while communication delays mainly influence local voltage but have a limited impact on bus currents. It is worth noting that communication node delays, as a key parameter of the communication network, present a non-negligible influence on the frequency of the power distribution network.

Future work will focus on the scalability of the proposed GSA framework and a more realistic assessment of delay-induced frequency disturbances. Potential solutions include model order reduction for higher dimensional CPPS framework and hierarchical or staged GSA strategies.

Chapter 5

Cyber-Physical Real-Time Digital Simulation for Microgrid Cybersecurity Analysis

Publications Related to This Chapter

This chapter combines the publications listed as follows:

- **Qiu, D.**, Liu, M., Zhang, R., Luo, T., Griffo, A., and Zhang, X.: Cyber-Physical Real-Time Digital Simulation for Cybersecurity Analysis in Microgrids. *IEEE Transactions on Industrial Cyber-Physical Systems*, vol. 3, pp. 429–441, 2025. doi: 10.1109/TICPS.2025.3569640.
- **Qiu, D.**, Liu, M., and Zhang, X.: Developing Cyber-Physical Power System Co-Simulation Platform with Real-Time Digital Interface. In *Proceedings of the 2025 IEEE Kiel PowerTech*, Kiel, Germany, 2025, pp. 1–6. doi: 10.1109/PowerTech59965.2025.11180418.
- **Qiu, D.**, Liu, M., and Zhang, X.: A Power-Communication Co-Simulation Platform for Real-Time Microgrid Cyber Security Analysis. In *Proceedings of the 2024 International Conference on Artificial Intelligence of Things and Systems (AIoTSys)*, Hangzhou, China, 2024, pp. 1–6. doi: 10.1109/AIoTSys63104.2024.10780642.

Chapter Overview

This chapter presents a series of studies on the development of cyber–physical co-simulation platforms for cybersecurity analysis in microgrids. The research progressed through three stages, which are presented as three publications included in this chapter.

The first study focuses on the development of an initial cyber–physical co-simulation

platform for microgrid cybersecurity analysis. In this work, a Typhoon HIL based microgrid simulator is integrated with the EXata communication network simulator. A master–slave synchronisation scheme is implemented to enable coordinated interaction between the power simulator and the communication network simulator. This platform provides a preliminary environment for analysing cyber–physical interactions in microgrids.

Building upon this initial platform, the second study develops a more scalable cyber–physical co-simulation architecture by integrating the OPAL-RT real-time digital simulator with the EXata communication network simulator. Compared with the Typhoon-based platform, the OPAL-RT system supports larger network sizes and smaller simulation time steps. A dedicated real-time digital interface and improved synchronisation mechanism are designed to enable high-fidelity interaction between power system dynamics and communication network behaviour.

The third study extends the previous developments and presents a unified cyber–physical real-time simulation framework for analysing cybersecurity vulnerabilities in microgrids. The proposed framework integrates power system dynamics and communication network behaviour to enable detailed analysis of cyber attacks such as false data injection(FDI), denial-of-service(DoS) and packet loss contingency.

Together, these three studies demonstrate the progressive development of cyber–physical simulation platforms and their application to cybersecurity analysis in microgrids. To improve readability and clarify the relationship between the three development stages, Table 5.1 summarises their configurations, main functions, advantages, and limitations.

Table 5.1: Summary of the three cyber–physical co-simulation platform-development stages in Chapter 5

Stage	**Platform configuration**	**Synchronisation scheme**	**Main advantages**	**Main limitations**
Stage 1: Initial microgrid platform	Typhoon HIL 602+ and EXata	TCP-based master–slave / leader–follower scheme	High-fidelity power-electronics emulation; simple platform structure; suitable for initial microgrid cybersecurity validation.	Limited scalability; mainly suitable for small-scale microgrids; less flexible for large CPPS models.
Stage 2: Real-time digital interface platform	OPAL-RT OP5033 and EXata	TCP-based time-stepped synchronisation	Larger model capacity; more flexible power-system modelling; improved temporal consistency through fixed-step data exchange.	Performance depends on synchronisation step; additional interface overhead; possible one-step data-exchange latency.
Stage 3: Consolidated cyber-security assessment framework	Typhoon HIL–EXata and OPAL-RT–EXata platforms	Comparison of leader–follower and time-stepped schemes	Supports systematic platform comparison; covers FDI, DoS, packet drop and delay attacks; includes platform performance assessment.	Higher implementation complexity; requires multiple simulator interfaces; optimal configuration depends on the target application.

5.1 A Power-Communication Co-Simulation Platform for Real-Time Microgrid Cyber Security Analysis

The rapid digitalisation process in power system has greatly benefited the large-scale integration of distributed energy resources (DERs), essentially accelerating the progress towards net zero. However, numerous cyber attacks such as false data injection (FDI) attacks are impeding the normal control and operation activities. This paper aims to establish a real-time microgrid co-simulation platform to fully study the impacts of realistic attack events on micorgrid's control performance. Although there exist a large number of power-communication co-simulation platforms for the power system, they are designed to mainly provide validation services for control and operation algorithms and little attention has been paid to the cyber security. In the established microgrid platform, power and communication parts are simulated in Typhoon Hardware-in-the-loop(HIL) 602+ and EXata Network Simulator, respectively, and a dedicated synchronisation scheme is developed and embedded in Raspberry Pis to achieve master-slave data exchange between them. Based on the advanced cyber libraries provided by EXata, realistic FDI and packet drop

attacks are mounted against the mapped communication links within EXata. The results indicate that these cyber attacks can severely influence the microgrid control performance including destabilising system states and specific state deviations, further demonstrating the necessity of deploying effective cyber-resilience enhancement mechanisms.

Step-based description of the platform. The Typhoon HIL–EXata platform is developed through five main steps:

(i) defining the master–slave co-simulation principle;

(ii) implementing the power-electronic microgrid model in Typhoon HIL;

(iii) constructing the corresponding communication network in EXata;

(iv) designing the TCP-based Raspberry Pi synchronisation interface; and

(v) validating the platform under normal operation, false data injection, and packet drop cases.

5.1.1 Introduction

The path to achieving net-zero emissions in the power system involves replacing conventional synchronous generators with distributed energy resources (DERs) such as solar and wind power. Benefiting from the integration of advanced information and communications technology, massive penetrated DERs can be effectively managed and controlled within small-scale microgrids. However, the rapid digitalisation process has also exposed microgrids to the threats of extensive cyber vulnerabilities like false data injection (FDI) and denial-of-service (DoS) attacks, which can severely deteriorate the operation and control performance. In recent years, the frequently reported attack incidents [126, 127] imply that the emerging DERs are gradually attracting the adversary's attention due to their easily-accessed and rapidly-growing characteristics. Furthermore, the growing maturation of machine learning technologies for power grid applications also exposes a wide range of cyber vulnerabilities [128]. Hence, it is important to pay attention to the cyber security issue of microgrids.

The research topics in the microgrid cyber security area can be divided into threat identification, protection deployment, intrusion detection, impact mitigation, and recovery schedule [16], whose validation requires a real-time and high-fidelity platform that possesses both precise power electronic dynamics and concurrent communication network events. Although the one-to-one reproduced full-hardware platform corresponding to industrial scenario can provide the most accurate validation performance, it may be too costly for the laboratory research activities. Meanwhile, the fixed setting of full-hardware platform may hinder the validation studies under various electrical parameters

and power/communication typologies. Considering these facts, the simulation and HIL enabled platforms have received widespread attention due to their well-established trade-off between fidelity and cost and their high flexibility.

There have been numerous mature simulation software and hardware products in the power and communication domains. The power simulation can be divided into steady-state and transient dynamics according to different simulation mechanisms. The former focusses on the models that can be purely described by algebraic equations such as PSCAD, DIgSILENT, etc., and the latter conducts micro electromagnetic transient analysis for distribution systems which contains differential equations, for example, OPAP-RT, Typhoon HIL and so on.

The simulation software for the communication network can be divided into two different categories. One is time-based simulator, such as Cisco Packet Tracer. The time-based simulation has a fixed time step during the simulation. It is commonly used for simulating continuous-time systems or applications that require high temporal precision, such as modelling network traffic variations over time. The other category is discrete-event simulator. Discrete-event simulation updates the system states based on the occurrence of events rather than at fixed time intervals, which makes the simulation highly efficient, as updates are only made in response to events. This allows for rapid handling of sporadic and infrequent events in the simulation process. This kind of simulator includes EXata, OPNET, NS-2, NS-3, etc. In particular, NS-2 and NS-3 are open sourced and have extremely high flexibility, but require heavy development and their interface and visualisation are not very intuitive. On the contrary, EXata and OPNET are commercial products that provide user-friendly GUIs and extensive cyber libraries, while their modelling and analysis flexibility are much more constrained.

In recent decades, a large number of research works have emerged aiming to achieve a co-simulated power system based on off-the-shelf simulation software and hardware. A number of co-simulation platforms that have been introduced. These platforms integrate power simulation software and communication simulation software. Table 5.2 lists some of the co-simulation platforms, their utilities and their components. Firstly, platforms in [61] and [64] focused on real-time simulation and network security, using tools such as OPAL-RT and EXata CPS for applications requiring high fidelity and real-time responsiveness. Secondly, paper [129] focused on microgrid management, utilising power simulators PSCAD and RT-LAB along with network simulators such as OMNeT++ and OPNET. Thirdly, multi-domain system simulations are supported by the platform designed in the [130] and [131], which integrated power simulators Pandapower and MATLAB/Simulink with network simulators PADE and QualNet. Lastly, [132] and [133] focused on transmission systems and protection control, employing power simulators such as PSCAD and DIgSILENT and network simulators like NS-2 and MATLAB to ensure the stability and security of transmission systems.

Table 5.2: Comparison of co-simulation platforms

	Device		
	Applicable Scenario	***Power simulator***	***Network simulator***
[61]	Real-time simulation	OPAL-RT	EXata CPS
[64]	Real-time simulation	OPAL-RT & Typhoon	MATLAB
[129]	Microgrid control	RT-LAB	OPNET
[130]	Multidomain system	Pandapower	PADE
[131]	Multidomain system	MATLAB/Simulink	QualNet
[132]	Protection and control	PSCAD	NS-2
[133]	Transmission system protection	DIgSILENT	MATLAB

However, existing power system co-simulation research mainly focuses on validating the control and operation performance after integrating the power and communication simulations as a whole. While a logical direction to study the impacts of cyber contingencies like cyber attacks using co-simulation method have not been paid enough attentions. Therefore, the main contributions of the paper are as follows:

1. This paper proposes a real-time microgrid co-simulation platform, where the power circuit is simulated in Typhoon HIL 602+, the communication network is implemented in EXata Network Simulator, and a master-slave synchronisation scheme is developed and embedded in Raspberry Pis for the data exchange between power and communication simulation.
2. Based on the advanced cyber libraries provided by EXata, this paper aims to systematically investigate realistic attack events' malicious impacts on microgrid's control performance.
3. Data generated from testing the platform under various attack case studies can provide valuable insights for the analysis of cyber-physical microgrid vulnerabilities.

The rest of this paper is organized as follows: In Section 5.1.2, a brief introduction to the concepts of power and communication simulation is illustrated. In Section 5.1.3, the paper shows the implementation of the proposed platform. The master-slave synchronisation is presented as well. Section 5.1.4 presents and analyses different case studies. Where section 5.1.5 concludes the paper.

5.1.2 Fundamental Knowledge of Power and Communication Simulation

In this section, fundamental concepts for understanding power and communication simulations are provided. Specifically, this section includes an overview of basic theoretical concepts and a description of the typical simulation procedures used in power and communication simulation.

5.1.2.1 Power System Simulation Mechanism

Power systems consist of many complicated individual physical components that perform a variety of tasks related to the power generation, transmission, distribution, storage and consumption. Despite their diverse functionalities and applications, these components are generally described by a set of differential-algebraic equations (DAEs) derived from fundamental physical relations including Kirchhoff laws and Maxwell equations. Depending on the simulation timescale, power system simulations can be divided into three main categories [134]: steady-state, root mean square(RMS) and electromagnetic transients(EMT). In this paper, Typhoon HIL is utilised to simulate the principles of Electromagnetic Transients (EMT), which is fundamentally based on pure differential equation models. EMT simulation involves solving a set of differential equations that describe the rapid changes in physical quantities such as voltage and current within a power system. This method is crucial for accurately modeling and analyzing the system's dynamic behavior over short time periods, especially under transient conditions like short-circuit faults, switching operations, and lightning strikes.

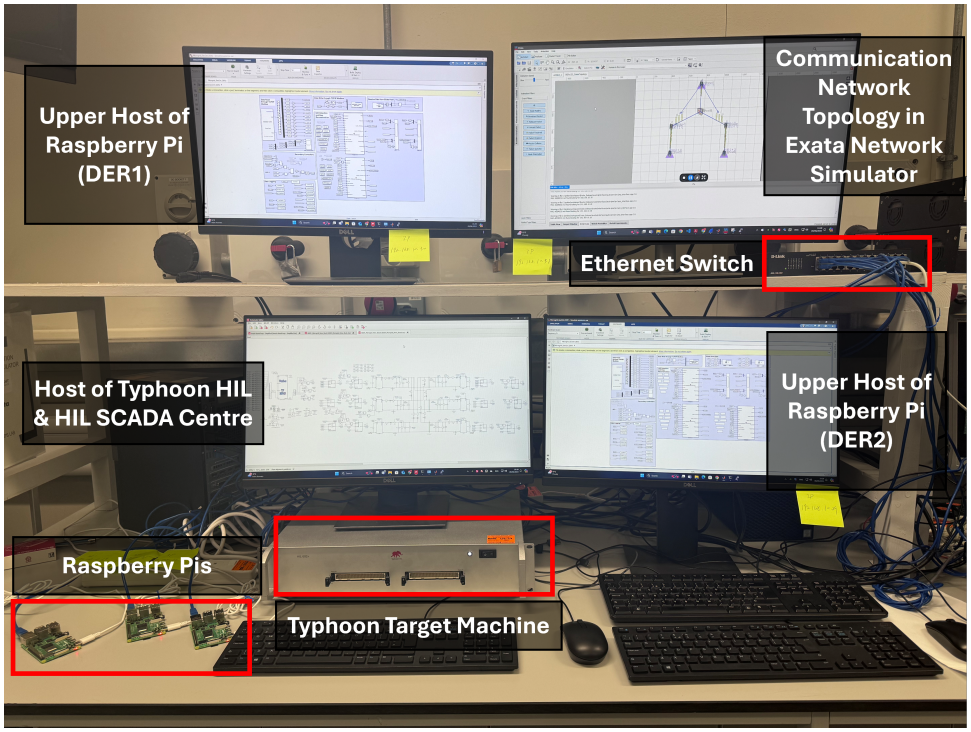
Nevertheless, power system simulation does not always rely on a state-space approach. Commercial tools such as RTDS and EMTP use a modelling approach based on the so-called Dommel algorithm, also known as the Resistive Companion method [135].

5.1.2.2 Communication Network Simulation Mechanism

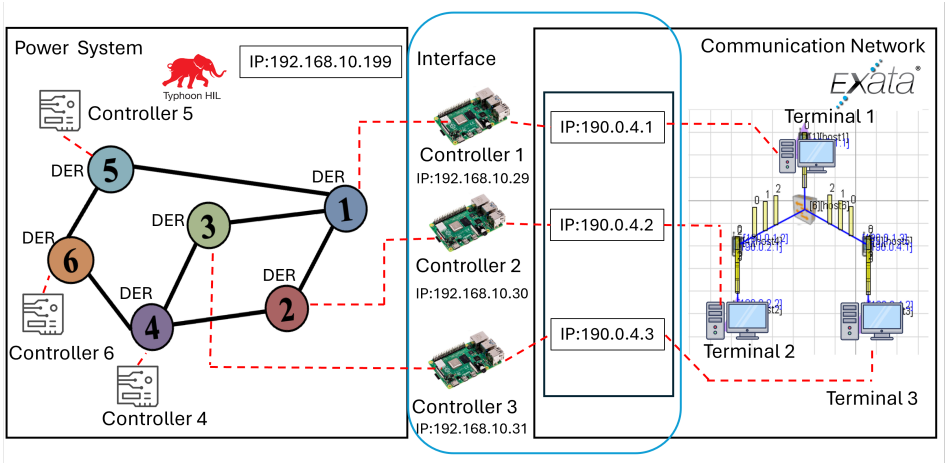
Communication networks are typically packet-switched networks (e.g., IP-based technologies), which can be modelled as discrete-event systems. These systems are characterised by events such as sending and receiving packets and the expiration of timers, occurring at non-uniform intervals. This is distinctly different from the time-stepped approach used in dynamic simulations of the power system, where events are scheduled at fixed intervals. In a communication network simulator, each event is linked with its execution time, and the simulation proceeds by executing events in a specific order of the simulation time. When an event is processed, it may generate zero, one, or several other events. The simulation will stop automatically when there are no further events left in the queue, or when a special "stop" event is triggered [136]. An event scheduler is responsible for maintaining a time-ordered list of all scheduled events, and the simulation time progresses from event to event.

5.1.3 Implementation of Real-Time Microgrid Co-simulation Platform

The implementation details of the real-time microgrid co-simulation platform are elaborated in this section, upon which insightful cyber security analysis will be conducted to evaluate the impacts of communication contingencies like FDI attacks on microgrid control performance. The platform is built based on the facilities in the Control and Power Systems (CAPS) laboratory at University of Sheffield as shown in Fig. 5.1 mainly including the communication simulator EXata version 8.13 and power simulator Typhoon HIL 602+, which will be synchronised by a dedicated interface deployed in Raspberry Pis. In the bottom-left corner, the PC served as Typhoon HIL host and HIL SCADA centre, with Typhoon target machine at the bottom. The PC in the top-right corner serves as the host for EXata, additionally, serving as the upper host for Raspberry Pi 3. The PC in the top-left and bottom-right corner serves as the upper host for Raspberry Pi 1 and 2, respectively. The area in the bottom left is highlighted with a red frame to indicate the Raspberry Pis 1, 2, and 3, which operate as the hardware controllers for DER 1, DER 2, and DER 3 and part of the data exchange interface within this platform. While the rest of the software controllers of DERs are built in the power system simulator. The subsequent part will focus on introducing the two individual simulators and the synchronisation scheme between them.



(a) Real-time co-simulation microgrid platform in CAPS lab at University of Sheffield



(b) Illustration of component connections

Figure 5.1: Design of the real-time microgrid co-simulation platform

5.1.3.1 Power System Simulator

Power system simulation in the platform is performed by the Typhoon HIL simulator [137]. The Typhoon HIL simulator is an advanced tool for real-time simulation of power electronics and power systems. The simulator type adopted in the co-simulation platform is Typhoon HIL 602+, enabling the emulation of up to six converters using a six-core processor with a timestep of 0.5 μs. It supports a microgrid control system simulated at a rate of up to $2MHz$. The Typhoon HIL 602+ allows the construction of power-stage models using a constantly expanding library of power electronics components and

pre-packaged examples. Communication with external units and systems is facilitated through standardised protocols such as IEC 61850, Modbus, DNP3, and OPC UA. These features make the Typhoon HIL 602+ a robust and versatile platform for high-fidelity power electronics emulation and controller testing.

In the Typhoon target machine, apart from the microgrid network, there are several modules that play important roles in the platform. There are N nodes in the power network presenting N DERs. In the power network, there are several components from the model library measure key parameters of each node such as voltage, power, and so on. The data integration module is to collect all data from the measuring components and send them to the next module. The Ethernet data transfer module is Modbus, which remains a request-response protocol implemented using a master-slave scheme. Data in form of numbers, several types of variables and constant can be sent and received by configuring the data sub-menu in the module setting. In our case, the IP address of the Typhoon target machine is set to 192.168.10.199, and the destination IP, which are the Raspberry Pis, are set to 192.168.10.29, 192.168.10.30, and 192.168.10.31, respectively. Using Ethernet data transfer module, the Typhoon target machine and the Raspberry Pis can exchange data in an almost real-time manner. Since the communication network is a discrete-event system, the data exchange frequency is constrained by the communication latency of Modbus protocol based network. Moreover, sampling module is important when data are received from the communication network simulator in Typhoon target machine. This module can change discrete data to the same sampling frequency as the target machine to ensure the normal simulation procedure in power system model. Then, one simulation loop in Typhoon target machine is completed.

5.1.3.2 Communication Network Simulator

For communication simulation, the EXata Network Simulator is chosen to implement the microgrid communication network, as it has advanced cyber libraries for introducing latency, packet dropping, and data modification can be conveniently integrated with external entity via the HIL emulation mode [138]. EXata uses a software virtual network to digitally represent the entire network, various protocol layers and devices, as shown in Fig. 5.2. The EXata protocol stack contains five layers from the top to bottom, i.e., application layer, transport layer, network layer, link (MAC) layer, physical layer.

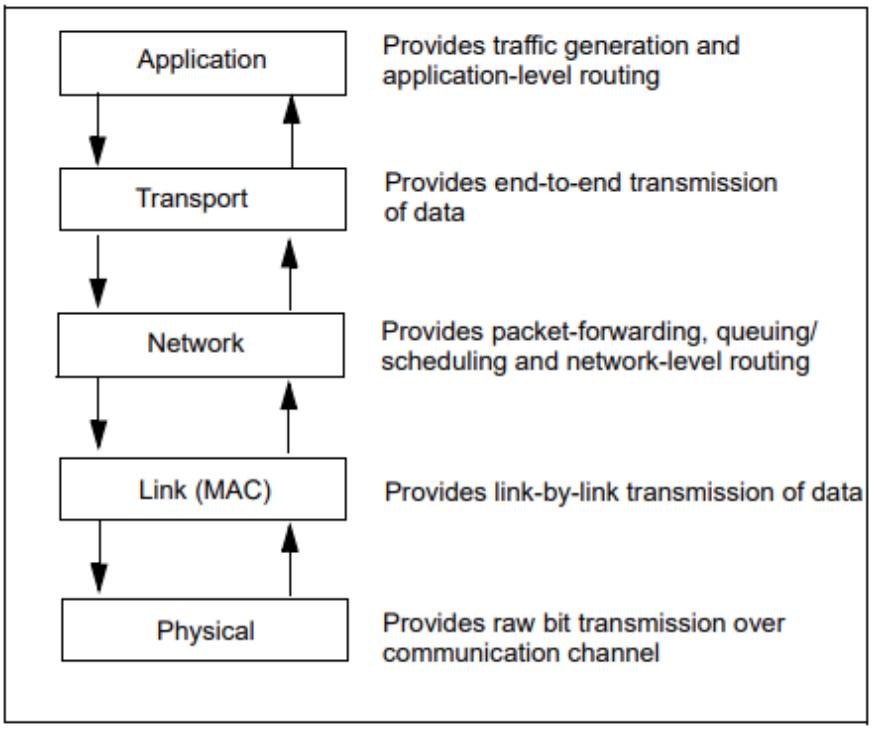


Figure 5.2: Five layers of EXata Network Simulator

Furthermore, the software can be connected to systems with real applications and real target machines. Any virtual node (so-called terminal) in the software can be defined to link with an external entity other than the host machine. The node that connects to another device is called an external node. When the connection is built, all the data packets flowing through the real PC can be found and modified in the EXata GUI. The default path algorithm in EXata for routing data packets is the Bellman-Ford algorithm. The Bellman-Ford algorithm is well-suited for handling graphs with negative weight edges and is capable of detecting negative weight cycles. In EXata, each node in the network initialises its routing table, periodically updates routes through the relaxation process, and forwards packets based on the shortest path estimation. This process ensures efficient data packet transmission and helps maintain network stability. The algorithm's ability to handle negative weights and detect negative cycles makes it ideal for simulating complex, real-world network scenarios.

The communication network is simulated in the EXata host. Compared with the modules in the Typhoon target machine, in EXata there is only one module, which is external node module, before the data are sent to the communication network model. The data of N nodes in power system are sent to the corresponding N virtual nodes in EXata via external node module. After that, within the EXata software, a communication system simulation is conducted. The real data packets are sent to the terminals in the EXata software. After running a communication simulation, the data are sent back to the

interface through the external node module again. Then, one simulation loop in EXata host is finished.

5.1.3.3 Master-slave Power-Communication Synchronisation Scheme

To ensure smooth data exchange between Typhoon and EXata, which is essential for efficient functionality of the platform, this paper designs an Ethernet-based data exchange interface as in Fig. 5.1b. Since the physical simulators are normally based on fixed time step, while the network simulators are discrete-event-driven, synchronisation mechanism between them is the most crucial issue leading to a successful co-simulation platform. The three main synchronisation methods include time-stepped, global event-driven, and master-slave methods. In our case, the Typhoon target machine serves as the primary simulation engine (master), while the EXata plays the role of slave of the master, as the Fig. 5.3 presents. The Raspberry Pis are part of the interface in the master-slave synchronisation procedure, providing data exchange service between master and slaves. The masters control the synchronisation between the slave programs and the data exchange parameters such as time step size and the variables exchanged.

