Novel cross-domain analysis of cyber-physical power systems using enhanced modelling and simulation techniques

A Thesis Submitted for the Degree of Doctor of Philosophy

By

Al Hussein Dabashi

Department of Electronic and Electrical Engineering, Brunel University London

2025

Declaration of Authorship

I, Al Hussein Dabashi, hereby affirm that the material contained within this thesis has not been previously submitted for any other academic award and is in compliance with the University's guidelines and regulations for research.

Additionally, I certify that all the work presented in this thesis is my own original work and that any assistance received in conducting the research and composing the thesis has been appropriately acknowledged and cited.

Signature

Al Hussein Dabashi
January 2025

Abstract

The modern power grid demands advanced modelling and simulation methods to address its evolving nature and increasing complexity. A critical focus is the application of cyber-physical systems (CPS) theory, especially with the rise of 5G, smart inverter-based resources (IBRs) and the prevalence of extreme weather events and cyber incidents. Research in cyber-physical power systems (CPPS) is pivotal for enhancing grid reliability and resiliency by enabling for the design and analysis of future grid-applicable cyber technologies.

While power system and communication network simulators suffice in their respective domains, integrated analysis is required. Consequently, this thesis proposes a whole-system graph-based CPPS model that links reduced power systems with abstracted communication networks, enabling cross-domain analysis. A novel Cyber Node Importance Index (CNII) assesses the criticality of cyber nodes by considering factors such as cascading failures and centrality measures. The CNII is applied on a GB-based CPPS model, demonstrating its applicability in identifying vulnerabilities and informing mitigation strategies for real and large infrastructure.

This thesis further details a methodology for the conversion of power system models from offline to real-time to enable real-time testing and dynamic CPPS analysis under communication contingencies. Also, the architecture of a real-time testbed is proposed. This testbed aims to evaluate CPPS resilience to cyberattacks and communication disruptions, integrating power system simulation, communication emulation, control schemes and industrial control system (ICS) protocols.

Key contributions of the thesis focus on improvements in taxonomy, vulnerability analysis, offline to real-time power system model conversion and real-time testbed design, collectively advancing CPPS modelling and simulation approaches.

Acknowledgements

I direct ultimate praise to Allah SwT, who surrounded me with supportive people and eased my PhD journey, enabling an achievement I once deemed unthinkable.

I want to give major thanks and show gratitude to my loving Mother and Father, whom this thesis is dedicated towards, and who have provided continuous encouragement, comfort and support throughout this PhD Journey.

My sincerest thanks to Professor Xin Zhang for believing in me and selecting me in late 2020 to pursue this life-changing path of learning and growth.

Major thanks to Professor Gareth Taylor who subsequently became my principal supervisor and was instrumental to my progress and successful completion. Professor constantly used his leadership and experience to support me. Professor gave me much needed firm-grounding and clear direction, as well as self-belief during periods of anxiousness. I am forever thankful to his committed support.

Major thanks to Dongmeng Qiu, Dr. Peter Imris and Chris Genganantha who were also significantly helpful to my progress by collaborating on publication ideas and assisting in the practical tasks and experiments.

Major thanks to my colleagues and staff as well as loved family and friends for their genuine support and who motivated me to last until the bitter-sweet end.

I would also like to express my gratitude towards the funders of this project: UK Engineering and Physical Sciences Research Council (EPSRC), High Voltage Substation Services Ltd (HVSS) and Brunel University of London.

"Knowledge will only grant you some of it, if you give it your all"

Contents

List of Figures

List of Tables

List of Abbreviations

AI ..... Artificial Intelligence

AMI ..... Advanced Metering Infrastructure

AoI ..... Age of Information

API ..... Application Programming Interface

BT 21CN ..... British Telecom's 21st Century Network

CCS ..... Centralised Control Scheme

CIM ..... Common Information Model

CNII ..... Cyber Node Importance Index

CNS ..... Communication Network Simulator

CPES ..... Cyber-Physical Energy Systems

CPPS ..... Cyber-Physical Power Systems

CPS ..... Cyber-Physical Systems

CSVC ..... Coordinated Secondary-Voltage Control

DER ..... Distributed Energy Resources

DOS ..... Denial of Service

DUT ..... Device Under Test

EMT ..... Electromagnetic Transients

FACTS ..... Flexible AC Transmission Systems

FDIA ..... False Data Injection Attack

FMI ..... Functional Mock-up Interface

GB TSRM ..... Great Britain Transmission System Reduced Model

HCS ..... Hierarchical Control System

HIL ..... Hardware-in-the-Loop

HLA ..... High-Level Architecture

ICS ..... Industrial Control System

ICT ..... Information and Communication Technology

IDS ..... Intrusion Detection System

IED ..... Intelligent Electronic Device

IoT ..... Internet of Things

LTE ..... Long-Term Evolution

MIMO ..... Multiple Input, Multiple Output

MITM ..... Man-In-The-Middle

ML ..... Machine Learning

NTP ..... Network Time Protocol

OLTA ..... Offline Transmission Analysis

P2P ..... Peer-to-Peer

PDC ..... Phasor Data Concentrator

PMU ..... Phasor Measurement Unit

PTP ..... Precision Time Protocol

QoS ..... Quality of Service

RES ..... Renewable Energy Sources

RMS ..... Root Mean Square

RT ..... Real-Time

RT ITL ..... Real-Time In-The-Loop

RTU ..... Remote Terminal Unit

SIL ..... Software-in-the-Loop

SISO ..... Single Input, Single Output

WAMPAC ..... Wide-Area Monitoring, Protection, and Control

Chapter 1

Introduction

1.1 Background

1.1.1 The Evolution of Electric Power Systems

An understanding of the evolution of electric power grids is essential to contextualise the necessity and challenges of cyber-physical modelling in modern power systems. Early power grids operated as isolated, electromechanical networks with minimal automation, rendering them fundamentally incompatible with today's digital control paradigms. By briefly examining their historical development, this section and section 1.1.1 highlights the technological milestones that gradually enabled, and now necessitate, cyber-physical integration. This perspective not only clarifies why early systems did not require such modelling but also underscores the accelerating role of digitalisation in shaping future grid resilience, efficiency, and complexity.

A Brief Appreciation for Early Electric Power Systems

At the very start of their emergence during the 1880s and 1890s, power systems operated in a local fashion and concerned supplying lighting. The inefficiencies in long-distance power transmission rendered broader connectivity impractical. The flow of power was one-way only, from generation to consumption, and this was the sole interaction within the system. Renewable energy contribution, as known today, was non-existent initially and remained insignificant for some time, as it was still in its developmental stages and lacked widespread adoption. Traditional power systems focused exclusively on physical infrastructure, as cyber technologies had not yet emerged.

Advancements in transmission technologies were under research and development during this period, and the concept of a large, unified electrical grid capable of serving multiple regions on a national scale had not yet materialised. This changed with the advent of AC technology in the 1890s, which proved effective for transmitting power over larger distances and safe for consumer use. Consequently, country-wide transmission networks, consisting of large pylons and long cables, were planned and constructed, connecting many power stations to consumers and various manufacturing industries. This transition marked the adoption of a centralised topology, where

fewer but larger power stations played a dominant role in energy production.

With regards to network topology and energy sources, the early stages of electricity grids adopted a distributed approach, bearing resemblance to today's high penetration of distributed energy resources (DERs). In contrast, the period between these two eras saw the predominance of centralised topologies and unified transmission networks.

Nowadays, while larger power stations still play a vital role in energy production, the trend has shifted towards decreased reliance on these centralised facilities. This is evidenced by the sequential decommissioning of coal-fired power stations, for example, and a move towards smaller, often aggregated, renewable energy sources (RES). These changes reflect a return to a distributed approach, leveraging modern technological advancements to address contemporary energy needs. See Table 1.1 for a comparison between traditional and modern grids.

Modern Day Power Grids and the Future Smart Grid

The modern power system includes much more sophisticated and interconnected technologies to support Wide Area Monitoring, Protection and Control (WAMPAC). Advanced technologies are integrated and interconnectors across countries are increasingly prevalent. Two flowing aspects exist: power flow and information flow, both flowing bi-directionally to and fro their point of demand. Whilst energy flows mainly from generation sources to consumers and industry, power from DERs can flow in reverse direction towards another area which requires the demand. For example, residents with rooftop solar panels and small wind turbines can sell unneeded electricity back to their supplier.

Digital substations represent a significant advancement in the transition towards smart grids, offering enhanced reliability, efficiency, and flexibility in modern power systems. Unlike conventional substations, which rely on extensive copper wiring for connections between primary equipment (such as current transformers and voltage transformers) and the control system, digital substations employ fibre-optic communication to transmit digital signals. This is achieved through the use of merging units that digitise measurements at the field level and transmit them via high-speed

Table 1.1: Comparison between traditional and modern smart power grids

Power System Aspect and Technology	Traditional Power Grid (Pre-2000s)	Modern Smart Grid (Post-2010s)	Explanation and Justification of Aspect
System Type	Electromechanical (e.g. relays, switches...etc.)	Digital smart grid (e.g. IEC 61850 substations, PMU-based monitoring...etc.)	Digitalisation allows faster response times, detailed analytics, and automated control.
System Topology	Centralised, reliance on few large power plants and transmission lines	Distributed, dependent on many smaller energy sources and more focused on distribution lines	Advances in distributed generation technologies enable efficient local energy production and consumption.
Generation Sources	Predominantly non-renewable (coal, gas, nuclear)	*Predominantly renewable (solar PV, wind, storage)	Driven by decarbonisation targets, feasbility of RES, lessen energy prices, and geopolitical reasons.
Generation Density and Size	Few large generators ($>$500MW)	High penetration of smaller generators (typically $<$100MW, down to residential-scale)	Smaller, distributed units reduce transmission losses and enable local resiliency.
Cable and Pylon Infrastructure	High-voltage transmission lines ($>$110kV)	Increased reliance on lower-voltage ($<$33kV) distribution and local grids	Reduction in transmission distances and improved efficiency for local generation integration.
Power Flow Direction	Uni-directional (from central generation to consumption)	Bi-directional flows enabled by power electronics and grid controls	Advances in inverter technology and grid management software allow two-way electricity flow.
Information Flow and Communication	SCADA based on serial communication, dedicated lines, copper cables...etc.	Real-time, bi-directional communication (IEC 61850, SCADA, IoT)	Real-time data communication is essential for dynamic control and enhanced grid responsiveness.
Cybersecurity and Resilience	Minimal due to low interdependence with cyber technology	High (Advanced cybersecurity frameworks, redundancy, self-healing networks)	Advanced grid architectures and digital tools significantly improve resilience but require strong cybersecurity measures.
Grid Monitoring Capability	Limited, slow response, low measurement rate (e.g. 1-2 samples per second)	Increasing deployment and real-time (PMUs, IoT sensors, advanced analytics)	Comprehensive monitoring improves real-time operational decisions and system reliability.
Consumer Participation	Passive end-user consumption	Active prosumer roles (demand response, V2G, local energy markets)	Smart meters, demand-side response, and EV technology actively engage consumers in grid operation.

*Note: This field and others in the table could vary slightly by country and region, for example in the UK, 2020 marked the first year in its history that electricity came predominantly from renewable energy [1].

Ethernet-based protocols, such as IEC 61850.

The use of fibre-optic cables significantly reduces the amount of wiring required,

leading to lower installation and maintenance costs and a simplified layout. The reduction in physical cabling also improves operational reliability and facilitates scalability, making it easier to upgrade or integrate new functionalities. Through these features, digital substations play a crucial role in enabling the real-time communication, automation, and data-driven control needed for the operation of smart grids.

Also usage behaviour and demand is accurately measured by advanced metering infrastructure (AMI), allowing consumers and industry access to useful information regarding their power usage. Close managing of the grid is possible due to advanced Wide Area Monitoring, Protection and Control (WAMPAC). This integration of Information and Communication Technologies (ICT) underscores the critical need for robust cybersecurity measures. The modern grid exemplifies a cyber-physical system (CPS) and is specifically referred to as a cyber-physical power system (CPPS).

A CPS describes a system with very close interaction and interdependency between its cyber and physical systems through integrations of computation, networking and physical processes. The physical system is controlled by computation and algorithms. Changes in the physical system causes changes of information in the cyber network. CPS typically consists of a collection of embedded systems which interact with the physical world using sensing instruments and actuators in a feedback loop [2]. Yohanandhan et al [3] defines a CPS as a" heterogeneous multidimensional system with integrated cyber part (control, computing, communication) to attain the characteristics of stability, robustness, efficiency, and reliability in physical systems applications". Besides smart grids, other examples of CPS are smart buildings, autonomous robotic systems, medical monitoring and industrial control systems. Figure 1.1 illustrates what the term cyber constitutes in this context.

In addition, modern power systems incorporate more RES each year. In the UK, power contribution from renewable electricity generation was 41.6% in the first quarter of 2021, and marginally higher than fossil fuel electricity generation [4]. Figure 1.2 shows the UK's electicity production by generation source. The graph shows the gradual decrease of reliance on coal and the increase of other sources such as gas and wind. The absolute demand of the UK since 1920 is shown in figure 1.3.

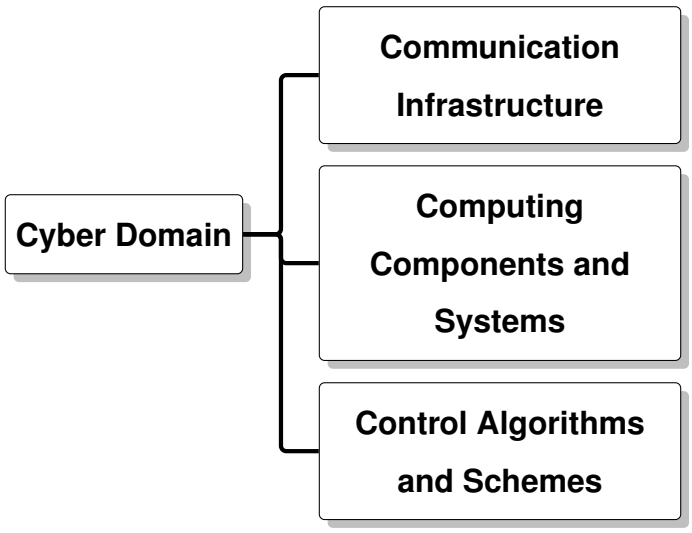

Figure 1.1: Three main parts of cyber domain

The ideal smart grid of the future envisions a system that fully leverages consumer behaviour and demand characteristics to optimise its operation with minimal human intervention. Equipped with advanced ICT, the grid would enable consumers to make informed decisions about their electricity usage. For instance, users could access real-time data on electricity prices, peak and off-peak times, and renewable energy availability, allowing them to schedule activities like operating washing machines or charging EVs at the most economical times. RES would dominate the electricity supply, with non-renewable sources relegated to strategic reserves and capacity markets to ensure system stability during unforeseen scenarios, namely system stress events (SSE). The vision aligns with research highlighting the importance of integrating demand-side flexibility and renewable energy to improve grid efficiency and sustainability [7], [8].

SSEs occur when faults or other disruptions prevent the available energy supply from meeting demand, necessitating the activation of strategic reserves. In the UK, the National Electricity System Operator (NESO) confirms such events during post-event analyses to identify gaps and enhance grid resilience. Strategic reserves, mainly comprising gas-fired power plants, are critical for maintaining system reliability during these high-demand periods [9]. Figure 1.4 illustrates GB's energy usage during October 2024, highlighting the growing contribution of RES alongside the persistent reliance on gas as a key component of the fuel mix. This trend underscores

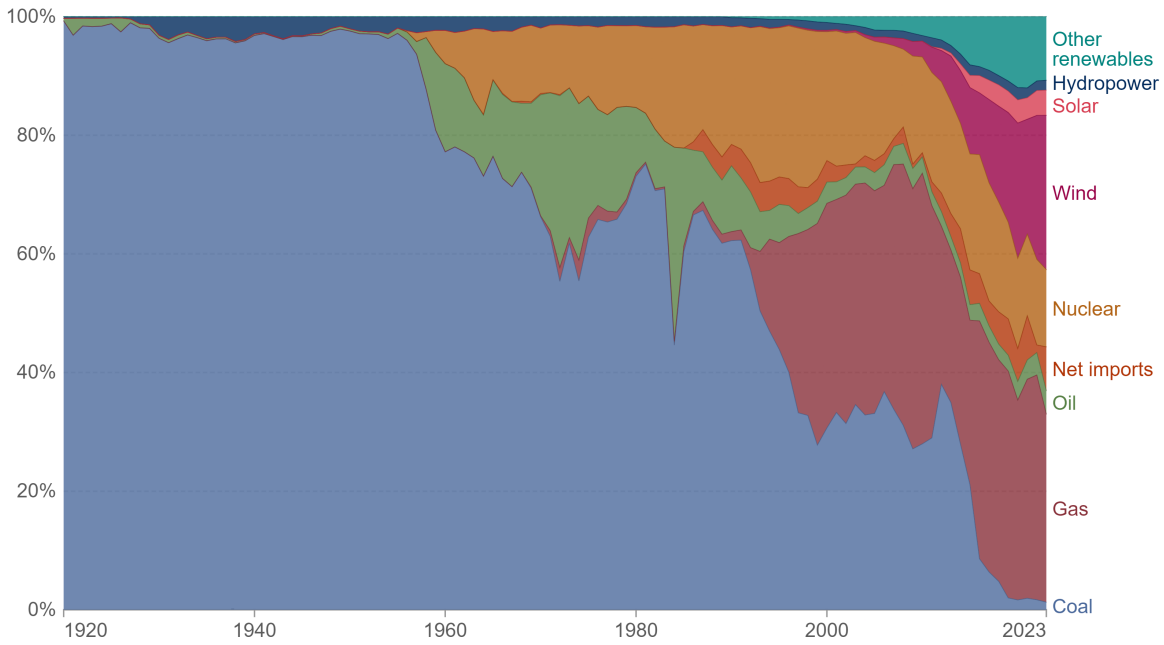

Figure 1.2: UK's electricity production by source [5]

the dual challenge of increasing renewable penetration while ensuring a stable and responsive backup system.

Furthermore, the decreasing reliance on fossil fuels, whilst adopting an increasing share of RES, could help contribute to lower and stabilised energy prices. This must be caveated however, with the weather's intermittency and uncontrollability, which could introduce volatility instead. Climate change exacerbates this point, posing the risk of increased frequency of weather extremes such as wind lulls, storms and heatwaves. Therefore, supporting technologies such as energy storage, demand response, grid interconnectors and dispatchable backup must also be deployed in a power grid to act in cooperation with RES to see those energy price benefits come to fruition. These advantages will benefit society, especially during periods of crisis, such as the ongoing UK energy crisis that began in September 2021 [10], [11]. This crisis saw a severe surge in gas and electricity prices, exceeding levels that many suppliers could pass on to customers, ultimately leading to the collapse of multiple energy companies [12], [13].

Another key aspect of smart grids is the adoption of EVs to support the grid through Vehicle-to-Grid (V2G) technology, which is continually expanding, alongside

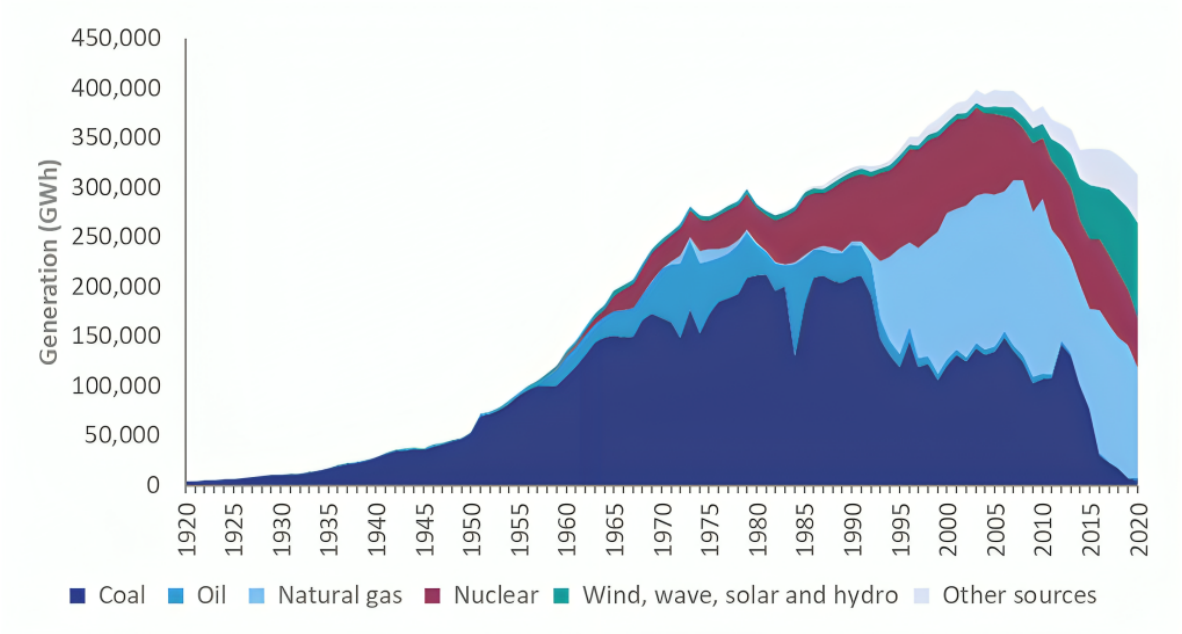

Figure 1.3: UK's absolute electricity generation by source (estimated) [6]

a parallel increase in the number of charging stations. V2G technology enables bi-directional energy flow between EVs and the power grid. During periods of high electricity demand, EVs can discharge stored energy back into the grid, helping to balance supply and demand while reducing reliance on peaking power plants. Conversely, during times of low demand or high renewable energy generation, EVs can recharge, functioning as distributed energy storage units. This capability not only strengthens grid stability and resilience but also facilitates the integration of renewable energy sources by providing a flexible buffer against their variability. Additionally, it offers economic benefits to EV owners through incentives for participating in V2G programs. Many EV-leading countries have either implemented or are planning deadlines to ban the sale of petrol and diesel vehicles in the near future.

Overall, a smart grid can be defined as an enhanced power system that constantly integrates and utilises new technologies to increase its reliability, efficiency, sustainability and security.