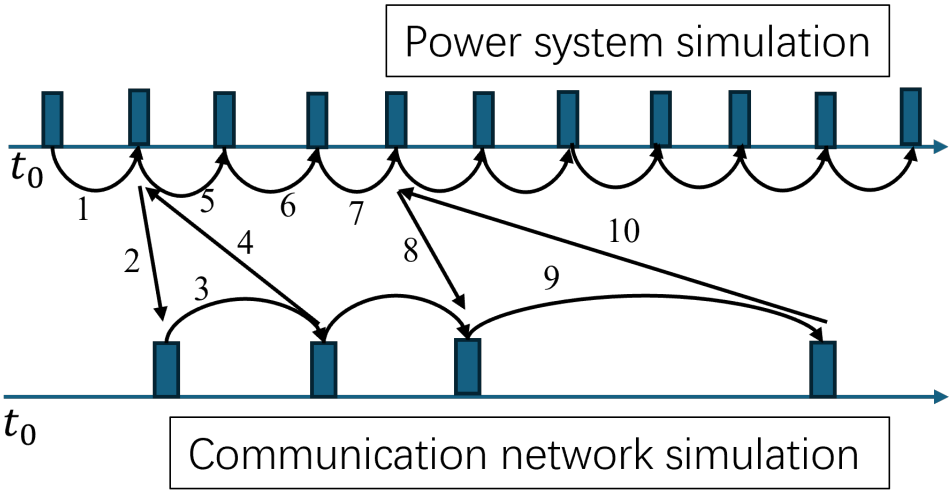


Figure 5.3: Master-slave power-communication synchronisation scheme

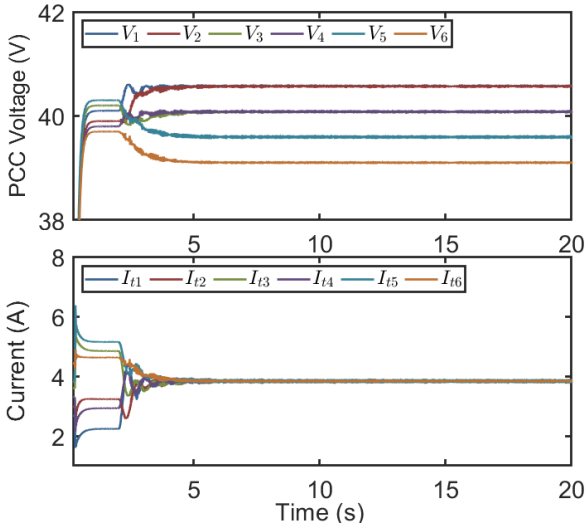
5.1.4 Case Studies and Results

This section demonstrates the cyber security test results based on the established real-time microgrid co-simulation platform, where a 6-DER DC microgrid is established in Typhoon HIL 602+ with the DER electrical parameters obtained from [139]. The communication topology is set to be the same as the electrical topology, and three secondary controllers are embedded into Raspberry Pis, which are mapped into the EXata Network Simulator as external nodes. The data exchange between Typhoon and EXata is the current of DER

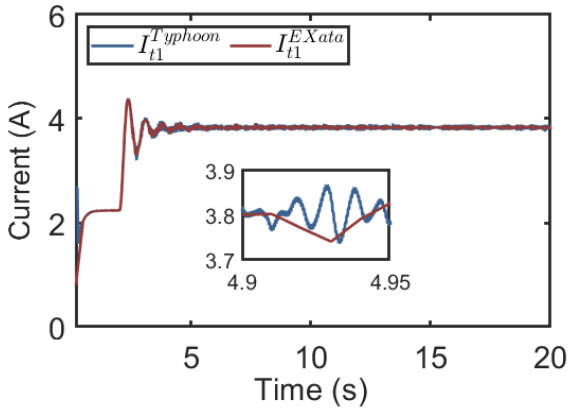
1, 2 and 3 for the secondary control. The HIL SCADA centre monitors and records data from Typhoon machine with sampling rate 40 μs, and the data exchange rate between Raspberry Pis is 10 ms.

5.1.4.1 Case 1: Normal Operation of Microgrid Co-Simulation

Simulation results in this case presents the performance of the co-simulation platform when there is no cyber contingencies. Fig. 5.4a shows the voltage and current measurements from Typhoon HIL under normal system operation. The plot shows the outcome of the Point of Common Coupling (PCC) voltage and the currents for different nodes within the microgrid. The implementation of secondary control on $t = 2$ s to achieves load sharing and voltage stability. The current becomes consistent and the voltage settle into stable states shortly after secondary control is applied, indicating that the control strategy is effective and validate the platform performance in the absence of cyber contingencies. In addition, Fig. 5.4b illustrates a comparison between the current measurements obtained from Typhoon HIL and the corresponding data received from the EXata Network Simulator. The extremely high sampling frequency of Typhoon HIL results in a much smoother data than the data that EXata provides. The comparison varifies the difference between a continuous-time simulator and a discrete-event simulator.



(a) System states in normal condition



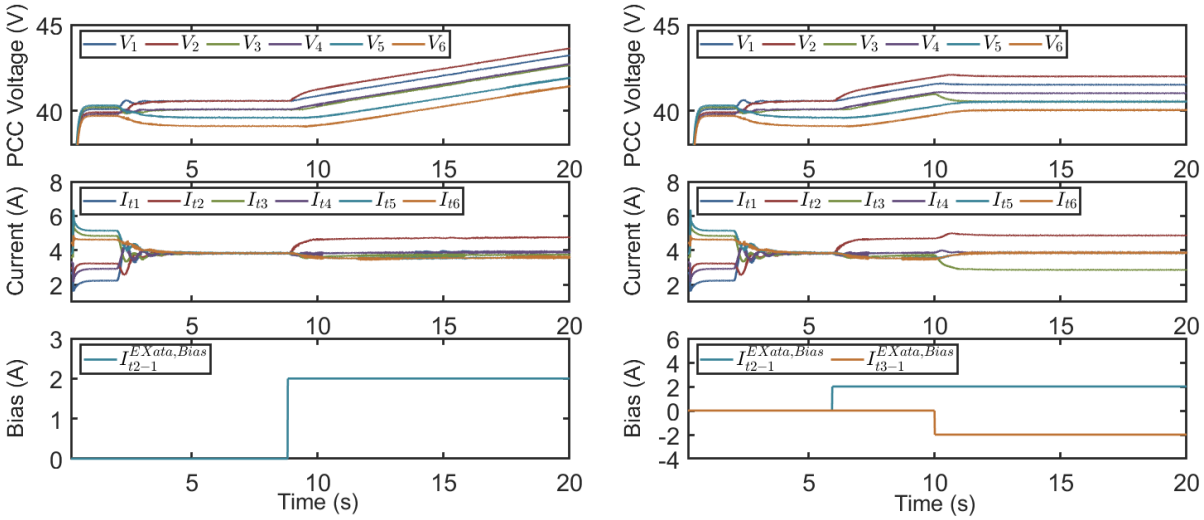
(b) Comparison between the current measurement from Typhoon and that from EXata

Figure 5.4: Simulation results in normal operation

5.1.4.2 Case 2: Single and Multiple FDI Attacks

FDI attacks are applied in the EXata Network simulator. All packets flowing through the attacked nodes will be modified to a certain value (2 or -2) in the byte stream. The byte stream is used to achieve secondary control in the microgrid.

Fig. 5.5a presents the result of single FDI attack injected into the communication link $(2, 1)$. This cyber contingency results in the change of the current in DER 2. The bias of the modified current is 2 A. When the FDI attack is launched when $t = 9s$, the current of I_{t2} increases. Because the attack makes the secondary control cannot achieve current consistency. As a result, the voltages of DERs become unstable and starts to increase simultaneously. Since there is no mitigation or recovery algorithm applied in the system, all voltages will continue to increase until the system breaks down.

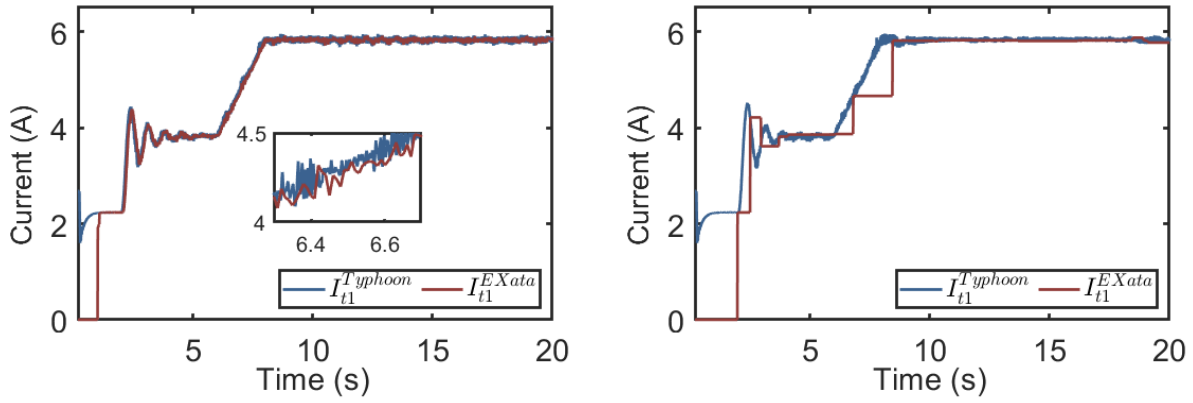


(a) System states under single FDI attack

(b) System states under coordinated FDI attacks

Figure 5.5: Simulation results in the presence of single and coordinated FDI attacks

Fig. 5.5b shows the result of the coordinated FDI attack injected into the links $(2, 1)$ and $(3, 1)$. The attack, in other words, results in the data modification of current in DER 2 and DER 3. The FDI attack on link $(2, 1)$ begins on $t = 6$ s while the attack on link $(3, 1)$ starts when $t = 10$ s. The voltages of the DERs increase from $t = 6$ s and become stable when $t = 10$ s. The reason why voltages become stable eventually rather than destabilise the microgrid is because the injection bias is balanced since the two FDI attacks have the opposite value. However, the secondary control of the current consistency can not be achieved. Due to the FDI attack, I_{t2} starts to increase when $t = 6$ s, while I_{t3} starts to drop when $t = 10$ s.



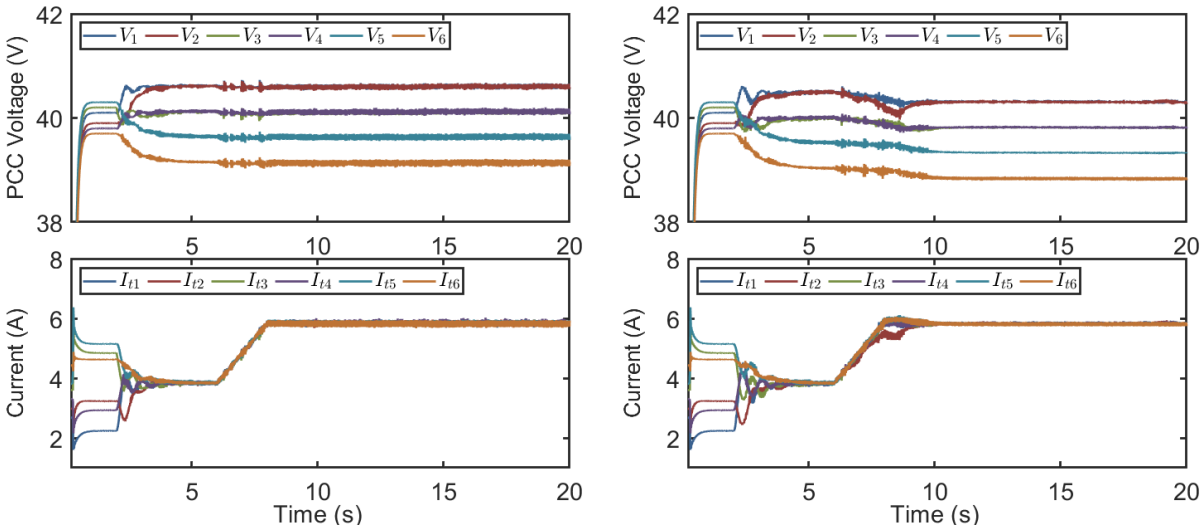
(a) Comparison between the current measurement from Typhoon and that from EXata without packet drop

(b) Comparison between the current measurement from Typhoon and that from EXata under 99% packet drop

Figure 5.6: Simulation results of current in different simulators

5.1.4.3 Case 3: Packet Drop Attack

In this case, we add load variation in the power system so that the effect of link packet drop probability can be seen more intuitively. The packet drop probability of link $(2, 1)$ is set to be 0% and 99%. This setting influences the data flowing between DER 1 and DER 2. The results of different packet drop probability are shown in Fig 5.6 and Fig 5.7, respectively. When there is no packet drop happens, the data distribution in Typhoon and in EXata are very similar, except for the slightly difference between continous-time and discrete-event simulation. When there is 99% probability of packet drop, the data received from EXata becomes abnormal because only 1% of the data packets can be delivered to the power system simulator. It can be seen from Fig 5.6a and Fig 5.7a that when packet drop do not happen in the link, the microgrid can reestablish load sharing with trivial fluctuations on system states. However, in Fig 5.6b and Fig 5.7b, when the packet drop probability is 99%, only 1% of the data are sent from DER 1 to DER 2. Due to the change of the system being significantly slower compared to the frequency of data exchange, even if only 1% of the data packets are successfully received by the Typhoon HIL, the system can ultimately maintain stability. It takes more time for the system to achieve steady states and the fluctuations on both voltages and current are more obvious than the case when no packet drop attack occurs.



(a) System states when packet drop probability is 0%

(b) System states when packet drop probability is 99%

Figure 5.7: System states in Typhoon HIL simulator

5.1.5 Section Conclusion

This paper focuses on power-communication co-simulation, proposes an architecture of real-time microgrid co-simulation platform, and develops a master-slave synchronisation mechanism to transfer data between power and communication simulators. The established platform consists of continuous-time simulator Typhoon HIL and discrete-event simulator EXata. The platform has the ability to co-simulate a microgrid and its communication network in an accurate and real-time manner. Several case studies are conducted to investigate the impacts of FDI attck and packet drop attack based on the EXata's advanced cyber libraries on the emulated microgrid in Typhoon HIL. The results indicate that these cyber contingencies can disrupt system states, causing deviations from the simulation outcomes, and result in abnormal fluctuations on system states. Investigation of appropriate defence strategies such as attack detection, impact mitigation, and cyber recovery is left for future work.

5.2 Developing Cyber-Physical Power System Co-Simulation Platform with Real-Time Digital Interface

The security issue of cyber-physical power systems (CPPS) is becoming increasingly complicated as advanced communication and computing components deployed expose growing vulnerabilities. To simulate, analyse and visualise the CPPS model, this study develops a real-time cyber-physical power system co-simulation platform. The platform uses OPAL-

RT as the power system simulator, with the EXata Network Simulator performing the communication network simulation. A real-time digital interface between the power and communication network simulators is developed, implementing a time-stepped synchronisation scheme for the CPPS co-simulation platform. Extensive case studies are conducted on the established platform to investigate the impacts of false data injection (FDI) attacks and packet drop contingencies on the operation of cyber-physical microgrid. The results demonstrate that these cyber contingencies can disrupt system states, cause deviations from simulation outcomes, and induce abnormal state fluctuations in the CPPS.

Step-based description of the platform. The OPAL-RT–EXata platform is developed through five main steps:

(i) defining the time-stepped co-simulation principle for coordinating continuous-time power system simulation and discrete-event communication network emulation;

(ii) implementing the microgrid or CPPS power system model in OPAL-RT to support real-time digital simulation with improved model scalability;

(iii) constructing the corresponding communication network in EXata to emulate routing, packet transmission, delay, and packet drop behaviours;

(iv) designing the TCP-based real-time digital interface to exchange cyber–physical data at each synchronisation step; and

(v) validating the platform under normal operation, false data injection attacks, and packet drop contingency cases.

5.2.1 Introduction

The digitalisation of the power grid is the key to capture the advantages of the low-carbon energy transition towards the Net Zero target [140], the UK Energy System Operator (ESO) digitalisation strategy [141] and SSE's Net Zero Transition Strategy [142]. Protential benefits for the National Grid ESO and renewable operators include improving system reliability and security, enabling flexible electricity delivery, and facilitating intelligent monitoring and control of renewable assets. CPPS cybersecurity research primarily addresses areas such as threat identification, protective measures, intrusion detection, impact mitigation, and recovery planning [16]. Validation of these aspects requires a high-fidelity real-time platform capable of accurately representing both power system operation and communication network events. Although full hardware platforms deliver exceptional accuracy, they are expensive and lack adaptability to diverse scenarios. Consequently, simulation and hardware-in-the-loop (HIL) platforms are frequently preferred due to their well-balanced combination of fidelity, cost-efficiency, and flexibility.

A range of advanced simulation tools and hardware have been developed for both power and communication systems [143]. Power system simulations are commonly divided into steady-state and transient dynamics, based on the underlying simulation principles. Steady-state simulations focus on algebraic equation-based models, such as PSCAD, whereas transient dynamics simulations emphasise electromagnetic transient analysis using differential equations, with OPAL-RT and Typhoon HIL being notable examples. In addition, some tools, such as DIgSILENT, can perform both steady-state and transient dynamic simulations.

Simulation software for communication networks can generally be divided into two categories. The first category is time-based simulators, such as Cisco Packet Tracer, which operate using fixed time steps. These simulators are particularly useful for modelling continuous-time systems or applications that require precise temporal accuracy, such as tracking changes in network traffic over time. The second category is discrete-event simulators [144], which update system states only when specific events occur, rather than at regular intervals. This makes them highly efficient, as they process updates only when needed, allowing for rapid handling of sporadic or infrequent events. Examples include EXata, OPNET, OMNET++ and NS-3. OMNET++ and NS-3 are open source simulators, offering great flexibility but demanding development effort, and their interfaces and visualisation features are not exactly user-friendly (less polished package). On the other hand, EXata and OPNET are commercial products with intuitive GUIs and rich cyber libraries, but they have less user-defined function to analyse special scenarios.

In recent decades, some research work has been done to develop a co-simulated power system based on off-the-shelf simulation software and hardware. Various co-simulation platforms have been introduced, integrating the power system simulator and communication system simulator. Table 5.3 lists several co-simulation platforms, including their application scenario and their components. The paper [145] focused on real-time simulation, using OPAL-RT and EXata CPS, demonstrating high performance and precision. In the context of microgrid control [129], RT-LAB and OPNET are used, reflecting their suitability for managing decentralised energy systems. For multi-domain system studies in [131], MATLAB/Simulink was paired with QualNet. In paper [146], PSCAD was combined with OPNET, providing tools for analysing distributed power systems. Lastly, in research [147], the platform consists of an RTDS, PMUs and IEDs, and is suitable for co-simulation in transmission network domains.

Table 5.3: Comparison of co-simulation platforms

	Co-simulation Platforms		
	Main Application	***Power Simulator***	***Communication Simulator***
[145]	Real-time Simulation	OPAL-RT	EXata CPS
[129]	Microgrid Control	RT-LAB	OPNET
[131]	Multidomain System	MATLAB/Simulink	QualNet
[146]	Distribution Network	PSCAD	OPNET
[147]	Transmission Network	RTDS	Hardware-in-the-loop

Although much of the existing research on cyber-physical co-simulation emphasises validating the combined control and operational performance of power and communication systems, the examination of cyber contingencies, such as attacks, through co-simulation approaches has not received enough attention. To address this gap, this paper proposes a real-time power system co-simulation platform. The power system is modelled using OPAL-RT OP5033, while the communication network is implemented through the EXata Network Simulator. A time-stepped synchronisation mechanism is integrated via Raspberry Pis to enable smooth data exchange between the two simulations. With the help of EXata's advanced cyber libraries, this study explores the adverse effects of realistic attack scenarios on the power system's control dynamics.

5.2.2 Real-time Cyber-Physical Co-simulation Platform and Implementation Framework

As Fig. 5.8 shows, the established cyber-physical co-simulation platform includes three layers: 1) The Cyber Layer contains the information technology (IT) and operation technology (OT) systems and can simulate various cyber contingencies within these systems; 2) The Interface is to connect the cyber and physical layers, enabling propagation from cyber-attacks to the power system components. Normally, synchronisation schemes are implemented using embedded Python scripts running on Raspberry Pis; 3) The Physical Layer represents the energy conversion and electrical circuit of power system including generators, transformers, etc., which are modelled as electromagnetic transient (EMT) dynamics and solved at microsecond level. The OPAL-RT architecture integrates CPU and FPGA, enabling detailed power electronics models for power system simulations.

The parts are organised following an introduction of the fundamental mechanism of power and communication simulations. Subsequently, the time-stepped co-simulation synchronisation method is presented, alongside a detailed description of the architecture of the platform.

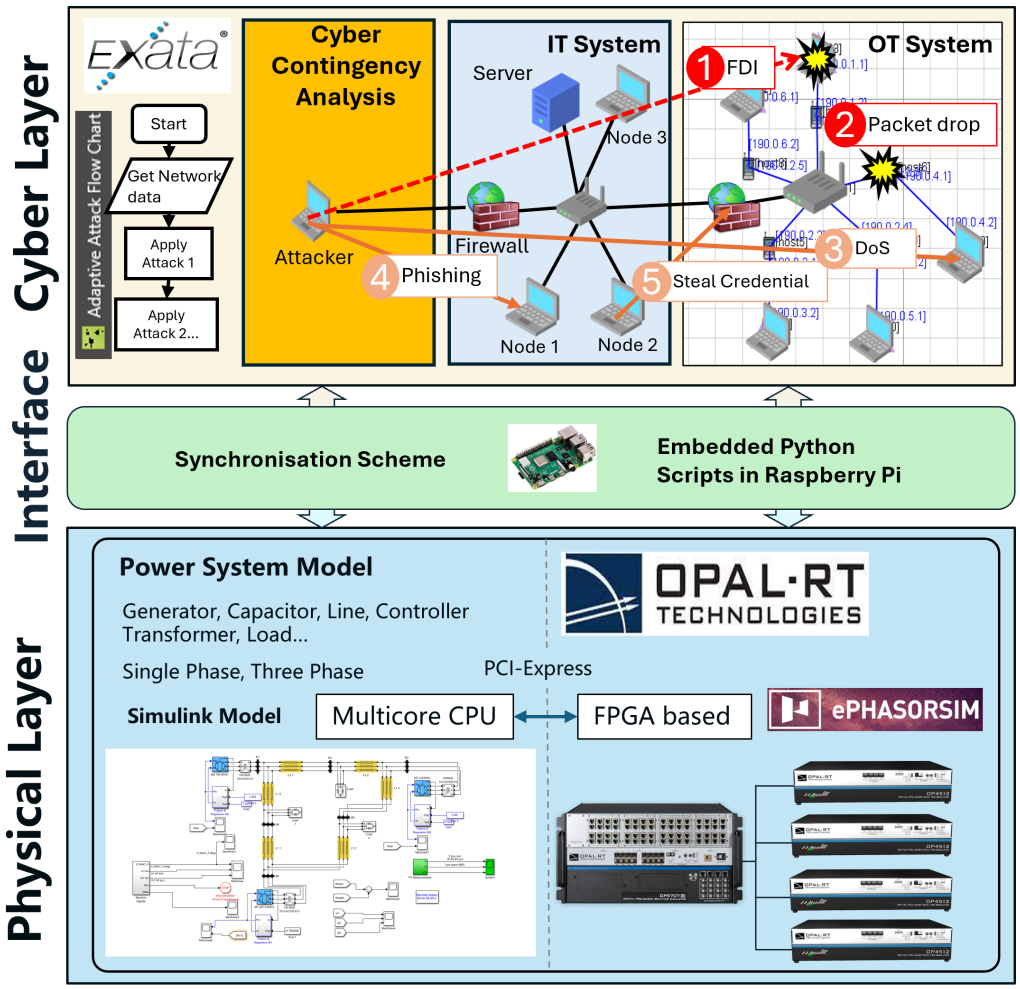


Figure 5.8: Structure of the Real-time Cyber-Physical Co-simulation Platform

5.2.2.1 Simulation Mechanism in Power and Communication Systems

5.2.2.1.1 Power System Simulation Mechanism Power systems consist of numerous complex physical components that perform various functions during the operations of power systems such as power generation, electricity transmission, energy storage, and power consumption. These individual components are generally described by sets of differential-algebraic equations (DAE) derived from fundamental physical principles, such as energy conservation or Maxwell equations. Based on the simulation mechanism, power system simulations can be divided into two categories: steady-state simulation ($\mathbf{f} = \mathbf{f}(\mathbf{x}^o, \mathbf{u})$) and transient dynamics simulation ($\frac{dS}{dt} = F(S, x, t)$).

5.2.2.1.2 Communication Network Simulation Mechanism Communication networks are standard packet-switched networks (e.g. IP-based technologies), which are best modelled as discrete event driven systems. These systems are characterised by events such as sending and receiving packets and the expiration of timers, occurring at irregular

intervals. These operations require an event scheduler to manage the event time list [148].

The state variables of communication components are represented as discrete values, updated during specific discrete events, and selected from discrete sets instead of evolving through a continuous process. Mathematically, the communication system can be expressed using the following equations [6]: Let $\eta \in \Upsilon$ represent the state of the system, where $\Upsilon \subset \mathbb{R}^{n_c}$ is the Euclidean space of the state. The dynamics of η are governed by a difference inclusion with the right-hand side defined by the set-valued map G_C. The input signal is denoted by $\nu \in V \subset \mathbb{R}^{m_c}$, and the system output is $\zeta \in \mathbb{R}^{r_c}$, given by the output function K, which depends on both the state and the input.

$$\eta^+ \in G_C(\nu, \eta), \quad \zeta = K(\nu, \eta). \tag{5.1}$$

In specific cases, setting a limit set D_C for the state values and input to the system is important. Such conditions can be modelled by imposing that ν and η belong to a subset of their state and input space, respectively:

$$(\nu, \eta) \in D_C \subset \Upsilon \times \nu. \tag{5.2}$$

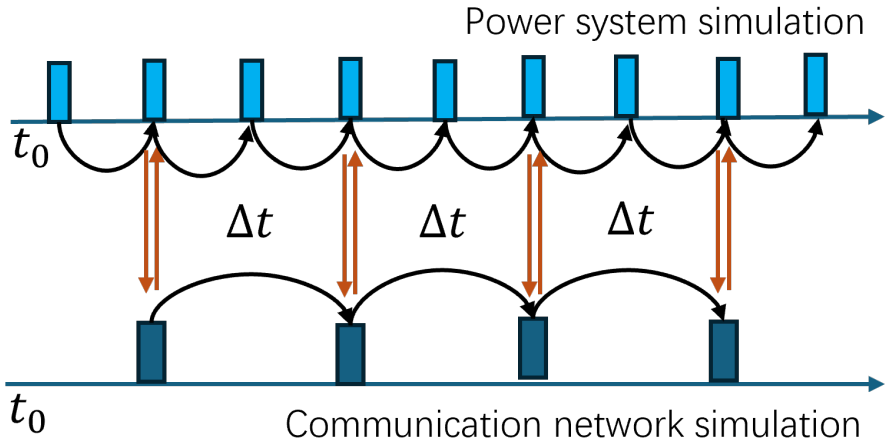


Figure 5.9: Time-stepped Synchronisation Process

5.2.2.2 Time-Stepped Synchronisation Scheme

As the physical system is typically simulated using fixed steps, whereas the communication system is event-driven, synchronisation is critical for co-simulation. There are three types of co-simulation synchronisation method: master-slave, time-stepped, and global event-driven. In our case, to deal with massive data in a short time interval, the time-stepped method is selected as the synchronisation scheme in this study.