In an ideal smart grid, all physical power-related processes are automatically controlled by decisions made through computation and algorithms. In practicality, the aim is to reliably automate as many processes as possible with minimal human intervention. The typical cyber-physical measurement and control loop interaction of

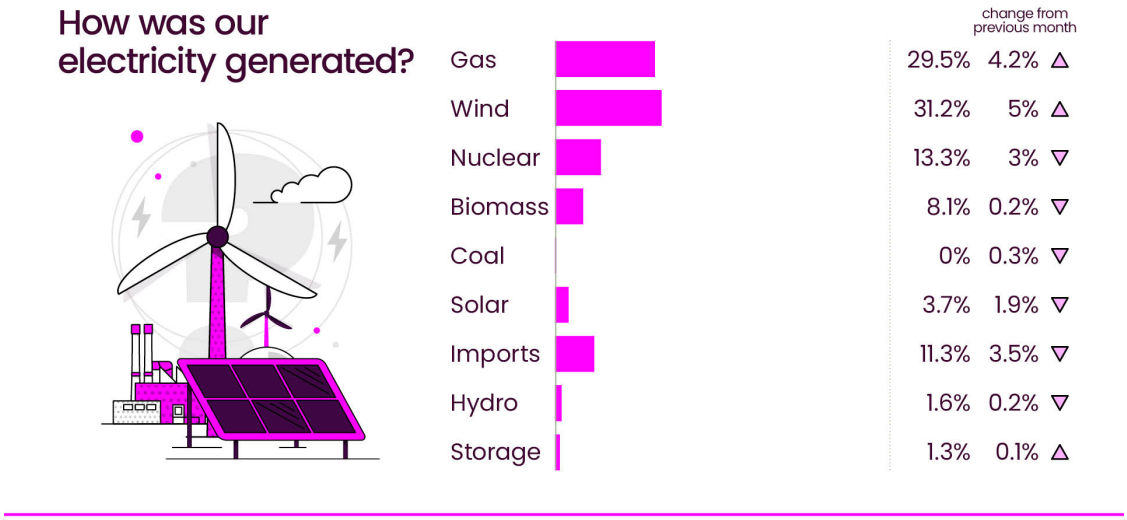

Figure 1.4: Great Britain's energy usage during October 2024 [14]

power grids, managed by a hierarchical control system (HCS), is illustrated in Figure 1.5:

The process is as follows, [15]:

1. The physical state variables of various power system components, such as voltage magnitudes, current flows, and power levels, are measured using advanced instruments and Phasor Measurement Units (PMUs). This is shown in Figure 1.5 on the left side under step number 1 in the orange circle.

2. These measurements are transmitted to the control centre through a robust communication infrastructure, which may include fibre optics, wireless networks, or satellite links.

3. At the control centre, algorithms and computational tools process the received data to analyse system stability, optimise operational parameters, and generate control commands.

4. The control commands are relayed back to field components, such as digital substations, power transformers, and Flexible AC Transmission Systems (FACTS), through the same communication infrastructure.

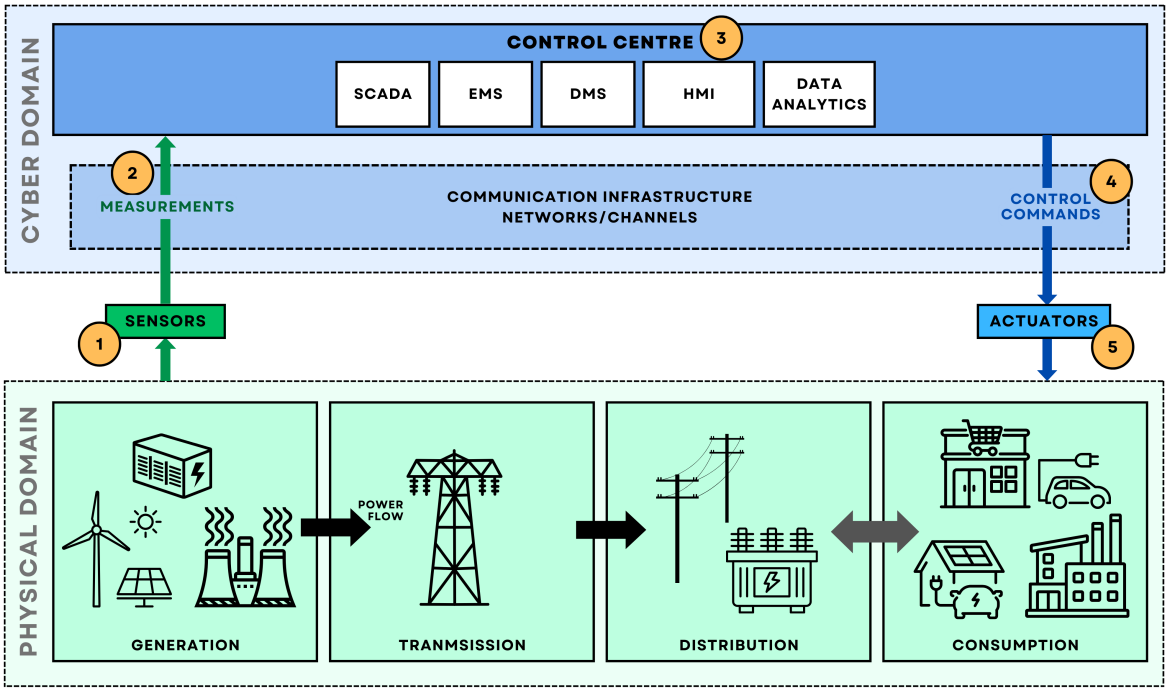

Figure 1.5: Typical cyber-physical measurement and control loop interaction of power grids

5. The power system components execute the received control commands, resulting in adjustments to their operational states. This feedback mechanism forms a closed-loop control system, ensuring dynamic stability and optimal performance of the power grid.

1.1.2 Phasor Measurement Units and Wide Area Monitoring

A PMU is a high-precision measuring instrument strategically installed in power systems to quantify voltage and current signal parameters by computing their phasors and associating these measurements with precise time stamps using GPS signals. PMUs are also referred to as synchrophasors due to their ability to synchronise measurements across geographically dispersed locations using a common time reference. The voltage and current signals are captured as analogue inputs from instrument transformers, specifically current transformers (CTs) and voltage transformers (VTs). The key signal parameters obtained include magnitude, phase angle, frequency, and the rate of change of frequency (RoCoF). These measurements enable

real-time insight into power system behaviour, with PMUs typically installed in transmission substations and generation plants and now commonly distribution substations also [16].

In AC power systems, sinusoidal waveforms are best described using phasors, which are complex-number representations of these waveforms defined by their amplitude and phase angle, as shown in Figure 1.6. A phasor is derived under the assumption of a known nominal frequency (usually 50 or 60 Hz), and it captures the steady-state properties of the waveform [17]. An electrical signal $v(t) = V\cos(\omega t + \phi)$ is thus represented as a rotating vector (phasor) with magnitude $V/\sqrt{2}$ and angular position ϕ relative to a common reference [18]. This abstraction simplifies the analysis and comparison of signals from different points in the grid, especially when synchronised by GPS.

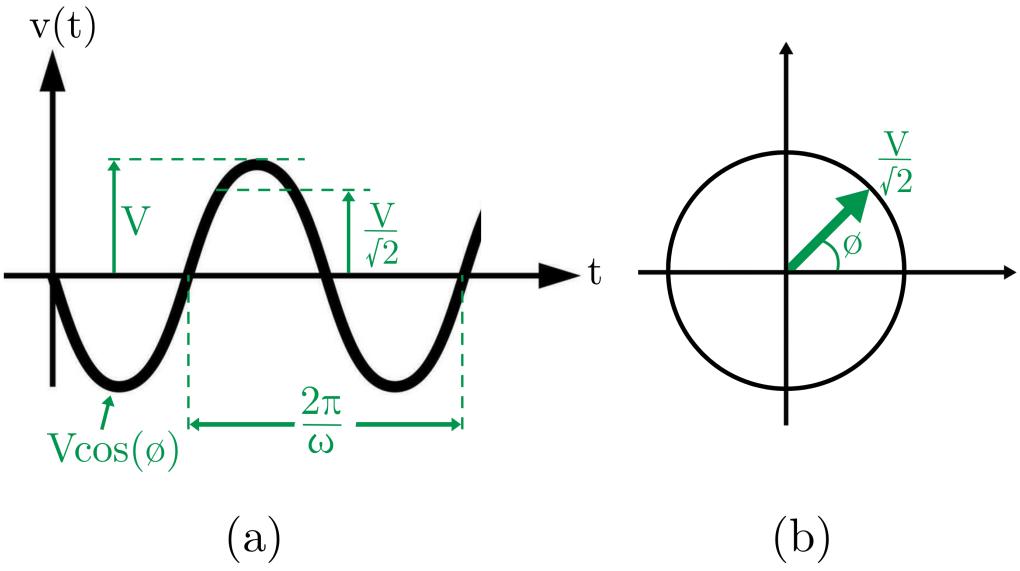

Figure 1.6: (a) Sinusoid of a waveform with parameters (b) phasor representation of an electrical waveform

PMUs are essential building blocks of WAMPAC systems, a critical technology of modern smart grids. The high-resolution time-stamped data that PMUs generate is transmitted to Phasor Data Concentrators (PDCs) for aggregation and processing. A PDC collects data from multiple PMUs, aligns it in time, and filters or processes it before passing it on to control centres or data storage systems. This enables a coherent, system-wide view of the electrical grid, facilitating real-time decision-

making. Wide Area Networks (WANs) provide the communication infrastructure that links PMUs, PDCs, and control centres. These networks must support high data throughput and low latency to ensure the integrity of the synchronised measurements. WANs often utilise dedicated fibre-optic lines, virtual private networks (VPNs), or utility-owned communication systems to maintain performance and cybersecurity standards [16].

The importance of WAMPAC in modern power systems stems from its ability to detect, diagnose, and respond to dynamic events such as faults, oscillations, voltage instability, and frequency deviations. Traditional SCADA systems operate with lower resolution and higher latency, typically providing data every 2–4 seconds. In contrast, PMUs can provide synchronised measurements at rates up to 60 samples per second, enabling real-time grid awareness and advanced protection schemes [19]. For instance, PMU data can be used to trigger wide-area protection relays, implement adaptive islanding schemes, and support real-time stability assessments, particularly in systems with high penetrations of renewable energy sources where rapid changes are frequent. Thus, PMUs, supported by PDCs and WANs, enable a holistic and time-coherent picture of grid behaviour across vast geographical areas. This capability is essential for ensuring grid resilience, improving operational reliability, and supporting the integration of decentralised and variable energy sources within cyber-physical power systems.

1.1.3 Simulation Technologies of Power Systems

A simulation represents a system through a mathematical and computational model that encapsulates its states, variables, and parameters, executed over time to facilitate experimentation and analysis. This approach enables a deeper understanding of system behaviour by replicating real-world dynamics under controlled conditions, providing a framework for evaluating operational strategies and decision-making processes [20]. Simulations are particularly valuable in complex systems where analytical solutions are intractable or where physical experimentation is impractical, expensive, or hazardous. By leveraging computational power, simulations allow for scenario testing, sensitivity analysis, and performance optimisation without the risks

associated with live system trials.

Prior to the construction of actual infrastructure, power networks and renewable energy projects are first designed and analysed in software tools, which enable engineers and consultants to conduct power system studies that ensure confidence in developing safe, reliable, and economically viable power systems. These analyses include the verification and optimisation of various power system aspects, such as the equipment selected, network configurations, stability margins, and fault response characteristics. Software tools are safe, cost-effective, and provide a controlled environment for retesting and running multiple simulations under varying conditions, such as different load profiles, generation mixes, and contingency scenarios. Offline Transmission Analysis (OLTA), for example, is the term used by the National Energy System Operator (NESO) of Great Britain (GB) as their main method for network design and planning, covering studies from long-term (up to 10 years ahead) down to short-term (day-ahead) operational procedures [21]. OLTA and similar offline simulation tools are essential for ensuring grid reliability, assessing compliance with regulatory standards, and mitigating risks before physical implementation.

In addition to offline simulation of power systems, real-time simulation is used extensively for developing and verifying real or virtual components, such as protection schemes, power electronic controllers, and grid-forming inverters, while connected to a virtual power network executed in real-time. Real-time simulation bridges the gap between offline studies and physical deployment by enabling Hardware-in-the-Loop (HIL) and Software-in-the-Loop (SIL) testing, where actual devices interact with simulated environments under realistic dynamic conditions. The virtual power network in this case is known as the 'plant' system in HIL terms, representing the electrical grid with sufficient fidelity to ensure accurate interaction with connected hardware. This approach is critical for validating control algorithms, testing protection relay coordination, and assessing system stability under transient conditions, such as faults or sudden generation losses.

However, whether in offline or real-time simulation, power system simulators typically do not contain models of systems relevant to the cyber domain, such as communication networks, data acquisition systems, or cyber-physical security mechanisms,

and vice versa [22]. To understand why this is the case, other than the separation of domains due to differing use cases and the nature of early power systems as described in Section 1.1.1, the main challenge in combining power system models with communication models must be understood. These challenges include differences in fundamental modelling techniques, as will be discussed in the next section.

1.1.4 Discrete-Time vs Discrete-Event Simulation

Dynamic simulation and discrete-event simulation represent two fundamentally different modelling techniques, each suited to the unique nature of the systems they model. In dynamic simulation, power systems are modelled as continuous time-varying systems, where system states evolve over time according to differential equations. Power systems are inherently dynamic due to the constant variation in generation, load demand, voltage and frequency. Dynamic simulation captures these continuous changes by solving the system's differential equations, which describe how quantities such as voltages, currents and generator speeds change over time. These simulations are crucial for studying system stability, fault response, load flows and transient behaviours under both normal and disturbed conditions. They provide insights into how a power system responds to disruptions, such as sudden changes in load, faults, or integration of intermittent RES. Because these systems exhibit time-dependent behaviour, time-stepping algorithms are typically used to simulate their evolution in steps of equal duration. This is known as discrete-time or fixed time-step simulation.

In contrast, discrete-event simulation is ideal for systems where changes occur at discrete points in time rather than continuously. Communication networks, for example, are modelled through discrete events like data packet transmissions, link failures, and message arrivals. Between these events, the state of the network remains unchanged. This feature allows discrete-event simulations to efficiently simulate large, complex communication systems by advancing directly from one event to the next, rather than advancing through time step by step. This method is particularly useful for studying packet-switched networks, where packets are transmitted between nodes, experiencing delays, queueing, and losses. The discrete-event model helps

simulate scenarios like network congestion, routing protocols, and quality of service (QoS), without the computational overhead associated with continuous time models.

This difference in fundamental modelling technique between that of power systems and communication networks constitutes the main challenge in developing adequate approaches to interdependent cross-domain analysis of CPPS.

1.1.5 Approaches to Realise Combined Analysis

Current Taxonomy of Approaches

According to Muller et al in 2018 [22], and shown in Figure 1.7, approaches to enable interdependent cross-domain analysis of CPPS can be classified into three groups:

1. General purpose tools (e.g. MATLAB): Disadvantages include lack of necessary modelling libraries and the available models are not sufficiently validated. Since they are not specialised they show inferior performance compared with specialised tools.

2. Co-simulation approaches: Specialised applications simulating each domain are coupled. This means the most adequate models are used for each domain however challenges and errors arise due to the need to synchronise the two (or more) applications properly at runtime and due to the lack of (application programming interfaces) APIs of each application.

3. Hardware-in-the-loop (HIL) approaches: Coupling a hardware device-under-test (DUT) for the whole or part of a domain with a simulation tool to allow for hardware and software testing under realistic conditions to ensure verification before implementation in real infrastructure. The disadvantages of HIL approaches are similar to co-simulation approaches; synchronisation and APIs. HIL also has the issue of guaranteeing the execution of the simulator in line with the real-time constraint of the DUT.

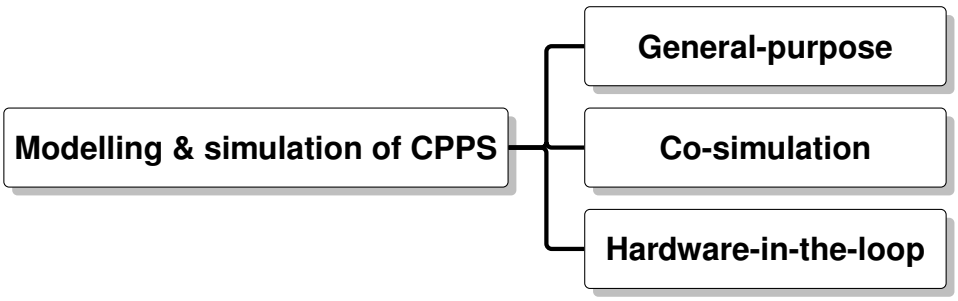

Figure 1.7: Three main categories of approaches to CPPS modelling and simulation according to [22]

Improved Taxonomy of Approaches

Based on the review of literature on this topic, this thesis proposes an improved nomenclature for the taxonomy of these three approaches to CPPS modelling and simulation, and they are: model-based, co-simulations and real-time in-the-loop (RT ITL) approaches as shown in Figure 1.8. The term 'model-based' is preferred over 'general-purpose-based' for two key reasons. First, 'general-purpose' can imply a scope that extends beyond the niche domain of CPPS, which focuses on highly specialised modelling and simulation requirements. Second, 'general-purpose' derives from the description of the tools used (e.g., MATLAB) rather than the methodological focus of the approach. In contrast, 'model-based' explicitly conveys that this approach is grounded in fundamental mathematical equations and abstractions, thereby aligning more closely with the theoretical underpinnings of CPPS analysis.

It could be argued that the term 'RT ITL' could also be derived from a description of their respective tools or frameworks to some extent, but this term is already entrenched in the literature and recognised. Their established usage across multiple domains, such as power systems, communication networks, and embedded systems, makes them less amenable to redefinition without risking confusion or fragmentation in the field. In contrast, terms like 'general-purpose-based' lack the same level of standardisation or widespread adoption in CPPS research. This flexibility allows for a more deliberate and justified refinement of terminology, particularly when the proposed alternative (model-based) more accurately reflects the methodological focus on abstracted mathematical representations rather than the choice of tools. Thus, while consistency in nomenclature is important, the priority here is to resolve

ambiguity where it exists, rather than disrupt well-established conventions that already serve their purpose effectively.

Similarly, the term real-time in-the-loop (RT ITL) is more appropriate than HIL, as it encompasses a broader range of subset configurations, including HIL, software-in-the-loop (SIL), and other emerging variants. While HIL is a well-known simulation technique, limiting the nomenclature to this term risks excluding SIL and other real-time simulation methodologies. Additionally, specialised terms like power hardware-in-the-loop (PHIL) or controller-in-the-loop (CIL), though technically falling under HIL, are often used independently in practice so by adopting the more inclusive 'RT ITL' term, this taxonomy avoids the misleading implication that the approach is confined to a single type of real-time simulation, thereby better reflecting the diversity of methodologies employed under this approach in CPPS research.

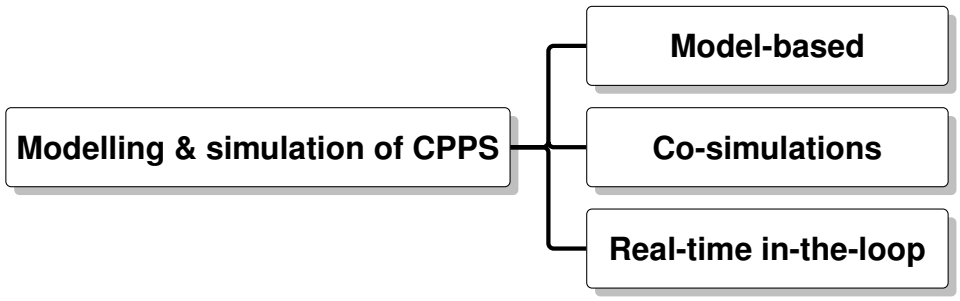

Figure 1.8: Three main categories of approaches according to this thesis

1.2 Research Motification

Communication systems in power grids are critical to maintaining the safe, stable, and reliable operation of the grid by supporting essential functions such as monitoring, protection, and control. These systems are deeply intertwined with the grid's performance, and any issues or failures in communication can significantly disrupt these functions, leading to potential operational failures. Since modern power grids are increasingly integrated with ICT systems, they function as a complex CPPS. Consequently, disruptions in communication can have far-reaching and potentially catas-

trophic impacts, including disrupting public, commercial and industrial functions of society.

One effective approach to studying and mitigating the negative impacts of communication failures in power systems is through simulation. Simulation provides a safe, practical, collaborative, and cost-effective means to analyse the effects of communication issues on power grid operations. By using simulation tools, researchers, scientists, and engineers can identify potential communication vulnerabilities, explore possible solutions, and test their effectiveness in a controlled environment. This iterative process not only helps in addressing existing communication challenges but also in anticipating future issues as the grid evolves.

As electric grids evolve into smarter, more advanced systems, their complexity increases, driven by the integration of new technologies and the expansion of grid infrastructure. These advancements make communication systems even more crucial, as they must handle larger volumes of data that need to be transmitted quickly across increasingly extensive networks. The successful implementation of these technologies depends on robust communication systems that can support the grid's expanded monitoring, protection, and control requirements. Power system communication simulation plays a vital role in this context by enabling the comprehensive analysis of new communication and ICT technologies within the grid. Through simulation, researchers can assess the feasibility, applicability, interoperability, and effectiveness of these technologies, ensuring that they can be seamlessly integrated into the future smart grid.

Despite the importance of this field, there is currently a lack of well-established power system communication simulators. Furthermore, many of the widely used power system simulators do not adequately model communication systems. This gap in available tools highlights the need for focused research in this area. One of the most promising approaches to achieving comprehensive analysis of both communication and power systems is through the integration of dedicated communication system simulators with power system simulators. This approach shows great potential for creating a robust research platform that can drive advancements in grid communication, ultimately contributing to the enhancement of power grid reliability

and resilience. By improving our understanding and management of grid communications, these research efforts will benefit society as a whole, ensuring the continued stability and efficiency of this critical infrastructure.

1.3 Aims and Objectives

This research aims to contribute to the field of CPPS modelling and simulation by enabling for cross-domain analysis of modern power grids. The research focuses on three key aspects of CPPS modelling and simulation: model-based approaches, co-simulation approaches, and RT ITL approaches. By focusing on these three key aspects, the research project aims to design and develop new methods and analysis techniques that enable both the power domain and the cyber domain to be considered in studies from reduced models to more detailed and realistic real-time models. To achieve this, the following list provides the objectives and goals of this thesis:

1. To discuss and present the background and motivation behind CPPS modelling and simulation, and the most important application areas thereof.
2. To review and investigate the current and latest state-of-the-art approaches and methodologies of CPPS modelling and simulation.
3. To categorise those approaches, thereby enhancing the understanding of the concepts and uncovering meaningful insights and trends.
4. To contribute to offline model-based approaches by designing and developing whole-system CPPS models and novel vulnerability analysis methods which considers parameters from both the power domain and the cyber domain.
5. The developed CPPS model and vulnerability assessment method should be applicable to and demonstrated on abstracted models of real power systems and communication networks, such as GB networks.
6. To advance RT ITL approaches by designing a unique testbed to study communication contingencies' impact on power system stability and resilience.
7. To advice on and suggest future research trends and paths in this field.

1.4 Contribution to Knowledge

The main contributions to knowledge, as presented in this thesis, can be summarised as follows:

- Comprehensive Literature Review: This thesis provides a thorough review of the current and latest state-of-the-art approaches as related to CPPS. The main contributions include the categorisation of the three main approaches to modelling and simulating CPPS: model-based approaches, co-simulation approaches and real-time in-the-loop based approaches. The strengths, limitations, challenges and gaps of these methodologies have been identified and discussed. The application of graph-theory for efficient and effective CPPS modelling has also been discussed.

- Model-Based Approach: This thesis develops a novel importance index for ordering the cyber-nodes of any graph-based CPPS model. The index includes parameters of power station failure, betweenness centrality and average shortest path time delay difference. This is tested and applied on two reduced models of real infrastructure networks; the UK's transmission system and the BT UK wide fibre optic-based communication network. The method for modelling the CPPS is detailed and for calculating the cyber-node importance index also. Discussion of how this contribution demonstrates its capability to identify critical nodes and inform mitigation strategies is included.

- Offline to Real-Time Model Conversion: This thesis details the modelling methodology of interfacing PowerFactory and ePHASORSIM software tools to enable for real-time ITL studies. An in-depth documentation and explanation of the challenges faced and the resolutions developed is presented, as well as detailed break-downs of important modelling and simulation files. This serves as a significant contribution by establishing a reference for future studies in this area employing the same methods.

- Real-time Testbed for Software-in-the-Loop Studies: Finally, a significant contribution of this thesis is the work in chapter 5 which focused on the design

and architecture of a real-time CPPS testbed. The testbed architecture integrates electrical and communication network models with real-time control schemes and ICS protocols, enabling detailed analysis of CPPS resilience under diverse conditions such as communication errors, cyberattacks and system disturbances. The current capabilities of the testbed have been detailed such as evaluating the system's behaviour during critical scenarios. Additionally, the testbed serves as a robust platform for testing new technologies, validating innovative control strategies, and exploring the interdependencies between power and communication layers. Recommendations from this chapter extend the applicability of the testbed to future scenarios, including renewable energy integration and advanced grid management systems.

The overall contributions of this thesis advance the understanding of CPPS and the practical capabilities of its evaluation methods by bridging the gap between power and communication systems through innovative modelling and simulation techniques. By developing tools and methodologies for assessing vulnerabilities and improving resilience, the research addresses critical challenges in ensuring the reliability of modern power systems. Furthermore, the creation of real-time platforms provides a foundation for experimental validation, supporting the integration of emerging technologies and enabling more dynamic system responses to threats and disturbances. These contributions not only respond to current challenges in CPPS but also establish a pathway for ongoing innovation in designing secure, resilient, and efficient energy systems for the future.

1.5 Thesis Outline

The research is organised into six chapters, and can be visualised in a simple manner by Figure . Chapter 1 outlines the motivations of the research presented in this thesis. The research has been conducted to investigate, design and develop novel modelling and simulation approaches for cyber-physical cross-domain analysis in the scope of electrical power systems and communication networks. Thus, the section contains important background information. The main aims and objectives of the re-

search are presented in section 1.3. Following the introductory chapter, the next four chapters include more details regarding the latest state-of-the-art research efforts, the theoretical background and the thesis objectives.

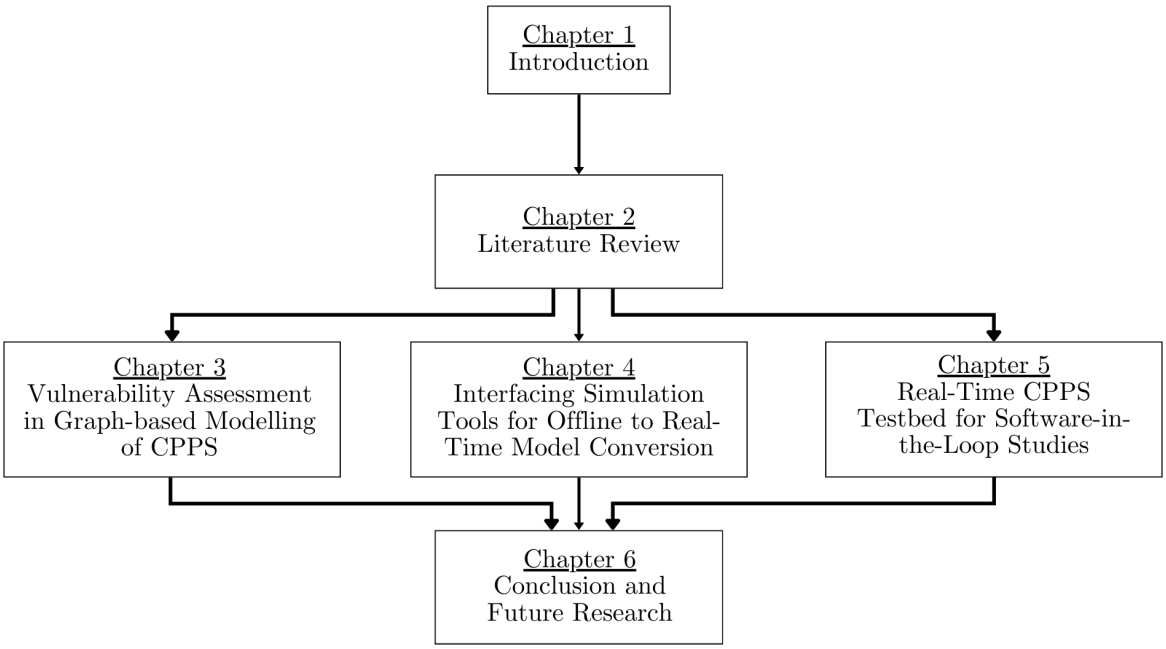

Figure 1.9: Organisation of the chapters of this thesis

In Chapter 2, the latest research and state-of-the-art approaches to the modelling and simulation techniques for cyber-physical domain analysis in the context of communication networks and electrical power systems is discussed. A common classification of the approaches in the literature is discussed whilst proposing an alternative improved classification grouping. The literature review is then organised according to this proposed alternative classification grouping.

Chapter 3 is focused on the model-based approach classification and provides the detailed study of a novel importance index methodology employed in CPPS vulnerability analysis. The proposed index considers cascading failure, betweenness centrality and the time delay of the shortest paths, which provides a more accurate representation of power systems. The index was tested on a cyber-physical model representation of the UK Grid and communication system. Subsequently, the method's enhanced accuracy and usefulness, along with its suitability for analysing cyber contingencies in graph-based CPPS models, is discussed.

Chapter 4 details the conversion of power system models from offline mode to real-time mode. The chapter details the interfacing technique between PowerFactory (an offline simulator by the company DIgSILENT) and ePHASORSIM (a real-time simulator by the company OPAL-RT) using the DGS export tool. The selected example power system model is a reduced model of NESO's 36 Bus System. Various issues and subsequent problem managements with the important XML file netlist is detailed.

Chapter 5 presents a detailed architecture of a real-time testbed for software-in-the-Loop Studies of CPPS. Three main hardware components were selected and justified, as well as the four main component concepts. The capability and research studies this testbed provides is suggested alongside future improvements for the testbed and for study and investigation scenarios as part of research suggestions.

Finally, in Chapter 6 the work presented in this thesis is summarised and the main contributions highlighted. Important methods in which this work can be expanded upon and the discussion of future trends is also discussed as part of the future research suggestions.

1.6 List of Publications

- **Dabashi, A. H.**, Qiu, D., Taylor, G., and Zhang, X., 2022, August. Determining Node Importance in Graph-Based Modelling of Cyber-Physical Power Systems. In *2022 57th International Universities Power Engineering Conference (UPEC)*. IEEE.

- Qiu, D., Zhang, R., **Dabashi, A. H.**, Zhou, Z., and Zhang, X. 2022, November. Cyber-Physical Contingency and Vulnerability Assessment using Double Power Flow Method. In *2022 12th IET International Conference on Advances in Power System Control, Operation and Management*. IET.

- In preparation: **Dabashi, A. H.**, Taylor, G., and Zhang, X. 2025, October. Innovative Techniques for Real-time Simulation of Cyber-Physical Energy and Power Systems. In *Electronics 2025*.

Chapter 2

Literature Review

2.1 Introduction

Building on the introductory text in Chapter 1 regarding the integration of electrical power system infrastructure with cyber technologies and the resulting need for cross-domain analysis, this chapter reviews the simulation approaches developed to enable such analysis. As mentioned, these approaches are categorised into three main types: model-based approaches, co-simulation approaches, and real-time approaches. These categories correspond to the structure of the subsequent sections of this chapter. It is worth noting that research efforts specifically dedicated to advancing modelling and simulation approaches for CPPS are fewer in number compared to the broader body of work addressing CPPS development as a whole. While the former focuses on the theory, tools, frameworks, and methodologies used to represent and analyse CPPS behaviour, the latter centres on applications such as control strategies, cybersecurity solutions, or operational enhancements, often using existing modelling platforms without contributing to their underlying development.

The model-based approach involves the use of fundamental mathematical formulations that represent both the power system and cyber domains. The theoretical aspect of this approach relies on models and definitions that capture the essential dynamics and interactions within each domain, while its practical implementation is typically realised using general-purpose software tools. This chapter outlines several prominent concepts and techniques within this category. A common example is the abstraction of power and communication networks using graph-theory and matrix-based methods, which appears frequently in the reviewed literature.

Co-simulation approaches, by contrast, depend on the integration of at least one, and more often two, domain-specific simulation tools. Typically, one tool represents the power system domain while the other the cyber domain. The central challenge in this approach is the programmatic interfacing of the simulators to manage the synchronisation of time steps and event data. This is critical to preserving the fidelity and accuracy of the simulation. While some commercial-off-the-shelf (COTS) simulators provide application programming interfaces (APIs), these are often not geared towards the challenge at hand, rendering such APIs insufficient for achieving precise synchronisation. As a result, researchers frequently develop custom scripts to bridge

the gap. More details and specific examples follow in this category's section.

Real-time simulation approaches make use of at least one high-fidelity, parallel-processing-based real-time simulator. These simulators present challenges similar to those encountered in co-simulation, but with the added complexity of interfacing with real hardware when applicable. Real-time testbeds are typically found in academic or research smart grid laboratory settings, with simulators from companies such as RTDS, OPAL-RT, and Typhoon HIL commonly used. These setups generally involve either real or virtual communication and control networks connected in-the-loop with a real-time simulator. Although rare, some research efforts have demonstrated the use of two real-time simulators in a single testbed. Due to the technical demands and the need for precision integration, real-time approaches, although the most accurate in resembling real CPPS behaviour, are widely recognised as the most difficult and time-intensive to develop.

The selection of a suitable simulation approach depends significantly on several practical considerations, including budget constraints, available skill levels, and specific research objectives. Model-based approaches, relying primarily on general-purpose software and mathematical abstractions, are the most accessible in terms of required expertise and associated costs, making them appropriate for preliminary studies or theoretical exploration. Conversely, co-simulation approaches demand greater technical proficiency, as researchers must effectively integrate multiple domain-specific software tools, thus increasing the complexity and potentially the financial requirements. Real-time approaches, offering the highest fidelity, require substantial investment not only in high-performance simulators and hardware but also in the specialised skills necessary for setting up, operating, and maintaining sophisticated testbeds. Consequently, researchers and institutions must carefully balance these factors when selecting their preferred method of CPPS simulation, ensuring that the chosen approach aligns with both their research aims and practical constraints.

2.2 Model-based Approaches: Employing Graph-based Methodologies

Model-based approaches for conducting CPPS analysis involve using abstracted and reduced models to represent the complex networks and interactions between physical power systems and cyber components, such as communication networks, control schemes, energy flow and information flow. These methodologies reduce the complexity of the actual system, allowing researchers to focus on key systems and interdependencies without excessive computational burdens. Common key words found in the literature review of model-based CPPS analysis include complex networks, hybrid modelling, graph-theory, information flow and energy flow. Figure 2.1 shows the specific modelling approaches that fall under model-based CPPS as mentioned by [3].

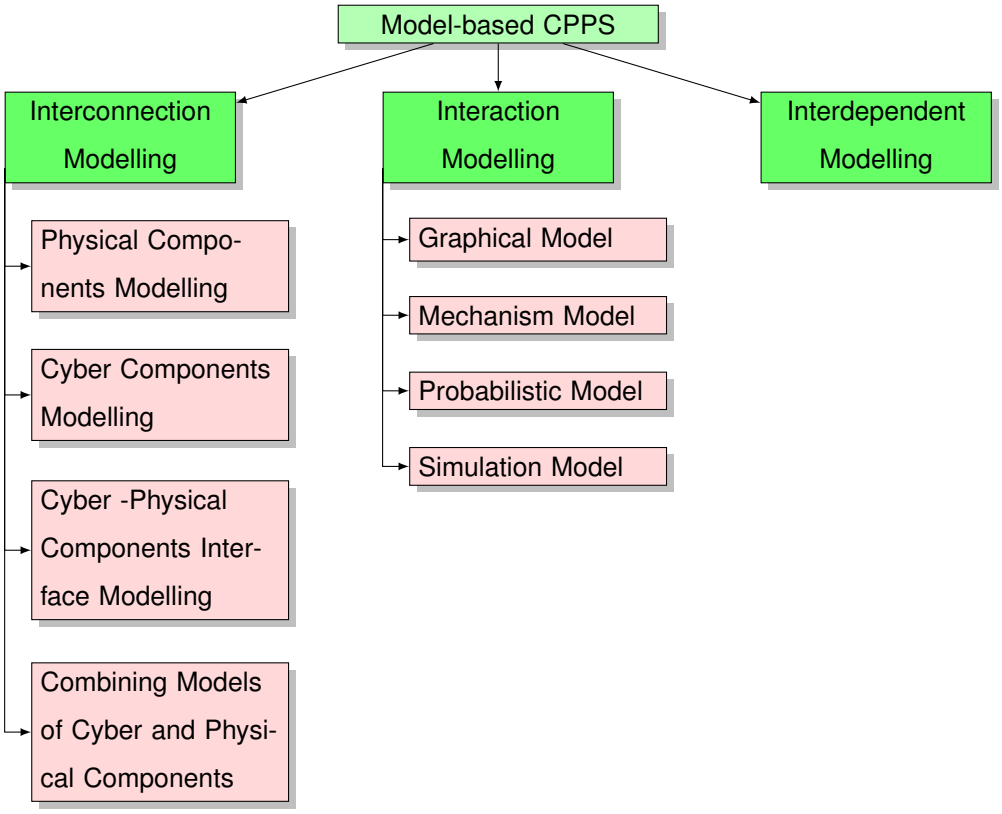

Figure 2.1: Approaches classified under model-based CPPS

In conducting CPPS analysis using model-based approaches, researchers of-

ten employ general-purpose simulation tools such as MATLAB or Simulink. These platforms offer flexibility and accessibility, enabling the creation of custom models to study specific cyber-physical interactions. However, while MATLAB and similar tools are versatile, they may lack specialized libraries, dedicated solvers, and validated models. As a result, these tools may not be fully optimised for accurate CPPS analysis and may show limitations in both performance and accuracy compared to specialized power system or communication network simulators, which are specifically designed for calculations within their respective domains [22].

2.2.1 Graphical Models for CPPS

In CPPS, electrical components such as generators, circuit breakers, protective relays, and loads are connected via transmission lines, while cyber components, such as routers, servers, switches, and control stations, are connected through communication networks. To monitor and control a CPPS, a typical assumption is that each physical component is to be integrated with a corresponding cyber component. State information from each component is transmitted to a remote control centre through a cyber network of routers, switches, and other communication infrastructure. Once received at the control centre, this information is processed, and a control signal is generated and sent back to controlled devices. Due to this close integration between the physical and cyber systems, the failure of any physical or cyber element could significantly impact each other.

Graph theory-based approaches are highly effective for analysing these interdependencies within CPPS. Due to the networking nature of both power systems and communications, they can be translated into mathematical graph models, representing their components, links and technical parameters. See Figure 2.2 for further approaches that fall under graphical models of CPPS according to [3].

A graph comprises a set of vertices V and edges E. In this context, physical power grid components are represented as vertices V_p, and transmission lines

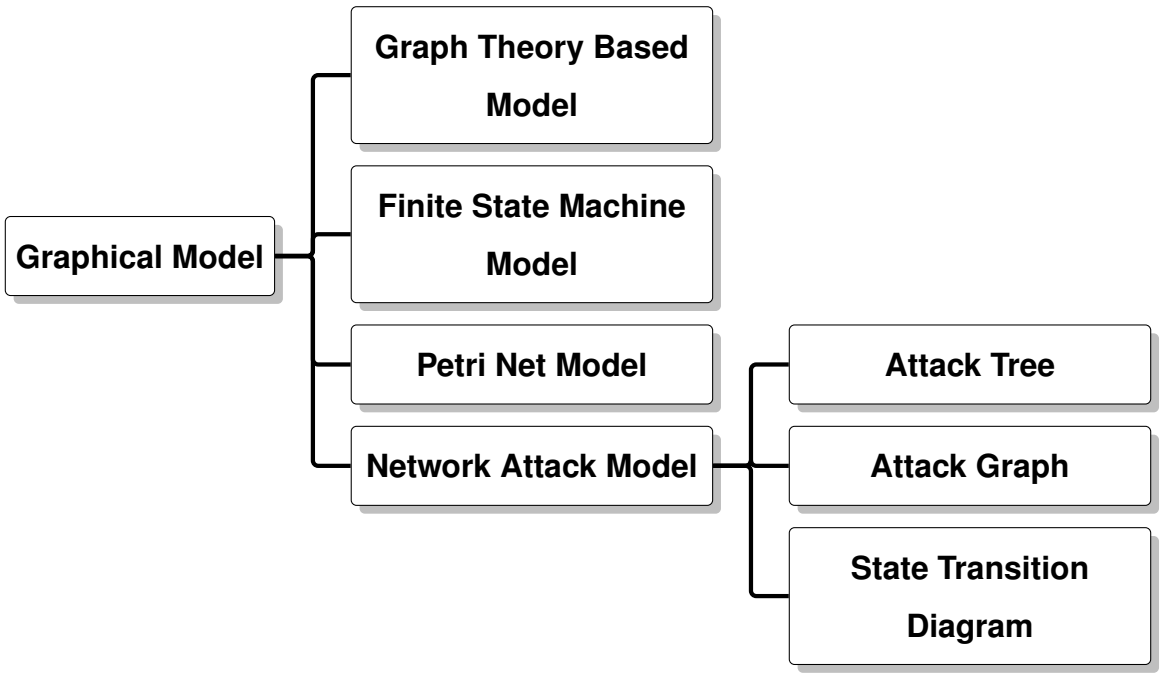

Figure 2.2: Further types of graphical modelling [3]

connecting them are represented as edges E_p, forming a directed, sparsely connected graph $G_p^D(V_p, E_p)$. Similarly, in the cyber network, components such as PMUs, routers and servers act as vertices V_c, with the wired or wireless connections between them forming edges E_c, resulting in a directed, sparsely connected graph $G_c^D(V_c, E_c)$.

Edges in the graph are represented with directional arrows to indicate positive power flow, P_{in}^i for $i \in \{1, 2\}$, from the head vertex V_{j}^{head} to the tail vertex V_{j}^{tail}. Here, $V_s \in \mathbb{R}^{N_s}$ and $V_t \in \mathbb{R}^{N_t}$ represent the source and sink vertices, respectively. In the cyber network, vertices serve as data nodes, with edges representing the information flow between them, indicated as I_{in}^i for $i \in \{1, 2\}$.

Power system contingencies, such as transmission line outages, are represented by removing edges in the graph G_p. Similarly, the removal of a vertex V_c in the graph G_c corresponds to a cyber node failure. The CPPS graphical model is represented as a directed topology graph, where physical and cyber system state variables are treated as "data nodes," and the information flow between the cyber and physical systems is captured as "information edges." This graph theory model can be integrated with a dynamic system model to analyse how cyber disturbances affect power system components as shown in Kundur et al [23].

2.2.2 Graph Computing and Graph Databases

CPPS systems become larger and more complex with developments and coupling between the physical and cyber side. The 2018 of Liu et al [24] introduces some graph computing systems and describes possible applications of graph systems to analyse CPPS problems. This paper also proposes a graph architecture for CPPS. The paper describes the background of a few large-scale graph computing systems. They are Pregel, Giraph, GraphLab and GraphChi, but the paper does not describe how each one can be advantageous to CPPS. There are very few applied research in the domain of graph computing technology as applied to power systems. This paper mentions some of the research that explore this topic as tabulated in table 2.1.

Table 2.1: Examples of graph theory applications in the field of CPPS

Reference	Main
G. Liu et al. [25]	- Part of the early initial works on the inestigation of the application of graph theory to CPPS modelling. - Details forward-throwing power flow algorithm for distribution networks and Gauss-Seidal power flow for transmission networks. - Based on graph data model and overall synchronous parallel theory.
J. Dai et al. [26]	- Models CPPS as a two-layer coupled network diagram (nodes & edges). - Based on Common Information Model (CIM/E). - Shortest path search example considering network delay.
D. Wang [27]	- Concerns solutions to power flow calculations. - Proposes that power flow calculations can be accelerated by using graph computation. - Proves that graph computing can be applied to the Gauss method (and some steps of the Newton-Raphson method).

CPPS form a coupling composed of two layers. Describing CPPS using graphs has the advantage of more convenient storage and more intuitive and organised programming. The graph database stores data through the use of the nodes, edges and attributes of the graph. Any real processing algorithms can be used as functions on the vertices between nodes. See table 2.2. OrientDB, an example of a typical graph database, and has convenient embedded graphical interface for the management and display of graphical data.

Table 2.2: Graphical features and functions

Graphical Feature	Graph Unit	Function
Graph database	Nodes, edges and attributes	Storage, management and visualisation of data
Graph computing	Functions on edges	Data processing and algorithm implementation
JDBC technology	-	Connects database and computing parts

The paper describes the proper design of the graph database of the cyber domain side. For instance, the link parameters have transmission speeds, transmission delays and bit error rates. Also “information acquisition delay” and “command processing delay” are involved when the two domains interact.

In their 2020 works on CPPS, Myhre et al [28], which has a similar outlook on the utilisation of CPPS as Liu et al [24], focuses on the introduction of complex network theory to measure the importance of nodes in a system and how to find them prior to measuring their importance. The nodes can be those pertaining to the electrical domain or the cyber domain. To measure the importance this paper mentions it uses two methods:

1. Betweenness centrality

2. Node attack method

Betweenness centrality is a way to prioritise the vertices in a network based on shortest path. A vertex will be promoted if it appears on more and more of the possible paths on the network. This means that the most important node of a network is the one located on the majority of possible paths. The node attack method illustrates how the system behaves when a specific node is removed. The more important the node, the more negative effect it has on the system when it is removed. In Myhre et al’s [28] case, the negative effect is measured by energy not supplied when each node is removed. This papers’ successful findings include:

- Success of the two aforementioned methods in capturing the important nodes in the system, however with differing criteria of each of the methods.

- Results are somewhat consistent, with the electrical side's results being more consistent.

- Node attack method is more suitable for the power domain since it does not include the cyber side to any extent.

- Advises from system operator's point of view to use the node attack method more because it considers energy not supplied and "and illustrates how an outage in the communication network or the electrical power system influence the power flow."

In their works on graph theory, in 2017 Dai et al [26] proposes to use graph database and graph computing instead of matrix computation to model and simulate CPPS. The cyber-physical power system it wants to model is composed of 3-layers. With the complexity of power systems increasing, this paper's motive is to show that graph computing can handle the increasing large-scale data and executing parallel computation algorithms. The paper concludes its experimentation by showing that the "time latency's calculation" through simulation has been significantly simplified due to graph computing which converted matrix computation problems to graph traversal problems.