The time-stepped synchronisation process, shown in Fig. 5.9, involves two simulators

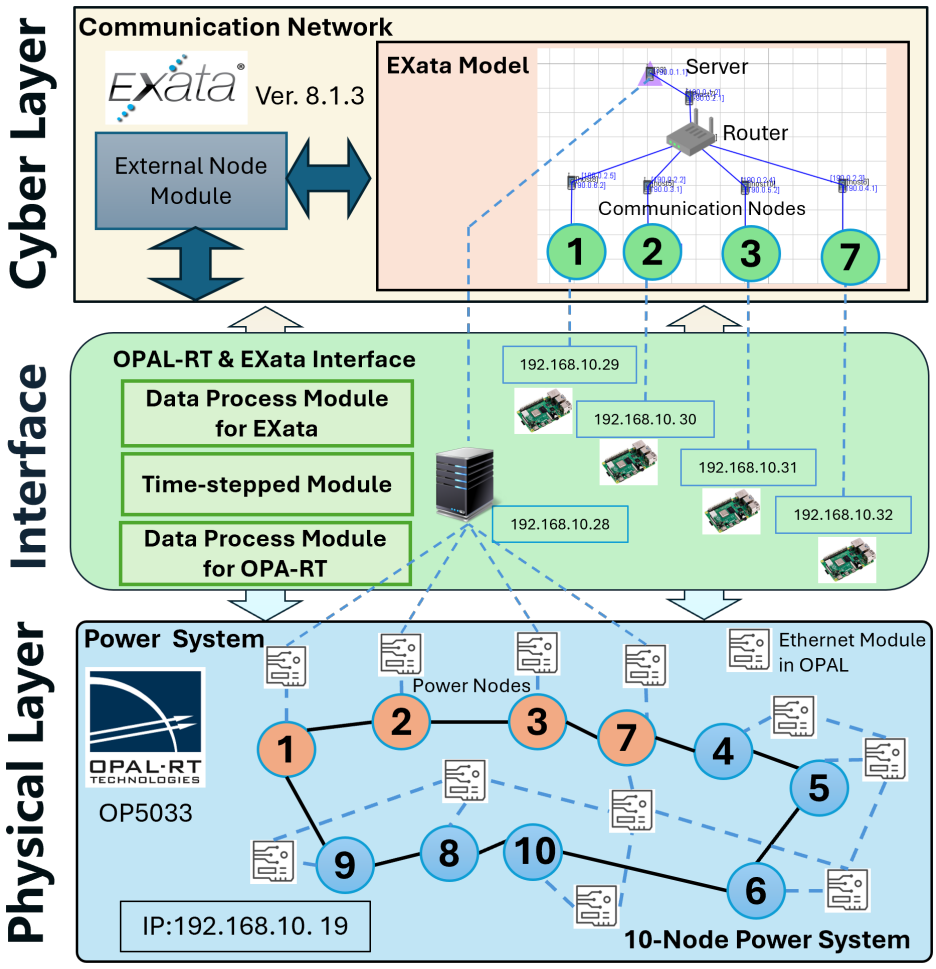


Figure 5.10: Implementation Framework of the Proposed Cyber-Physical Co-Simulation Power System Platform

operating independently. These simulators pause at fixed intervals Δt to exchange data based on a predefined synchronisation frequency. This approach is necessary because the synchronisation time intervals vary between the two simulators. If an event requires data exchange, the data must be saved in a cache until the next synchronisation point. Consequently, this method is unsuitable for time-sensitive applications requiring rapid data exchange. To address this limitation, a data exchange interface is necessary to manage data effectively.

5.2.2.3 Implementation Framework of Co-simulation Platform

The implementation framework of the proposed cyber-physical co-simulation platform is shown in Fig. 5.10. The platform synchronisation scheme that integrates OPAL-RT and EXata is time-stepped. The platform is designed with the ring topology for an isolated 10-node power system. Four adjacent nodes form a communication network in EXata.

The other six nodes exchange the data directly in OPAL-RT rather than in EXata. The modules in OPAL-RT includes the Data Integration Module, Ethernet Data Transfer Module, and Data Distribution Module. In the Ethernet Data Transfer Module, data are packed and unpacked before being sent or received by the power system simulator. This communication is conducted through several Ethernet ports to make sure each node has its own communication port on the OPAL-RT. The function of the External Node Module is to link external devices to the virtual IPs in EXata.

Algorithm 1: Real-time Time-stepped Synchronisation Algorithm

Input: Starting time t_{now}, time step Δt, delay threshold σ
Data: Pending Event List (PEL) for Pending Events

Initialize:
Set t_{now} as the starting time;
Define time-step Δt and threshold σ;
Initialize PEL for each PE;

PEL Generation:
for *new event* **do**
    Record t_p (pending event time);
    if $t_p > t_{now}$ **then**
        Add event to PEL;

Time-Stepping Loop:
while *simulation is running* **do**
    $t_{\text{now}} \leftarrow t_{\text{now}} + \Delta t$;
    for *event in PEL* **do**
        if $t_p \leq t_{now}$ **then**
            Execute and remove from PEL;
        else if $t_p < t_{now} - \sigma$ **then**
            Discard and remove from PEL;

On the OPAL-RT and EXata platform, a time-stepped synchronisation method is used to exchange data between two simulators. Different from traditional time-stepped methods, this study implements a real-time time-stepped algorithm with expired event discarding, as detailed in Algorithm 1. The algorithm is embedded in the Time-stepped Module as shown in Fig. 5.10. Discarding expired events prevents the system from processing events that are invalidated after exceeding σ, therefore avoiding meaningless calculations, saving resources, thus improving the efficiency of event scheduling and querying, and ensuring real-time synchronisation.

OPAL-RT and the Data Transfer Centre have IP addresses 192.168.10.19 and 192.168.10.28, respectively, as shown in Fig 5.10. The OPAL-RT transfers the data to the data trans-

fer centre via UDP protocol. After that, the data from four nodes are distributed and sent separately to the virtual IPs in EXata via TCP/IP protocol. The key to achieving real-time performance in the proposed co-simulation platform lies in the ability of the power and communication simulation systems to operate in real time or faster than real time. RT-LAB is a real-time simulation system capable of accurately simulating a specified number of power nodes in real time. Similarly, EXata, an event-driven simulation software, can perform tasks in real time within a certain range of event frequencies. The frequency limitation of the platform arises from the data processing speed of the Python host and the data transmission speed within the physical network.

5.2.3 Case Studies and Results Discussion

This section demonstrates the cybersecurity case studies and results based on the established CPPS co-simulation platform. The platform is constructed based on the facilities in the Control and Power Systems (CAPS) laboratory at the University of Sheffield, as shown in Fig. 5.11. At the bottom of the figure there is an OP5033 simulator, with the Raspberry Pis on top. The PC on the left serves as a data transfer centre, while the PC on the right serves as an RT-Lab host. The upper left monitor presents the RT-Lab and the monitor in the upper right is the EXata Network Simulator. All equipments are connected under the same subnet via an Ethernet switch. The proposed platform can conduct co-simulation in several scenarios, such as transmission and distribution networks and microgrids.

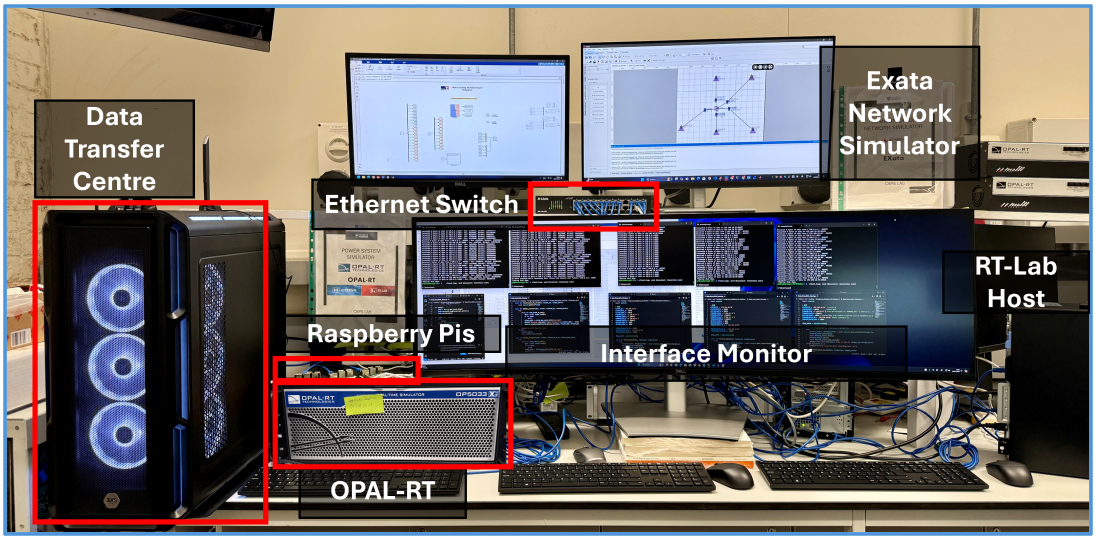


Figure 5.11: The Established OPAL-RT OP5033 & EXata Network Simulator Platform in CAPS lab at the University of Sheffield

As shown in Fig. 5.10, the test system used in this section is a 10-node DC microgrid with a ring-type electrical topology. The detailed electrical parameters of the DER units,

lines, loads, and controllers are adopted from the benchmark DC microgrid reported in [139]. Since these parameters have been fully reported in the original reference, this section focuses on how the test system is implemented and coupled within the proposed OPAL-RT–EXata real-time co-simulation platform.

In the proposed configuration, the 10-node power-system model is embedded in the OPAL-RT OP5033 simulator. Four adjacent nodes are selected and mapped into EXata as external communication nodes to emulate cyber-layer data exchange through the designed real-time digital interface. The remaining six nodes exchange data internally within OPAL-RT. Therefore, the test system used in this case study consists of a 10-node ring-type electrical microgrid and a four-node external communication network coupled through the OPAL-RT–EXata interface. To conduct further investigation of the platform and its cybersecurity capabilities, we select microgrid as the scenario, with several case studies and results presented in the following content: *Case 1:* Normal State, *Case 2:* FDI Attack, *Case 3:* Packet Drop Contingency

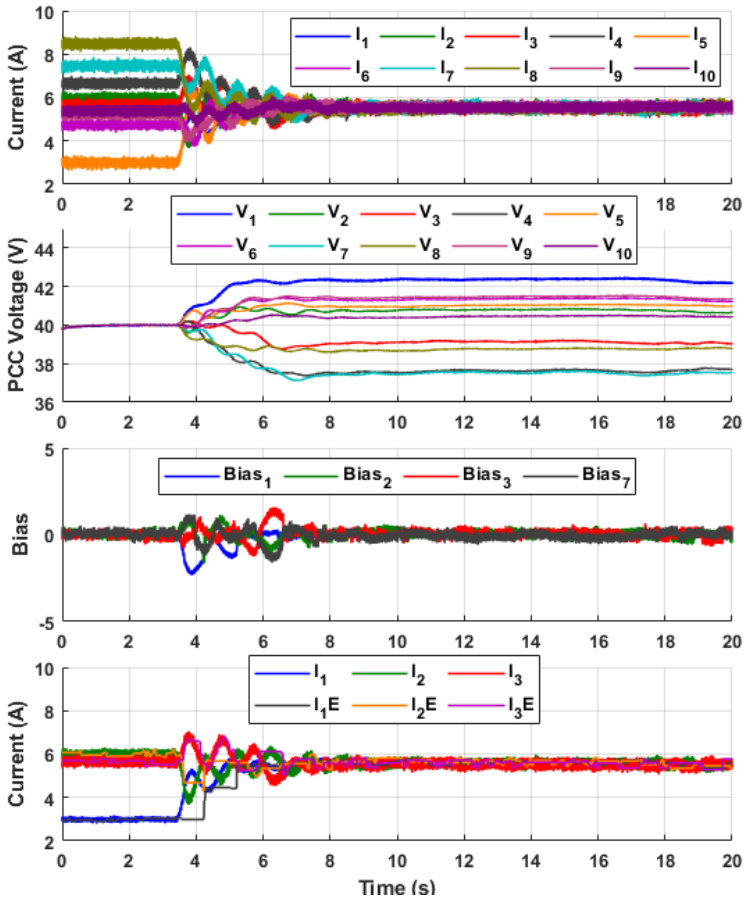


Figure 5.12: Normal State of the Microgrid in the Established Platform

Before presenting the case studies, the microgrid test system is clarified by referring to the implementation framework and topology mapping shown in Fig. 5.10. The case study

is based on a 10-node DC microgrid with a ring-type electrical topology, and the detailed electrical parameters of the DER units, lines, loads, and controllers are adopted from the benchmark system reported in [139]. In the proposed OPAL-RT–EXata co-simulation configuration, the 10-node power-system model is embedded in OPAL-RT OP5033. Four adjacent nodes are mapped into EXata as external communication nodes for cyber-layer data exchange, while the remaining six nodes exchange data internally within OPAL-RT. Therefore, Fig. 5.10 illustrates not only the implementation framework of the platform, but also the topology mapping between the 10-node microgrid and the four-node external communication network used in the following case studies.

5.2.3.1 Case 1: Normal State

Fig. 5.12 presents the results of the microgrid states conducted on the established platform with no contingencies. Specifically, the top two figures display the current and Point of Common Coupling (PCC) voltage of a 10-node power system obtained in OPAL-RT, respectively. Under primary and secondary control, the power system achieves a stable state with load sharing. The bias shows the data comparison between cyber and physical data. Once the secondary control becomes active, the bias begins to fluctuate until the secondary control procedure is finished. This behaviour arises due to data variations caused by the delay between the two systems. Furthermore, as each node operates with an independent data transition link, the bias fluctuates differently across nodes, reflecting the variations in their respective delays. The last figure in Fig. 5.12 can validate the results.

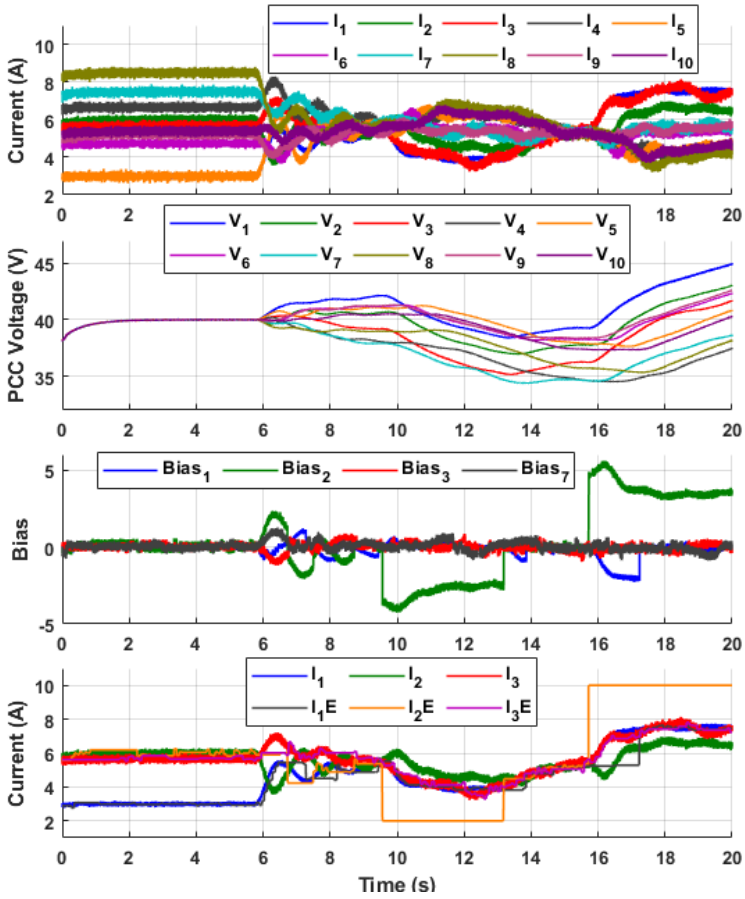


Figure 5.13: FDI Attack Results of the CPPS in the Established Platform

5.2.3.2 Case 2: FDI Attack

Fig. 5.13 shows the results of the FDI attacks injected into Node 2. The first attack on node 2 occurs from $t = 9.5s$ to $t = 11s$ with false data $I = 2A$. The second attack on the same node starts when $t = 15.8s$ and ends when $t = 20s$ with false data $I = 10A$. The two attacks have different value offsets. During the first attack, received data are lower than measured data, causing a voltage decrease across all nodes and disrupting load sharing. In contrast, the second attack leads to a voltage increase. Both attacks can affect the load sharing and voltage stability. However, there is a short stable state between two attacks, which demonstrates that, if the attack is not severe, and its duration is not long enough, the system is capable of returning to a stable state after an attack.

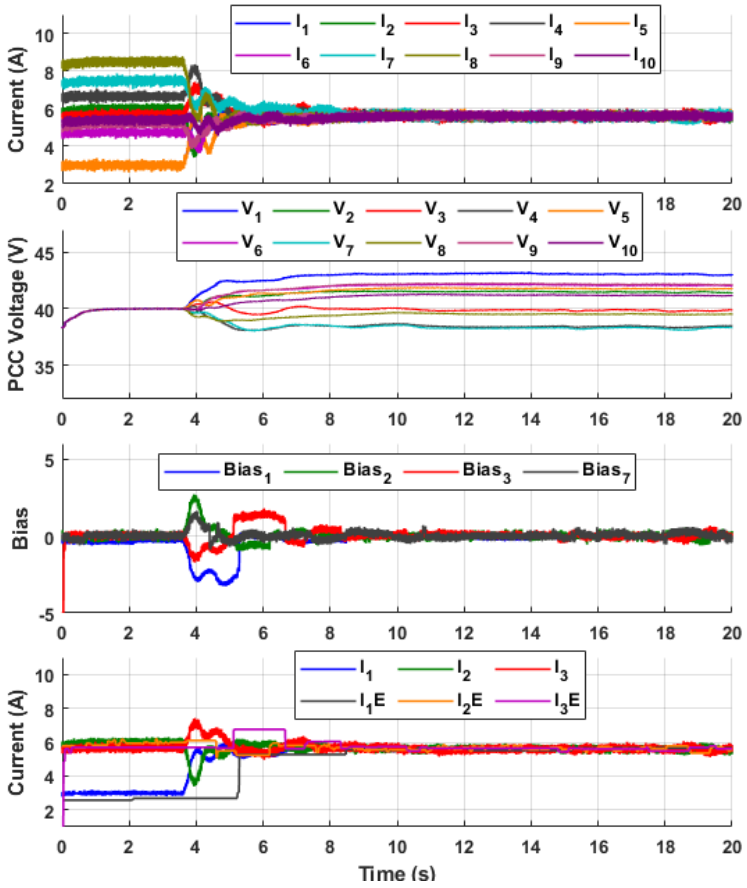


Figure 5.14: Packet Drop Contingency when the Drop Rate is under 50%

5.2.3.3 Case 3: Packet Drop Contingency

The occurrence of packet drops can have several causes, including jamming attacks and man-in-the-middle attacks. In this study, we design two different packet drop rates to observe how such attacks impact the CPPS. The packet drop contingency occurs on communication lines 1, 3, and 7. The result presented in Fig. 5.14 is when lines 1, 3, and 7 have 10% 20% and 30% packet drop rates, respectively. Fig. 5.15 shows the result when the corresponding drop rate increases to 60%, 70% and 80%.

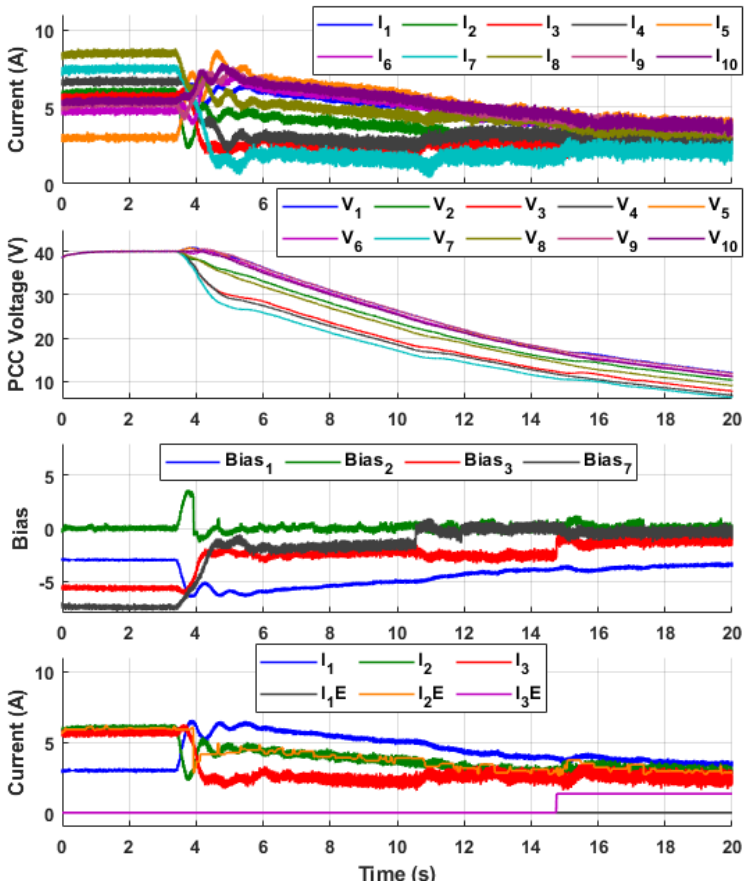


Figure 5.15: Packet Drop Contingency when the Drop Rate is over 50%

As observed in Fig. 5.14, lower packet drop rates (under 50%) have minimal impact on the system. This is due to the short duration of the secondary control, where few data packets are sufficient to stabilise the load. Fig. 5.15 shows that when the drop rate increases, the successful transmission of normal data becomes challenging. Even if some data packets can be transmitted, the inability to deliver the majority of data severely impacts the system, leading to a continuous decline in both current and voltage.

5.2.4 Section Conclusion

This study focusses on cyber-physical co-simulation ,and introduces a real-time CPPS co-simulation platform. It develops a time-stepped synchronisation method to transfer data packets between power and communication simulators. The established platform integrates the continuous-time simulator OPAL-RT OP5033 and discrete-event simulator EXata Network Simulator 8.1.3, enabling real-time co-simulation of a power system and its communication network. Multiple case studies are carried out to examine the effects of FDI attack and packet drop contingency based on the EXata's advanced cyber libraries on the microgrid as an example in OPAL-RT. The results indicate that these cyber con-

tingencies can disrupt system states, causing deviations from the simulation outcomes, and trigger abnormal fluctuations in system states. Investigation of defence strategies and mitigation methods will be required for future research.

5.3 Cyber-Physical Real-Time Digital Simulation for Cybersecurity Analysis in Microgrids

The rapid power grid digitalisation is increasingly addressing the importance of a real-time and high-fidelity cyber-physical co-simulation platform, which enables risk-free validation before the real-world implementation, especially for the cybersecurity research. Existing related works mainly focus on the impact analysis of attacks in massive power grid scenarios, while a thorough investigation regarding the implementation framework, cybersecurity analysis, and suitability assessment is lacking. Towards this end, we first propose a general implementation framework for real-time leader-follower and time-stepped co-simulation schemes, which are used to establish two cyber-physical co-simulation platforms based on off-the-shelf power and communication simulators. Then, thorough cybersecurity studies are conducted to showcase the relations between co-simulation configurations such as the communication network topology and attack compatibility. Finally, a set of metrics derived from synchronisation computational overhead, latency, simulation scalability, and attack compatibility is presented to assess the suitability of a co-simulation platform for cybersecurity research. Recommendations are given to provide guidelines for industry practitioners and academia researchers in the establishment of cyber-physical co-simulation platforms that drive cybersecurity advancements.

Step-based description of the framework. The consolidated cybersecurity assessment framework is developed through five main steps:

(i) defining the overall real-time cyber–physical co-simulation principle for microgrid cybersecurity analysis;

(ii) establishing two representative platform configurations, namely the Typhoon HIL–EXata platform with leader–follower synchronisation and the OPAL-RT–EXata platform with time-stepped synchronisation;

(iii) implementing representative cyber-attack modules in the communication layer, including false data injection, denial-of-service, packet drop, and delay attacks;

(iv) validating the two platforms under normal operation and multiple cyber-attack scenarios to analyse their impacts on microgrid dynamic behaviour; and

(v) comparing the platforms using assessment metrics related to synchronisation

performance, latency, scalability, and cyber-attack compatibility.

5.3.1 Introduction

Power grid digitalisation is the key to capture the benefits of the low carbon energy transition towards the Net Zero target. Potential benefits for the National Grid ESO [149] and renewable operator [150] include reliable, secure system operation, flexible electricity delivery, as well as intelligent renewable asset monitoring and control. Benefiting from the widespread integration of advanced information and communication technologies (ICT), massively penetrated DERs can be effectively managed and controlled by regional microgrids.

However, the rapid digitalisation process has also exposed microgrids to the threats of extensive cyber vulnerabilities such as phishing emails and supply chain issues [151], which can severely deteriorate the operation and control performance, leading to hazardous consequences. In 2021, REvil attacked the US renewable energy company and caused data leakage and in 2022, the Ukraine power grid was hacked by Sandworm and led to power substation interruption [16]. The frequently reported attack incidents in recent years imply that the growing DERs are gradually attracting the adversary's attention due to their easily-accessed and rapidly-growing characteristics. Hence, the cybersecurity of microgrids has attracted significant attention from both industry and academic communities.

Microgrid cybersecurity and cyber-physical system (CPS) security are closely interconnected and share significant overlaps in principles and challenges [152]. They both aim to safeguard critical infrastructure from cyber threats, ensuring stable operations and preventing physical damage, such as power outages or equipment failure. They rely on cyber-physical co-simulation platforms to model attack scenarios and evaluate system resilience. Additionally, both systems are vulnerable to common threats such as False Data Injection (FDI) and Denial-of-Service (DoS) attacks, which compromise data integrity and availability, ultimately impacting the operation of the physical systems. However, notable differences exist. Microgrids are small-scale, distributed power systems primarily focused on energy management, emphasizing real-time resilience in power control and load balancing, where cyberattacks may directly lead to instability or outages [153]. In contrast, CPSs span broader domains such as transportation, healthcare, and industrial automation, featuring more complex architectures and diverse, domain-specific security requirements.