Taking a substation as an example, modelling it in CIM/E into graph database has to be done prior to further steps. This is so graph computing can be performed on it. When converted to graph database, all the component objects of the CIM/E standard data are represented by vertices. Advantages include easier data management and graph model manipulation. From this, the circuit breakers and disconnectors can be modelled by edges and this reduces the model set. A Python package was developed to convert CIM/E files to the loading files used by graph database. Further experimentation was used to show decrease in time-latency.

2.2.3 CPPS Modeling using Incidence Matrices

The communication network of CPPS can be modelled by an incidence matrix where the elements hold more than one value to represent the parameters such as latency and error probability as shown by Li et al [29] in 2020. The construction of the matrix model for the communication channel can be shown like so:

$$C_{m\times m} = \begin{bmatrix} C_{11} & \dots & C_{1j} & \dots & C_{1m} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ C_{i1} & \dots & C_{ij} & \dots & C_{im} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ C_{m1} & \dots & C_{mj} & \dots & C_{mm} \end{bmatrix} \tag{2.1}$$

$$C_{ij} = (T_{ij},\ P_{Bij},\ P_{Mij}) \begin{cases} i = j, & \text{nodes} \\ i \neq j, & \text{branches} \end{cases}$$

where: T_{ij} = latency
P_{Bij} = interruption probability
P_{Mij} = bit error probability

Then, the secondary device network matrix can be constructed like so:

$$S_{ii} = (F_{ii}(a_{input}),\ T_{ii}(F_{ii}),\ P_{ii}(F_{ii})...\ )$$

where: $F_{ii}(a_{input})$ = information processing algorithm
$P_{ii}(F_{ii})$ = error probability

2.2.4 Modelling Cyber Modules as Directed Cyber Branches

In Xin's 2015 paper on hierarchical control systems (HCS) [15] their CPPS model's branches are modelled as data mappings from their input-nodes to their output-nodes. The property of each cyber module corresponds to the mapping relations

of the input and output data nodes of a branch. Also, any branch is deemed the out-branch for its input-node and the input-branch for its output-node. The modelling of the three cyber modules as directed branches are explained as follows:

1. Data Transmission Branch:

   A data transmission branch, branch $k = b_k$, is a single-input single-output (SISO) branch, which implements a one-to-one mapping function from input-node to output-node. The mapping is modelled by:

$$b_k: \quad x_k \rightarrow y_k = I_k \cdot x_k$$

2. Data Processing Branch:

   A data processing branch, branch $l = b_l$, is also a SISO branch. The input-node is mapped to the output-node by a particular function as modelled below:

$$b_l: \quad x_l \rightarrow y_l = F_l \cdot x_l$$

   The operator F_l represents the mapping function.

3. Data Pool Branch:

   A data pool branch, branch $m = b_m$, can be a multi-input multi-output (MIMO) branch. All data from the input-nodes are first gathered to form a data pool. A data pool branch is modelled as the combination of several sub-branches, each of which corresponds to the mapping from the union set of all input-nodes to a particular output-node.

$$b_m: \quad \left(x_m^1 \cdots x_m^{w_m^{in}}\right) \rightarrow \left(y_m^1 \cdots y_m^{w_m^{out}}\right)$$

$$\Rightarrow \forall 1 \leq i \leq w_m^{out},\ b_m^i: \quad \left(x_m^1 \cdots x_m^{w_m^{in}}\right) \rightarrow y_m^i = G_m^i \cdot \left(\bigcup_{j=1}^{w_m^{in}} x_m^j\right)$$

In 2017, Xin's work on cyber-physical modelling [30] states an expansion in current steady-state power flow analysis theory, through its proposal of an information-energy flow model and development of a matrix-based computational approach. These methods help directly calculate the mutual influence of the cyber and physical parts on each other. It proposes an "information-flow-oriented network model" and for its information flow, a matrix-based computation. Xin et al. [30] also states that it addresses non-linearity issues associated with data-processing which occur in complex cyber networks. The research discusses cyber-physical sensitivity and vulnerability issues. The case study involves calculating information-energy flow of an "IEEE 14-node system with real-time voltage stability monitoring and control applications and compare the results with simulation results." The research says that the similarity of the results verifies the effectiveness of their approach. In addition, the research states that with calculated sensitivity indices, you can "rapidly estimate the physical impacts of different cyber contingencies based only on the normal state data."

The research works in [15] and [30] both mention calculating information flow and involve matrix-based computation in their modelling of CPPS. The difference however is [30] focuses more on information-energy flow rather than just information flow. Also [30]'s matrix computations describe the effects that the cyber and physical parts have on each other whereas in [15] matrices are used to describe the connectivity of the information between the nodes and through the branches. The research work of [30] models more aspects of CPPS, offering a more matured and enhanced work than in [15].

Modelling Challenges

In Xin et al's work [15], they describe two major challenges in their approach to modelling and performing cyber-contingency assessment (cyber-CA) for an HCS system: system modelling and CA. Regarding system modelling, in addition to the previously mentioned points regarding model simplification and the model constituents, the impact of cyber contingencies can be described by changing two factors: firstly, the branches' mapping relations and secondly, the branches' and the nodes' incidence

relations. The branches' and nodes' incidence relations are described using a node-branch incidence matrix. With regard to CA, simple matrix calculations are used for rapid quantitative assessment of the physical impact caused by special cyber contingencies in the presented model-based cyber-CA, further detailed discussion regarding this will follow. The information flow model consists of numerous data mappings, which means that cyber contingencies can be modelled as modifications of the original mappings.

Concerning information flow, the two cyber modules of an HCS are data-processing modules and data-transmission modules. Data-transmission modules are any data exchange between cyber units in which it is not intended for the data to be changed in any way. So data-transmission can be described as a one-to-one mapping of data between different cyber units. In [15], to achieve a general model, the model includes the data exchange between the cyber and physical side such as measurement or feedback control as well as traditional data gathering and command issuing. In contrast, data-processing modules occur in one cyber unit only and concern the changing of the data from the input of the cyber unit to its output by means of calculations and functions. State estimation and power flow solutions are some examples of data processing in this context.

During the operation of an HCS however, the output from one cyber module can be collected with the output(s) of one or more other cyber module(s) and be inputted to one or more other cyber module(s). This multi-input multi-output part of the information flow is modelled as a data pool, and is another cyber module. In this model, data sets are modelled as data nodes and cyber-modules are modelled as directed branches (or cyber branches). The components in an HCS are arranged in a hierarchical tree structure, so the authors of [15] use this to describe an HCS as a directed graph or a hierarchical tree made up of data nodes and directed cyber branches. Like other topological networks, the operating characteristics of an HCS are decided by two factors:

1. The properties of the modules, which describe the characteristics of a single branch.

2. The cyber topology, which describes the arrangement and connections of all

the nodes and branches.

2.3 Co-simulation Approaches: Interfacing Power System Simulators with ICT Simulators

There exists significant efforts in interfacing dedicated power system simulation tools with dedicated communication network simulators by means of an interface program. The objective of combining the separate tools is to provide cross-domain analysis of the interdependencies of power systems and communications. In this approach, the separate simulators execute relevant calculations and events within their own domain whilst communicating with each other through the interface method which considers various developmental challenges such as time-strategy and event-handling.

Whilst the employment of dedicated simulators provides a clear advantage of a ready simulator as well as simulation accuracy, the development of the interface poses significant challenges such as the need for adequate application programming interfaces (APIs) and the requirement to synchronise the separate simulators sufficiently with respect to time and events.

Some of the most common methodologies include utilising APIs and simulation frameworks. Where available, these tools enable interaction and control with domain-specific simulators, significantly reducing developmental complexity and the need to develop ad-hoc programs. As a result, the required skills and time to develop the interface are minimized, making the process more efficient and feasible for researchers.

Where APIs are not readily provided by the software tools, some researchers resort to open-source tools, such as OpenDSS for power distribution systems and ns-3 for communication networks, to develop their own interfacing files. The considerations when selecting software tools include the availability of GUI/IDEs and APIs, the need for specific models, and the availability of customisations to allow for simulation flexibility. Table 2.3 details the comparison of key aspects of the most common communication simulators used [31], [32].

Table 2.3: Comparison of common CNS used in CPPS research

Aspect	Exata	Riverbed Modeler	OMNeT++	NS-3
Type	Proprietary	Proprietary	Open-source (academic use)	Open-source
License Cost	Moderate	High	Free	Free
Ease of Use	User-friendly GUI; requires training for advanced features	Intuitive GUI; steep learning curve for complex simulations	Moderate; requires familiarity with C++ and NED language	Challenging; requires proficiency in C++ and Python
Key Features	Matured communication models, real-time network emulation support, integration with live networks	Comprehensive protocol library, detailed modeling capabilities, strong visualization tools	Modular architecture, extensive frameworks (INET, Castalia), strong community support	Realistic internet protocol modeling, support for emulation, active development community, native RT support
Disadvantages	High cost; limited access to source code; less community support compared to open-source alternatives	Expensive; proprietary; limited flexibility for custom protocol development	Steeper learning curve for beginners; less industry adoption compared to commercial tools, no native RT support	No native GUI; steep learning curve; limited visualization tools
Usage in CPPS Research	Low	Moderate (formerly OPNET)	Moderate	High

Note: Riverbed Modeler was formerly OPNET. Exata is the standalone software package provided Keysight, not to be confused with Exata CPS (the same software but in collaboration with OPAL-RT).

2.3.1 Approach Challenges

The approach of designing a successful interface between power simulators and communication simulators faces significant developmental challenges which need to be addressed in the interfaces' design. These challenges are:

1. Time synchronisation:

   The simulators must progress with time sufficiently, updating each other and not progress to further events or actions before they are supposed to do so. Within the design of the interface, an approach to addressing this time synchronisation problem must be addressed [22].

2. Data exchange:

   This mainly involves the type of data to be exchanged between the simulators, the implementation of the method and its complexity, and the efficiency [22]. For instance does a whole packet of data containing multiple data types need

to be sent when the other simulator is only requesting one type at that moment in time?

3. APIs:
   A lack of APIs provided by the simulators means developers have to build the APIs to create the link from each simulator to the interface [22]. This is not only complex and time-consuming, it is also difficult to create APIs for commercial simulation tools which provide no access to the source code due to proprietary reasons. This explains a preference in the research community for adopting open-source tools.

4. Models for applications:
   Models for applications that depend on the communication network to provide a function to the grid need to be developed. These include monitoring and control algorithms as examples.

2.3.2 Employing Co-simulation Frameworks

In recent advancements in co-simulation, the adoption of co-simulation frameworks has significantly increased to address the complex interactions between separate simulators and models. These frameworks play a critical role in enabling seamless integration and coordination among various domain-specific simulation tools. Among the most notable are co-simulation frameworks such as Mosaik [33] and HELICS (Hierarchical Engine for Large-scale Infrastructure Co-Simulation), which have gained significant attention in recent literature for their effectiveness and widespread usage [34], [35].

Mosaik is a flexible co-simulation framework that enables users to combine various simulation models into a single test scenario. It emphasizes the modularity of the simulation components, allowing the integration of different tools and models to represent diverse subsystems in power grids. Users define components such as simulators, data sources, and controllers and then link them via an interface that coordinates their execution. Mosaik's primary strength lies in managing the varying simulation timescales and steps of different tools, allowing for a smooth integration

of discrete event simulations with continuous dynamic models.

Regarding HELICS, it was developed to coordinate complex systems of federated simulators and designed to handle large-scale co-simulations involving multiple domain simulators such as those for power grids, communication networks, and economic markets. HELICS operates on a federation-based approach, where each simulator, called a federate, interacts with a central coordinator that facilitates message passing and time management. The core concept of HELICS is to provide time-synchronised data exchange across different simulators, enabling accurate synchronization across diverse platforms.

2.3.3 Application Programming Interfaces

A common method is the use of APIs which are integral to the co-simulation process as they provide the necessary communication pathways between different software tools. APIs allow external control and data exchange between simulators by abstracting the internal workings of each program, enabling seamless communication. Through APIs, developers can automate the input and output data exchange between platforms like PowerFactory, MATLAB, and OpenDSS. APIs provide standard methods for data retrieval and system control, which are critical in co-simulation for coordinating simulations running on different physical or logical machines. The interoperability provided by APIs ensures that time-step differences between simulators can be managed without disrupting the overall simulation flow.

2.3.4 Techniques for Time and Event-handling

Time synchronization is a crucial aspect of co-simulation, particularly when integrating simulators with different time steps or models that operate in real-time or quasi-real-time. Various methodologies are employed to ensure that the data exchanged between simulators is temporally aligned. One common method involves discrete-event synchronization, where simulators pause until they receive the necessary input from other simulators before proceeding. Moreover, time-synchronization protocols like PTP (Precision Time Protocol) [36] or NTP (Network Time Protocol) [37], [38]

are employed for high-precision coordination in real-time simulations involving HIL systems.

In designing the interface, it is crucial for the interface to manage time progression across the simulators involved. This requires addressing both time and event synchronization to ensure the simulators advance in sync, continuously exchanging accurate data with one another. By doing so, each simulator receives the precise data it needs at the exact moment for its subsequent computations, thereby preserving the accuracy and reliability of the overall system. Any initial synchronization errors can propagate, leading to cascading inaccuracies down the line.

The synchronization challenge arises from the fundamental differences in modeling approaches between power systems and communication networks. Power system simulators focus on modeling power generation, transmission, and distribution, relying on dynamic variables, such as voltage and frequency, which are governed by differential equations. These equations reflect system dynamics and require discretization through fixed time steps, as continuous time calculations are computationally impractical.

In contrast, communication network simulators adopt an event-driven approach without differential equations. Here, the simulation revolves around discrete events, with no changes in system state between consecutive events. The simulator schedules and executes events as they occur. This difference in time progression, fixed time steps for power systems versus event scheduling for communication networks, necessitates careful synchronisation to ensure cohesive and reliable operation of the combined simulation.

The main approaches to addressing the time-synchronisation issues are [39]:

1. Time-stepped:

   The concerned simulators progress independently with time stopping at synchronisation points to exchange data between each other. The time between synchronisation points is chosen by fixed time intervals. Events occurring in between synchronisation points have to wait for the next synchronisation point to be exchanged and so this method is prone to the accumulation of errors. For time-critical scenarios whereby multiple events may occur in between synchro-

nisation points, this is an undesired approach. See Figure 2.3.

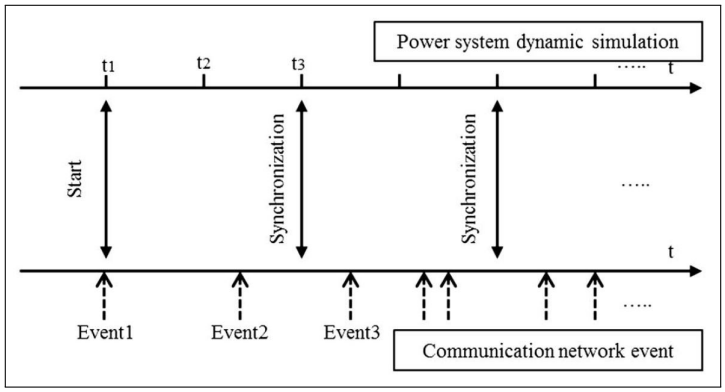

Figure 2.3: Time-stepped synchronisation method [39]

2. Global-event driven:

   As opposed to the time-stepped method, this method allows only one simulator to progress with time before switching to the other. The advantage of this is that this leads to higher accuracy but the disadvantage is the slower simulation speeds. Executing the events in the correct order is the responsibility of an event scheduler which also combines the events belonging to the power system simulator and the events of the communication network simulator. See Figure 2.4.

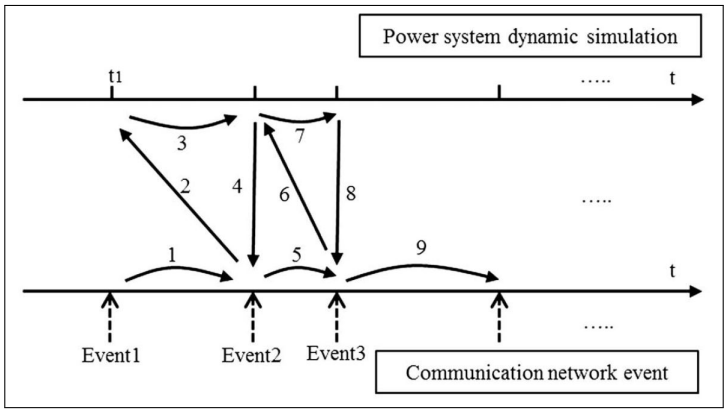

Figure 2.4: Global-event driven synchronisation method [39]

3. Master-slave:

   The master-slave method is the simplest out of the three. Any simulator can take over and become the master, which grant it higher priority and will decide the time-steps taken during its simulation lifetime as a master. See Figure 2.5.

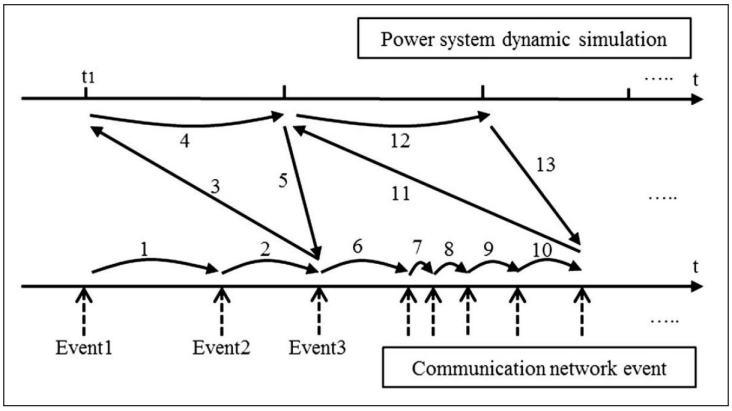

Figure 2.5: Master-slave synchronisation method [39]

2.3.5 Recent Significant Works

Table 2.4 summarises various co-simulation approaches used in CPPS research, highlighting the unique focus and configurations of each approach. The EPOCHS framework focuses on multi-agent-based PAC simulations, leveraging PSCAD/EMTDC and PSLF for power system simulation and NS-2 for communication network modelling. It adopts the IEEE 1516-2000 HLA framework and employs a fixed time-stepped strategy for large-scale systems.

ADEVS is a framework designed for WAMPAC applications, utilising ADEVS as the power system simulator integrated with NS-2 for communication. This approach employs an ad-hoc DEVS simulation framework for large systems. Bergmann et al. explore simulations of DERs and virtual power plants (VPPS) using NETOMAC for power systems and NS-2 for communication, adopting a time-stepped strategy through an ad-hoc JNI-based integration for small-scale systems.

The VPNET framework is another WAMPAC-focused simulation approach, which uses VTB as the power system simulator and OPNET Modeler for communication. The system relies on socket-based ad-hoc integration with a time-stepped simulation strategy, suitable for small systems. PowerNet adopts a control-focused approach by combining Modelica for power system simulation with NS-2 for communication, using Unix-named pipes for integration within an ad-hoc framework. It also uses a time-stepped strategy for small-scale simulations.

GECO emphasises PMU-based WAMPAC simulations and integrates PSLF as

the power system simulator with NS-2 for communication through a TCL-based linking mechanism. The approach uses a global event-driven time strategy to accommodate large systems. GridSim, another WAMPAC-focused framework, employs Powertech TSAT for power systems and GridStat for communication, adopting a fixed time-stepped strategy within an ad-hoc framework for distributed system simulations.

INSPIRE is a framework designed for WAMPAC simulations, combining DIgSILENT PowerFactory for power systems with OPNET Modeler for communication. It leverages an IEEE 1516-2010 HLA evolved framework and employs a dynamic time-stepped strategy, making it suitable for large-scale systems. Lastly, Greenbench focuses on cybersecurity simulations, using PSCAD for power systems and OMNeT++ for communication. It adopts an ad-hoc IPC-based integration framework and a global event-driven time strategy for small-scale systems.

These approaches collectively showcase a diverse set of methodologies tailored to address various CPPS challenges, ranging from WAMPAC and DER simulations to cybersecurity and control applications.

Choudhury et al in 2024 [51] propose a new framework called C-SPAACE, which stands for Coordinated Set Point Automatic Adjustment with Correction Enabled. The goal of this system is to enable real-time control and coordination between IBRs in microgrids using 5G communication. One key benefit of 5G technology is its ability to support low-latency communication, which is critical for the real-time needs of power systems. Specifically, the ”slicing” feature of 5G allows different use cases to have their own dedicated resources, meaning C-SPAACE can operate efficiently under normal conditions. However, there are challenges when it comes to managing the 5G network for power grid applications. Since each ”slice” of the network only has access to a limited amount of radio spectrum, poor management of these resources can negatively impact the communication performance of C-SPAACE. Therefore, the authors focus on finding a way to optimally allocate these spectrum resources among the IBRs in the network to ensure smooth operation. To solve this issue, the authors introduce a new scheduling technique based on a metric called Age of Information (AoI). This AoI-based scheduler ensures that the communication be-

Table 2.4: CPPS co-simulation approaches

Reference	Recent Focus	Power System Simulator	Comms. Network Simulator	Simulation Framework	Time Strategy	System Size
EPOCHS [40]	Multi-agent PAC	PSCAD/ EMTDC, PSLF	NS-2	IEEE 1516-2000 (HLA)	Fixed time stepped	Large
ADEVS [41]	WAMPAC	ADEVS	NS-2	Ad-hoc (integrated in NS-2)	DEVS	Large
Bergmann et al. [42]	DERs and VPPS	NETOMAC	NS-2	Ad-hoc (JNI)	Time stepped	Small
VPNET [43]	WAMPAC	VTB	OPNET Modeler	Ad-hoc (sockets)	Time stepped	Small
PowerNet [44]	Control	Modelica	NS-2	Ad-hoc (Unix named pipes)	Time stepped	Small
GECO [45] [46]	PMU-based WAMPAC	PSLF	NS-2	Ad-hoc (TCL linking)	Global event-driven	Large
GridSim [47]	WAMPAC	Powertech TSAT	GridStat	Ad-hoc	Fixed time stepped	Distributed
INSPIRE [48] [49]	WAMPAC	DIgSILENT PowerFactory	OPNET Modeler	IEEE 1516-2010 (HLA evolved)	Dynamic time stepped	Large
Greenbench [50]	Cybersecurity	PSCAD	OMNeT++	Ad-hoc (IPC)	Global event-driven	Small

tween the IBRs and the control system remains low-latency, even under constrained network conditions. The authors then create a co-simulation environment, combining PSCAD/EMTDC (for power system simulation) with Python (for communication simulation), to test their proposed system. Finally, the performance of C-SPAACE is evaluated through time-domain simulations, comparing the AoI-based scheduler with other traditional (non-AoI) scheduling methods. These case studies help demonstrate the advantages of using the AoI-based approach in terms of maintaining reliable, real-time communication in microgrids using 5G technology.

Research works investigating the inclusion of 5G communications and its applications for power systems is becoming increasingly important. With regards to 5G performance, smart grids demand strict requirements of reliability and latency as mentioned by Parvez et al in [52]. For example, they mention that for dynamic control, a maximum delay of 100 ms of end-to-end (E2E) latency can be sustained for switching electrical generation sources on and off, such as PV and wind turbines.

However, for synchronous co-phasing of power generators, the E2E latency should not exceed 1 ms. Generally in a smart grid, 5G latency expectations fall in the range of 1-20 ms. For example, the IEC 61850 standard specifies that GOOSE messages, which are critical for real-time communication, should be generated, transmitted, and processed within a maximum of 4 milliseconds [53], [54]. Some specifications, like those in IEC 62351-6, even require a 3ms maximum [54]. This tight timing constraint is crucial for applications like distance protection and other critical functions where delayed or missed messages can lead to instability or cascading blackouts.

2.4 Real-Time Simulation Approaches: CPPS Testbeds

This section examines the third category of approaches for modelling and simulating CPPS: real-time in-the-loop (RT-ITL) methods. RT-ITL approaches are inherently complex, requiring advanced expertise in both framework configuration and model development. Despite these challenges, they remain a widely adopted methodology in CPPS research, particularly within larger academic and research institutions.

The section begins by outlining the common tools and frameworks used in RT-ITL approaches. Next, it presents a dedicated discussion on SIL simulations, highlighting their key characteristics. Following this, the primary applications and challenges of RT-ITL methods are analyzed, with specific examples drawn from cybersecurity, as well as systemic hurdles such as cost and synchronization. The section then reviews prominent recent works in this domain before concluding with an outlook on future research directions.

2.4.1 Common Simulation Tools Employed

Real-time power system simulators commonly used in various testbeds include simulators produced by the two companies Real-Time Digital Simulator (RTDS) and OPAL-RT, their products employed for their ability to emulate real-time power system dynamics with high accuracy. These simulators facilitate advanced studies on power system behaviour under various conditions, including natural disturbances and cyberattacks. They also enable integration with external hardware for HIL simulations,

providing a realistic environment for testing and validation. See Table 2.5 which shows the common simulators used by researchers.

Table 2.5: Common RT power and communication simulators employed

Common Simulators Employed	
RT Power System Simulators	ePHASORSIM OPAL-RT (HYPERSIM, eMEGASIM, ePHASORSIM) RTDS Typhoon HIL Speedgoat
Communication Simulators	NS-3 Riverbed Modeler (formerly OPNET) Exata Exata CPS OMNeT++ Hardware based

Communication simulators often used alongside real-time power system simulators include NS-3, OMNeT++ and Riverbed Modeler (formerly OPNET). These tools are employed to simulate the communication network layer of smart grids, assessing the effects of network delays, packet losses, and cyberattacks on the power system. In certain testbeds, communication simulation tools like Exata and QualNet are used for advanced network emulation.

For hardware-based communication simulation in testbeds, devices such as PMUs, IEDs, PLCs, and RTUs are commonly integrated. These components replicate the functionality of actual communication hardware in power grids, allowing the study of cyber-physical interactions under real-world conditions. Other devices such as routers, switches, and firewalls are used to simulate and secure communication pathways within the grid.

2.4.2 Software-in-the-Loop

Software-in-the-loop (SIL) is a similar simulation technique to HIL where software is replaced with the DUT. SIL is commonly used in the development and verification of embedded control software and algorithms. SIL's key characteristics and how it functions is detailed below:

- Simulation Environment: SIL typically involves running software components, such as control algorithms or software modules, in a computer-based simulation environment. This environment mimics the behaviour of the target system or hardware [55], [56].
- Virtual Hardware: Instead of connecting the software directly to physical hardware, SIL uses virtual representations of the hardware components. These virtual representations simulate the interactions and responses of the real hardware, allowing the software to interface with them as if they were real [55].
- Early Development and Testing: SIL allows engineers and developers to test software components early in the development cycle, even before the physical hardware is available or fully functional. This early testing helps identify and resolve software-related issues before they can affect the actual hardware [55], [56].
- Realistic Simulations: SIL simulations aim to provide a high level of realism to ensure that the software behaves as expected in real-world scenarios. This may involve simulating sensor inputs, environmental conditions, and hardware interactions [55].
- Integration Testing: SIL can be used to test the integration of multiple software modules or components within a system. It helps ensure that these components work together correctly before they are implemented in the actual hardware [55], [56].
- Debugging and Analysis: Developers can use SIL to debug and analyse the software's behaviour under different conditions and scenarios. This helps in identifying and resolving issues early in the development process [55], [56].

SIL is commonly used in industries where software plays a critical role in controlling complex systems, such as automotive control systems, flight control software in aircraft, industrial automation, and in power systems. It serves as an essential step in the software development and validation process, helping to ensure that software components meet the required performance, safety, and reliability standards before they are deployed in the field.

2.4.3 Approach Applications

The reviewed studies highlight the significant role of real-time HIL simulations in enhancing the resilience and performance of CPPS. These simulations allow for the simultaneous co-simulation of cyber and physical layers, enabling a more accurate representation of system dynamics and interactions under various operational conditions, including cyber-attacks and communication failures [57], [58]. The effectiveness of these platforms is demonstrated through their ability to analyse communication delays and their impact on system stability, thereby providing insights into the resilience of control strategies against disturbances [59], [60]. Furthermore, the integration of real-time data from physical devices enhances the reliability of simulations, allowing for the validation of control strategies in authentic CPPS environments [58], [61]. Overall, these findings underscore the importance of real-time simulations in improving the operational stability and security of CPPS.

One of the biggest application areas of CPPS ITL testbeds is in monitoring, protection and control research which is critical for maintaining grid security and reliability [62]. Multiple efforts in this area connect protection and control devices to real-time simulators most prominently relays, PMUs, PDCs and IEDs for various specialised research investigations. For instance, the CPS testbed at the University of Carolina, Charlotte [63], was used to model and validate synchronous generators using a 2 kW generator and Real-Time Digital Simulator (RTDS). It employs various instruments like PMUs and protection automation controllers (SEL 421 relays). In [64], the authors focus on developing an anomaly detection and mitigation algorithm using machine learning for WADC measurement and control signals, which are used in interconnected multi-area power systems. They use IEEE-C37.118.2 protocol for

the data communication of the synchrophasors, and the DNP3 and IEC-61850 communication protocols for the SCADA data and control signal communications across the control centres, actuators, intelligent electronic devices (IEDs) and remote terminal units (RTUs).

Another increasingly important application area is cyber security for power systems. For example, India built its first cyber-security testbed in 2020 which aims to conduct research and well as educate and train in the areas of vulnerability studies and protection of critical infrastructure [65]. The accuracy and realistic conditions of the experimental study activity conducted on this testbed are its primary qualities. Replicating the realistic environment found in automated manufacturing units, smart transit systems, smart homes, and smart grids, the C3i centre offers an environment that can be customised to suit the research requirements.

2.4.4 Approach Challenges

HIL setups for research in CPPS faces a variety of complex challenges including [66]:

- **Synchronisation:** Similar to co-simulation approaches, time-synchronisation of two or more simulators is required. The setup has to address the issue of guaranteeing the execution of the simulator in accordance with the real time constraint of the DUT.
- **Model Validation:** For accurate simulation of the environment, models need to be validated against real-world data. Inaccurate models lead to incorrect results and hence may not reflect the actual behaviour of power system environment.
- **Hardware Integration:** Integrating physical hardware components into the simulation can be complex and time-consuming. The DUT requires satisfactory connections with the simulation environment and this poses significant challenges.
- **Communication Delays:** In a CPPS, communication between components,

such as controllers and sensors, include delays. Managing and accounting for these delays in the simulation is essential for accurate testing.

- **Scalability:** Scaling up HIL setups to model larger and more complex power systems is required in a lot of cases as part of the validation process so it is of utmost importance. However scalability poses a challenge, for example due to computation limitations. Coordinating multiple physical components and ensuring synchronization can become increasingly difficult as the system size grows.
- **Cost:** Building and maintaining a HIL setup for CPPS research can be expensive. It involves the cost of hardware, simulation software, and ongoing maintenance, which may be a barrier for some organizations.
- **Standardisation:** Lack of standardized interfaces and protocols can hinder the interoperability of different components and simulation tools. This can lead to compatibility issues when integrating hardware and software from different vendors and serve as a significant barrier. Just like in the co-simulation approach, this approach can be hindered by the lack of APIs provided by simulators.

2.4.5 Latest Works

Xie et al make significant contributions to SIL in their 2021 paper [67]. The modelling technique described in this article uses SIL to simulate the effects of erratic communication on centralised volt-var control performance and to develop an encoding technique to lessen those effects. In order to facilitate multi-rate co-simulation of a distribution system with numerous inverter-based distributed energy resources (DERs), an asynchronous real-time SIL simulation platform is first presented. Micro-second-based power electronic models represent the DERs, while millisecond phasor-based models represent the distribution system. Modbus links and the Long Term Evolution (LTE) network are used to create communication links between smart inverters and the centralised volt-var controller (modelled externally to the HIL testbed). An enhanced, augmented Lagrangian multiplier based encoded data recovery (EALM-EDR) algorithm is developed and validated on this co-simulation platform to mitigate

the impact of unreliable communication. The outcomes of the simulations show how effective the HIL-based co-simulation platform is as a digital twin of the power grid for creating algorithms that manage numerous heterogeneous control systems via wired and wireless communication links.

Another research with significance in HIL CPPS testbeds is by Tong et al in their 2019 paper [57]. The authors develop a versatile HIL testbed to investigate CPPS. Different co-simulation systems are generated for different purposes by utilising the flexible interface. Three sample co-simulators are designed and developed as proofs based on this testbed. A case study of a false data injection attack on automation voltage control is examined, followed by the introduction of an HIL power and communication co-simulator with a non-real-time synchronisation mechanism. The performance of stability control equipment is then demonstrated by simulating a case that considers the effect of communication bit error on the stability control system using a real-time power and communication HIL co-simulator. Lastly, a case study of a MITM attack on the data link is simulated to illustrate the impact of a cyber attack on the stability control system. This co-simulator replicates an actual cyber attack on the system.

Also Aftab et al raises importance of the effects of cyber attacks on VVO after the IEEE 1547 Upgrade in their 2023 paper [68]. In their article they present the development of a real-time co-simulation setup for the assessment of the impact of cyberattacks on VVO. The setup comprises a real-time power system simulator, a communication network emulator, and a master controller in a system-in-the-loop configuration. The DNP3 communication protocol is employed for the underlying communication infrastructure. The results demonstrate that corrupted communication messages can result in the violation of voltage limits, an increased number of setpoint updates of VRs, and economic loss.

In 2018, OPAL-RT Technologies, a company that provides real-time simulations hardware and software, collaborated with SCALABLE Network Technologies (part of Keysight Technologies), specialists in network emulation and modelling. This collaboration led to the development of solution that integrates OPAL-RT's HYPERSIM platform with SCALABLE's EXata CPS tool. HYPERSIM, which specialises in sim-

ulating electromagnetic transients in power systems, now works with EXata CPS, which emulates communication networks and tests their resilience to cyberattacks. Together, they provide a comprehensive cyber-physical testbed for electrical grids, addressing not just the physical system's operation but also its vulnerabilities to cyber threats. The collaboration aimed to address the growing need for robust solutions in power grid security, especially as modern grids become more complex and reliant on digital communications.

The result of this collaboration is HYPERSIM 2019.2, which allows for the real-time simulation of large-scale electrical systems alongside their communication networks, helping utilities and grid operators test various cyberattack scenarios. This integration supports critical communication protocols such as GOOSE, DNP3, and IEC 61850, allowing for the simulation of realistic attacks like Denial of Service (DOS) and packet manipulation. By enabling users to model both physical and cyber threats in a controlled environment, HYPERSIM 2019.2 offers a powerful tool for evaluating grid resilience, testing system responses, and developing mitigation strategies. This partnership represents a significant leap forward in ensuring the cybersecurity and operational integrity of power grids, addressing the urgent need to protect critical infrastructure from the dual challenges of increasing complexity and rising cyber vulnerabilities.

Table 2.6 outlines the latest real-time CPPS testbeds, showcasing their focus areas, simulators, frameworks, and scalability. Babazadeh et al. developed a testbed centered on WAMC, HVDC systems, and low to mid-voltage grids. The testbed integrates OPAL-RT for power system simulation and OPNET for communication, utilising an ad-hoc framework with emulated sockets. It supports small-scale systems in HIL mode and medium-scale systems in emulated setups.

Nguyen et al. [71] focus on cybersecurity applications, such as phishing, DoS, and MITM attacks. Their testbed combines OPAL-RT and RTDS for power system simulation with Exata for communication, leveraging an Exata-enabled framework. This setup is scalable for very large systems, enabling the study of sophisticated cyber threats.

Pham et al. [72] present a testbed designed for monitoring, control, and OPF.

Table 2.6: Real-time CPPS testbeds

Reference	Recent Focus	Power System Simulator	Communication Network Simulator	Simulation Framework	Scalability	Year
Babazadaeh et al. [69][70]	WAMC, HVDC, low/mid voltage grid	OPAL-RT	OPNET	Ad-hoc, emulated sockets	Small (HIL), medium (emulated)	2014
Nguyen et al. [71]	Cybersecurity, e.g. phishing, DoS, MITM	OPAL-RT and RTDS	Exata	Exata-enabled	Very large systems	2024
Pham et al. [72]	Monitoring and control, OPF	Typhoon HIL	Python & Typhoon SCADA Panel	Python-based	Large systems	2024
Mishchenko et al. [73]	Cybersecurity, e.g. MITM, reconnaissance	OPAL-RT	hardware-based	OPAL-RT-enabled	Medium systems	2024

It employs Typhoon HIL for power system simulation and a Python-based SCADA panel for control, forming a Python-enabled framework. This testbed is scalable for large systems, providing a robust environment for real-time operational studies.

Mishchenko et al. [73] focus on cybersecurity threats such as MITM attacks and reconnaissance activities. Their testbed integrates OPAL-RT with a hardware-based communication system, operating under an OPAL-RT-enabled framework. It is designed for medium-sized systems, offering real-time capabilities to explore cybersecurity vulnerabilities and mitigation strategies.

2.4.6 Future Directions

Advancing simulation techniques remains essential for improving the accuracy and scalability of real-time power system analysis. Integrating AI and ML into these simulations can enhance predictive capabilities, optimise system performance, and enable more adaptive modelling of dynamic behaviours. These technologies also hold potential for managing vast datasets and accurately simulating complex, uncertain power system scenarios.

Cybersecurity in CPPS requires deeper exploration into advanced attack models and robust defence mechanisms. Research must prioritise developing real-time intrusion detection systems (IDS) capable of adapting to evolving threats such as ad-

vanced persistent threats and zero-day exploits. Additionally, decentralised security frameworks, including blockchain-based architectures and peer-to-peer communication protocols, could address the unique challenges posed by DER integration and IoT-driven grids. Tools that enable real-time threat simulation and cyber-physical co-simulation would further enhance grid resilience by evaluating the impact of attacks and testing effective response strategies.

The transition to renewable energy requires large-scale, high-fidelity electromagnetic transient (EMT) models that can capture fast transients and switching dynamics introduced by inverter-based resources. Unlike RMS models, EMT simulations allow for more precise analysis of stability challenges in renewable-heavy grids. As grids evolve to include more complex control structures, these simulations will become vital for ensuring operational reliability and flexibility.

Finally, AI and ML offer transformative potential for real-time grid optimisation and predictive maintenance. Research should focus on developing AI-driven control systems capable of managing the dynamic nature of modern power systems, optimising power flows, and integrating renewable energy more efficiently. Furthermore, AI can enhance situational awareness in control centres, providing grid operators with actionable insights during emergencies and enabling more informed decision-making.

2.5 Chapter Summary

This chapter has reviewed the current state of research in the modelling and simulation of CPPS, highlighting the integration of cyber technologies into modern power grids and their role in the energy transition. The chapter categorised existing approaches into three main methodologies: model-based, co-simulation, and in-the-loop RT testbed approaches.

- Model-Based Approaches: These use abstracted and reduced model techniques, an example of which are graph-based methodologies to represent the physical and cyber components of CPPSs, focusing on their interdependencies. Graph theory models, such as attack graphs and Petri nets, have proven effective for analysing vulnerabilities and impacts of failures. The adoption of

graph computing systems like OrientDB has facilitated data management and complex analyses. However, challenges remain in scalability and validation of these models.

- Co-simulation Approaches: By interfacing dedicated power system simulators (e.g. PowerFactory) with communication network simulators (e.g. NS-3), researchers have enabled cross-domain analysis. Frameworks like HELICS and Mosaik have emerged as efficient tools to synchronise time and events across simulators, addressing key challenges such as scalability and the lack of standardised APIs. Despite their advantages, co-simulation requires significant computational resources and careful handling of time synchronisation.

- In-the-Loop Approaches: Real-time testbeds, including HIL and SIL systems, provide a platform for evaluating CPPS resilience under dynamic conditions. These systems enable the integration of physical hardware and real-time data, allowing for advanced studies in monitoring, protection, and control. HIL systems like OPAL-RT and partnerships with tools such as EXata CPS have demonstrated effectiveness in simulating cyber-physical interactions, including cyber-attack scenarios.

Key challenges identified across these methodologies include the complexity of synchronising simulators, ensuring model validation, managing communication delays, and achieving scalability for large-scale systems. The chapter concludes by emphasising the need for further research in CPPS modelling, particularly in standardisation, scalability, and cybersecurity measures. Collaboration between academia, industry, and government is vital to advance the field and meet the demands of modern power systems.

Chapter 3

Vulnerability Assessment in Graph-based Modelling of CPPS

3.1 Introduction

In CPPS analysis, vulnerability assessment is one of the most important type of studies researchers and engineers conduct, particularly in investigating the effects of cyber contingencies on power system operation. This is due to a number of reasons. Firstly, the most common cyber contingencies can be identified so that prevention, detection and mitigation technologies can be designed and implemented. Such assessments could also provide insights into the cyber errors, attacks and issues that cause the most damage. As a result, mitigating measures to hinder and suppress those specific cyber contingencies can be undertaken.

Secondly, the most vulnerable power system components and systems will be identified, so they should receive the required attention in terms of closer monitoring, higher protection and designing preventative and reliability methods and systems.

Finally, the weakest links of the various aspects of the cyber domain can also be highlighted, such as the most delayed or error-prone communication channels, so reliability or channel strengthening efforts can be planned and implemented thereafter. This will ultimately help in building increasingly robust, secure and reliable power systems required in the future where the cyber domain's analysis is fed back actively and continuously in the overall analysis of smart grids.

Therefore, the focus in this section is on a novel vulnerability index that allows the importance of each cyber node, in a graph-based CPPS model, to be analysed effectively. The developed Cyber Node Importance Index (CNII) considers:

1. The cascading failure effects due to the failure of an initially chosen cyber node.

2. The Betweenness centrality of all the cyber nodes in the CPPS model.

3. The time delay of the shortest paths in the cyber network.

In the next sections, the CPPS model development and the CNII are detailed followed by a case study where the UK's British Telecom 21st Century Network is linked with a reduced model of the GB Transmission System. The experimental results show the utility of this methodology as well as the applicability of analysing cyber contingencies in graph-based CPPS models. Regarding limitations, it is im-

portant to note that this scenario has been chosen as a means of demonstrating the method rather than it modelling realistic deployment.

3.2 Development of CPPS Model

3.2.1 Representing Networks using Adjacency Matrices

A model-based methodology for integrating the physical and cyber domains involves combining the adjacency matrices of respective networks from each domain. To obtain an adjacency matrix, the networks must first be represented as graphs. This process is more straightforward to conduct for a cyber network compared to a power system network, as cyber networks inherently consist of well-defined nodes and links.

In graph theory, a graph can be represented by $G(V, E)$ where V is the set of nodes denoted by $V = \{v_1, v_2...v_i\}$ and hence $v_i \in V$ and where E is the set of links between any node v_i to any other node v_j denoted by $E = \{e_{11}, e_{12}...e_{ij}\}$ and hence $e_{ij} \in E$. Such graphs can be represented by an adjacency matrix which contains information pertaining the connectivity of the graph of the network. See Figure 3.1 where each element of the matrix represents whether or not a link exists between its column node and row node.

Beyond the standard logical adjacency matrix, in which elements are binary, the elements of an adjacency matrix can also be used to represent specific network characteristics, such as transmission delays across links or error probabilities as, detailed by equation 2.1 in the literature review, section 2.2.2.

3.2.2 Cross-domain Linkage

In this work, the logical adjacency matrix is employed such that any element M_{mn} represents a directed link existing from node m to node n as shown by Equation (3.1). If all the links in the network are bidirectional then this matrix will be symmetrical.

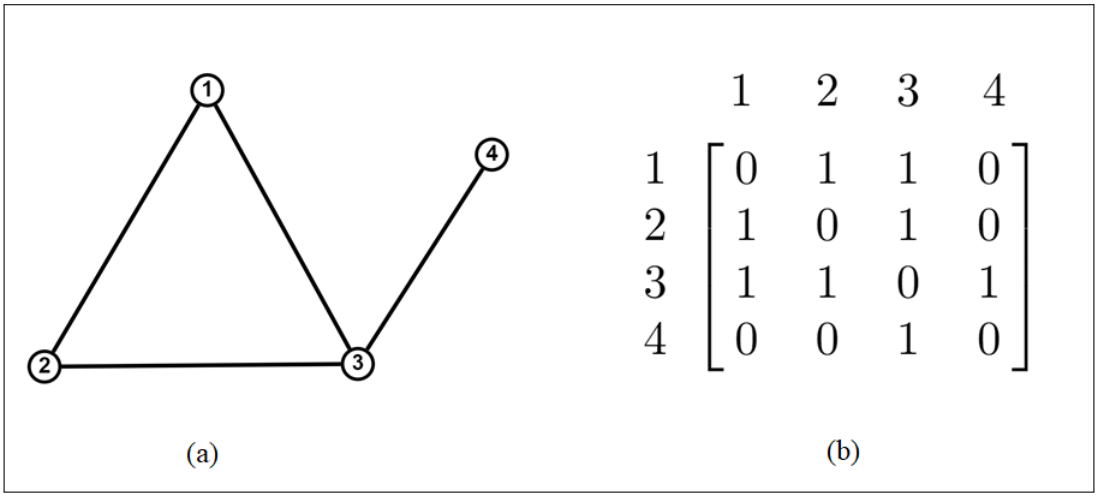

Figure 3.1: (a) An unweighted, undirected 4-node graph (b) Its corresponding adjacency matrix with column and row numbers representing the nodes

$$M_{mn} = \begin{array}{c} \\ \text{from} \\ \text{node} \end{array} \begin{array}{c} \text{to node} \\ \begin{bmatrix} M_{11} & M_{12} & \cdots & M_{1n} \\ M_{21} & M_{22} & \cdots & M_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ M_{m1} & M_{m2} & \cdots & M_{mn} \end{bmatrix} \end{array} \tag{3.1}$$

where: $M_{mn} = \begin{cases} 0, & \text{no link exists from node } m \text{ to node } n \\ 1, & \text{link exists from node } m \text{ to node } n \end{cases}$

Using Equation (3.1), adjacency matrices for a power system network and for a cyber network can be defined. These are termed as M_p and M_c respectively. Then, they are joined in a diagonal fashion which forms two new diagonally aligned sub-matrices but on the mirrored plane. The top-right submatrix represents the interface links from the cyber network to the power network, and the second bottom-left sub-matrix represents the reverse, that is the interface links form the power network to the cyber network. These are referred to as M_{cp} and M_{pc} respectively. This results in Equation (3.2).

$$M_{CPPS} = \left[\begin{array}{c|c} M_c & M_{cp} \\ \hline M_{pc} & M_p \end{array}\right] \tag{3.2}$$

where: M_c = communication layer
M_{cp} = communication-to-power layer
M_{pc} = power-to-communication layer
M_p = power layer

3.3 Cyber Node Importance Index and Parameters

3.3.1 Equation Definition

Proposed in Equation (3.3), is the Cyber Node Importance Index (CNII), a methodology for determining the importance of each cyber node in a graph-based CPPS. The CNII takes into account the cascading failure (the number of power stations that fail) due to the failure of each cyber node, the betweenness centrality of each cyber node and the time delay difference of the average shortest paths.

$$I_i(n) = \frac{F_p(n)}{N_p} + \frac{C_B(n)}{C_{B_T}} + \Delta t_d(n) \tag{3.3}$$

where: $F_p(n)$ = Total power stations failed due to failure of communication node n
N_p = Total power stations in network
$C_B(n)$ = Betweenness centrality of communication node n
C_{B_T} = Sum of betweenness centrality of all communication nodes
$\Delta t_d(n)$ = Average shortest paths time delay difference (ASPTDD)

3.3.2 Cascading Failure Parameter and Algorithm

$F_p(n)$ is the number of power stations that have failed due to the failure of communication node n. The total number of power station nodes in the network is denoted by N_p.