Research interests in cybersecurity can be divided into threat identification [154], protection deployment [155], intrusion detection [156, 157], impact mitigation [158], and recovery schedule [159], all of which require a high fidelity and real-time validation plat-

form that can address the electrical circuit dynamics, communication network events, and cyber-physical interlink [160]. Additionally, several AI-based methods provide alternative cybersecurity solutions, including intrusion detection based on deep reinforcement learning [161] and threat mitigation through machine learning [162]. In contrast to model-based methods, AI-based approaches are capable of adapting to evolving conditions within the power grid. However, they require a substantial dataset for prior training and may not react promptly to the events not included in the training dataset.

The advancement of information technology (IT) and operation technology (OT) has led to advanced tools for simulating power systems and communication networks. Power simulations are divided into steady-state (e.g. MATPOWER) and transient dynamics (e.g. Typhoon HIL, OPAL-RT), focusing on algebraic and differential models. Notably, some tools such as DIgSILENT, PowerWorld and PSCAD can perform both types of simulations.

Simulation software for communication networks includes two categories: 1) Time-based simulators, e.g. Cisco Packet Tracer, use fixed time steps for continuous systems requiring high temporal precision, such as modelling network traffic variations; 2) Discrete-event simulators, such as EXata, OPNET, OMNeT++, and NS-3, update states based on events, enhancing efficiency by responding only to occurrences, making them ideal for sporadic events. OMNeT++ and NS-3 are open-source and highly flexible but require significant development and have less intuitive interfaces. In contrast, EXata and OPNET, as commercial tools, offer user-friendly GUIs and extensive libraries but are less customisable. Moreover, software-defined networking (SDN) introduces a paradigm shift by decoupling the control plane from the data plane, enabling centralised and programmable network management through a standardised protocol such as OpenFlow [163]. This architecture is highly relevant to co-simulation platforms, which integrate multiple simulation tools to model complex cyber-physical systems. Within such platforms, SDN can effectively function as the communication network simulator.

Despite the remarkable achievement in simulating either power systems or communication networks, the efficient orchestration of these simulators to accurately account for the cyber-physical characteristics of microgrids while guaranteeing their real-time control and operation performance still remains a huge challenge. For example, delays in control signals can directly lead to system instability. Furthermore, power systems face various cybersecurity threats that may occur in hybrid attacks, such as simultaneous delay and data tampering attacks. In addition, the resilience of cyber-physical power systems (CPPS) needs to be paid special attention.

Towards this end, various cyber-physical co-simulation platforms have been introduced based on off-the-shelf power and communication simulators for diverse application scenarios as shown in TABLE 5.4. Platforms established in [64, 130, 164] integrated the simulators of power system and communication network for validating the performance

Table 5.4: Comparison between the Established Platforms and Existing Related Ones

	Simulator		***Scenario & Application***	***Implemented Capability***			
Platform	**Power System**	**Comm. Network**		**Comm. Scale**	**Synchronisation Scheme**	**Cyber Contingency**	**Suitability Assessment**
[64]	OPAL-RT & Typhoon	Real network	IEEE 9-bus system, Frequency control	OT	Not mentioned	None	None
[130]	Pandapower	PADE	Distribution network, Transactive system	OT	Not mentioned	None	None
[164]	Typhoon /OpenDSS	Typhoon SCADA	Distribution network, Reactive power control	OT	Not mentioned	None	None
[165]	RTDS /DIgSILENT	QualNet	IEEE 39-bus system, SDN Network	OT	Not mentioned	DoS	None
[61]	OPAL-RT	EXata CPS	Microgrid, Attack impact analysis	OT	Not mentioned	Delay, FDI	None
[129]	RT-LAB	OPNET	Microgrid control	OT	Time-stepped	Link congestion, Link failure	None
[65]	RTDS and OPAL-RT	EXata	New York State power grid, STATCOM control	IT, OT	Not mentioned	Phishing email, Credential steal, DoS, MITM	None
Proposed	**Typhoon and OPAL-RT**	**EXata**	**Microgrid control (Scalable to distribution/transmission systems)**	**IT, OT**	**Time-stepped, Leader-follower**	**FDI, DoS, Packet drop, Phishing email, Credential steal**	**Synchronisation accuracy and latency, Simulation scalability, and Attack compatibility metrics**

of emergency frequency control, transactive energy system, and reactive power control in distribution and transmission networks. Nevertheless, the issue of cyber contingencies is not investigated within these cyber-physical power system platforms. More recently, cyber contingencies such as the link congestion/failure, man-in-the-middle (MITM) attack, FDI attack, and denial-of-service (DoS) attack were taken into account in the establishment of cyber-physical grid platforms and their impacts on the control and operational performance have been extensively validated [61,65,129]. Zhang *et al.* used virtual links for the cyber-physical data synchronisation, which can be conveniently accomplished within one single machine, but might lead to high computation overhead as the machine core needs to handle both cyber and physical simulation events. Moreover, the process of penetration and propagation from the IT network to the OT network, exploiting phishing email and credential stealing, was integrated into the simulation based on extensive cyber library of EXata [65].

However, research gaps still exist in detailing the implementation framework of real-time cyber-physical co-simulation schemes. These aspects are elaborated as follows: 1) Although numerous research works have been devoted to applying cyber-physical co-simulation platforms to massive scenarios such as frequency control and adaptive attacks [166], there still lacks a universal implementation framework for real-time co-simulation schemes on top of off-the-shelf power and communication simulators that can provide useful guidelines for industry practitioners and academic researchers. 2) More attention needs to be paid to network security issues. Existing literature lacks an in-depth analysis of the relationship between co-simulation configurations, such as the impact of different network topologies and the compatibility for various attacks [5]. 3) A set of metrics that can comprehensively assess the suitability of a cyber-physical co-simulation platform for cybersecurity related research is missing. The lack of useful metrics makes it difficult to select suitable experimental platforms for various requirements. 4) The complex structure of power systems necessitates a co-simulation platform that is both scalable and adaptable. For cybersecurity verification, the platform must be capable of simulating diverse attack scenarios across various power system configurations to assess their potential impacts. 5) Moreover, the challenge of simulating realistic IT and OT network environments is crucial as it usually involves numerous prototype and industrial-proprietary communication protocols. These protocols can impact real-time simulation, because different protocols lead to various data transmission latency.

To fill these research gaps, this paper provides an implementation framework and conducts a thorough analysis to reveal the intrinsic links between real-time co-simulation and cybersecurity analysis. The main contributions of the paper are as follows:

- We propose a general implementation framework for real-time leader-follower and time-stepped co-simulation schemes on microgrids. It can be conveniently integrated into embedding devices such as Raspberry Pis and thus has great scalability.

- A data exchange interface is developed within the co-simulation framework using Python scripts to improve computational efficiency and ensure smooth, easy-to-implement data transfer.
- By conducting thorough cybersecurity studies in two established platforms, which vary in co-simulation schemes and power simulators, the intrinsic links between the network topology configuration and attack compatibility are revealed for the first time.
- We develop a set of metrics spanning computational overhead, latency, simulation scalability, and attack compatibility to assess the suitability of a cyber-physical co-simulation platform for cybersecurity research.

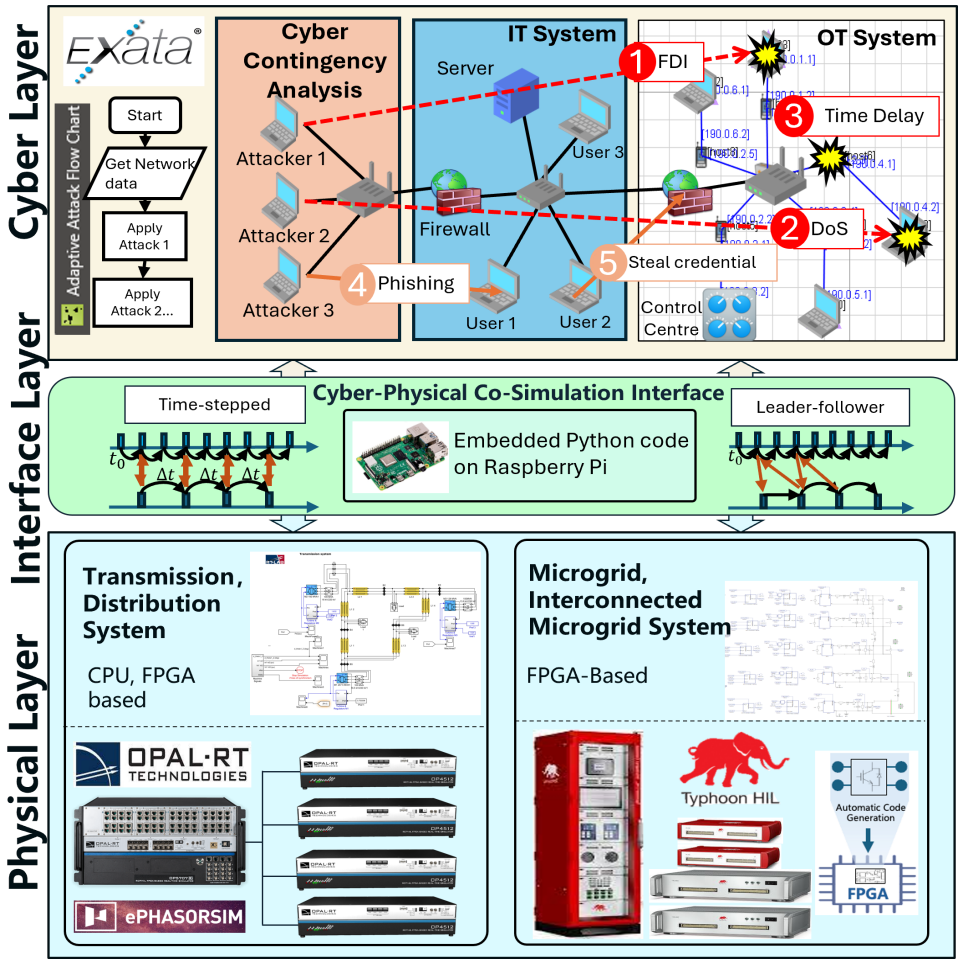


Figure 5.16: Real-time Cyber-Physical Co-Simulation Architecture

5.3.2 Real-time Cyber-Physical Co-simulation Platform, Synchronisation Schemes and Assessment Metrics

As presented in Fig. 5.16, the proposed cyber-physical co-simulation platform consists of three distinct layers: 1) The Cyber Layer, which includes the IT and OT systems and simulates massive cyber attacks targeting these systems, such as FDI, DoS, etc. 2) The Interface Layer, which connects the cyber and physical layers, facilitating the propagation of cyber-attacks to power system components, with data synchronisation schemes such as time-stepped and leader-follower implemented through embedded Python scripts running on Raspberry Pis; 3) The Physical Layer, which models the power generation and electrical circuits of the power systems as electromagnetic transient (EMT) dynamics, resolved at the microsecond time scale. The OPAL-RT platform is suitable for simulating transmission and distribution networks. By leveraging parallel computing to connect multiple OPAL-RT units, computational efficiency can be enhanced, providing a robust solution for addressing co-simulation challenges in large-scale networks. The Typhoon HIL offers cost-effective performance for microgrid-level simulations. Interconnected microgrids can be simulated by adding multiple gateways and setting up configurations in the Raspberry Pis.

The following parts are organised following a brief description of power and communication simulations, and then special attention is paid to the co-simulation schemes, as well as assessment metrics.

5.3.2.1 Simulation Mechanism in Power and Communication Systems

5.3.2.1.1 Power System Simulation : Power systems consist of many complicated individual physical devices that have different functions including generation, transmission, distribution, storage, and consumption of energy. These individual devices are generally described by sets of differential-algebraic equations (DAEs) derived from fundamental physical laws such as energy conservation or Maxwell's equations. Based on the simulation mechanism, power system simulations can be divided into two categories [134]: steady-state simulation ($\mathbf{f} = \mathbf{f}(\mathbf{x}^o, \mathbf{u})$) and transient dynamics simulation ($\frac{dS}{dt} = F(S, x, t)$).

Power system simulation in the platform is performed by two simulators, and one of them is the Typhoon HIL 602+ which is an advanced FPGA-based tool for real-time simulation of power electronics and power systems. The other power system simulator is the OPAL-RT OP5600 real-time simulator which is an integrated simulation system containing a high-performance target computer, a reconfigurable FPGA, and signal processing for up to 256 I/Os. Based on the hardware performance of these devices, they are capable of accurately capturing the microsecond level power electronics dynamics of microgrids.

The microgrids with DERs, measurement components, and control modules are built in the power system simulators. The primary controller of the microgrid is implemented based on local measurements, while the secondary controller proceeds based on the data received from the cyber layer [167]. The primary controller is responsible for local voltage regulation and the input $u_{V,i}$ follows

$$u_{V,i} = K_V \int \Delta V_i \, dt = K_V \int (V_o - V_i) \, dt \tag{5.3}$$

where ΔV_i denotes the voltage tracking error and K_V is the control gain that determines the speed of voltage tracking. After receiving the neighbouring DERs' data from the cyber layer, the nominal reference voltage V_o is adjusted by the consensus-based secondary control input $u_{I,i}$, i.e.,

$$V_o = V_o + u_{I,i} = V_o + K_I \int_{j \in \mathcal{N}_i} (I_j - I_i) \, dt \tag{5.4}$$

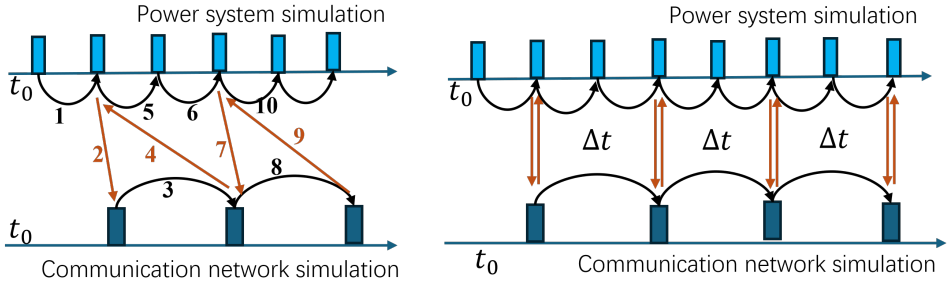
where K_I is the control gain and $\mathcal{N}_i$ signifies the cyber neighbouring set of DER i.

5.3.2.1.2 Communication Network Simulation : Communication networks are packet-switched networks (e.g., TCP/IP, VoIP, and Cellular technologies), which are best modelled as discrete event systems. The state variables of communication components are updated during specific events and are defined over discrete sets, rather than derived from a continuous process. Mathematically, the communication system can be described as follows [6]. Let $\eta \in \Upsilon$ represent the system state, where $\Upsilon \subset \mathbb{R}^{n_c}$ is the Euclidean space of the state. The dynamics of η are governed by a difference inclusion with the right-hand side defined by the set-valued map G_C. The input signal is denoted by $\nu \in V \subset \mathbb{R}^{m_c}$, and the system output is $\zeta \in \mathbb{R}^{r_c}$, given by the output function K, which depends on both the state and the input.

$$\eta^+ \in G_C(\nu, \eta), \quad \zeta = K(\nu, \eta). \tag{5.5}$$

The EXata Network Simulator is a discrete-event network simulator designed by Keysight Company, using a virtual software network to digitally represent the entire network, various protocol layers, and devices in OT and IT systems. The software can be connected to systems with real applications and real target machines such as the Typhoon HIL and OPAL-RT simulators. The routing algorithm in EXata for the simulation of communication networks is the Bellman-Ford algorithm, which is as follows: firstly, set the distance to each vertex m as

$$\text{distance}[m] = \begin{cases} 0 & \text{if } m = s, \\ \infty & \text{if } m \neq s, \end{cases} \tag{5.6}$$



(a) Leader-follower Synchronisation (b) Time-stepped Synchronisation

Figure 5.17: Two Co-simulation Synchronisation Schemes

where s is the source vertex. After that, initialize the predecessor of each vertex m to be

$$\text{predecessor}[m] = \text{null}. \tag{5.7}$$

After that, for each edge (u, m) with weight $w(u, m)$, update the distance and predecessor as follows:

$$\text{distance}[m] = \min(\text{distance}[m], \text{distance}[u] + w(u, m)). \tag{5.8}$$

If a shorter path is found, then update the predecessor:

$$\text{predecessor}[m] = u. \tag{5.9}$$

In EXata, each node in the network initialises its routing table, periodically updates routes through the relaxation process, and forwards packets based on the algorithm. This process ensures efficient data packet transmission and helps maintain network stability. To align with the cyber-physical co-simulation theme of this paper, the validation results are presented with the focus on FDI and DoS attacks in the OT domain. Interested readers in the implementation of phishing email and credential stealing are referred to [65].

5.3.2.2 Co-Simulation Synchronisation Schemes

The physical system is normally regarded as a continuous-time system and simulated in fixed time steps, while the communication system operates in an event-driven manner. To connect these two systems, leader-follower, time-stepped, and global event-driven methods [168] are commonly used, among which the first two types are paid special attention due to the real-time consideration as illustrated in Fig. 5.17. It can be seen that because power system simulation has smaller time step, some of the data are not synchronised to the communication simulation.

leader-follower: In the co-simulation process, the master simulator has higher priority and is responsible for coordinating the simulation steps. The leader-follower syn-

chronisation mechanism is illustrated in sub-figure (a) in Fig. 5.17, where the power system simulator serves as the Master and the communication system simulator acts as the Slave. Only when the variation of the measured value reaches a threshold does the Master starts a data exchange process.

Time-stepped: The time-stepped synchronisation process is presented in sub-figure (b) in Fig. 5.17. Normally, two different simulators run their simulations independently and pause at a fixed synchronisation frequency to exchange data. If an event requires data exchange, it should wait in the cache until the next synchronisation point occurs.

5.3.2.3 Platform Assessment Metrics

To assess the suitability of a cyber-physical co-simulation platform for cybersecurity-related studies, it is essential to define a platform assessment index (PAI) that can comprehensively measure its effectiveness in performance matrics such as synchronisation accuracy and latency, simulation scalability, and attack compatibility. In this paper, a Weighted Sum Method (WSM) widely used for the multi-criteria decision analysis [169] is adopted as follows:

$$PAI = \max_{i} \sum_{j=1}^{N} a_{ij} w_j, \tag{5.10}$$

where PAI_M represents the best co-simulation platform according to certain metrics using the WSM. Herein, index j represents the performance metrics and i denotes the i-th platform to be assessed. Moreover, a_{ij} is the performance score of the i-th option with respect to the j-th metric, indicating how effectively the option performs on that specific criterion, and w_j is the weight assigned to the j-th metric, representing its relative importance in the overall decision-making process. The WSM score is calculated for each platform candidate, and the platform with the highest score is identified as the most favourable choice.

In this paper, the set of performance metrics are denoted by

$$a_{ij} \in \mathcal{A} = \{L_D, S_C, P_S, R_S, N_A\} \tag{5.11}$$

where each metric is assigned a score of 5(Low), 7($Medium$) or 10($High$) based on its hardware of software performance in the co-simulation process. The specific scoring metrics are presented in Table 5.5.

The latency L_D between the simulators, inherent to the framework, can affect the accuracy of the transferred data. Consequently, lower latency leads to improved co-simulation performance. The computation time S_C of the synchronisation scheme is slightly longer than L_D because it includes data distribution and data transition time. The processors P_S in the power system simulator determine the scalability of the power

Table 5.5: Performance Metrics for the Assessment of Co-Simulation Platforms

Metrics	***Low=5***	***Medium=7***	***High=10***
Latency between simulators L_D	10+ ms	0.5-10 ms	0-0.5 ms
Synchronisation computation time S_C	100+ ms	10-100 ms	0-10 ms
Processors of power simulator P_S	1-2 cores	3-8 cores	8+ cores
RAM of communication simulator R_S	4-8 GB	8-32 GB	32+ GB
Number of applicable attacks N_A	1-2	3-6	6+

system, the more processors available, the larger the network scale that can be simulated. For example, a core in Typhoon can perform a real-time simulation of 20 (3-phase) nodes power system complexity at starting from $3\mu s$ to $1s$ simulation time step [170]. Similarly, the RAM of the communication system simulator R_S influences scalability in the same manner. The number of applicable attacks serves as a metric for evaluating the performance of the co-simulation platform, as it validates its compatibility for cybersecurity research. In summary, a higher PAI indicates that the tested platform has better performance in simulating different CPPS scenarios with high accuracy and enabling convincing investigation into various cyber contingencies.

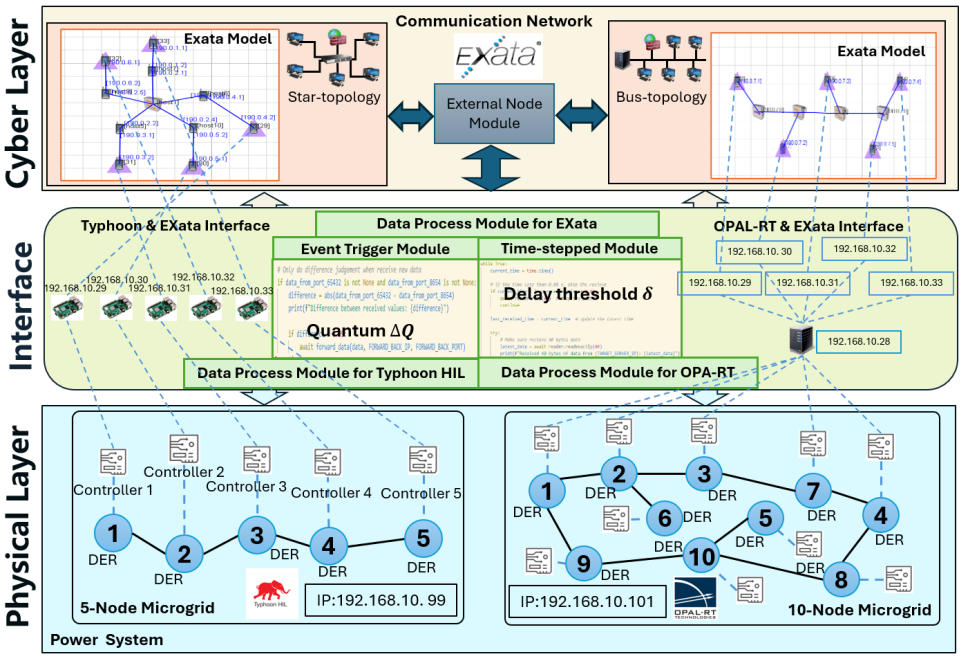


Figure 5.18: Implementation Framework for Data Synchronisation Schemes in the Cyber-Physical Co-simulation Platform

5.3.3 Implementation Framework

This paper has provided the Ethernet-based implementation framework for two real-time co-simulation schemes. The implemented co-simulation interfaces are built in the

form of Python scripts and run in the Raspberry Pis that are configured in the Linux environment. In Fig. 5.18, the leader-follower co-simulation scheme between Typhoon and EXata contains three modules. A 5-Node Microgrid system and a 10-Node Microgrid system are implemented into the Typhoon and OPAL-RT target machines, respectively. Furthermore, star-topology and bus-topology are chosen to be the communication network in the proposed platform. The Data Process Module is designed to receive data from Typhoon power system simulator. The Data Process Module for EXata is to exchanging data with the communication network simulator. The TCP/IP protocol is used in the platform to guarantee the accuracy of data transmission.

The key module of the interface is the Event Trigger Module, which will be illustrated in Section 5.3.3.1. The key module of the interface is the time-stepped Module which is illustrated in Section 5.3.3.2.

5.3.3.1 Leader-Follower Co-Simulation Between Typhoon and EXata

The interface in Typhoon and EXata platform uses leader-follower synchronisation scheme, where a Quantised State Systems Method (QSS) [171] is applied. The theory of QSS method can be described as follows: Let an initial value problem be specified as follows:

$$\dot{x}(t) = f(x(t), t), \quad x(t_0) = x_0 \tag{5.12}$$

The first-order QSS method, known as QSS1, approximates the above system by

$$\dot{x}(t) = f(q(t), t), \quad q(t_0) = x_0 \tag{5.13}$$

where x and q are related by a hysteretic quantization function:

$$q(t) = \begin{cases} x(t) & \text{if } |x(t) - q(t^-)| \geq \Delta Q, \\ q(t^-) & \text{otherwise.} \end{cases} \tag{5.14}$$

where ΔQ is called a quantum. Notice that this quantisation function is hysteretic because it has memory, i.e., its output is determined by both the current state and its previous value. The equation 5.14 therefore approximates the state by a piecewise constant function, $q(t)$, that updates its value as soon as the state deviates from this approximation by one quantum.

In this way, a fixed time step can be turned into a dynamic time step, and data are exchanged only when the variation of the observations exceeds the quantum ΔQ , which improves the computational efficiency at the expense of a certain degree of accuracy.

5.3.3.2 Time-Stepped Co-Simulation Between OPAL-RT and EXata

The structure of the OPAl-RT and EXata platform is shown in the right part of Fig. 5.18. In the OPAL-RT and EXata platforms, a time-stepped synchronisation method is used to exchange data between two simulators. Different from the traditional time-stepped method [168], a real-time time-stepped algorithm with expired event discarding is adopted here. The basic process of the algorithm is generates Pending Event List and repeat updating it. If an event is outdated, it will be removed from the queue. The algorithm is embedded in the Time-Step Module as shown in Fig 5.18. Discarding expired events ensures that the system will not process events that have been invalidated by waiting for more than δ.

The real-time synchronisation mechanism is implemented using a time-stepped approach combined with an event-driven Pending Event List (PEL). The procedure is described as follows:

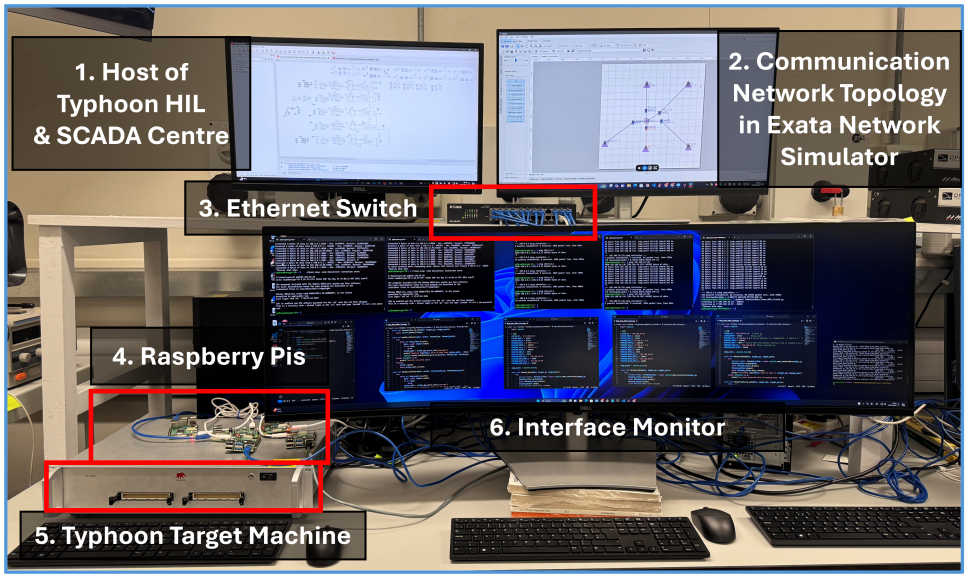
1. **Initialisation:** Set the starting time t_{current}, define the time step Δt and delay threshold δ, and initialise the PEL for each processing element (PE).
2. **Event registration:** For each incoming event with timestamp t_e, add it to the PEL if $t_e > t_{\text{current}}$; otherwise, discard it as expired.
3. **Time advancement:** Increment the simulation time as $t_{\text{current}} \leftarrow t_{\text{current}} + \Delta t$.
4. **Event execution:** For each event in the PEL:
   - If $t_e \leq t_{\text{current}}$, execute and remove the event.
   - If $t_e < t_{\text{current}} - \delta$, discard the event due to excessive delay.
5. **Iteration:** Repeat Steps 3–4 until the simulation terminates.

5.3.3.3 Ease-of-Implementation and Scalability

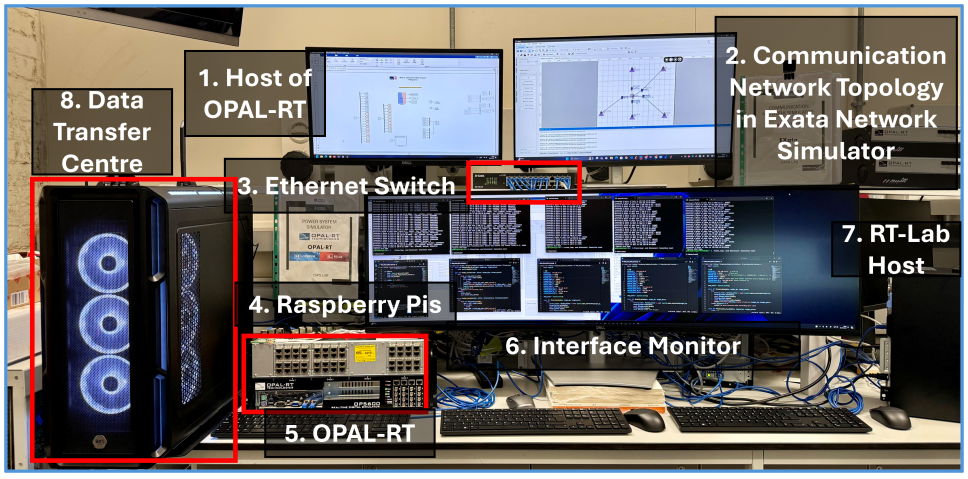
The proposed platform architecture provides clear implementation guidance, significantly reducing the learning curve for users. By modularising key components, such as data processing and event triggering modules, the platform simplifies configuration complexity at the interface layer. Additionally, it is designed to support various cyber-physical modelling needs by incorporating appropriate synchronisation schemes. In contrast, the approach in [64] features a detailed power grid model but represents the communication network in a simplified form. Conversely, in [65], the communication system is modelled in greater detail, while the power grid is reduced to a basic structure. In our platform, the scripts deployed on Raspberry Pis can be easily adapted to handle various data formats,

allowing seamless integration with either simplified or complex models. Compared to the methods presented in prior studies, our platform offers enhanced flexibility and ease of implementation.

As shown in Fig. 5.18, each physical node is mapped to a dedicated Raspberry Pi device. The scalability of the proposed interface is demonstrated by its ability to expand the network through the addition of Raspberry Pis, thereby enabling the platform to accommodate larger power system models. Furthermore, tasks such as data distribution and conversion can be offloaded to Raspberry Pis or other embedded devices, effectively reducing the computational burden on both the cyber and physical simulators. This distributed approach enhances simulation efficiency compared to traditional architectures that rely on direct connections or virtual links.



(a) Typhoon HIL 602+ & EXata Network Simulators based Platform



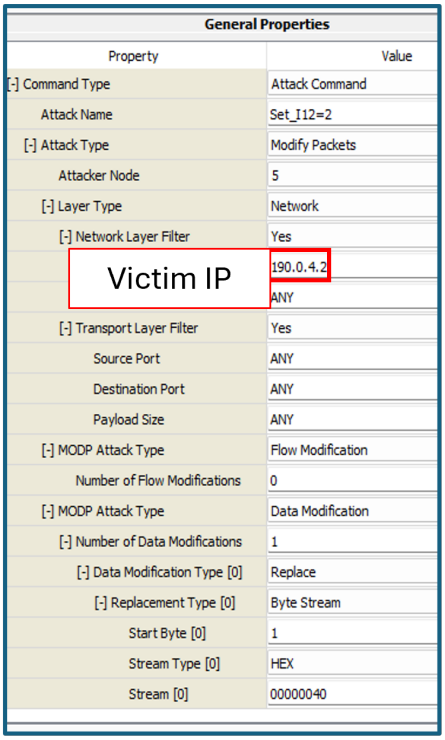
(b) OPAL-RT OP5600 & EXata Network Simulators based Platform

Figure 5.19: The Established Cyber-Physical Co-simulation Platforms in CAPS lab at the University of Sheffield.

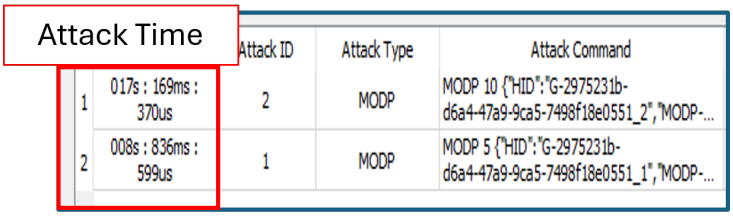
5.3.4 Case Studies and Results

This section demonstrates the cybersecurity test results based on the established cyber-physical co-simulation platforms. The platforms are constructed based on the facilities in the CAPS laboratory at the University of Sheffield, as shown in Fig. 5.19. The platforms mainly include the communication simulator EXata version 8.1.3, the power simulators Typhoon HIL 602+ and OPAL-RT OP5600 as shown in Fig. 5.19a and Fig. 5.19b, respectively. These simulators are synchronised through a dedicated interface deployed in Raspberry Pis. Device 1 PC serves as the upper host for the Typhoon HIL and OPAL-RT simulators, with the Typhoon and OPAL target machines as device 5. Device 2 PC serves as the host for EXata. The device 4 highlighted with a red frame to indicate Raspberry Pis, which function as the data exchange interface connecting the power system and communication system simulators. The device 6 serves as the upper host for the remote control of Raspberry Pis.

In this paper, the cybersecurity of microgrids is analysed using the proposed platform. Beyond its relevance to the research, the microgrid environment offers a smaller-scale network with distributed energy resources, enabling more controllable but representative experimentation. By focusing on microgrids, the effectiveness of the platform is demonstrated within a specific and widely relevant scenario in smart grids, which is both intuitive and illustrative of its practical utility. One of the platforms integrates a 5-DER DC microgrid in Typhoon HIL 602 + with the electrical parameters of DER obtained from [139]. The other platform includes a 10-DER DC microgrid built in OPAL-RT 5600 with the same electrical parameters. To investigate the co-simulation performance of platforms and their cybersecurity analysis capability, four case studies are conducted in this section: *Case 1:* Normal Operation, *Case 2:* Various FDI Attack, *Case 3:* DoS Attack, *Case 4:* Delay Attack. Fig. 5.20a presents the attack template that the proposed platforms use. The figure shows that the attack is launched in the network layer. Fig. 5.20b displays a cyber-attack history in the platform.



(a) Attack Template in EXata



(b) Attack History in EXata

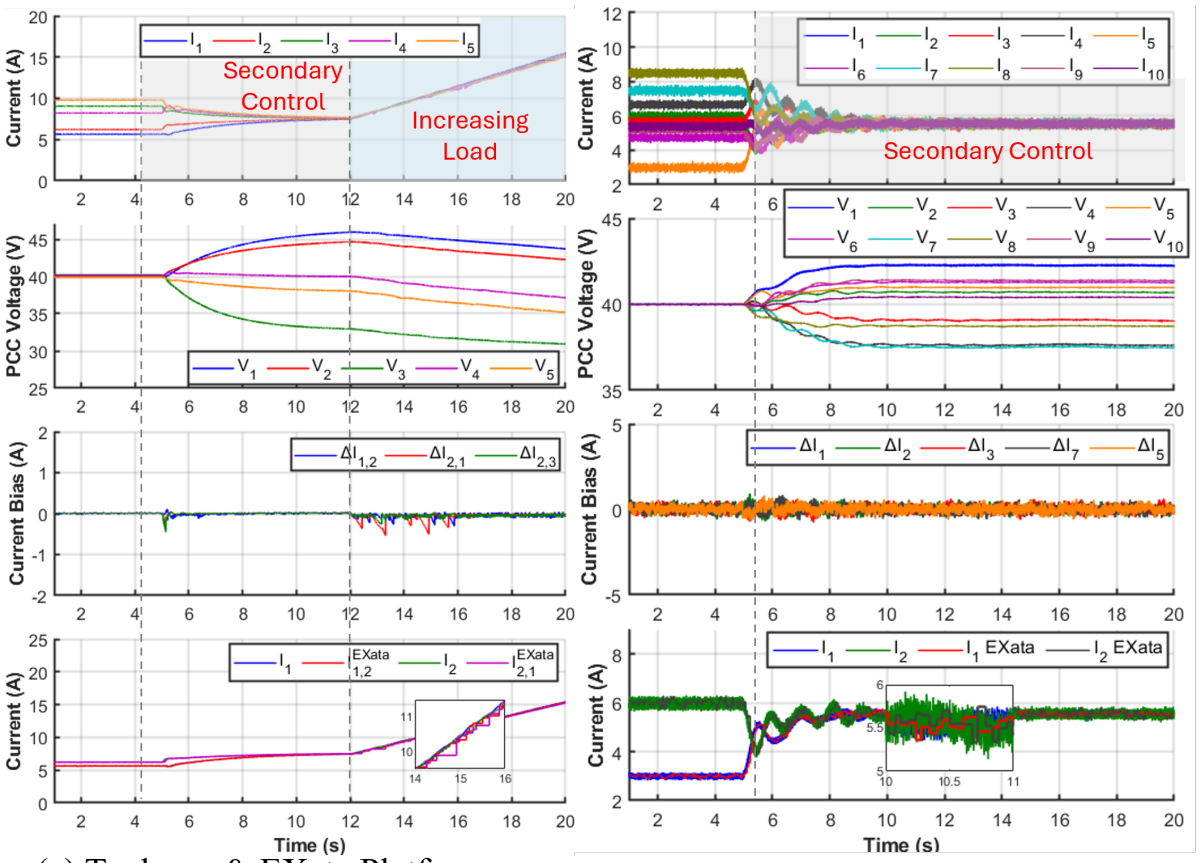
Figure 5.20: Attack Module in EXata

5.3.4.1 Case 1: Normal Operation

Simulation results in this case present the performance of the co-simulation platform when there are no cyber contingencies. The data are captured by the SCADA system of Typhoon HIL and OPAL-RT in a sampling time of 500 ns. Fig. 5.21a shows the current and point of common coupling (PCC) voltage states of a 5-DER microgrid from Typhoon HIL and the comparison between the current measurement flowing through the communication network and that from the power simulator, signified by $\Delta I_{i,j} = |I_i - I_{i,j}^{EXa}|$, where $I_{i,j}^{EXa}$ is the measurement of DER i received by DER j. To showcase the difference between two platforms, a constantly increasing load is installed into the Typhoon and EXata co-simulation platform after $t = 12$s. By extracting and zooming in on the simulation data from 14s to 16s, it shows that the data received from EXata can track the actual varying measurement with certain biases. The tracking bias is caused

by the leader-follower data synchronisation scheme, which only exchanges data when the deviation of current data from the previous one is larger than the quantum $\Delta Q = 0.35$A.

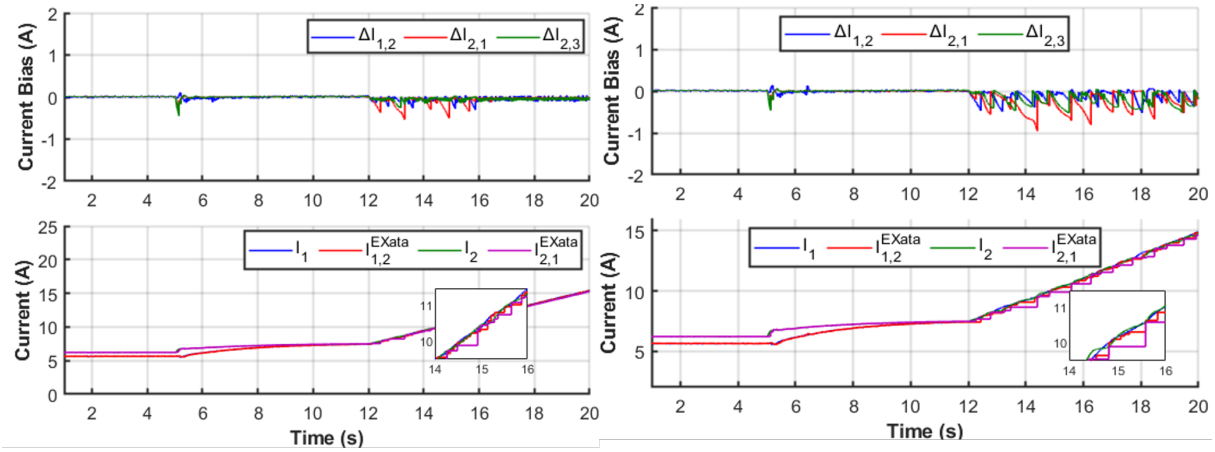
The quantum is determined by the network parameters and the transition time between simulators. Fig. 5.22 shows a comparison for different ΔQ values. In Fig. 5.22b, when ΔQ increases from 0.35A to 0.45A, the absolute maximum current bias increases from approximately 0.5A to 1A. Although a smaller ΔQ is preferable, the power system simulator has a limitation in handling smaller ΔQ because it leads to a faster data exchange rate. To balance data bias and simulation efficiency, $\Delta Q = 0.35$A is chosen as the quantum for subsequent simulations. The bias $\Delta I_{i,j}$ is also bounded by ΔQ as the latency of data transmission between the simulators is negligible. Despite this obvious current bias under the leader-follower synchronisation scheme, load sharing can still be achieved as the load current increases.



(a) Typhoon & EXata Platform Simulation Result in Normal Operation (Leader-follower Synchronisation)

(b) OPAL-RT & EXata Platform Simulation Result in Normal Operation (Time-stepped Synchronisation)

Figure 5.21: Normal Operation in the Two Established Co-simulation Platforms (Case 1)



(a) Typhoon & EXata Platform Simulation Result in Normal Operation when ΔQ=0.35 A

(b) Typhoon & EXata Platform Simulation Result in Normal Operation when ΔQ=0.45 A

Figure 5.22: Normal Operation in Different Value of ΔQ

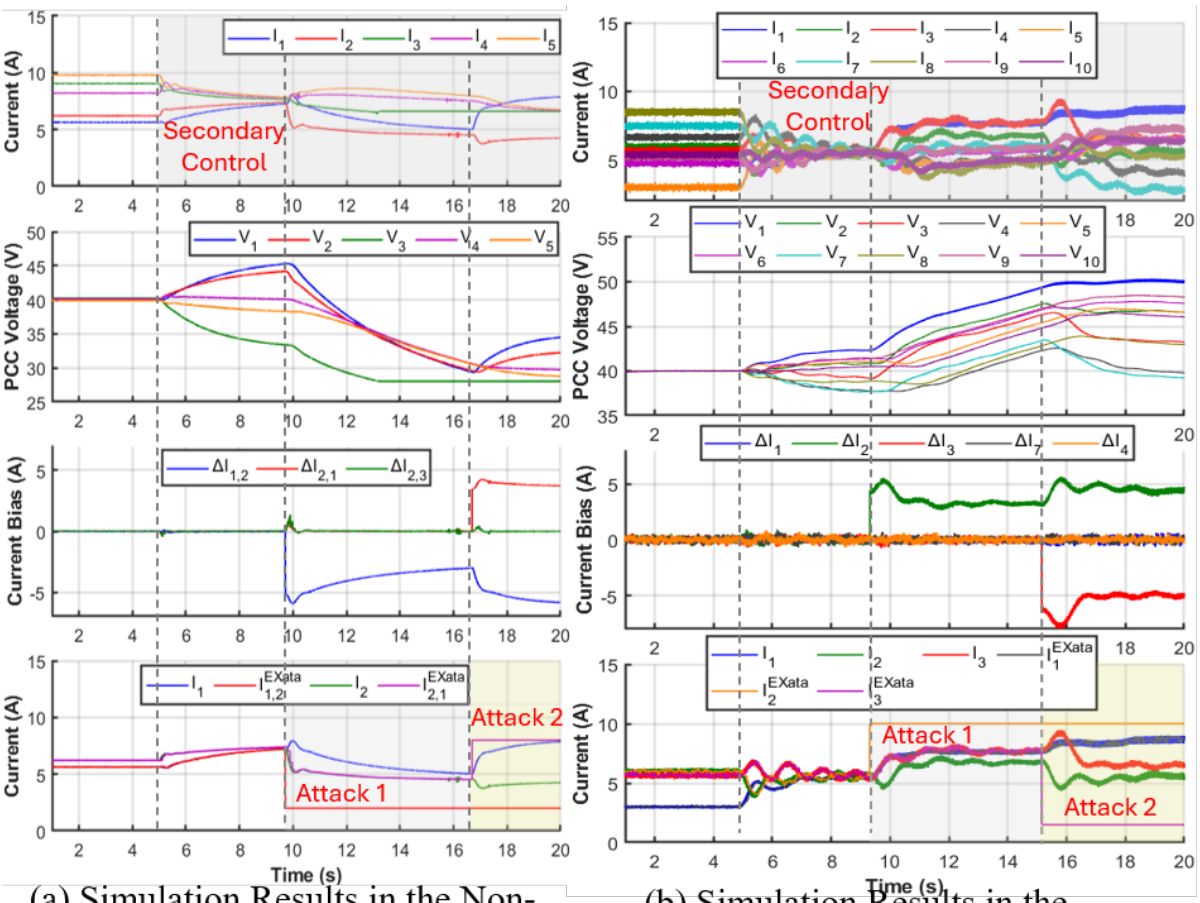
The results from the OPAL-RT and EXata co-simulation platform are presented in Fig 5.21b. Specifically, the top 2 sub-figures show the current and voltage of a 10-DER microgrid simulated in OPAL-RT, showing greater fluctuations compared with the results from Typhoon HIL since the cyber-physical complexity increases dramatically as the scale of microgrid increases. Both platforms have limited bias within the range $(-0.5, 0.5)$ under normal operation. In the time-stepped synchronisation scheme, the transmitted data via EXata will be updated every fixed time step $\delta = 0.08$s which is greater than the computation time in the interface, leaving one time-step bias between the received EXata data and the measured value. However, if a larger time step δ is set, exceeding the maximum step size in the leader-follower synchronisation scheme, the time-stepped synchronisation becomes less sensitive to data variations compared with the leader-follower approach. In our case, the hardware capabilities of the OPAL-RT platform support a smaller δ for experimentation, resulting in the time-stepped synchronisation method outperforming the leader-follower scheme in the normal state performance.

5.3.4.2 Case 2: Non-Coordinated and Coordinated FDI Attacks

Two types of FDI attacks are designed against the communication links of secondary control and launched in EXata using a dedicated data modification module, where constant bias is added at the original data flow following the byte stream.

The result of non-coordinated FDI attack injected into the communication nodes 1 and 2 in the Typhoon and EXata co-simulation platform is illustrated in Fig. 5.23a. The first FDI attack is launched at $t = 9\,s$ against node 1 and the current data are

manipulated to be 2A permanently. As a result, the load sharing status is disrupted and all PCC voltages keep decreasing with a quick rate. At $t = 17\,s$, the second FDI attack is launched against Node 2, where I_2 is maliciously compromised as 8A. This non-coordinated FDI attack cannot stabilise PCC voltages as the sum of injected biases is not zero all the time. Therefore, the PCC voltages will show a growth trend after the activation of the second FDI attack.



(a) Simulation Results in the Non-Coordinated FDI Attack (Typhoon HIL)

(b) Simulation Results in the Coordinated FDI Attack (OPAL-RT)

Figure 5.23: Various FDI Attacks in the Two Established Platforms (Case 2)

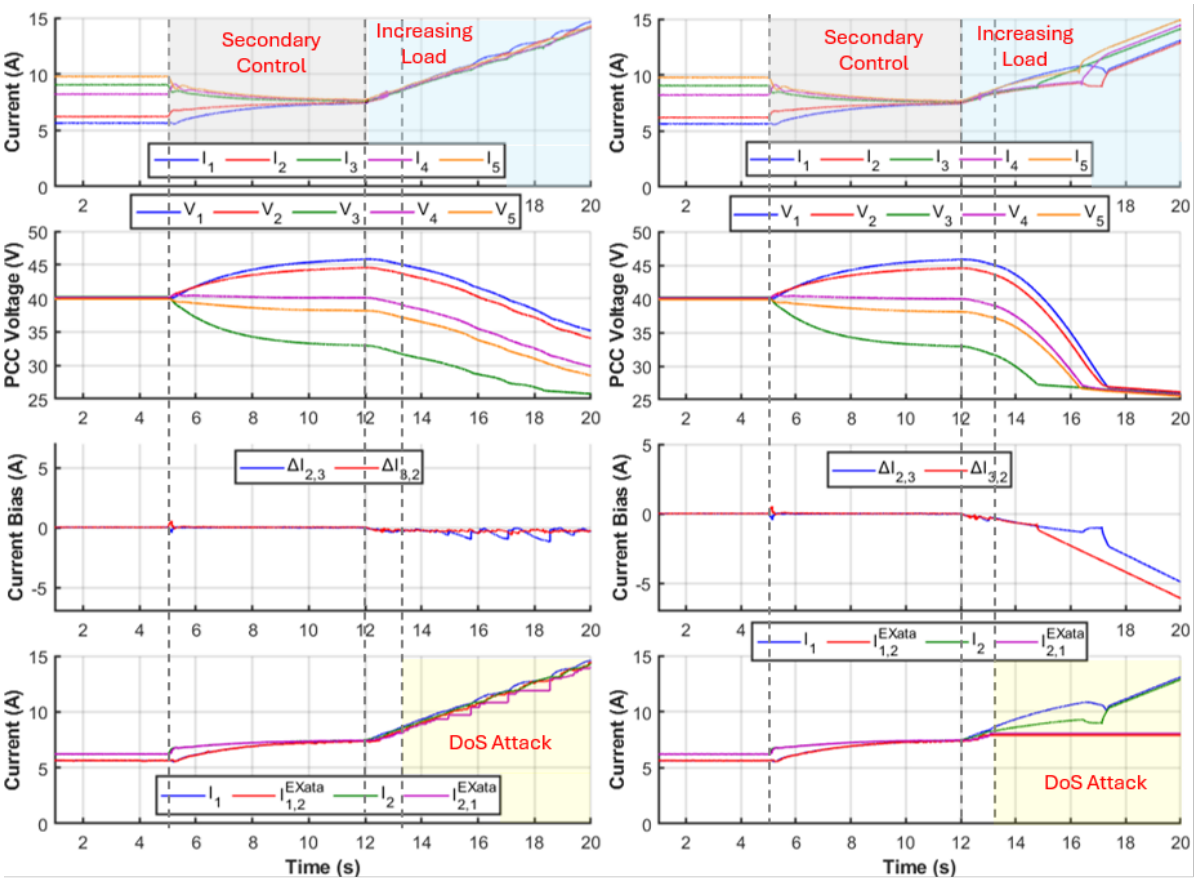
The investigation of coordinated FDI attack is conducted in the OPAL-RT and EXata co-simulation platform, where the attack targets include nodes 2 and 3 and the results are shown in Fig. 5.23b. For the coordinated FDI attack, the injected bias have opposite value offsets, e.g., 5A and -5A, and thus will induce specific deviations on system states from normal values rather than simply destabilising PCC voltages as the non-coordinated FDI attack. In this regard, the coordinated FDI attack will absolutely gain more favour from the adversary but, at the same time, requires stronger coordination capability on multiple FDI attacks.

Comparing the FDI attack simulation results for the two platforms indicates that dif-

ferent network topologies have minimal impact on FDI attacks. This is because variations in network topology do not change the data in the packets and the FDI attack targets the transited data specifically. As packets are still transmitted to different nodes across various network topologies, FDI attacks can be executed in different network structures and have a similar impact.

5.3.4.3 Case 3: DoS Attacks with Numerous Intensity Levels

In this case, DoS attacks with different intensity levels are applied to node 2 in the EXata network simulator. The intensity of DoS attack is measured by the number of attack packets sent to the victim per second. As shown in Fig. 5.24a, which is in the Typhoon platform, when the DoS intensity is 25, the system state is merely slightly affected since the data exchange between nodes can be still accomplished with obvious data packet loss. Under such circumstancess, load sharing can almost be achieved but with increasing error, and the variation of PCC voltage is significantly enlarged by the low-intensity DoS attack.



(a) Simulation Results when DoS Attack Level is 25 (Typhoon HIL)

(b) Simulation Results when DoS Attack Level is 1000 (Typhoon HIL)

Figure 5.24: DoS Attacks with Different Intendity Levels in the Typhoon and EXata Co-simulation Platform (Case 3)

When the intensity of DoS attack is increased to 1000, the impact of DoS attack is significantly amplified as shown in Fig. 5.24b. First of all, the data transmission links from DER 2 to its neighbouring DERs are fully interrupted, severely disrupting the currents and PCC voltages. Moreover, besides the data transmission links originating from DER 2, other links in the EXata are also heavily affected. For example, the bias $\Delta I_{3,2}$ also shows rapid growth upon the launch of the high-intensity DoS attack, meaning that DER 3 has difficulty in receiving data from DER 2.