Initially, a random communication node is deliberately failed to simulate a communication node outage. Since it is assumed that the failure of a communication node directly results in the failure of its corresponding power system node, the power system node cross-domain linked to the failed communication node is also taken offline. Subsequently, the failure of this power system node triggers the failure of additional power system nodes to which it supplies power, creating a cascading effect. This cascade of failures continues until it reaches the final power node, which is not linked to or does not supply power to any other node. The flowchart is shown in Figure 3.2. Considering cascading failure as a parameter in the formation of the CNII is crucial because it is a clear measurement of importance of a cyber node. The more damage the failure of a cyber node causes, the more critical it is.

3.3.3 Betweenness Centrality Parameter

Betweenness centrality is one of many approaches pertaining centrality measures in graph theory which determines the importance of a node in a network. The betweenness centrality of a node is the number of times it appears in the path of the shortest path of two other nodes. If said node fails, a packet will need to compute another 2nd most shortest path, thereby increasing the latency of the total journey.

$$C_B(n) = \sum_{i \neq n \neq j} \frac{\sigma_{ij}(n)}{\sigma_{ij}} \tag{3.4}$$

Output $C_B(n)$ represents the betweenness centrality of communication node n as calculated by Equation (3.4). The total number of shortest paths from node i to j is represented by σ_{ij} and $\sigma_{ij}(n)$ is the number of those paths where n passes through them.

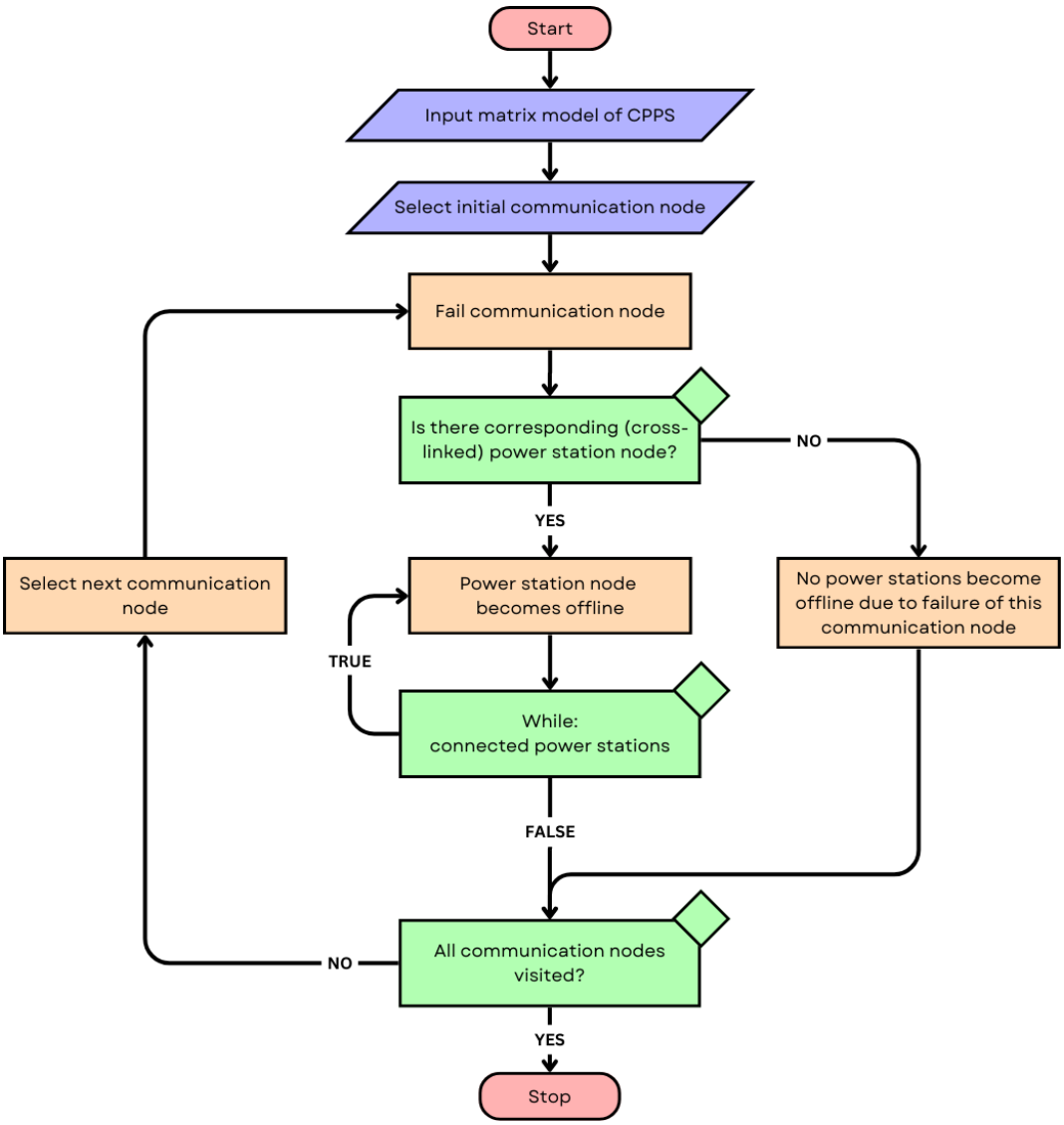

Figure 3.2: Flowchart of cyber-physical cascading failure algorithm

3.3.4 Average Shortest Paths Time Delay Difference Parameter

$\Delta t_d(n)$ is the average shortest paths time delay difference (ASPTDD), which represents the time delay difference between the average time delay of all the shortest paths under normal operation, t_{avg}, and when a communication node n fails, $t_d(n)$.

$$\Delta t_d(n) = t_d(n) - t_{avg} \tag{3.5}$$

where:

$$t_{avg} = \frac{\sum_{i \neq j} t_{ij}}{N_{sp}} \tag{3.6}$$

where: t_{ij} = shortest path time between node i and j in seconds

N_{sp} = number of shortest paths in the network

Although cascading failure and betweenness centrality has been considered in previous research works such as in [28] and [74], the CNII introduced in this work also considers the ASPTDD, which is an important metric to factor into the equation due to the time effect the inclusion or removal of some cyber nodes have on the system. A positive ASPTDD value for a communication node n, for example, immediately displays the fact that the removal of n has an adverse effect because the average shortest paths is now greater than before. Considering ASPTDD will increase the accuracy of ordering the importance of each cyber node. If time delay is not considered, inaccurate results will be produced showing that other nodes are more important. This is presented by the achieved results in the following case study.

Dijkstra's Algorithm for Shortest Path

As mentioned, for computing for the betweenness centrality of the networks and the novel ASPTDD, the shortest path between every two nodes needs to be calculated. We employ the Dijkstra's algorithm for this and implement this in MATLAB. The algorithm conducts a series of programming steps to save the shortest journey distance from a source or starting node to a destination or target node. A conceptual flowchart of Dijkstra's algorithm is shown in Figure 3.3.

3.4 Development of GB CPPS Model

A GB CPPS model was developed using the graph and matrix based models described in the previous section. Suitable large networks were selected to perform the case study. The selected communications and electrical transmission networks were the BT 21st Century Network [75] and the reduced model of the GB transmission system [76] respectively. To produce the adjacency matrices for the BT 21CN and the GB TSRM, both networks were represented as separate graphs with nodes and links. Then, the two adjacency matrices were combined to form the whole GB

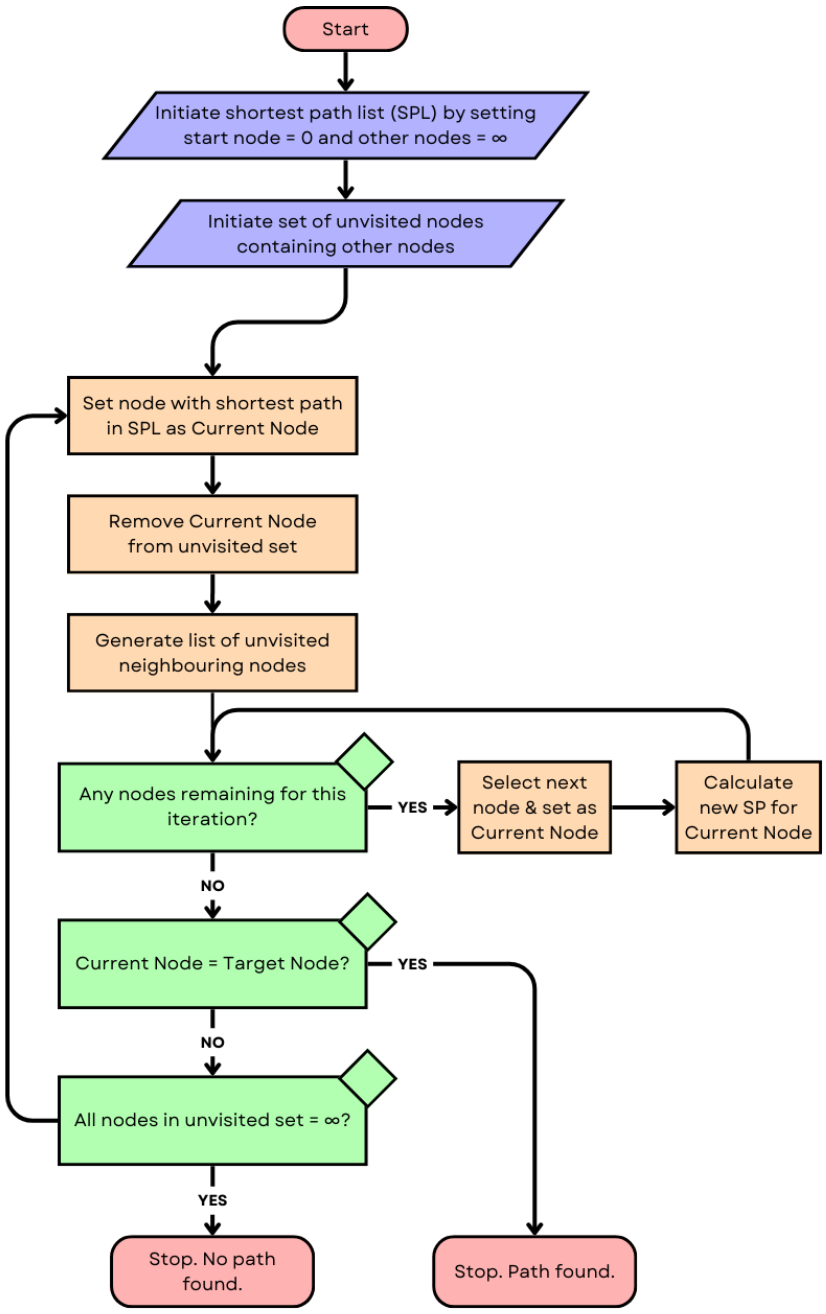

Figure 3.3: Flowchart of Dijkstra's Algorithm for finding shortest path

CPPS model. Henceforth, we refer to the linked BT 21CN and GB TSRM as the GB CPPS model, see Figure 3.4 showing the combination of both networks to form one cyber-physical network. Important assumptions have been made during the model development and running of the study which are explained in section 3.4.3.

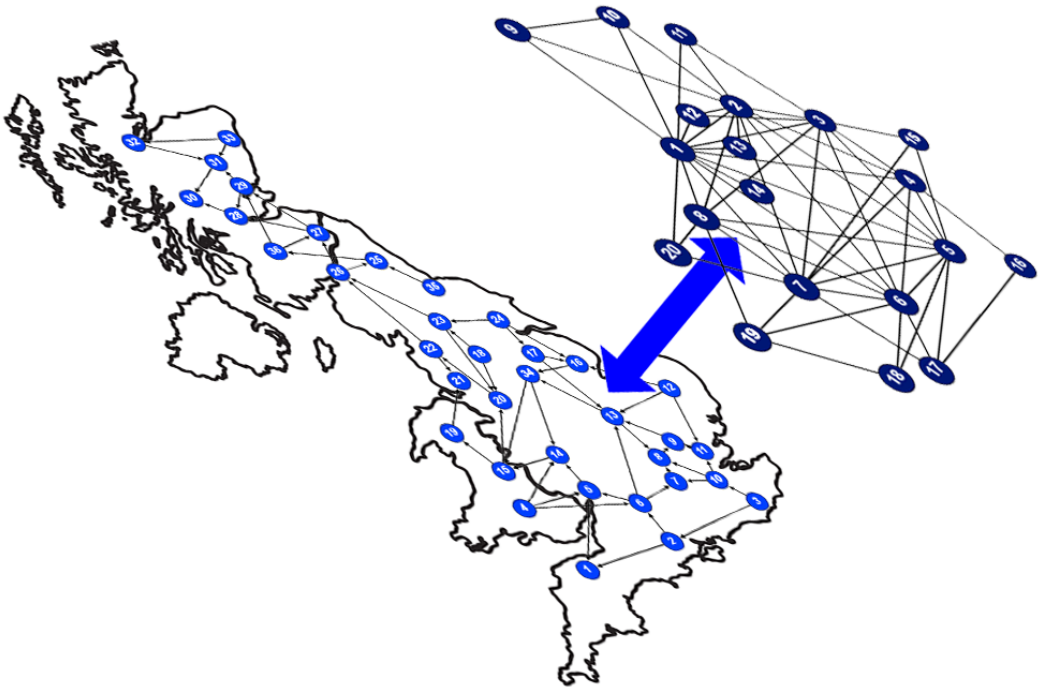

Figure 3.4: GB CPPS: Linking BT 21CN (upper network) with GB TSRM (lower network).

3.4.1 Selection of Communication Network

The BT 21CN fibre core network was selected as the communications networks for the CPPS model to be developed because current power grid services have strict communication requirements. The communication architecture must meet strict quality of service (QoS) requirements, most notably in its latency specifications, due to the high reliability required in the power grid. Switching to a commercially available fibre network would enable cost reduction while ensuring the required QoS.

The BT 21CN core network comprises 20 nodes interconnected by 68 links. 8 inner and 12 outer core nodes make up the core nodes. While the 12 outer nodes are connected to at least three other nodes, each of the 8 inner core nodes are completely meshed with each other. As a result, certain nodes are not directly connected to one another. The network topology and list of cities is shown in Figure 3.5.

The protocol used is IP over Wavelength Division Multiplexing (IPoWDM), which allows for multiple communication links to use a common transmission fiber by transmitting different wavelengths at the same time. IPoWDM contains a number of delays

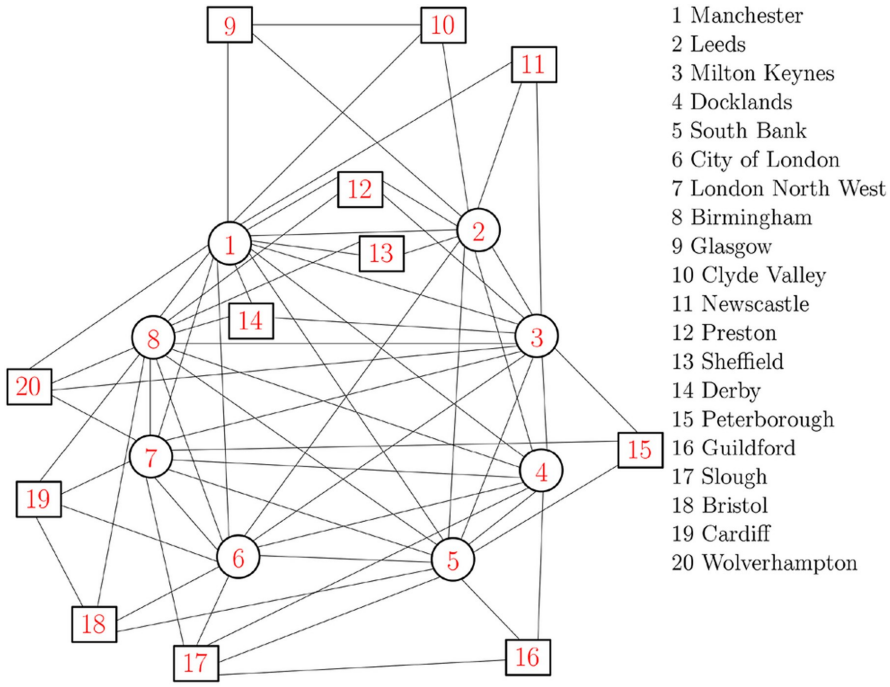

Figure 3.5: The BT 21st Century Fibre Core Network [60]

due to the processes and network components [60], [77]. The delays are:

- Propagation delay: The travel time through the transmission medium.
- Queuing delay: Time experienced by traffic packets in buffers waiting to be processed or transmitted.
- Switching delay: Time experienced due to processes at optical switches. E.g. an optical switching delay of 60 µs in [60].
- Processing delay: Time experienced due to processes at routers and transponders. E.g. 100 µs and 10 µs for core router processing delay and transponder processing delay respectively in [60].
- Transmission delay: Time required to place all the bits of a packet to be sent onto the transmission link.
- Amplifying delay: Time experienced due to processes at erbium-doped fibre amplifiers (EDFAs). E.g around 50 µs in [60].

3.4.2 Selection of Power System Model

The description of the GB TSRM is discussed in section 4.3

Table 3.1: Core Nodes of the BT 21CN

City Number	City Name	Core Node Type
1	Manchester	Inner
2	Leeds	Inner
3	Milton Keynes	Inner
4	Docklands	Inner
5	South Bank	Inner
6	City of London	Inner
7	London North West	Inner
8	Birmingham	Inner
9	Glasgow	Outer
10	Clyde Valley	Outer
11	Newcastle	Outer
12	Preston	Outer
13	Sheffield	Outer
14	Derby	Outer
15	Peterborough	Outer
16	Guildford	Outer
17	Slough	Outer
18	Bristol	Outer
19	Cardiff	Outer
20	Wolverhampton	Outer

3.4.3 Case Study Assumptions: Graphs and Cross-Links

Firstly, a directed graph was derived from the GB TSRM network by conducting a power flow of the network in PowerFactory and observing the power flow between the nodes. The direction of the power flow would indicate the same power flow and dependency. For instance, if power flows from node A to node B, then the directed edge would point to node B and node B is dependent on node A, such that if node A fails, node B fails as a result but not vice versa. Secondly, for the BT 21CN, other

than the time delay of the links between its nodes, all other time characteristics of the network such as node processing time was assumed to be zero. The data for this is sourced from [60] and a table of the time delays is provided in Appendix A, shown in Table A.1.

Table 3.2: Cross domain links between GB TSRM and BT 21CN

City Number	City Name	GB TSRM Zone
1	Manchester	Zone 20
2	Leeds	Zone 23
3	Milton Keynes	Zone 13
4	Docklands	Zone 10
5	South Bank	Zone 7
6	City of London	Zone 9
7	London North West	Zone 8
8	Birmingham	No link
9	Glasgow	Zone 28
10	Clyde Valley	Zone 27
11	Newcastle	No link
12	Preston	Zone 22
13	Sheffield	Zone 18
14	Derby	No link
15	Peterborough	Zone 17
16	Guildford	No link
17	Slough	No link
18	Bristol	Zone 1
19	Cardiff	Zone 4
20	Wolverhampton	No link

Finally, two important assumptions were made regarding the co-location between the power station nodes of the GB TSRM and the communication nodes of the BT 21CN. The first is that cross-links were only established were the corresponding communication node of the same location (of power station node) exists. See Table 3.2 to see the example of no link for Birmingham and a link between Manchester and Zone 20. The total number of cross-domain links were 14. This approach differs from the study conducted in [60], were for the unassigned power stations, they assigned

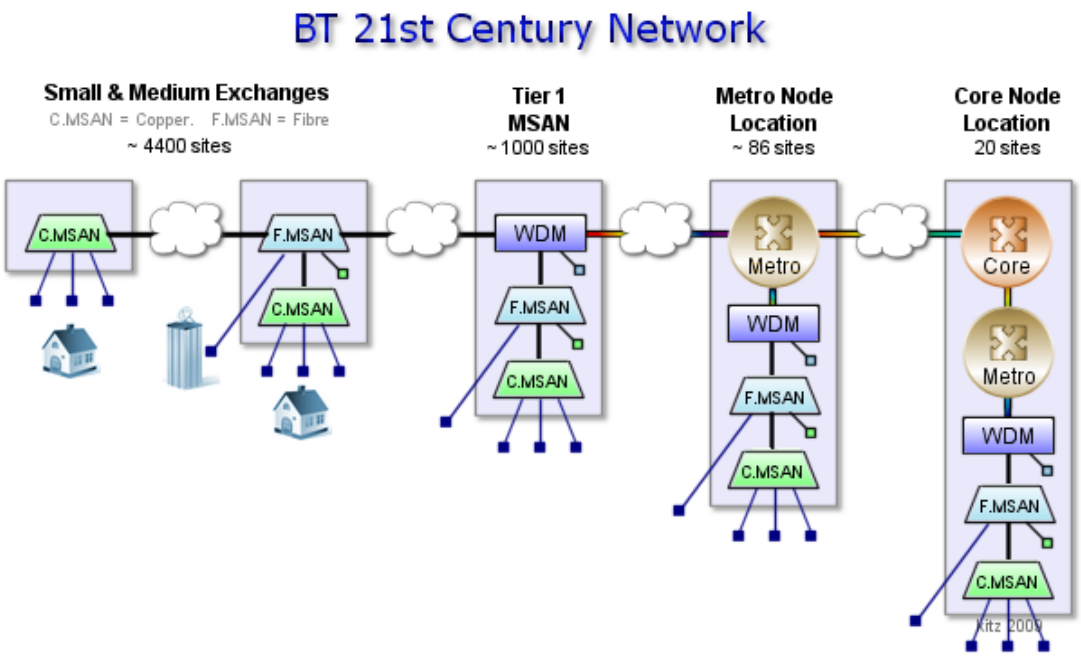

Figure 3.6: Connection of access points, exchanges and communication nodes of the BT 21CN [75]

the communications node that was closest to that location, meaning all communication nodes had a link. The second assumption was that the power station node was directly connected to the communication node with no last-mile communication technology modelled, which would have represented a more realistic setup. See Figure 3.6 to see this visualised, and shows that instead of the power station nodes connecting directly into the core nodes of the BT 21CN, it would connect to an access or node [75].