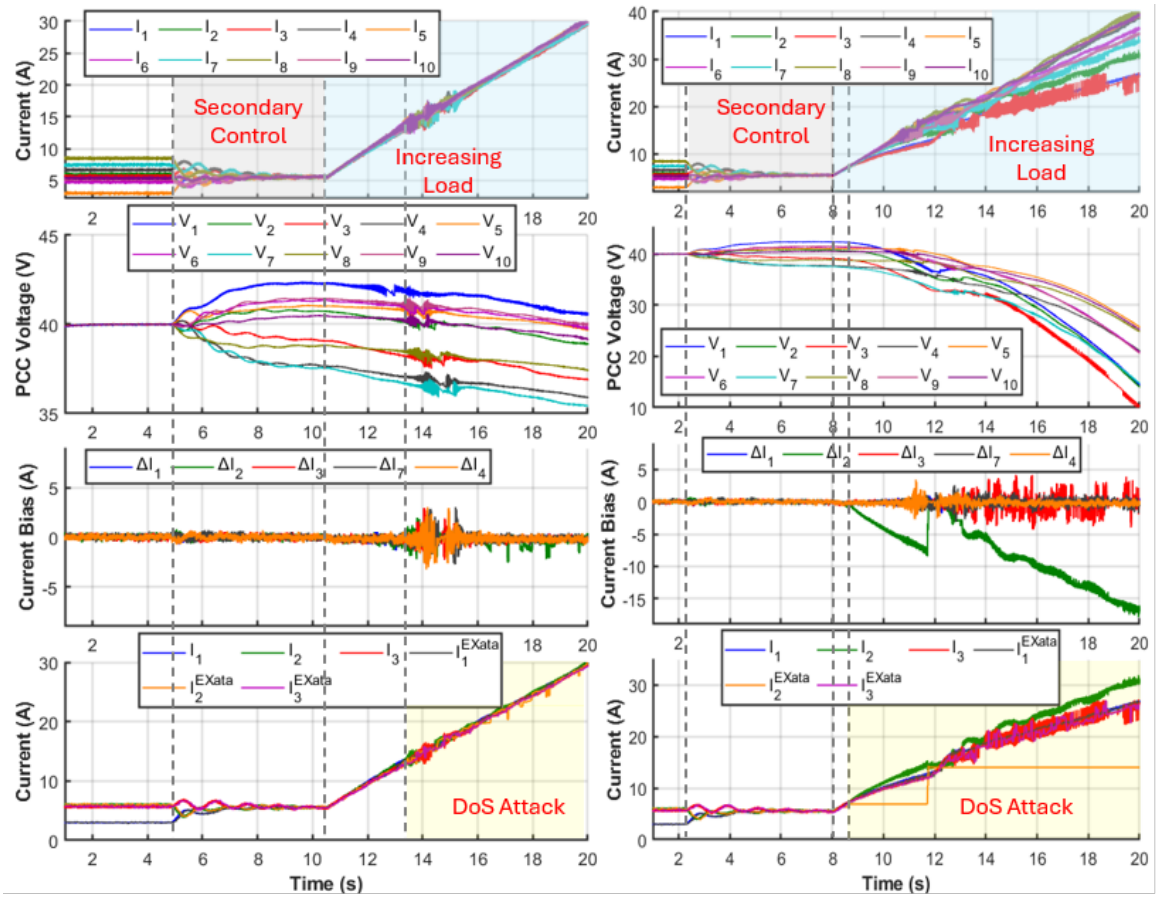
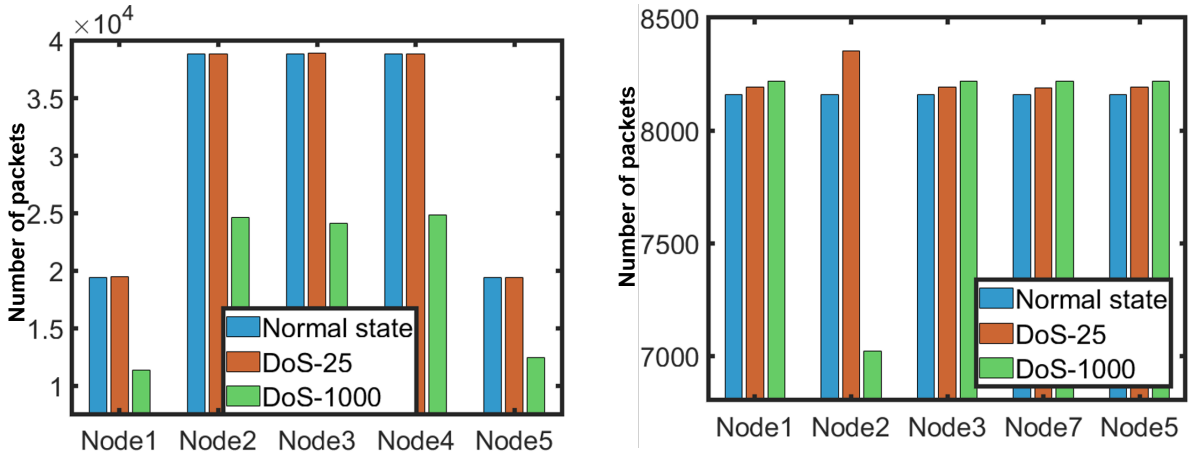


Figure 5.25: DoS Attacks with Different Intendity Levels in the OPAL-RT and EXata Co-simulation Platform (Case 3)

The DoS attacks with intensity 25 and 1000 are applied to the OPAL-RT and EXata co-simulation platform, and the results are depicted in Fig 5.25. Similar phenomena emerge where the system states become unstable when the intensity of the DoS increases. However, when seen from the current bias, only ΔI_2 is affected, which has obvious differences from the results of Typhoon and EXata co-simulation platform. It is because the communication network topology in this platform is a bus structure. From an architectural point of view, it does not need to exchange data through neighbouring nodes, but

directly interact with the data centre, such that the DoS attack will not affect nodes other than node 2.



(a) Packets received in communication nodes (Typhoon & EXata co-simulation platform)

(b) Packets received in communication nodes (OPAL-RT & EXata co-simulation platform)

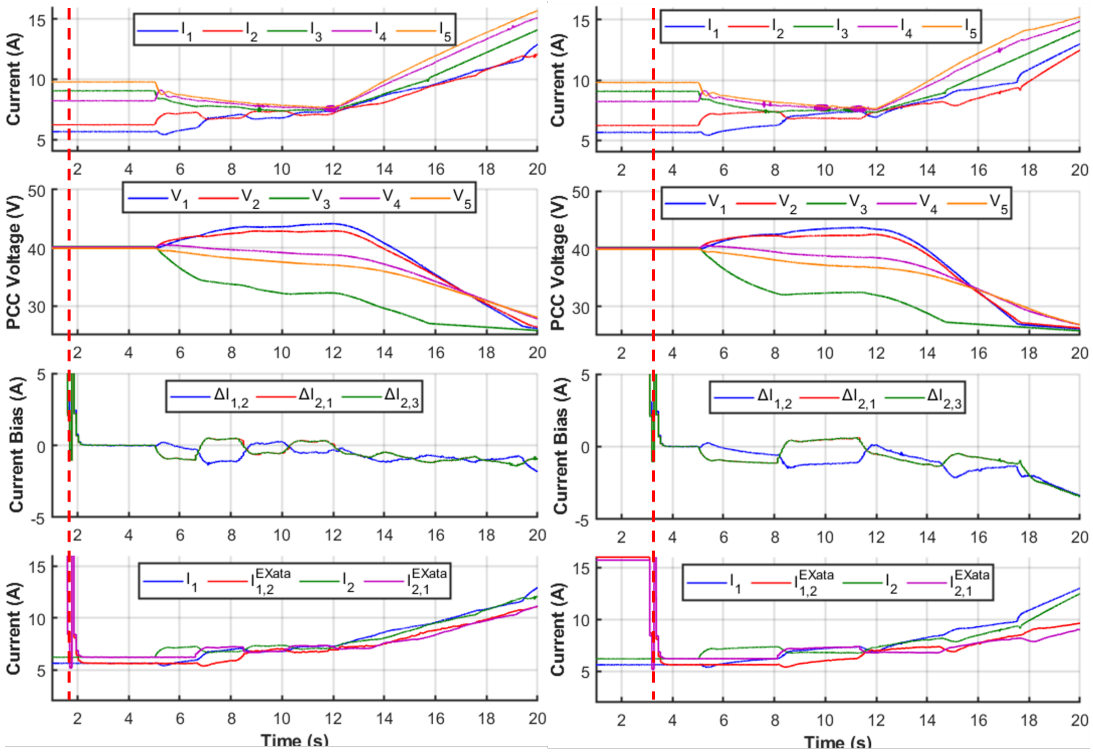
Figure 5.26: Number of Received Data Packets in the Presence of DoS Attacks with Different Intensity Levels

To clearly illustrate the impact of network architecture on the DoS attack analysis, the number of received packets of all nodes in the two platforms is captured by EXata in the form of SQLite database, and the results are presented in Fig. 5.26. The DoS attack against node 2 affects all the other nodes in the Typhoon and EXata co-simulation platform, while it only affects node 2 in the OPAL and EXata co-simulation platform. This is because, in a star-topology, when a DoS attack is mounted to node 2, the neighbouring nodes of node 2 are affected first. These neighbouring nodes, in turn, impact their neighbouring nodes, ultimately influencing the entire communication network. In bus-topology, the DoS attack only affects the attacked node as the EXata nodes directly interact with the external nodes.

Seen from Fig.5.24, Fig.5.25, and Fig.5.26, a summary can be given: 1) Structurally, employing a bus-topology can accurately disclose the impact of any single DoS attack within the communication network. A star-topology may impact the entire network rather than a single node, while a bus-topology typically affects only the targeted node. This difference arises because, in a star topology, a central node (e.g., a switch) manages data transmission, allowing an attack to propagate to all connected nodes, as observed in the Typhoon and EXata platform. In contrast, a bus-topology relies on a single shared bus for direct communication without centralised processing, limiting the spread of an attack, as seen in the OPAL-RT and EXata platform. 2) The leader-follower approach can cause bias shifts that may be indistinguishable from the impact resulting from a low-intensity DoS attack. Therefore, the implementation of a bus-topology communication network based on the time-stepped synchronisation scheme that interacts with the power simulator is

recommended for conducting DoS attack related research activities.

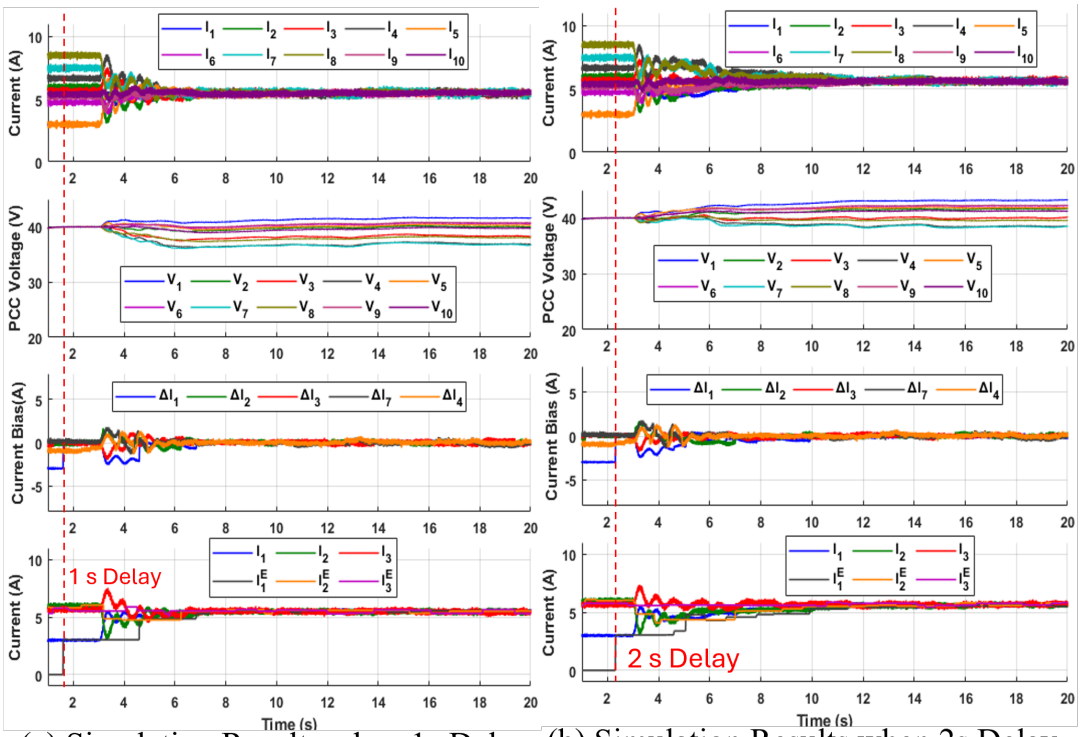
5.3.4.4 Case 4: Delay Attacks with Various Latency Levels



(a) Simulation Results when 1s Delay Attack is on Node 2 (Typhoon HIL)

(b) Simulation Results when 2s Delay Attack is on Node 2 (Typhoon HIL)

Figure 5.27: Delay Attacks with Various Latency Levels in the Typhoon and EXata Co-simulation Platform (Case 4)



(a) Simulation Results when 1s Delay Attack is on Node 1 (OPAL-RT)

(b) Simulation Results when 2s Delay Attack Level is on Node 1 (OPAL-RT)

Figure 5.28: Delay Attacks with Various Latency Levels in the OPAL-RT and EXata Co-simulation Platform (Case 4)

In Case 4, the effects of the delay attack (1s and 2s latency levels) on microgrid operations are investigated on the two co-simulation platforms. Fig. 5.27 presents the simulation results on Typhoon and EXata platform. The result shows that the bias becomes larger when the delay increases from 1s to 2s. Moreover, both delay scenarios prevent the system from achieving the desired load sharing state, which is due to delayed control signals that affect the coordination among DERs. Fig. 5.28 shows the performance of delay attacks on the OPAL-RT and EXata platform. Both scenarios can reach similar steady-state voltage levels. However, the 2s delay prolongs the stabilising duration, indicating that longer latency amplifies the destabilising effect on voltage regulation.

When comparing the simulation results from the two platforms, the Typhoon-based co-simulation exhibits pronounced oscillatory waveforms, whereas the OPAL-RT-based co-simulation shows only minor fluctuations. This behaviour can be attributed to the amplification effect introduced by the leader-follower synchronisation scheme. Specifically, this scheme updates data between the cyber and physical simulators only when the deviation exceeds a predefined quantum. When combined with communication latency, this approach amplifies the impact of delay attacks. As illustrated in Fig. 5.27, the significantly outdated information, exhibiting a delay several times greater than the initially introduced latency, repeatedly triggers large secondary control adjustments, ultimately

inducing severe oscillations in the system states. In contrast, the time-stepped synchronisation method proves more compatible with time-delay attacks, as it more accurately reflects the effects of actual data latency.

5.3.4.5 Platform Assessment

In this section, the computational overhead of synchronisation schemes and the effectiveness of the established cyber-physical co-simulation platforms are evaluated and presented here.

Table 5.6: Comparison of Synchronisation Schemes

Computational overhead	***Leader-follower***	***Time-stepped***
Computation time	0.183±0.004 ms	30±0.5 ms
Data packet size	50 Bytes	200 Bytes
RAM usage	1.36% 106 MB	6.85% 535 MB
Python script file size	12 KB	28 KB

The Table 5.6 presents the computation overhead of two synchronisation schemes in the platforms. The computational time limits the minimum simulation step and the shorter the simulation length, the higher the synchronisation accuracy that can be achieved. The RAM usage of the leader-follower and time-stepped synchronisation schemes takes up 1. 36% and 6. 85% of the total memory of 8 GB, respectively. As each Raspberry Pi currently manages a single node, one Raspberry Pi can support up to approximately 70 nodes. This design facilitates scalability for larger grids in the future. For instance, expanding to 1,000-node power grid would require only 15 Raspberry Pis. Furthermore, increasing the RAM or optimising the Python script can further enhance the scalability of the network. The file size of the scripts is only 12 KB or 28 KB, and it has little effect on storage.

The PAI index for each platform is calculated using Eq. 5.10. In this paper, the weight w_j of each metric j are set to 1, as they are considered equally important. The metrics L_D, S_C, C_A, P_S, N_A are categorised into three levels, as outlined earlier in Table 5.5: $Low = 5$, $Medium = 7$, and $High = 10$. The results of the two platforms are presented in Fig. 5.29.

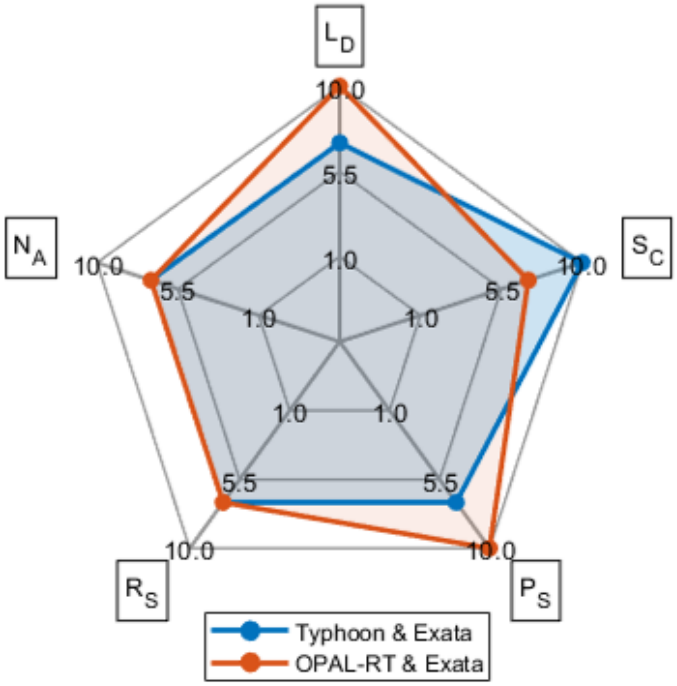


Figure 5.29: PAI Results of the Two Established Cyber-Physical Co-simulation Platforms

Given that the latency between Typhoon and EXata is 1.459ms, and the latency between OPAL-RT and EXata is 0.498ms, it follows that $L_D(1) = 7$ and $L_D(2) = 10$, according to Table 5.5. The value of S_C is determined based on the computation time in Table 5.6: the synchronisation computation time for the Typhoon and EXata platform is approximately 0.183ms while that for the OPAL-RT and EXata platform is approximately 30ms. Therefore the $S_C(1) = 10$ and $S_C(2) = 7$. The values $P_S(1) = 7$ and $P_S(2) = 5$ result from the fact that the Typhoon HIL has 6 cores and OPAL-RT has 16 cores, respectively. The values $P_S(1) = P_S(2) = 7$ are equal for both platforms, as they use the same communication simulator, EXata, with 16 G RAM. The values $N_A(1) = N_A(2) = 7$, as both of the platforms are capable of simulating three different cyber-attacks.

The score for the Typhoon and EXata platform is $PAI(1) = 38$, while that for the OPAL-RT and EXata platform is $PAI(2) = 36$.

5.3.5 Section Conclusion

This paper focuses on the real-time cyber-physical digital simulation for cybersecurity analysis in the context of microgrids, proposes an implementation framework for real-time leader-follower and time-stepped co-simulation schemes, and develops a set of metrics to assess the feasibility of a co-simulation platform for cybersecurity analysis. Two cyber-physical microgrid platforms are established based on OPAL-RT and Typhoon simulators

as well as EXata network simulator. Extensive case studies are conducted to showcase the analysis capability of the two platforms, which have different co-simulation schemes and communication network topologies, under FDI, DoS and delay contingencies. The assessment metrics are applied to the established platforms and recommendations are provided for choosing appropriate platforms for cybersecurity analysis.

However, the platform has some limitations: Although the proposed platform can simulate several CPPS scenarios in the laboratory, it has not been tested in real microgrid environments. Data transmission delays, which are inevitable but can be mitigated, can undermine the accuracy of the simulation, particularly in high-frequency attack scenarios where rapid data exchange is essential. Moreover, when simulating ultra-large-scale power systems, computational resources and simulation time may become limiting factors.

Future work will focus on several key areas: Build up more scenarios for cybersecurity research using the proposed platforms to large-scale network such as transmission network [172, 173]. Integrate deep reinforcement learning into cybersecurity solutions. Validate the effectiveness of proposed evaluation scheme on different cyber-physical co-simulation platforms and test the platform in real-world environments.

5.4 Conclusion

This chapter presents the development of cyber–physical real-time co-simulation platforms for cybersecurity analysis in microgrids, structured by three sequential studies.

The first study establishes an initial real-time microgrid co-simulation platform by integrating the Typhoon HIL simulator with the EXata network simulator. A master–slave synchronisation scheme is developed to enable coordinated interaction between the power and communication domains. The results demonstrate that the platform is capable of capturing the impacts of cyber contingencies such as FDI attacks and packet drops on microgrid control performance, thereby providing a foundational environment for cyber–physical security analysis.

Building upon this, the second study develops a more scalable and flexible co-simulation architecture by integrating the OPAL-RT power system simulator with EXata network simulator. A time-stepped synchronisation scheme with a real-time data exchange interface is proposed to improve computational efficiency and support larger network sizes with shorter simulation time steps. The results show that the enhanced platform enables more stable and scalable cyber–physical simulations, while accurately reflecting the impacts of cyber disturbances on system dynamics.

The third study further generalises the previous developments and proposes a unified implementation framework for real-time cyber–physical co-simulation, incorporating

both leader–follower and time-stepped synchronisation schemes. In addition, a set of quantitative assessment metrics is introduced to evaluate platform performance in terms of synchronisation accuracy, latency, scalability, and attack compatibility. Through extensive case studies involving FDI, DoS, and delay attacks, the intrinsic relationships between synchronisation mechanisms, communication network topology, and cyber attack impacts are systematically assessed.

Overall, this chapter demonstrates that cyber–physical co-simulation is an essential tool for analysing the vulnerability and resilience of microgrids under cyber attacks. It highlights that both synchronisation schemes and communication network configurations play critical roles in shaping system responses, and therefore must be carefully designed in cybersecurity studies.

Chapter 6

Conclusion and Future Work

This thesis investigates cyber–physical co-simulation modelling, uncertainty analysis, and real-time digital simulation methodologies for modern power systems, with a particular focus on distribution networks and microgrids with renewable energy sources. As power systems evolve towards increased digitalisation and decentralisation, the tight coupling between electrical infrastructures and communication networks introduces new challenges in system modelling, analysis, and validation. This thesis addresses these challenges by developing a unified cyber–physical framework in which communication dynamics are explicitly embedded into power system modelling, analysis, and validation.

A unified modelling framework has been developed by integrating differential–algebraic equation (DAE)-based power system models with communication network characteristics. Within this framework, node-specific communication delays are explicitly embedded into the system equations, enabling a more realistic representation of cyber–physical interactions. Compared with existing approaches that rely on abstract network representations or simplified delay assumptions, the proposed formulation captures both physical dynamics and communication-induced effects in a consistent and physically interpretable manner.

Building upon this modelling framework, a Virtual Power–Physical Flow (VPPF) method has been proposed to analyse cyber–physical interactions and system vulnerabilities in CPPS. This method provides a novel perspective for representing and analysing cyber–physical interactions beyond conventional power flow-based formulations. Within this framework, both a vulnerability index and a GSA approach are developed to quantify system vulnerabilities and uncertainty impacts from complementary perspectives. By incorporating both physical uncertainties, such as renewable generation and load variability, and cyber uncertainties, including communication delays, as stochastic inputs, the proposed approach enables a systematic assessment of how disturbances propagate across cyber and physical layers. The results demonstrate that communication-induced effects

can significantly influence system behaviour and interact nonlinearly with physical dynamics, highlighting the importance of explicitly modelling cyber-layer characteristics in CPPS analysis.

To support validation, a cyber–physical real-time co-simulation platform structure has been developed, integrating real-time digital simulators with communication network emulators. Multiple architectures have been designed, including TCP-based master–slave schemes, time-stepped synchronisation mechanisms, and UDP-based shared-memory interfaces, enabling flexible and scalable coupling between power and communication domains. In addition, an evaluation metric, named as the PAI index, has been proposed to quantitatively assess the performance of the co-simulation platform in terms of efficiency, cyberattacks simulation capability, and communication capability. This provides a systematic method to compare different co-simulation architectures and to analyse their efficiency under varying simulation conditions. Together, the developed platforms and evaluation framework enable high-fidelity, closed-loop validation of cyber–physical interactions under realistic operating conditions, and provide a practical model for analysing system behaviour under combined cyber and physical disturbances.

The proposed methodologies have been validated through case studies on distribution networks and microgrid systems. The results demonstrate that the modelling framework effectively captures cyber-physical effects, the GSA approach provides meaningful insights into uncertainty propagation, and the real-time simulation platforms enable reliable experimental validation.

Overall, this thesis enhances the understanding of cyber–physical interactions in modern power systems by bridging modelling, uncertainty analysis, and real-time validation within a unified framework. The proposed methodologies not only improve the fidelity of CPPS modelling and analysis but also provide a systematic foundation for future research in cyber–physical security, distributed control, and resilient power system operation.

Future Work

Although this thesis has developed a systematic framework for modelling, analysing, and validating cyber–physical power systems, several important research directions remain to be further investigated.

First of all, future work should incorporate more detailed communication network modelling and cyberattack representation. In this thesis, communication effects are mainly represented through node-specific communication delays. This approach is suitable for system-level cyber–physical analysis, but it does not fully capture protocol-level behaviours, packet-level dynamics, routing mechanisms, and device-level communication

characteristics. This direction is important because realistic communication protocols and packet-level events may directly influence the timing, reliability, and effectiveness of control actions in CPPS. To address this limitation, future research can integrate more detailed communication models based on industrial protocols, routing strategies, and packet-level traffic characteristics.

In addition, future work can extend the proposed global sensitivity analysis framework to support large-scale and more complex CPPS. The Sobol-based sensitivity analysis used in this thesis provides quantitative insight into the contributions of renewable generation uncertainty and communication delay uncertainty. However, variance-based global sensitivity analysis is computationally expensive, especially when the number of uncertain inputs increases. This limitation becomes more significant for large-scale transmission and distribution networks, interconnected microgrids, and systems with multiple types of uncertainties. Therefore, improving scalability and computational efficiency is essential. Possible solutions include surrogate modelling, reduced-order modelling, adaptive sampling, and parallel computing. For example, Gaussian-process models, polynomial chaos expansion, or neural-network-based surrogate models can be trained using high-fidelity co-simulation data and then used to estimate sensitivity indices with lower computational cost.

Moreover, strengthening real-time hardware-in-the-loop validation and practical deployment can be future work. The real-time co-simulation platforms developed in this thesis provide a flexible and risk-free environment for analysing CPPS cybersecurity and uncertainty impacts. However, practical CPPS operation involves real controllers, protection devices, communication hardware, measurement units, and power electronic interfaces, whose behaviours may introduce additional constraints and uncertainties. Therefore, tighter hardware integration is required to bridge the gap between simulation-based studies and real-world deployment. This can be achieved by connecting real controllers, embedded devices, protection relays, phasor measurement units, and converter control hardware to the developed co-simulation platforms. Hardware-in-the-loop experiments can then be used to validate cyberattack detection, mitigation, and recovery strategies under realistic timing and communication constraints.

In summary, this thesis provides a foundation for modelling, uncertainty analysis, and real-time validation of cyber–physical power systems. Future research should further improve the fidelity of communication modelling, enhance the scalability of uncertainty quantification methods, and strengthen hardware-in-the-loop validation for practical CPPS resilience and cybersecurity applications.

Appendix A

Hardware and Software Used in This Thesis

This appendix summarises the main hardware, software, communication interfaces, and synchronisation mechanisms used in this thesis. These tools support the modelling, co-simulation, uncertainty analysis, and real-time validation studies presented in Chapters 3–5.

A.1 Hardware and Software Components

Table A.1: Main hardware and software used in this thesis

Component	**Used in**	**Brief role**
OPAL-RT real-time simulator	Chapters 4, 5.2, 5.3	Real-time power system simulation for distribution networks and microgrids.
Typhoon HIL 602+	Chapters 5.1, 5.3	Real-time HIL simulation of power-electronic microgrids.
Raspberry Pi	Chapter 5	Embedded interface for real-time data exchange between simulators.
Ethernet switch and cables	Chapters 4, 5	Physical network infrastructure for data transmission.
MATLAB	Chapters 3, 4	Numerical modelling, data processing, and sensitivity analysis.
MATPOWER	Chapter 3	Power flow and OPF calculation for IEEE test systems.
RT-LAB	Chapters 4, 5	OPAL-RT model execution, monitoring, and real-time control.
Typhoon HIL software	Chapter 5	Microgrid model construction and HIL monitoring.
EXata Network Simulator	Chapter 5	Communication network emulation and cyberattack modelling.
OMNeT++ and INET	Chapter 4	Discrete-event communication network modelling.
Python and C++	Chapters 4, 5	Interface scripting, data exchange, and simulation support.

A.2 Communication Interfaces and Synchronisation Mechanisms

Table A.2: Main interfaces and synchronisation mechanisms used in this thesis

Interface / Mechanism	**Used in**	**Brief role**
TCP/IP	Chapter 5	Reliable Ethernet-based data exchange between simulators.
UDP	Chapter 4	Lightweight data transmission between OPAL-RT and OMNeT++.
Modbus	Chapter 5.1	Data exchange protocol used in the Typhoon HIL platform.
Shared memory	Chapter 4	Low-overhead data exchange for OPAL-RT–OMNeT++ co-simulation.
EXata external node	Chapter 5	Connects real data interfaces with virtual communication nodes.
Master–slave synchronisation	Chapters 5.1, 5.3	Event-triggered data exchange between Typhoon HIL and EXata.
Time-stepped synchronisation	Chapters 4, 5.2, 5.3	Fixed-interval data exchange between power and communication simulators.
RealTimeScheduler	Chapter 4	Aligns OMNeT++ simulation time with real time.

Bibliography

[1] J. Leslie and N. G. ESO, "Zero carbon operation 2025," 2019, author: Head of National Control.

[2] REN21, "Renewables 2025 global status report: Solar photovoltaics (pv)," Paris, France, 2025.

[3] Q. Hou, E. Du, N. Zhang, and C. Kang, "Impact of high renewable penetration on the power system operation mode: A data-driven approach," *IEEE Transactions on Power Systems*, vol. 35, DOI 10.1109/TPWRS.2019.2929276, no. 1, pp. 731–741, 2020.

[4] S. Sridhar, A. Hahn, and M. Govindarasu, "Cyber–physical system security for the electric power grid," *Proc. IEEE*, vol. 100, DOI 10.1109/JPROC.2011.2165269, no. 1, pp. 210–224, 2012.

[5] B. Achaal, M. Adda, M. Berger, and A. Awde, "Study of smart grid cyber-security, examining architectures, communication networks, cyber-attacks, countermeasure techniques, and challenges," *Cybersecurity*, vol. 7, DOI 10.1186/s42400-023-00200-w, no. 10, 2024.

[6] R. V. Yohanandhan, R. M. Elavarasan, P. Manoharan, and L. Mihet-Popa, "Cyber-physical power system (cpps): A review on modeling, simulation, and analysis with cyber security applications," *IEEE Access*, vol. 8, DOI 10.1109/ACCESS.2020.3016826, pp. 151 019–151 064, 2020.

[7] M. Khalaf, A. Ayad, M. H. K. Tushar, M. Kassouf, and D. Kundur, "A survey on cyber-physical security of active distribution networks in smart grids," *IEEE Access*, vol. 12, DOI 10.1109/ACCESS.2024.3364362, pp. 29 414–29 444, 2024.

[8] J. M. Morales, A. J. Conejo, H. Madsen, P. Pinson, and M. Zugno, *Renewable Energy Sources—Modeling and Forecasting*, pp. 15–56. Boston, MA: Springer US, 2014. [Online]. Available: https://doi.org/10.1007/978-1-4614-9411-9_2

[9] W. Luo, P. Lu, H. Liu, and C. Du, "Event-triggered networked predictive output tracking control of cyber–physical systems with model uncertainty and communi-

cation constraints," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 70, DOI 10.1109/TCSII.2022.3233666, no. 6, pp. 2166–2170, 2023.

[10] D. Yang and V. Ajjarapu, "A decoupled time-domain simulation method via invariant subspace partition for power system analysis," *IEEE Transactions on Power Systems*, vol. 21, DOI 10.1109/TPWRS.2005.860937, no. 1, pp. 11–18, 2006.

[11] W. Jiang, "Graph-based deep learning for communication networks: A survey," *Computer Communications*, vol. 185, DOI https://doi.org/10.1016/j.comcom.2021.12.015, pp. 40–54, 2022. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0140366421004874

[12] K. Ye, J. Zhao, F. Ding, R. Yang, X. Chen, and G. W. Dobbins, "Global sensitivity analysis of large distribution system with pvs using deep gaussian process," *IEEE Transactions on Power Systems*, vol. 36, DOI 10.1109/TPWRS.2021.3084455, no. 5, pp. 4888–4891, 2021.

[13] Y. Li, Y. Xu, S. Yao, S. Lu, W. Gu, L. Mili, and M. Korkali, "Global sensitivity analysis for integrated heat and electricity energy system," *IEEE Transactions on Power Systems*, vol. 40, DOI 10.1109/TPWRS.2024.3500214, no. 3, pp. 2078–2090, 2025.

[14] Y. Shuai, Y. Zhang, F. Liu, X. Qiao, Y. Xiong, and Y. Zeng, "Co-simulation of power grid, information network and transportation network simulation system," in *2022 IEEE 2nd International Conference on Software Engineering and Artificial Intelligence (SEAI)*, DOI 10.1109/SEAI55746.2022.9832036, pp. 199–203, 2022.

[15] X. Ning and J. Jiang, "Design, analysis and implementation of a security assessment/enhancement platform for cyber-physical systems," *IEEE Transactions on Industrial Informatics*, vol. 18, DOI 10.1109/TII.2021.3085543, no. 2, pp. 1154–1164, 2022.

[16] M. Liu, F. Teng, Z. Zhang, P. Ge, M. Sun, R. Deng, P. Cheng, and J. Chen, "Enhancing cyber-resiliency of der-based smart grid: A survey," *IEEE Transactions on Smart Grid*, 2024.

[17] A. Ehsan and Q. Yang, "State-of-the-art techniques for modelling of uncertainties in active distribution network planning: A review," *Applied Energy*, vol. 239, DOI https://doi.org/10.1016/j.apenergy.2019.01.211, pp. 1509–1523, 2019. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0306261919302247

[18] G. Papaefthymiou and D. Kurowicka, "Using copulas for modeling stochastic dependence in power system uncertainty analysis," *IEEE Transactions on Power Systems*, vol. 24, DOI 10.1109/TPWRS.2008.2004728, no. 1, pp. 40–49, 2009.

[19] M. Abdelmalak, V. Venkataramanan, and R. Macwan, "A survey of cyber-physical power system modeling methods for future energy systems," *IEEE Access*, vol. 10, DOI 10.1109/ACCESS.2022.3206830, pp. 99 875–99 896, 2022.

[20] H. Gill, "From vision to reality: Cyber-physical systems," Presentation at the National Workshop on New Research Directions for High Confidence Transportation Cyber-Physical Systems: Automotive, Aviation and Rail, 2008, national Science Foundation (NSF).

[21] E. A. Lee, "Cyber physical systems: Design challenges," in *Proceedings of the 11th IEEE International Symposium on Object-Oriented Real-Time Distributed Computing (ISORC)*, DOI 10.1109/ISORC.2008.25, pp. 363–369. IEEE, 2008.

[22] E. A. Lee, "Cyber physical systems: Design challenges," in *Proceedings of the 11th IEEE International Symposium on Object and Component-Oriented Real-Time Distributed Computing*, DOI 10.1109/ISORC.2008.25, pp. 363–369, 2008.

[23] R. Rajkumar, I. Lee, L. Sha, and J. Stankovic, "Cyber-physical systems: The next computing revolution," in *Proceedings of the 47th Design Automation Conference*, DOI 10.1145/1837274.1837461, pp. 731–736, 2010.

[24] R. Baheti and H. Gill, "Cyber-physical systems," in *The Impact of Control Technology*, T. Samad and A. M. Annaswamy, Eds., pp. 161–166. IEEE Control Systems Society, 2011.

[25] P. Tabuada, *Verification and Control of Hybrid Systems: A Symbolic Approach*. Springer, 2009.

[26] R. Rajkumar, I. Lee, L. Sha, and J. Stankovic, "Cyber-physical systems: The next computing revolution," in *Proceedings of the 47th Design Automation Conference*, DOI 10.1145/1837274.1837461, pp. 731–736, 2010.

[27] J. Sanchez, R. Caire, and N. Hadjsaid, "Ict and electric power systems interdependencies modeling," in *ETG Congress*, 2013, eTG-Fachbericht, vol. 139, pp. 7–12.

[28] S. F. Myhre, O. B. Fosso, P. E. Heegaard, O. Gjerde, and G. H. Kjolle, "Modeling interdependencies with complex network theory in a combined electrical power and ict system," in *International Conference on Probabilistic Methods Applied to Power Systems (PMAPS)*, DOI 10.1109/PMAPS47429.2020.9183667, pp. 1–6. IEEE, 2020.

[29] W. Zhu and J. V. Milanović, "Cyber-physical system failure analysis based on complex network theory," in *IEEE EUROCON 2017 -17th International Conference on Smart Technologies*, DOI 10.1109/EUROCON.2017.8011177, pp. 571–575, 2017.

[30] X. Gao, M. Peng, C. K. Tse, and H. Zhang, "A stochastic model of cascading failure dynamics in cyber-physical power systems," *IEEE Systems Journal*, vol. 14, DOI 10.1109/JSYST.2020.2964624, no. 3, pp. 4626–4637, 2020.

[31] X. Gao, X. Li, and X. Yang, "Robustness assessment of the cyber-physical system against cascading failure in a virtual power plant based on complex network theory," *International Transactions on Electrical Energy Systems*, vol. 31, DOI 10.1002/2050-7038.13039, no. 11, pp. 1–27, 2021.

[32] W. Zhu and J. V. Milanovic, "Assessment of the robustness of cyber-physical systems using small-worldness of weighted complex networks," *International Journal of Electrical Power and Energy Systems*, vol. 125, DOI 10.1016/j.ijepes.2020.106486, p. 106486, 2021.

[33] H. Pan, H. Lian, C. Na, and X. Li, "Modeling and vulnerability analysis of cyber-physical power systems based on community theory," *IEEE Systems Journal*, vol. 14, DOI 10.1109/JSYST.2020.2969023, no. 3, pp. 3938–3948, 2020.

[34] J. Dai, Z. Yao, G. Zhang, G. Liu, R. Dai, and Z. Wang, "Graph computing-based real-time network topology analysis for power system," in *IEEE Power and Energy Society General Meeting*, DOI 10.1109/PESGM40551.2019.8973614. IEEE, 2019.

[35] X. Liu, D. Wang, L. Xu, Q. Guo, Y. Huang, and Z. Wu, "Graph database and graph computing for cyber-physical power systems," in *IEEE Conference on Energy Internet and Energy System Integration (EI2)*, DOI 10.1109/EI2.2018.8581924, pp. 1–5, 2018.

[36] W. Di and Q. Guo, "Feasibility analysis and application of graph processing in gauss and newton-raphson power flow calculation," pp. 1–6, 2017.

[37] S. Xin, Q. Guo, H. Sun, B. Zhang, J. Wang, and C. Chen, "Cyber-physical modeling and cyber-contingency assessment of hierarchical control systems," *IEEE Transactions on Smart Grid*, vol. 6, DOI 10.1109/TSG.2014.2387381, no. 5, pp. 2375–2385, 2015.

[38] X. Gao, M. Peng, and C. K. Tse, "Cascading failure analysis of cyber physical power systems considering routing strategy," *IEEE Transactions on Circuits and Systems II: Express Briefs*, DOI 10.1109/TCSII.2021.3071920, 2021.

[39] H. Liu, X. Chen, L. Huo, Y. Zhang, and C. Niu, "Impact of inter-network assortativity on robustness against cascading failures in cyber–physical power systems," *Reliability Engineering & System Safety*, vol. 217, DOI 10.1016/j.ress.2021.108068, p. 108068, 2022.

[40] Y. Xue, M. Li, J. Luo, M. Ni, Q. Chen, and T. Yi, "Modeling method for coupling relations in cyber physical power systems based on correlation characteristic matrix," *Dianli Xitong Zidonghua/Automation of Electric Power Systems*, vol. 42, DOI 10.7500/AEPS20170705006, pp. 11–19, 01 2018.

[41] Y. Wang, Q. Chen, T. Hong, and C. Kang, "Vulnerability assessment of electrical cyber-physical systems against cyber attacks," *Applied Sciences*, vol. 8, DOI 10.3390/app8050768, no. 5, p. 768, 2018.

[42] Q. Zhou, J. Davidson, and A. Fouad, "Application of artificial neural networks in power system security and vulnerability assessment," *IEEE Transactions on Power Systems*, vol. 9, DOI 10.1109/59.317570, no. 1, pp. 525–532, 1994.

[43] Z. Xu, Y. Ge, J. Cao, S. Yang, Q. Lin, and X. Zhou, "Robustness analysis of cyber-physical power system based on adjacent matrix evolution," in *2021 China Automation Congress (CAC)*, DOI 10.1109/CAC53003.2021.9727501, pp. 2104–2109, 2021.

[44] C. Wang, H. Sun, and X. Dong, "Analysis of power system vulnerability considering multiple disturbances corresponding to information and physics," *Journal of Physics: Conference Series*, vol. 1187, DOI 10.1088/1742-6596/1187/2/022048, no. 2, p. 022048, Apr. 2019. [Online]. Available: https://doi.org/10.1088/1742-6596/1187/2/022048

[45] A. K. Srivastava, T. A. Ernster, R. Liu, and V. G. Krishnan, "Graph-theoretic algorithms for cyber-physical vulnerability analysis of power grid with incomplete information," *Journal of Modern Power Systems and Clean Energy*, vol. 6, DOI 10.1007/s40565-018-0448-7, no. 5, pp. 887–899, 2018.

[46] R. Meyur, "A bayesian attack tree based approach to assess cyber-physical security of power system," in *2020 IEEE Texas Power and Energy Conference (TPEC)*, DOI 10.1109/TPEC48276.2020.9042529, pp. 1–6, 2020.

[47] X. Ji, B. Wang, D. Liu, G. Chen, F. Tang, D. Wei, and L. Tu, "Improving interdependent networks robustness by adding connectivity links," *Physica A: Statistical Mechanics and its Applications*, vol. 444, DOI https://doi.org/10.1016/j.physa.2015.10.010, pp. 9–19, 2016. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0378437115008560

[48] J. Ospina, V. Venkataramanan, and C. Konstantinou, "Cpes-qsm: A quantitative method toward the secure operation of cyber–physical energy systems," *IEEE Internet of Things Journal*, vol. 10, DOI 10.1109/JIOT.2022.3210402, no. 9, pp. 7577–7590, 2023.

[49] I. Sobol, "Global sensitivity indices for nonlinear mathematical models and their monte carlo estimates," *Mathematics and Computers in Simulation*, vol. 55, DOI https://doi.org/10.1016/S0378-4754(00)00270-6, no. 1, pp. 271–280, 2001, the Second IMACS Seminar on Monte Carlo Methods. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0378475400002706

[50] A. Saltelli, M. Ratto, T. Andres, F. Campolongo, J. Cariboni, D. Gatelli, M. Saisana, and S. Tarantola, *Global Sensitivity Analysis: The Primer*. Wiley, 2008.

[51] B. Iooss and P. Lemaître, "A review on global sensitivity analysis methods," 2014. [Online]. Available: https://arxiv.org/abs/1404.2405

[52] A. Saltelli, P. Annoni, I. Azzini, F. Campolongo, M. Ratto, and S. Tarantola, "Variance based sensitivity analysis of model output. design and estimator for the total sensitivity index," *Computer Physics Communications*, vol. 181, DOI 10.1016/j.cpc.2009.09.018, no. 2, pp. 259–270, 2010.

[53] Y. Gao, X. Xu, Z. Yan, H. Wang, J. Ping, B. Yang, and X. Guan, "Analytical probabilistic power flow and global sensitivity analysis of distribution systems based on gaussian mixture model of input-output variables," *IEEE Transactions on Power Systems*, vol. 39, DOI 10.1109/TPWRS.2023.3329197, no. 3, pp. 5283–5296, 2024.

[54] S. Peng, X. Lin, J. Tang, K. Xie, F. Ponci, and A. Monti, "A set of novel global sensitivity analysis indices for probabilistic static voltage stability assessment with correlated uncertainty sources," *IEEE Transactions on Power Systems*, vol. 39, DOI 10.1109/TPWRS.2023.3304384, no. 2, pp. 2543–2557, 2024.

[55] P. Mihal, M. Schvarcbacher, B. Rossi, and T. Pitner, "Smart grids co-simulations: Survey research directions," *Sustainable Computing: Informatics and Systems*, vol. 35, DOI https://doi.org/10.1016/j.suscom.2022.100726, p. 100726, 2022. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2210537922000610

[56] U. C. Nwaneto, Y. Liu, W. Du, F. K. Tuffner, Z. Chen, and H. Liu, "Improvement of the interface models of a per-phase phasor/emt co-simulation platform for studying transients and dynamics in distribution grids with ibrs," *IEEE Transactions on Smart Grid*, vol. 16, DOI 10.1109/TSG.2025.3592672, no. 6, pp. 4880–4893, 2025.

[57] T. Mîndra and A. M. Anghel, "Hybrid co-simulation framework for cyber-physical systems-based applications," in *2024 International Conference on Applied Mathematics Computer Science (ICAMCS)*, DOI 10.1109/ICAMCS62774.2024.00020, pp. 102–109, 2024.

[58] R. Wagle, L. N. H. Pham, G. Tricarico, P. Sharma, J. L. Rueda, and F. Gonzalez-Longatt, "Experiences in a cyber-physical co-simulation testbed development for a smart-er distribution network," in *2023 IEEE PES Conference on Innovative Smart Grid Technologies - Middle East (ISGT Middle East)*, DOI 10.1109/ISGT-MiddleEast56437.2023.10078722, pp. 1–5, 2023.

[59] Z. Wang, J. Wang, X. Duan, and D. Shi, "A coordinator-event-axis-based time synchronization strategy for cyber-physical power system co-simulation," *IEEE Transactions on Smart Grid*, vol. 15, DOI 10.1109/TSG.2023.3348191, no. 4, pp. 4090–4103, 2024.

[60] V. Venkataramanan, P. S. Sarker, K. S. Sajan, A. Srivastava, and A. Hahn, "Real-time federated cyber-transmission-distribution testbed architecture for the resiliency analysis," *IEEE Transactions on Industry Applications*, vol. 56, DOI 10.1109/TIA.2020.3023669, no. 6, pp. 7121–7131, 2020.

[61] L. Zhang, S. Li, L. Wihl, M. Kazemtabrizi, S. Q. Ali, J.-N. Paquin, and S. Labbé, "Cybersecurity study of power system utilizing advanced cps simulation tools," in *Proceedings of the 2019 PAC World Americas Conference, Raleigh, NC, USA*, pp. 19–22, 2019.

[62] Z. Liu, Q. Wang, and Y. Tang, "Design of a cosimulation platform with hardware-in-the-loop for cyber-attacks on cyber-physical power systems," *IEEE Access*, vol. 8, DOI 10.1109/ACCESS.2020.2995743, pp. 95 997–96 005, 2020.

[63] F. Alasali, N. El-Naily, W. Holderbaum, H. Y. Mustafa, A. AlMajali, and A. Itradat, "A hybrid physical and co-simulation modern adaptive power protection testbed for testing the resilience of smart grids under cyber-physical threats," *Energy Reports*, vol. 12, DOI https://doi.org/10.1016/j.egyr.2024.07.051, pp. 1655–1672, 2024. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2352484724004761

[64] J. M. Riquelme-Dominguez, F. Gonzalez-Longatt, A. F. S. Melo, J. L. Rueda, and P. Palensky, "Cyber-physical testbed co-simulation real-time: Normal and abnormal system frequency response," *IEEE Transactions on Industry Applications*, vol. 60, DOI 10.1109/TIA.2023.3342764, no. 2, pp. 2643–2652, 2024.

[65] T.-T. Nguyen, R. Kadavil, and H. Hooshyar, "A real-time cyber-physical simulation testbed for cybersecurity assessment of large-scale power systems," *IEEE Transactions on Industry Applications*, vol. PP, DOI 10.1109/TIA.2024.3457877, pp. 1–13, 2024.

[66] D. Henner and REN21, "Renewables 2021 global status report," 2021, online; accessed 2026-02-04. [Online]. Available: https://abdn.pure.elsevier.com/en/en/researchoutput/ren21(5d1212f6-d863-45f7-8979-5f68a61e380e).html

[67] I. Komusanac, G. Brindley, D. Fraile, and L. Ramirez, "Wind energy in europe 2021," 2022. [Online]. Available: https://proceedings.windeurope.org/biplatform/rails/active_storage/blobs/redirect/eyJfcmFpbHMiOnsibWVzc2FnZSI6IkJBaHBBZ2dFIiwiZXhwIjpudWxsLCJwdXIiOiJibG9iX2lkIn
WindEurope%20-%20Wind%20energy%20in%20Europe%20-%202022.pdf

[68] Y. Wang, "Modeling technique and vulnerability assessment of elecrical cyber physical system considering cyber attacks," Ph.D. dissertation, Zhejiang University, 2019.

[69] N. Kostyuk and Y. M. Zhukov, "Invisible digital front: Can cyber attacks shape battlefield events?" *Journal of Conflict Resolution*, vol. 63, DOI 10.1177/0022002717737138, no. 2, pp. 317–347, 2019.

[70] R. Dube and M. Castro, "Venezuela blackout plunges millions into darkness," The Wall Street Journal, 2019, online. [Online]. Available: https://www.wsj.com/articles/venezuela-blackout-stretches-across-country-closing-schools-and-businesses-11552053011

[71] Y. Liu, X. Yang, W. Wen, and M. Xia, "Smarter grid in the 5g era: A framework integrating power internet of things with a cyber physical system," *Frontiers in Communications and Networks*, vol. 2, DOI 10.3389/frcmn.2021.689590, pp. 1–14, 2021.

[72] X. Gao, M. Peng, C. K. Tse, and H. Zhang, "A stochastic model of cascading failure dynamics in cyber-physical power systems," *IEEE Systems Journal*, vol. 14, DOI 10.1109/JSYST.2020.2964624, no. 3, pp. 4626–4637, 2020.

[73] J. Sanchez, R. Caire, and N. Hadjsaid, "Ict and electric power systems interdependencies modeling," in *ETG-Fachbericht*, pp. 7–12, 2013.

[74] S. F. Myhre, O. B. Fosso, P. E. Heegaard, O. Gjerde, and G. H. Kjolle, "Modeling interdependencies with complex network theory in a combined electrical power and ict system," in *2020 International Conference on Probabilistic Methods Applied to Power Systems (PMAPS)*, DOI 10.1109/PMAPS47429.2020.9183667, 2020.

[75] W. Zhu, "Cyber-physical system failure analysis based on complex network theory," 2017, unpublished/technical note.

[76] D. J. Watts and S. H. Strogatz, "Collective dynamics of 'small-world' networks," *Nature*, vol. 393, pp. 440–442, 1998.

[77] X. Gao, X. Li, and X. Yang, "Robustness assessment of the cyber-physical system against cascading failure in a virtual power plant based on complex network theory," *International Transactions on Electrical Energy Systems*, vol. 31, DOI 10.1002/2050-7038.13039, no. 11, pp. 1–27, 2021.

[78] W. Di and G. Qinglai, "Feasibility analysis and application of graph processing in gauss and newton-raphson power flow calculation," 2017.

[79] Z. Li, Q. Guo, H. Sun, and J. Wang, "Coordinated transmission and distribution ac optimal power flow," *IEEE Transactions on Smart Grid*, vol. 9, DOI 10.1109/TSG.2016.2582221, no. 2, pp. 1228–1240, 2018.