3.4.4 Simulation Setup

MATLAB (version R2025a) was used to build the GB CPPS model described in the previous sections, and to execute the cascading failure, the betweenness centrality and ASPTDD algorithms, ultimately attaining the CNII for each cyber node. MATLAB was used due to its accessibility, familiarity and ease of use especially for matrix-based calculations. Seperate MATLAB .m files were used to calculate each parameter. The MATLAB code for the CNII equation can be seen in Figure 3.7 alongside the relevant parameters of Fp, Np, C_B, S_CB, which represent the values of the total

power stations failed per communication node, the total number of power stations in the GB model (which is 36), the betweenness centrality of each communication, the sum of betweenness centrality of all communication nodes, and the ASPTDD respectively, as detailed prior and presented by Equation 3.3 in Section 3.3.1.

D:\Documents\MATLAB\GB_CPPS\importance_index.m

```
% Calculating communication node importance index as given by the equation
% available in this matlab folder (GB_CPPS) as an image file.

load('total_failed_powerstations.mat')
load('bc_nodes_distr.mat')
% load('t_d') % old delta_t_d based on old delays
% load('delta_t.at') new delta_t_d based on new delays

I = zeros(1,20); % Preallocation
Np  = 36; % Total number of power stations
Fp  = total_failed_powerstations; % per node'n'
C_B = bc_nodes_distr; % betweenness centrality of each node
S_CB = sum(bc_nodes_distr); % sum of bc of all nodes

% calculating cyber node importance index:
for n=1:20
    I(n)=(Fp(n)/Np)+(C_B(n)/S_CB)+delta_t(n);
end
I

```

Figure 3.7: MATLAB code for the Cyber Node Importance Index (CNII) equation

The cascading failure algorithm, which was introduced in Section 3.3.2), was implemented by two functions. The first function (fail_power) iterates through the GB CPPS matrix to analyse the number of power (stations) nodes failed due to the failure of an initially selected power node, and this is calulcated for all the power nodes. The MATLAB code of this first function is presented in Figure 3.8. The second function (fail_cascade), analyses the total number of power stations failed due to the failure of an initially selected communication node. This is programmed by including employing the first function in this second function, as shown by Figure 3.9. Similar to the first function, the number of total failed power nodes is calculated for all the communication nodes. The results of these parameters and the CNII is discussed in the next section.

The MATLAB code for the remaining parameters can be found in the appendix;

D:\Documents\MATLAB\GB_CPPS\fail_power.m

```
function power_nodes_failed = fail_power(P)
%Calculates number of power stations failed due to failure of
%a selected power (station) node.
%   Input:
%       P                   - index of initially selected power node.
%
%   Outputs:
%       power_nodes_failed  - number of power nodes failed.

global CPPS_adj_mtx

CPPS_adj_0 = zeros(size(CPPS_adj_mtx,1),size(CPPS_adj_mtx,2));
for i = 1:size(CPPS_adj_mtx,1)
    for j = 1:size(CPPS_adj_mtx,2)
        CPPS_adj_0(i,j) = CPPS_adj_mtx(i,j);
    end
end

P1_out   = [P];
Nodes    = 1;
FromNode = [P]; % e.g 5
NextNode = [];

while ~isempty(FromNode)
    NextNode = [];
    for i = 1:length(FromNode)
        for j = 22:57
            if CPPS_adj_0(FromNode(i),j) == 1
                NextNode = [NextNode j];
                P1_out = [P1_out j] ;
                CPPS_adj_0(FromNode(i),j) = 0;
            end
        end
    end
    FromNode = [];
    for i = 1:length(NextNode)
        FromNode(i) = NextNode(i);
    end
end
P1_out = unique(P1_out);
X = ['Power node ',num2str(P), ' causes the subsequent failure of power node(s): ',num2str(P1_out),];
disp(X);
power_nodes_failed = size(P1_out,2)
end
```

Figure 3.8: MATLAB code for analysing the impact of failing an initially selected power node.

the ASPTDD in Appendix B and the betweennes centrality in Appendix C.

3.5 Results and Discussion

3.5.1 Cascading Failure

Each communication node of the BT 21CN was intentionally failed in turn to investigate its cross-domain effect on the GB TSRM by studying the total number of power

D:\Documents\MATLAB\GB_CPPS\fail_cascade.m

```
function x = fail_cascade(C)
%Calculates number of power stations failed due to failure of
%a selected communication node.
%   Input:
%       C   - index of initially selected communication node.

global CPPS_adj_mtx

load('CPPS_adj_mtx.mat')

P_out = [];

if C > 21
    disp('ERROR: Communication node index input should be 21 or smaller')
    return
else
    for j = 22:57
        if CPPS_adj_mtx(C, j) == 1
            P_out = [P_out j];
        end
    end
    if ~isempty(P_out)
        output = ['Communication node ',num2str(C), ' causes the subsequent failure of power node(s): ',num2str(P_out),];
        disp(output);
        for i = 1:length(P_out)
            fail_power(P_out(i));
        end
    else
        output = ['Communication node ',num2str(C), ' does not cause any subsequent failure.'];
        disp(output);
    end
end
end

```

Figure 3.9: MATLAB code for analysing the impact of failing an initially selected communication node.

stations that fail as a result. The results of this can be observed from Figure 3.10. The results show a clear variation in the adverse effects that certain communication nodes have over others with the maximum number of power stations failed, which is 23, caused by the failure of communication node Cardiff and the least amount, excluding zero, is 1 failed power station caused by the failure of London and Bristol. Both London and Bristol are major UK cities so the resulting miniature effect they had was unexpected. The communication nodes that caused no failed power stations in this study are Derby, Guildford, Slough and Wolverhampton, which was somewhat expected due to them not being major cities.

Since the inner core nodes of the BT 21CN network are the most important, it was predicted that the total effect of failing them would cause much more damage than failing the outer core nodes, however the total number of power stations failed

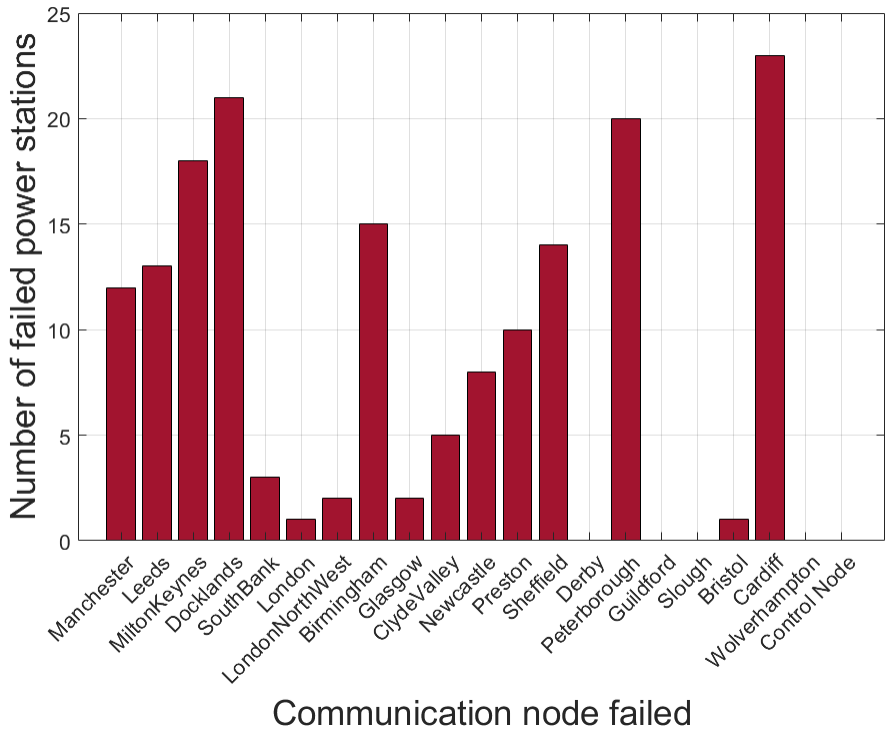

Figure 3.10: Power station cascading failure for each communication node

due to the failure of all the inner core nodes is 85 whilst that of the outer core nodes is 83. This difference was lower than expected but could arise due to the unique inter-meshing of all the core nodes. There are 4 communication nodes that cause the total failure of half of the power grid nodes or more: Milton Keynes, Docklands, Peterborough and Cardiff, so these nodes should be identified as critical nodes and receive due attention accordingly.

3.5.2 Cyber Node Importance Index

The CNII, as defined in Equation (3.3), was calculated for each node in the BT 21CN network to quantify their relative significance. The results as shown in Figure 3.5, ordered by decreasing CNII values, reveal a clear hierarchy of node importance across the network.

Cardiff emerged as the most critical node with a CNII of 0.6734, underscoring its pivotal role in the network's resilience. At the other extreme, Guildford, Slough, Derby, and Wolverhampton exhibited the lowest CNII values (0.0345 each), aligning

with expectations given their mostly peripheral status in the network. The distribution of CNII values between these extremes follows a gradual progression, with no abrupt disparities between adjacent nodes.

While the data does not exhibit distinct natural clusters, a tripartite classification offers practical insights:

- High-importance cities (CNII $>$ 0.5): Includes cities like cardiff and Birmingham, and reflects their signficant influence in the network.
- Medium-importance cities (0.1 $\leq$ CNII $\leq$ 0.5): Comprises nodes with moderate but non-negligible impact on network functionality.
- Low-importance cities (CNII $<$ 0.1): Encompasses nodes like Guildford and Derby, whose failure would have minimal cascading effects.

This classification is visualised in Figure 3.12, where nodes are colour-coded by their group, alongside the network topology, which is also colour-coded. The CNII framework is scalable and adaptable, making it suitable for analysing larger, more

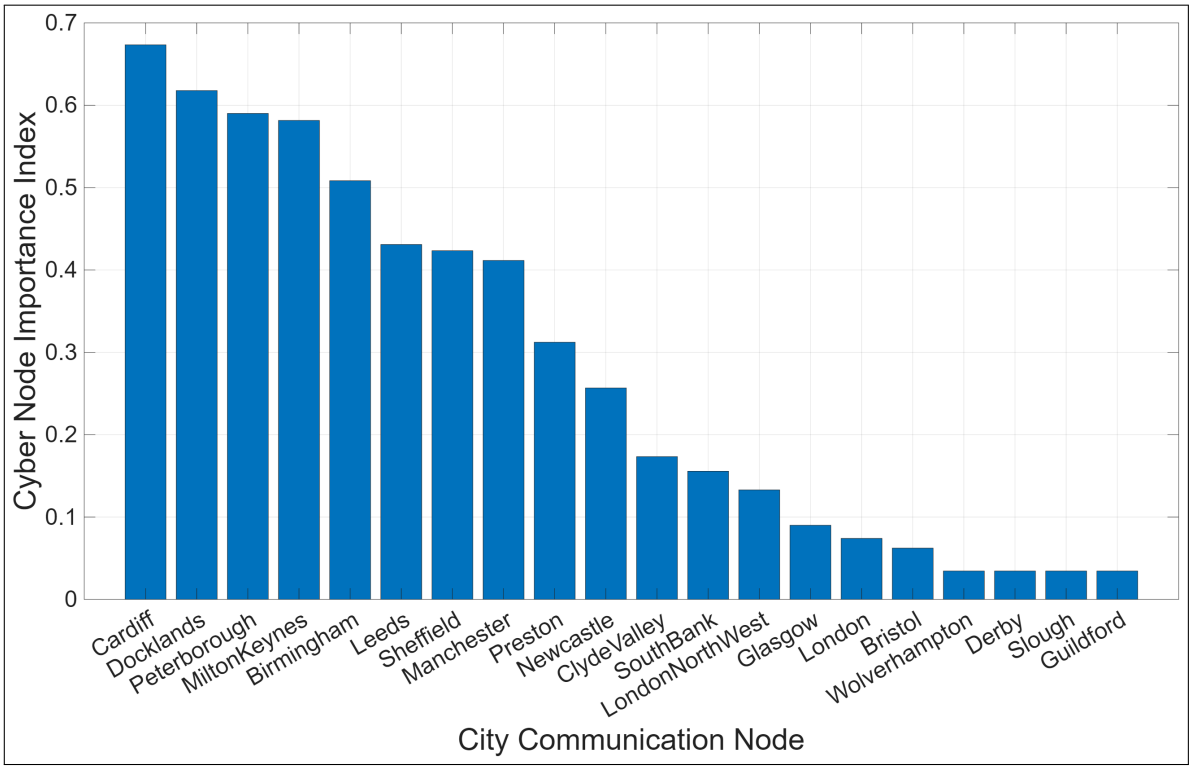

Figure 3.11: Cyber node importance index of each city communication node

complex CPPS models with hundreds of interconnected routers, switches, and end-user nodes. By identifying critical nodes such as Cardiff, stakeholders can prioritise resource allocation and protective measures to enhance overall network robustness.

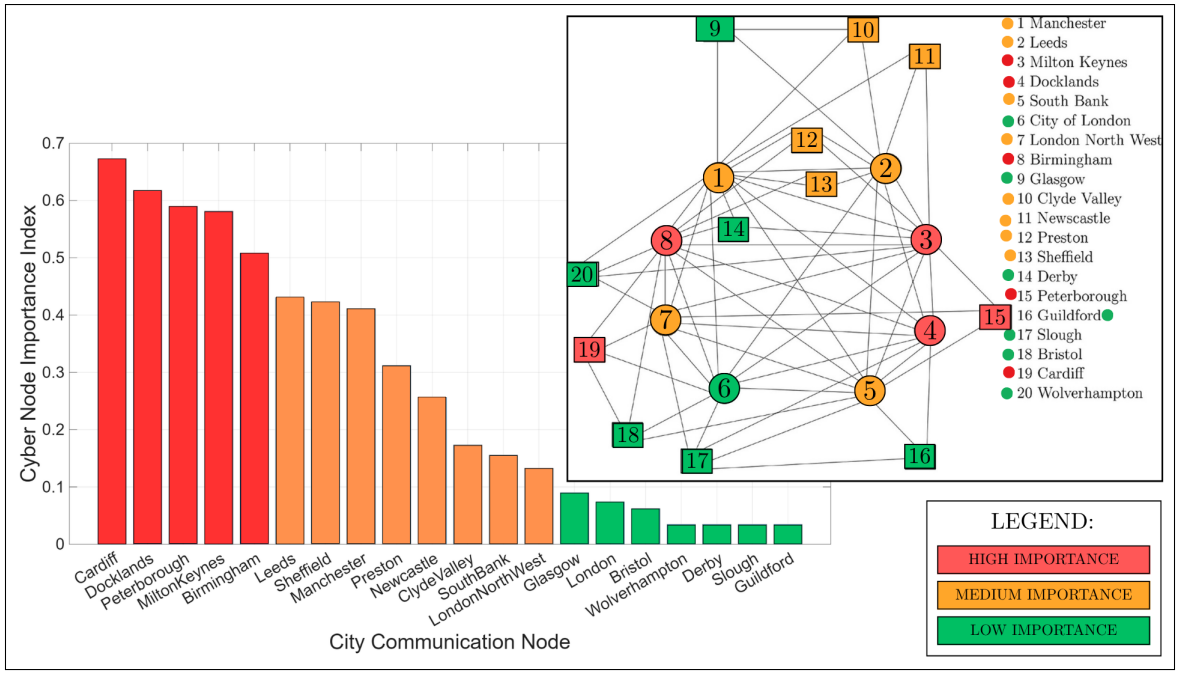

Figure 3.12: Cyber node importance index of each city assorted into three groups

3.5.3 Centralised vs Distributed Topology

To change the BT 21CN into a centralised topology, a Control Node was introduced through which all other transmissions must pass through. As seen in Figure 3.13, the betweenness centrality of the Control Node is significantly higher than most of the other nodes as expected. After the Control Node, the next most important nodes are all the inner core nodes as expected since they form a meshed network, meaning every inner core node is connected to every other inner core node whilst this is not true for the outer core nodes. Other than the heightened vulnerability of a centralised control node as a target, some other reasons a centralised topology is not preferred are because they are computationally expensive, use inefficient storage and are less private and less secure [78], [79].

In the distributed communication network topology, as shown in Figure 3.14, the maximum betweenness centrality is 109 displayed by Birmingham and the minimum

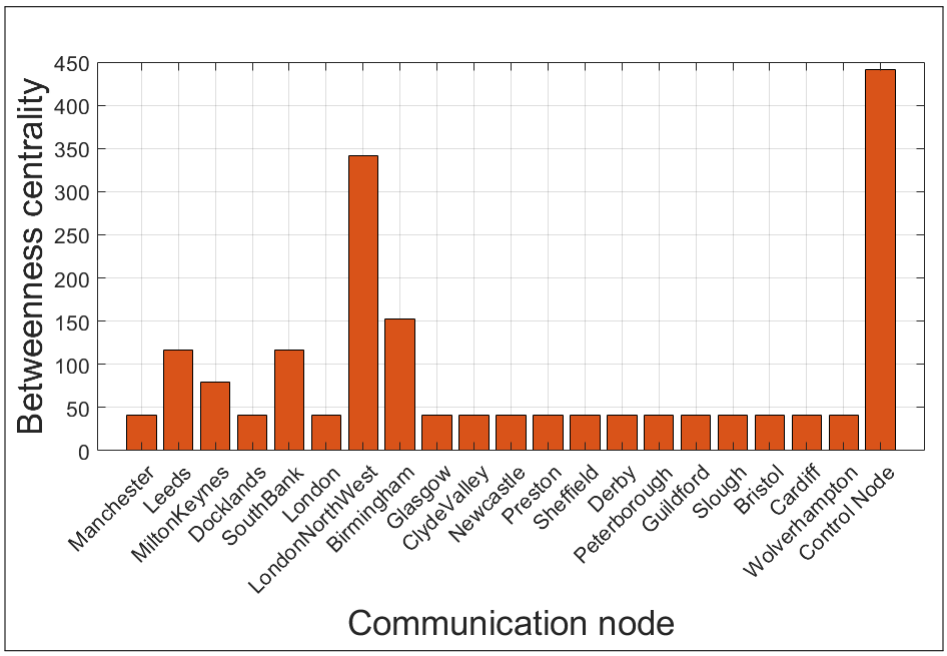

Figure 3.13: Betweenness centrality of nodes when BT 21CN is in centralised topology

is 41 shown by 14 other communication nodes. The most important nodes are all part of the inner core nodes as expected.

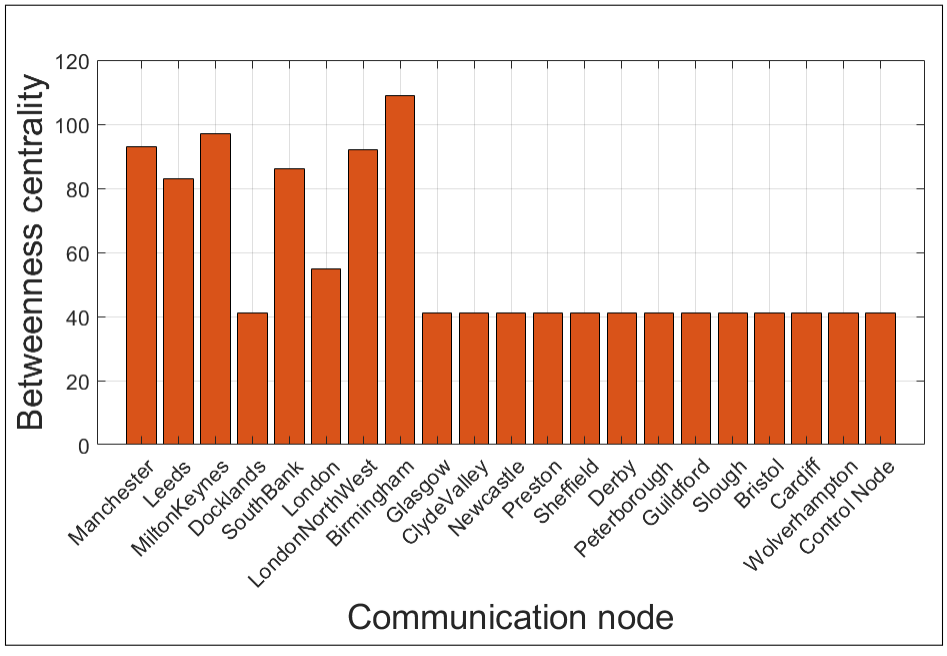

Figure 3.14: Betweenness centrality of nodes when BT 21CN is in distributed topology

3.6 Chapter Summary

This chapter has contributed to the first category of modelling and simulation approaches to CPPS, model-based approaches, by focusing on vulnerability-type studies of critical infrastructure and large networks, extracting practical benefits from theoretical frameworks. The chapter began by dissecting a graph theory-based method for representing networks, with the aim of accurately Modeling any chosen power system network and its associated communication infrastructure. The integration of these two representation of network to form a comprehensive CPPS representation was also detailed.

Next, the chapter introduced a novel node importance metric, termed the Cyber Node Importance Index (CNII), which evaluates the significance of cyber nodes within a graph-based CPPS model. The CNII incorporates cascading failure effects, betweenness centrality, and time delays of the shortest paths in the CPPS, providing a more holistic assessment of node criticality. To promote reproducibility and further advancements, MATLAB code for calculating these parameters has been shared.

Both the CPPS model representation and the CNII were applied to two realistic large-scale networks in Great Britain: the GB Transmission System Reliability Model (TSRM) for the power network and the BT 21CN for the communication network. Through cascading failure simulations, the impact of individual cyber node failures on the physical network was assessed. Additionally, betweenness centrality and time delays for each cyber node were computed. The results underscore the importance of incorporating time delays in the CNII, demonstrating its advantages for analysing node criticality in real-world CPPS models.

The methodologies and insights presented in this chapter advance the field of critical infrastructure resilience by providing a structured, graph-theoretical approach to assessing vulnerabilities in CPPS. The introduction of the CNII offers a more nuanced understanding of node importance, enabling better prioritisation of cyber-physical interdependencies in risk assessments. By validating these approaches on realistic GB networks, this work contributes directly to improving the security and reliability of modern power systems, supporting future research and practical implementations in infrastructure protection.

Chapter 4

Interfacing Simulation Tools for Offline to Real-Time Model Conversion

4.1 Introduction

This chapter focuses on a methodology of converting offline power system models to real-time mode. As modern power systems integrate complex and distributed energy resources, real-time simulation has become an essential tool for understanding dynamic behaviours, evaluating control strategies, and testing system stability under realistic conditions. The work presented in this chapter bridges the gap between offline and real-time analysis by addressing key challenges in interfacing simulation tools and ensuring robust, high-fidelity simulation environments.