[80] M. S. Sachdev and S. A. Ibrahim, "A modified newton raphson load flow technique and its use in simulating line and transformer outages," *IFAC Proceedings Volumes*, vol. 12, DOI 10.1016/S1474-6670(17)65295-9, no. 5, pp. 126–131, 1979.

[81] P. Echenique, J. Gómez-Gardeñes, and Y. Moreno, "Improved routing strategies for internet traffic delivery," *Physical Review E*, vol. 70, DOI 10.1103/PhysRevE.70.056105, no. 5, p. 056105, 2004.

[82] M. Ahmed and A. S. K. Pathan, "False data injection attack (fdia): an overview and new metrics for fair evaluation of its countermeasure," *Complex Adaptive Systems Modeling*, vol. 8, DOI 10.1186/s40294-020-00070-w, no. 1, 2020.

[83] M. Higgins, J. Zhang, N. Zhang, and F. Teng, "Topology learning aided false data injection attack without prior topology information," in *IEEE Power and Energy Society General Meeting*, DOI 10.1109/PESGM46819.2021.9638211, 2021.

[84] C. Gu, P. Jirutitijaroen, and M. Motani, "Detecting false data injection attacks in ac state estimation," *IEEE Transactions on Smart Grid*, vol. 6, DOI 10.1109/TSG.2015.2388545, no. 5, pp. 2476–2483, 2015.

[85] M. Du, L. Wang, and Y. Zhou, "High-stealth false data attacks on overloading multiple lines in power systems," *IEEE Transactions on Smart Grid*, vol. 14, DOI 10.1109/TSG.2022.3209524, no. 2, pp. 1321–1324, 2023.

[86] J. Zhang, Z. Chu, L. Sankar, and O. Kosut, "Can attackers with limited information exploit historical data to mount successful false data injection attacks on power systems?" *IEEE Transactions on Power Systems*, vol. 33, DOI 10.1109/TPWRS.2018.2818746, no. 5, pp. 4775–4786, 2018.

[87] Y. Zheng, Z. Yan, K. Chen, J. Sun, Y. Xu, and Y. Liu, "Vulnerability assessment of deep reinforcement learning models for power system topology optimization," *IEEE Transactions on Smart Grid*, vol. 12, DOI 10.1109/TSG.2021.3062700, no. 4, pp. 3613–3623, 2021.

[88] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Transactions on Information and System Security*, vol. 14, DOI 10.1145/1952982.1952995, no. 1, 2011.

[89] T. Yang, Y. Liu, and W. Li, "Attack and defence methods in cyber-physical power system," *IET Energy Systems Integration*, vol. 4, DOI 10.1049/esi2.12068, no. 2, pp. 159–170, 2022.

[90] S. Liu, X. P. Liu, and A. El Saddik, "Denial-of-service (dos) attacks on load frequency control in smart grids," in *2013 IEEE PES Innovative Smart Grid Technologies Conference (ISGT)*, DOI 10.1109/ISGT.2013.6497846, pp. 1–6, 2013.

[91] X. Li, C. Jiang, D. Du, W. Li, M. Fei, and L. Wu, "A novel state estimation method for smart grid under consecutive denial of service attacks," *IEEE Systems Journal*, vol. 17, DOI 10.1109/JSYST.2022.3171751, no. 1, pp. 513–524, 2022.

[92] K. Ding, X. Ren, and D. E. Quevedo, "Dos attacks on remote state estimation with asymmetric information," *IEEE Transactions on Control of Network Systems*, vol. 6, no. 2, pp. 653–666, 2019.

[93] K. Wang, C. Scoglio, and R. J. Thomas, "An electrical betweenness approach for vulnerability assessment of power grids," *Physica A: Statistical Mechanics and its Applications*, vol. 390, DOI 10.1016/j.physa.2011.07.031, no. 23–24, pp. 4692–4701, 2011.

[94] L. Cuadra, S. Salcedo-Sanz, J. Del Ser, S. Jiménez-Fernández, and Z. W. Geem, "A critical review of robustness in power grids using complex networks concepts," *Energies*, vol. 8, DOI 10.3390/en8099211, no. 9, pp. 9211–9265, 2015.

[95] A. Rostami, M. Mohammadi, and H. Karimipour, "Reliability assessment of cyber-physical power systems considering the impact of predicted cyber vulnerabilities," *International Journal of Electrical Power & Energy Systems*, vol. 147, DOI 10.1016/j.ijepes.2022.108892, p. 108892, 2023.

[96] T. Arslan, Y. M. Bulut, and A. A. Yavuz, "Comparative study of numerical methods for determining weibull parameters for wind energy potential," *Renewable and Sustainable Energy Reviews*, vol. 40, DOI 10.1016/j.rser.2014.08.009, pp. 820–825, 2014.

[97] M. Kuzlu, M. Pipattanasomporn, and S. Rahman, "Communication network requirements for major smart grid applications in han, nan and wan," *Computer Networks*, vol. 67, DOI 10.1016/j.comnet.2014.03.029, pp. 74–88, 2014.

[98] B. Liu, H. Wu, Q. Yang, and H. Zhang, "Random-enabled hidden moving target defense against false data injection alert attackers," *Processes*, vol. 11, DOI 10.3390/pr11020348, no. 2, p. 348, 2023.

[99] Scottish and Southern Energy plc, "From Targets to Action – SSE's Net Zero Transition Plan," Scottish and Southern Energy plc, Tech. Rep., Jun. 2025,

accessed: Sep. 8, 2025. [Online]. Available: https://www.sse.com/media/iwoduslk/net-zero-transition-report-2025.pdf

[100] M. Du, X. Liu, Z. Li, and H. Lin, "Robust mitigation strategy against dummy data attacks in power systems," *IEEE Transactions on Smart Grid*, vol. 14, DOI 10.1109/TSG.2022.3225469, no. 4, pp. 3102–3113, 2023.

[101] Y. Jiang, S. Wu, R. Ma, M. Liu, H. Luo, and O. Kaynak, "Monitoring and defense of industrial cyber-physical systems under typical attacks: From a systems and control perspective," *IEEE Transactions on Industrial Cyber-Physical Systems*, vol. 1, DOI 10.1109/TICPS.2023.3317237, pp. 192–207, 2023.

[102] R. Zeng, Y. Li, S. Hu, X. Shao, Y. Xu, X. Yang, and Y. Cao, "Edge resilient control for feeder automation system under hybrid attacks: A hybrid physical model-driven and data-driven approach," *IEEE Transactions on Smart Grid*, DOI 10.1109/TSG.2025.3581370, pp. 1–1, 2025.

[103] A. Ehsan and Q. Yang, "State-of-the-art techniques for modelling of uncertainties in active distribution network planning: A review," *Applied Energy*, vol. 239, DOI https://doi.org/10.1016/j.apenergy.2019.01.211, pp. 1509–1523, 2019. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0306261919302247

[104] D. Bian, M. Kuzlu, M. Pipattanasomporn, S. Rahman, and D. Shi, "Performance evaluation of communication technologies and network structure for smart grid applications," *IET Communications*, vol. 13, DOI 10.1049/iet-com.2018.5408, no. 8, pp. 1025–1033, 2019.

[105] M. Bessani, R. Z. Fanucchi, A. C. C. Delbem, and C. D. Maciel, "Impact of operators' performance in the reliability of cyber-physical power distribution systems," *IET Generation, Transmission & Distribution*, vol. 10, DOI https://doi.org/10.1049/iet-gtd.2015.1062, no. 11, pp. 2640–2646, 2016. [Online]. Available: https://ietresearch.onlinelibrary.wiley.com/doi/abs/10.1049/iet-gtd.2015.1062

[106] X. Wang, Q. Kang, X. Wei, L. Guo, and Z. Liang, "Resilience assessment and recovery of distribution network considering the influence of communication network," *International Journal of Electrical Power Energy Systems*, vol. 152, DOI https://doi.org/10.1016/j.ijepes.2023.109280, p. 109280, 2023. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S014206152300337X

[107] N. V. C. Goncalves, M. E. C. Bento, T. C. C. Fernandes, M. U. Cildoz, A. G. M. Moraco, A. P. Grilo-Pavani, and R. A. Ramos, "Identifying sensitive communication failure combinations for wide-area damping controllers," in *2022 IEEE Power & Energy Society General Meeting (PESGM)*, DOI 10.1109/PESGM48719.2022.9917071, pp. 1–5, Denver, CO, USA, 2022.

[108] F. Gao, J. Wang, and G. Li, "Integrated planning of active distribution networks considering cyber-physical coupling," *IET Generation, Transmission & Distribution*, vol. 16, DOI 10.1049/gtd2.12277, no. 5, pp. 887–897, 2022.

[109] P. Delcourt, M. Tushar, and A. K. Srivastava, "Time synchronization attack detection in unbalanced distribution systems," *IEEE Transactions on Smart Grid*, vol. 12, DOI 10.1109/TSG.2021.3054159, no. 4, pp. 3052–3062, 2021.

[110] S. Weng, D. Yue, J. Chen, X. Xie, and C. Dou, "Distributed resilient self-triggered cooperative control for multiple photovoltaic generators under denial-of-service attack," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 53, DOI 10.1109/TSMC.2022.3176460, no. 1, pp. 226–237, Jan. 2023.

[111] T. Ding, C. Li, C. Yan, F. Li, and Z. Bie, "A bilevel optimization model for risk assessment and contingency ranking in distribution system reliability evaluation," *IEEE Transactions on Power Systems*, vol. 35, DOI 10.1109/TPWRS.2020.2965294, no. 5, pp. 3803–3813, 2020.

[112] P. Kundur, *Power System Stability and Control*. McGraw-Hill, 1994.

[113] A. Yazdani and R. Iravani, *Voltage-Sourced Converters in Power Systems: Modeling, Control, and Applications*. Wiley-IEEE Press, 2010.

[114] W. Liu, W. Gu, P. Li, G. Cao, W. Shi, and W. Liu, "Non-iterative semi-implicit integration method for active distribution networks with a high penetration of distributed generations," *IEEE Transactions on Power Systems*, vol. 36, DOI 10.1109/TPWRS.2020.3003367, no. 1, pp. 438–450, 2021.

[115] D. Qiu, M. Liu, R. Zhang, T. Luo, A. Griffo, and X. Zhang, "Cyber-physical real-time digital simulation for cybersecurity analysis in microgrids," *IEEE Transactions on Industrial Cyber-Physical Systems*, vol. 3, DOI 10.1109/TICPS.2025.3569640, pp. 429–441, 2025.

[116] J. F. Kurose and K. W. Ross, *Computer Networking: A Top-Down Approach*, 8th ed. Pearson, 2021.

[117] H. Sheng and X. Wang, "Probabilistic power flow calculation using non-intrusive low-rank approximation method," *IEEE Transactions on Power Systems*, vol. 34, DOI 10.1109/TPWRS.2019.2896219, no. 4, pp. 3014–3025, 2019.

[118] M. Aien, M. Fotuhi-Firuzabad, and M. Rashidinejad, "Probabilistic optimal power flow in correlated hybrid wind–photovoltaic power systems," *IEEE Transactions on Smart Grid*, vol. 5, DOI 10.1109/TSG.2013.2293352, no. 1, pp. 130–138, 2014.

[119] Y. Xia and D. Tse, "Inference of link delay in communication networks," *IEEE Journal on Selected Areas in Communications*, vol. 24, DOI 10.1109/JSAC.2006.884022, no. 12, pp. 2235–2248, 2006.

[120] S. Wang, M. Yu, and X. Sun, "Robust H_∞ control for time-delay networked control systems with probability constraints," *IET Control Theory & Applications*, vol. 9, DOI 10.1049/iet-cta.2015.0143, no. 16, pp. 2482–2489, 2015.

[121] K. Demir, A. Sathiaseelan, M. Cristea, and J. Crowcroft, "Robust qos-aware communication in the smart distribution grid," *Computer Networks*, vol. 119, DOI 10.1016/j.comnet.2017.03.025, pp. 52–69, 2017.

[122] S. Kucherenko, S. Tarantola, and P. Annoni, "Estimation of global sensitivity indices for models with dependent variables," *Computer Physics Communications*, vol. 183, DOI 10.1016/j.cpc.2011.12.020, no. 4, pp. 937–946, 2012.

[123] T. A. Mara and S. Tarantola, "Variance-based sensitivity indices for models with dependent inputs," *Reliability Engineering & System Safety*, vol. 107, DOI 10.1016/j.ress.2011.08.008, pp. 115–121, 2012.

[124] W. Li, M. Ferdowsi, M. Stevic, A. Monti, and F. Ponci, "Cosimulation for smart grid communications," *IEEE Transactions on Industrial Informatics*, vol. 10, DOI 10.1109/TII.2014.2338740, no. 4, pp. 2374–2384, 2014.

[125] L. Ren, Y. Qin, B. Wang, P. Zhang, P. B. Luh, and R. Jin, "Enabling resilient microgrid through programmable network," *IEEE Transactions on Smart Grid*, vol. 8, DOI 10.1109/TSG.2016.2589903, no. 6, pp. 2826–2836, 2017.

[126] Vestas Wind Systems A/S, "Third update on cyber incident," (Accessed: 2023). [Online]. Available: https://www.vestas.com/en/media/company-news/2021/third-update-on-cyber-incident-c3466518

[127] Reuters, "Satellite outage knocks out thousands of enercon's wind turbines," (Accessed: 2023). [Online]. Available: https://www.reuters.com/business/energy/satellite-outage-knocks-out-control-enercon-wind-turbines-2022-02-28/

[128] Z. Zhang, M. Liu, M. Sun, R. Deng, P. Cheng, D. Niyato, M.-Y. Chow, and J. Chen, "Vulnerability of machine learning approaches applied in iot-based smart grid: A review," *IEEE Internet of Things Journal*, vol. 11, DOI 10.1109/JIOT.2024.3349381, no. 11, pp. 18 951–18 975, 2024.

[129] G. Cao, W. Gu, C. Gu, W. Sheng, J. Pan, R. Li, and L. Sun, "Real-time cyber-physical system co-simulation testbed for microgrids control," *IET Cyber-Physical Systems: Theory & Applications*, vol. 4, no. 1, pp. 38–45, 2019.

[130] L. S. Melo, F. L. Tofoli, D. Issicaba, M. E. P. Monteiro, G. C. Barroso, R. F. Sampaio, and R. P. S. Leão, "Co-simulation platform for the assessment of transactive energy systems," *Electric Power Systems Research*, vol. 223, DOI https://doi.org/10.1016/j.epsr.2023.109693, p. 109693, 2023. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0378779623005825

[131] A. Suzuki, K. Masutomi, I. Ono, H. Ishii, and T. Onoda, "Cps-sim: Co-simulation for cyber-physical systems with accurate time synchronization," *IFAC-PapersOnLine*, vol. 51, DOI https://doi.org/10.1016/j.ifacol.2018.12.013, no. 23, pp. 70–75, 2018, 7th IFAC Workshop on Distributed Estimation and Control in Networked Systems NECSYS 2018. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2405896318335456

[132] K. Hopkinson, X. 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*, vol. 21, DOI 10.1109/TPWRS.2006.873129, no. 2, pp. 548–558, 2006.

[133] C.-C. Sun, J. Hong, and C.-C. Liu, "A co-simulation environment for integrated cyber and power systems," in *2015 IEEE International Conference on Smart Grid Communications (SmartGridComm)*, DOI 10.1109/SmartGridComm.2015.7436289, pp. 133–138, 2015.

[134] K. Mets, J. A. Ojea, and C. Develder, "Combining power and communication network simulation for cost-effective smart grid analysis," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 3, pp. 1771–1796, 2014.

[135] C. A. Thompson, "A study of numerical integration techniques for use in the companion circult method of transient circuit analysis," *ECE Technical Reports*, p. 297, 1992.

[136] L. Campanile, M. Gribaudo, M. Iacono, F. Marulli, and M. Mastroianni, "Computer network simulation with ns-3: A systematic literature review," *Electronics*, vol. 9, DOI 10.3390/electronics9020272, no. 2, 2020. [Online]. Available: https://www.mdpi.com/2079-9292/9/2/272

[137] P. Maloney, "Building a better microgrid with hardware in the loop," *Microgrid Knowledge White Paper Library*, 1996.

[138] 'Keysight'. [Online]. Available: https://www.keysight.com/us/en/product/SN100EXBA/exata-network-modeling.html

[139] M. Liu, C. Zhao, J. Xia, R. Deng, P. Cheng, and J. Chen, "Pddl: Proactive distributed detection and localization against stealthy deception attacks in dc micro-

grids," *IEEE Transactions on Smart Grid*, vol. 14, DOI 10.1109/TSG.2022.3188489, no. 1, pp. 714–731, 2023.

[140] N. Burnett, I. Stewart *et al.*, "The UK's plans and progress to reach net zero by 2050," UK Parliament Research Briefing, 2023, accessed: 2024-11-15. [Online]. Available: https://researchbriefings.files.parliament.uk/documents/CBP-9888/CBP-9888.pdf

[141] National Grid Electricity System Operator, "The ESO digitalisation strategy and action plan," Online, 2023, accessed: 2024-11-21. [Online]. Available: https://www.neso.energy/document/282631/download

[142] Scottish and Southern Energy plc, "Net zero transition plan 2023," Online, 2023, accessed: 2024-11-21. [Online]. Available: https://www.sse.com/media/32bch32o/net-zero-transition-plan-2023-final.pdf

[143] L. Zhang, S. Li, L. Wihl, M. Kazemtabrizi, S. Q. Ali, J.-N. Paquin, and S. Labbe, "Cybersecurity study of power system utilizing advanced CPS simulation tools," in *Proceedings of the 2019 PAC World Americas Conference*, pp. 19–22, Raleigh, NC, USA, 2019.

[144] A. R. Khan, S. M. Bilal, and M. Othman, "A performance comparison of open source network simulators for wireless networks," in *2012 IEEE International Conference on Control System, Computing and Engineering (ICCSCE)*, DOI 10.1109/ICCSCE.2012.6487111, pp. 34–38, Penang, Malaysia, 2012.

[145] Q. Wang, Z. Liu, and Y. Tang, "SCCO: A state-caching-based coagulation platform for cyber-physical power system evaluation," *IEEE Transactions on Smart Grid*, vol. 12, DOI 10.1109/TSG.2020.3032689, no. 2, pp. 1615–1625, Mar. 2021.

[146] C. Shum, W.-H. Lau, T. Mao, H. S.-H. Chung, K.-F. Tsang, N. C.-F. Tse, and L. L. Lai, "Co-simulation of distributed smart grid software using direct-execution simulation," *IEEE Access*, vol. 6, pp. 20 531–20 544, 2018.

[147] V. P. Tran, S. Kamalasadan, and J. Enslin, "Real-time modeling and model validation of synchronous generator using synchrophasor measurements," in *2013 North American Power Symposium (NAPS)*, DOI 10.1109/NAPS.2013.6666965, pp. 1–5, Manhattan, KS, USA, 2013.

[148] D. Qiu, M. Liu, and X. Zhang, "A power-communication co-simulation platform for real-time microgrid cyber security analysis," in *2024 International Conference on Artificial Intelligence of Things and Systems (AIoTSys)*, DOI 10.1109/AIoTSys63104.2024.10780642, pp. 1–6, Hangzhou, China, 2024.

[149] National Grid Electricity System Operator, "The ESO digitalisation strategy and action plan," https://www.neso.energy/document/282631/download, 2023, accessed: 2024-11-21.

[150] Scottish and Southern Energy plc, "Net zero transition plan 2023," https://www.sse.com/media/32bch32o/net-zero-transition-plan-2023-ffnal.pdf, 2023, accessed: 2024-11-21.

[151] G. Liang, S. R. Weller, J. Zhao, F. Luo, and Z. Y. Dong, "The 2015 ukraine blackout: Implications for false data injection attacks," *IEEE Transactions on Power Systems*, vol. 32, no. 4, pp. 3317–3318, 2016.

[152] Z. Yu, H. Gao, X. Cong, N. Wu, and H. H. Song, "A survey on cyber–physical systems security," *IEEE Internet of Things Journal*, vol. 10, DOI 10.1109/JIOT.2023.3289625, no. 24, pp. 21 670–21 686, 2023.

[153] P. S. Nair, S. K. Mandal, and N. Sharma, "Securing smart microgrids: A cybersecurity survey," in *2023 International Conference on Power Energy, Environment Intelligent Control (PEEIC)*, DOI 10.1109/PEEIC59336.2023.10452046, pp. 1318–1322, 2023.

[154] Y. Liu, L. Cheng, and D. Ye, "Stealthy false data injection attacks against the summation detector in cyber-physical systems," *IEEE Transactions on Industrial Cyber-Physical Systems*, vol. 2, DOI 10.1109/TICPS.2024.3446469, pp. 391–403, 2024.

[155] T. L. Nguyen, A. Alrashide, and O. Mohammed, "A cyber-physical platform to assess power system operation with communication network and heterogeneous controllers," *IEEE Transactions on Industry Applications*, vol. 60, DOI 10.1109/TIA.2024.3370689, no. 3, pp. 4776–4785, 2024.

[156] Y. Xue, J. Pan, Y. Geng, Z. Yang, M. Liu, and R. Deng, "Real-time intrusion detection based on decision fusion in industrial control systems," *IEEE Transactions on Industrial Cyber-Physical Systems*, vol. 2, DOI 10.1109/TICPS.2024.3406505, pp. 143–153, 2024.

[157] F. Mohammadi and M. Saif, "An intrusion detection and mitigation framework for automatic generation control systems," *IEEE Transactions on Industrial Cyber-Physical Systems*, vol. 2, DOI 10.1109/TICPS.2024.3452681, pp. 412–421, 2024.

[158] Y. Jiang, S. Wu, R. Ma, M. Liu, H. Luo, and O. Kaynak, "Monitoring and defense of industrial cyber-physical systems under typical attacks: From a systems and control perspective," *IEEE Transactions on Industrial Cyber-Physical Systems*, vol. 1, DOI 10.1109/TICPS.2023.3317237, pp. 192–207, 2023.

[159] S. Wu, Q. Wang, Q. Chen, C. Yu, and Y. Tang, "Cyber-physical integrated planning of distribution networks considering spatial-temporal flexible resources," *Protection and Control of Modern Power Systems*, vol. 9, DOI 10.23919/PCMP.2023.000316, no. 3, pp. 142–156, 2024.

[160] J. Liu, J. Vatn, and S. Yin, "A case study for enhancing maintenance of cyber-physical systems with digital twin," *IEEE Transactions on Industrial Cyber-Physical Systems*, vol. 2, DOI 10.1109/TICPS.2024.3485038, pp. 597–605, 2024.

[161] F. Sangoleye, J. Johnson, and E. Eleni Tsiropoulou, "Intrusion detection in industrial control systems based on deep reinforcement learning," *IEEE Access*, vol. 12, DOI 10.1109/ACCESS.2024.3477415, pp. 151 444–151 459, 2024.

[162] R. Huang and Y. Li, "Adversarial attack mitigation strategy for machine learning-based network attack detection model in power system," *IEEE Transactions on Smart Grid*, vol. 14, DOI 10.1109/TSG.2022.3217060, no. 3, pp. 2367–2376, 2023.

[163] M. Parashar, A. Poonia, and K. Satish, "A survey of attacks and their mitigations in software defined networks," in *2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, DOI 10.1109/ICCCNT45670.2019.8944621, pp. 1–8, 2019.

[164] R. Wagle, G. Tricarico, P. Sharma, C. Sharma, J. L. Rueda, and F. Gonzalez-Lonzatt, "Cyber-physical co-simulation testbed for real-time reactive power control in smart distribution network," in *2022 IEEE PES Innovative Smart Grid Technologies - Asia (ISGT Asia)*, DOI 10.1109/ISGTAsia54193.2022.10003553, pp. 11–15, 2022.

[165] Y. Shuai, Y. Zhang, F. Liu, X. Qiao, Y. Xiong, and Y. Zeng, "Co-simulation of power grid, information network and transportation network simulation system," in *2022 IEEE 2nd International Conference on Software Engineering and Artificial Intelligence (SEAI)*, DOI 10.1109/SEAI55746.2022.9832036, pp. 199–203, 2022.

[166] H. Zhu, L. Xu, Z. Bao, Y. Liu, L. Yin, W. Yao, C. Wu, and L. Wu, "Secure control against multiplicative and additive false data injection attacks," *IEEE Transactions on Industrial Cyber-Physical Systems*, vol. 1, DOI 10.1109/TICPS.2023.3293789, pp. 92–100, 2023.

[167] Y. Yu, G.-P. Liu, Y. Huang, and J. M. Guerrero, "Coordinated predictive secondary control for dc microgrids based on high-order fully actuated system approaches," *IEEE Transactions on Smart Grid*, vol. 15, no. 1, pp. 19–33, 2023.

[168] W. Li, M. Ferdowsi, M. Stevic, A. Monti, and F. Ponci, "Cosimulation for smart grid communications," *IEEE Transactions on Industrial Informatics*, vol. 10, no. 4, pp. 2374–2384, 2014.

[169] S. Pohekar and M. Ramachandran, "Application of multi-criteria decision making to sustainable energy planning—a review," *Renewable and Sustainable Energy Reviews*, vol. 8, DOI https://doi.org/10.1016/j.rser.2003.12.007, no. 4, pp. 365–381, 2004. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1364032104000073

[170] Quarbz Info Systems, "Typhoon HIL602+: Real-time emulator, model: HIL 602+, technical specifications," https://quarbz.com/Typhoon-HIL602-Brochure.pdf, n.d., accessed: 2025-04-14.

[171] G. Migoni, E. Kofman, and F. Cellier, "Quantization-based new integration methods for stiff ordinary differential equations," *SIMULATION*, vol. 88, DOI 10.1177/0037549711403645, no. 4, pp. 387–407, 2012. [Online]. Available: https://doi.org/10.1177/0037549711403645

[172] M. Liu, Z. Chu, and F. Teng, "Cyber recovery from dynamic load altering attacks: Linking electricity, transportation, and cyber networks," *IEEE Transactions on Information Forensics and Security*, vol. 20, DOI 10.1109/TIFS.2025.3553079, pp. 3862–3876, 2025.

[173] M. Liu, C. Zhao, Z. Zhang, and R. Deng, "Explicit analysis on effectiveness and hiddenness of moving target defense in ac power systems," *IEEE Transactions on Power Systems*, vol. 37, DOI 10.1109/TPWRS.2022.3152801, no. 6, pp. 4732–4746, 2022.