Figure 4.1 shows a block diagram of the organisation of this chapter; firstly, the origin and background of the GB Transmission System Reduced Model (GB TSRM), the selected real infrastructure model in this work. Its significance is outlined followed by a discussion of important modelling details and power system components, such as HVDC models.

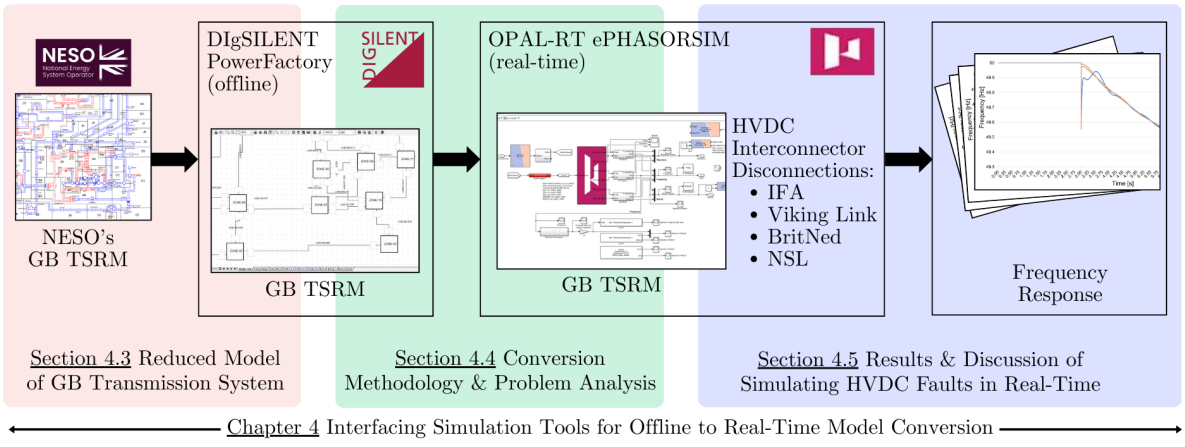

Figure 4.1: Block diagram of the core sections of this chapter, illustrating the workflow from the NESO's GB model to attaining the frequency response results

The core of this chapter is dedicated to interfacing DIgSILENT PowerFactory with OPAL-RT's ePHASORSIM, enabling the transition from offline models to real-time simulation environments. The methodology involves overcoming challenges related to compatibility, data exchange, and synchronisation between these tools. A step-by-step approach is detailed for the conversion. This integration facilitates HIL and SIL testing and the dynamic analysis of power systems, including stability and protection

mechanisms.

The contributions of this chapter lay the groundwork for further advancements in real-time simulation and HIL platforms. Future research could build on this work by incorporating additional functionalities, such as advanced visualisation tools, integration of renewable energy resources, and the testing of emerging grid technologies. Expanding the framework to include communication network models and studying the interactions between power and communication systems would also provide valuable insights for CPPS. These directions can help ensure that future power systems are not only efficient and reliable but also resilient to the challenges posed by an increasingly interconnected energy landscape.

4.2 Selected Software and Hardware Tools

For this research, the chosen tools for offline and real-time power system simulations are DIgSILENT PowerFactory and OPAL-RT's ePHASORSIM, respectively. PowerFactory is a widely used offline simulation tool that supports a wide range of power system analyses functions including load flow, short-circuit and stability studies. It is particularly well-suited for analysing large-scale transmission and distribution networks, making it an ideal choice for steady-state and dynamic analysis of the power grid. PowerFactory's robust modeling capabilities, extensive library of components and user-defined modelling capability enable detailed representation of complex power systems, including advanced models for RES and FACTS.

ePHASORSIM is a real-time simulator designed specifically for large-scale, phasor-based simulations of power systems. It operates within the OPAL-RT real-time simulation environment and is capable of running complex network models at high simulation rates. ePHASORSIM supports the integration of hardware devices through HIL configurations, enabling the testing and validation of control and protection schemes in a real-time environment. This capability is crucial for evaluating the performance of the power grid under varying operating conditions and for developing strategies to enhance grid stability and resilience.

A reduced model of GB transmission system produced in-house by BIPS (Brunel

Interdisciplinary Power Systems) will be used in this project. It is a modified version of the original reduced model developed by National Grid which is in turn based off their full GB model developed in PowerFactory for offline transmission analysis (OLTA) [80].

The modifications of the in-house model were performed on the synchronous machine controllers since NESO's reduced model contained customised synchronous machines controllers whilst ePHASORSIM only supports common controllers such as GOVs, AVRs and PSSs [81].

4.3 Reduced Model of GB Transmission System

4.3.1 Background

NESO, formerly National Grid ESO, uses offline transmission analysis (OLTA) as its primary tool for the analysis of the GB transmission system during their network planning processes and design studies for up to ten years ahead [80]. In order to do so successfully, NESO employs a complete model of the GB transmission system in DIgSILENT PowerFactory [82], which is an industry-standard in the power system tools market. This complete model contains the full topology, generations, transmission capacities, HVDC links, and distribution network representations of the real GB transmission system. Therefore its static and dynamic behaviours will closely resemble those of the real GB system.

OLTA is specifically used to assist in designing and configuring the network to be both secure and cost-effective before real-time operations. The model includes all transmission-level switches and representative distribution-level switches, ensuring realistic operation during normal conditions and fault scenarios. However, this detailed and accurate model is not publicly accessible due to third-party confidentiality concerns. To address this, NESO developed a reduced model in 2012, using only non-confidential data, which facilitates the rapid creation of various future scenarios, making it particularly valuable for academic research and collaborations. As a result, researchers at Brunel have further developed and modified the original reduced

model to suit the requirements of RT HIL simulation [81].

The full model of the GB transmission system, published in the National Grid's Electricity Ten-Year Statement (ETYS) [80], identifies 96 distinct system zones. The reduced model was created by aggregating these ETYS zones into a smaller set of broader zones. For example, Zone 02 in the reduced model represents a combination of ETYS zones B1 and B2 from the full model.

4.3.2 Model Description

Each zone is simplified further by its representation with a single substation. These substations have equivalent structures, reflecting the relevant mix of generation types and load within that zone, as illustrated in Figure 4. The original 2012 reduced model includes common generation types found in the GB system, such as gas, coal, nuclear, pumped storage, oil, hydro, marine, biomass, and wind. The generators in each zone are modelled as the total generation of each fuel type for that zone. If a zone does not have a particular fuel type, the corresponding generator is set to zero and treated as inactive during the simulation. Similarly, the total load in each zone is consolidated and represented by a single demand bus. The power lines in the reduced model serve as virtual representations of the aggregated circuits from the full system, using realistic equivalent impedances to connect the zones.

In the reduced model, the controllers of the generators are non-standard and user-defined models developed by NESO based on data provided by the generators. This methodology was required to closely resemble each type of generation in the zones. A detailed HVDC model, which is based on line commutated converter (LCC) technology, has also been incorporated into the reduced network to symbolise interconnectors to the GB system. Figure 4.2 shows part of the GB TSRM in DIgSILENT PowerFactory.

4.4 Conversion Methodology and Problem Analysis

The real-time RMS-based simulator ePHASORSIM can import the eXtensible Markup Language (XML) file, which acts as a netlist, produced by PowerFactory's DGS ex-

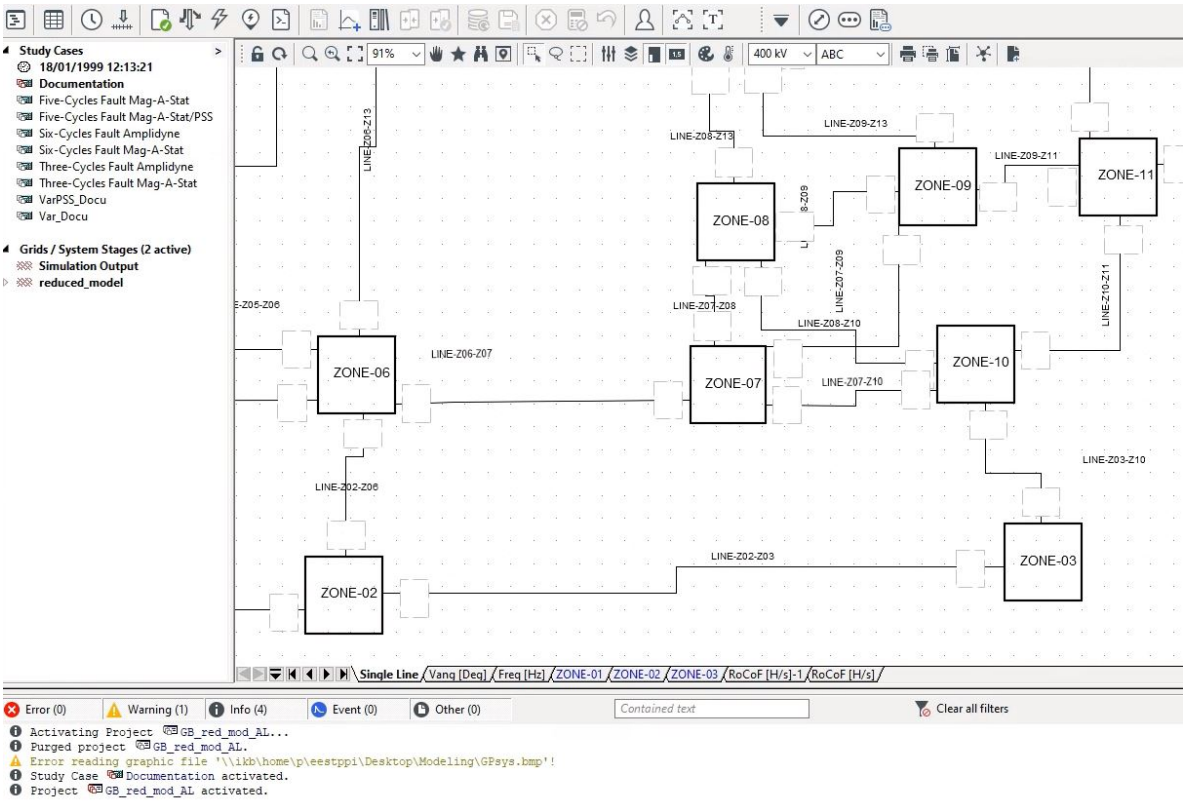

Figure 4.2: Part of the GB TSRM in PowerFactory

port tool. The imported XML file will have its data mapped to a positive sequence library of models, which are representative of transmission systems. This capability is used in this work to allow for an offline model in PowerFactory to be interfaced with ePHASORSIM for simulating a power system in real-time to enable for HIL and SIL setups, such as protection relay testing and real-time communications modelling respectively.

4.4.1 Model Conversion Process

PowerFactory has the ability to import and export models in order to interface with other proprietary software packages and for data conversion. For example, power system models created or available in tools such as PSS/e and Neplan can be imported into PowerFactory. Bi-directional data exchange is possible using a DGS interface tool which supports a range of formats such as ASCII and XML which further also contain GIS and SCADA metadata support. In this work we will be employ-

ing this DGS interface tool capability to export the GB TSRM as an XML file format which includes all data for the network topology and component parameters. We term the generated and exported file as the ”DGS-XML file” and will be using this term henceforth.

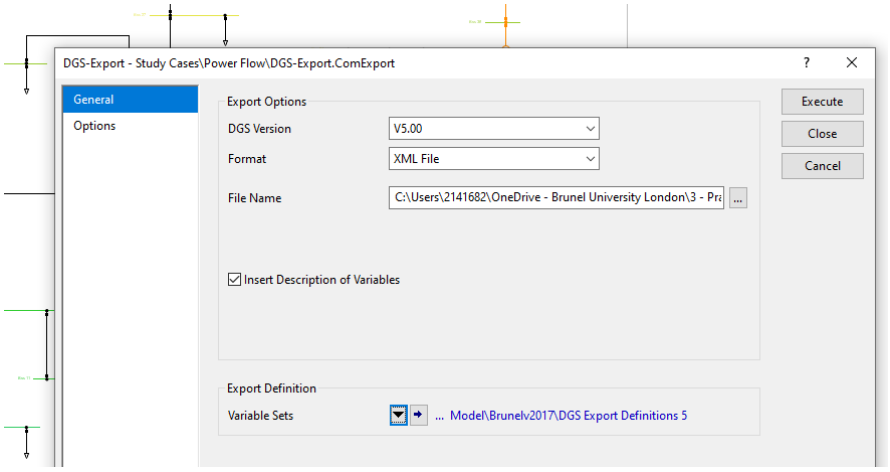

Figure 4.3: The DGS exporting tool menu on PowerFactory with options and settings

Figure 4.3 shows the PowerFactory menu for exporting its models via DGS. For this work, version 5 of the DGS versions is needed as stipulated by OPAL-RT's guide at the time of this writing [83]. The format of the DGS export required is in the XML format which is a flexible and self-descriptive markup language designed to store, structure, and transport data in a hierarchical format that is both human-readable and machine-readable [84].

4.4.2 DGS-XML File

As an example, shown below, in Listing 4.1, is an extract from the DGS-XML file of the IEEE 9 Bus System. This system model is available in the examples in PowerFactory. The IEEE 9 Bus System which is available in the example power system models from PowerFactory. The different sections of the DGS-XML file are explained in detail to familiarise with some of the main content that a typical DGS-XML file contains. This is important for two main reasons:

1. To understand how ePHASORSIM maps the data from the DGS-XML file to

its own library of models which allows for model development (e.g. deciding a power system event such as a fault, selection of variables to measure or interact with such as voltage magnitude and frequency). For this the I/O pins file is a vital part, and will be mentioned later.

2. To be able to debug and identify any issues arising from the ePHASORSIM rejecting or not capable of executing the DGS-XML file. This enables for root-cause analysis of the issue and the error or specification-mismatch will be pin-pointed further enabling for potential solutions. This major concept has been employed to solve and successfully debug the DGS-XML file and allow for seamless execution of a real-time power system model.

Listing 4.1: Extract from the DGS-XML file of the exported IEEE 9-Bus System

```
1  <?xml version="1.0" encoding="UTF-8" standalone="no" ?>
2  <DGS application="DIgSILENT■(C)■PowerFactory■V19.0.5" date="
       2023-02-20T20:20:43" format="DIgSILENT■(R)■DGS■Export■V1.8.4"
       project="Nine-bus■System" studycase="01-■Load■Flow" xmlns:xsi="
       http://www.w3.org/2001/XMLSchema-instance"
       xsi:noNamespaceSchemaLocation="IEEE9_AL_PF_no_descr_var.xsd">
3
4    <ElmComp>
5      <ID>2</ID>
6      <loc_name>Plant_G2</loc_name>
7      <fold_id>12</fold_id>
8      <outserv>0</outserv>
9      <typ_id></typ_id>
10     <pelm.SIZEROW>7</pelm.SIZEROW>
11     <pelm.0>14</pelm.0>
12     <pelm.1></pelm.1>
13     <pelm.2></pelm.2>
14     <pelm.3></pelm.3>
15     <pelm.4></pelm.4>
16     <pelm.5></pelm.5>
17     <pelm.6></pelm.6>
18   </ElmComp>
19
```

```
20    <ElmLne>
21      <ID>3</ID>
22      <loc_name>Line 4-5</loc_name>
23      <fold_id>12</fold_id>
24      <typ_id>70</typ_id>
25      <dline>1</dline>
26      <chr_name></chr_name>
27    </ElmLne>
```

In OPAL-RT's online documentation for using ePHASORSIM [85], the DGS-XML code shown in Listing 4.1 is referred to as the 'PowerFactory File'. This file needs to be stored in the ePHASORSIM folder on the computer (also known as the host) which is connected to the OPAL-RT hardware target. A general example file tree is shown in Figure 4.4 and the actual folders and files are shown in Figures E.1 and E.2 in Appendix B.

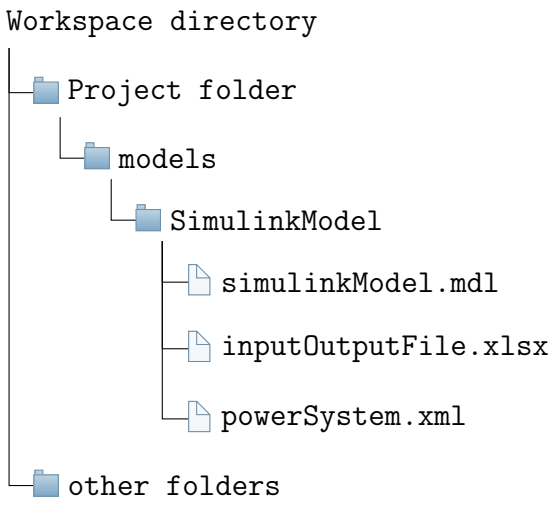

Figure 4.4: Directory file system tree illustrating important model files

The file contains the 'PowerFactory Data' and begins with the XML Declaration as shown in line 1. This declaration specifies the CML version "(1.0)" and character encoding "(UTF-8)" whilst the "standalone=0" indicates that the XML depends on an external schema for validation which has the file extension of .xsd put after the same file name as the .xml. For the root element in line 2 "DGS" there exists several

attributes:

- application: Indicates the software version used for exporting (PowerFactory V19.0.5).
- date: Timestamp of the export (2023-02-20T20:20:43 in ISO 8601 format).
- format: Specifies the export file format version (V1.8.4).
- project: The project name (Nine-bus System).
- studycase: The specific simulation case (e.g., 01-Load Flow).
- xmlns:xsi: Namespace for XML Schema validation.
- xsi:noNamespaceSchemaLocation: Path to the schema file (IEEE9ALPFnodescrvar.xsd), used for validating the structure of this XML file.

Beginning from line 4, the first Child Element is shown, named ”ElmComp”. This represents a general component in the system such as generator or plant. In this example, the child elements are:

- ID: Unique identifier for the component (2).
- locname: Name of the component (Plant G2).
- foldid: Folder ID or grouping identifier (12), likely for organisational purposes.
- outserv: Indicates if the component is out of service (0 means in service).
- typid: Type ID of the component (empty in this case, may refer to a predefined type).
- pelm: Stores parameters related to the component.
- SIZEROW: Number of rows for a parameter matrix (7).
- P0, P1: etc.: Parameter values. For example, P0 has a value of 14.

The data for a transmission line is shown at line 20 of the code in Listing 4.1. It is composed of the child elements:

- ID: Unique identifier for the line (3).
- locname: Name of the line (Line 4-5).
- foldid: Folder ID, grouping the line under a specific category (12).
- typid: Type ID of the line (70), referencing predefined line types.
- dline: Indicates if the line is active (1 means active).
- chrname: Reserved for an optional characteristic name, which is empty in this case.

In this extract, the XML file describes the components ElmComp and the lines ElmLne of the IEEE 9-Bus System that was available in PowerFactory examples and exported from using the DGS export tool. Generally, the XML file also contains metadata and configuration details for simulations such as load flow analysis. The XML file ensures consistency and validation via a linked schema file, which in this case is the ”IEEE9ALPFnodescrvar.xsd” file. The overall process can be understood from the block diagram as shown in Figure 4.5. More information regarding the DGS-XML file export as well as netlist mapping can be found in the ePHASORSIM User Documentation which is available on the OPAL-RT website online [86]–[88].

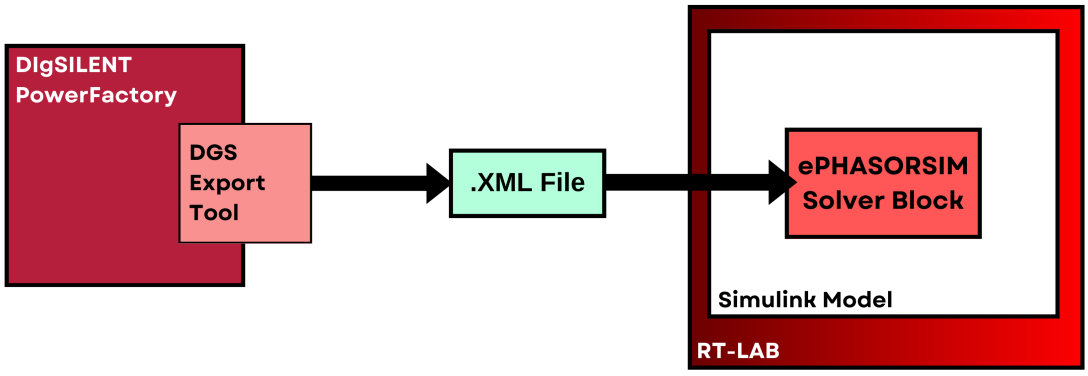

Figure 4.5: Block diagram of PowerFactory-ePHASORSIM Interface Process

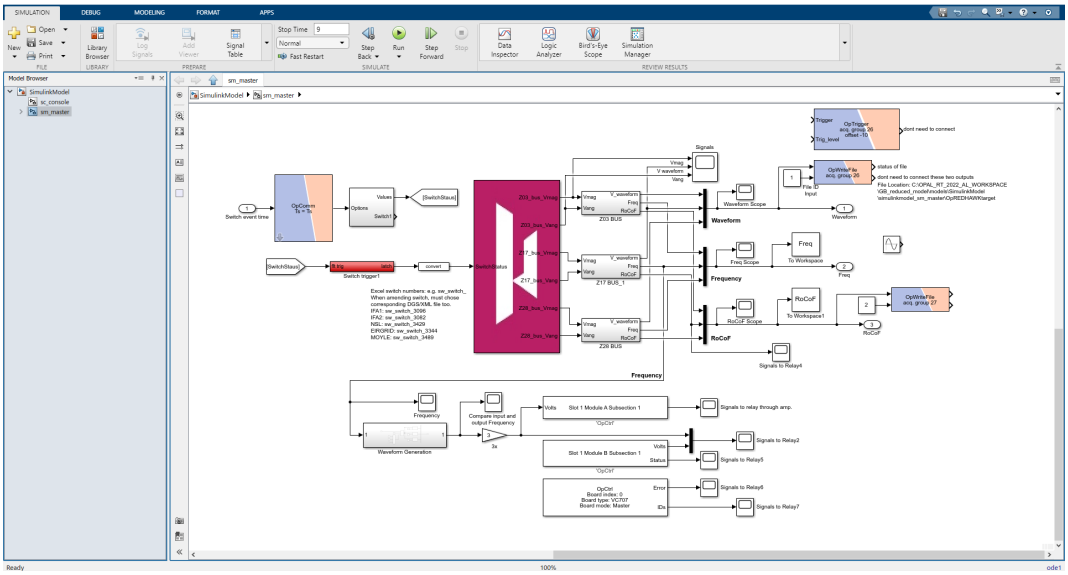

Figure 4.6: Overview of the simulink model of the HIL study

4.4.3 Import Process

Figure 4.6 shows the actual working environment concerning the ePHASORSIM Solver Block (in red) and the simulink environment all embedded into the RT-LAB software development environment window. It is this space which allows for model development, power system importing and simulation configuration.

Figure 4.7 shows the configuration and options window which appears after double-clicking on the ePHASORSIM Solver Block. This window is where the aforementioned DGS-XML file can be imported, as well as the I/O pins excel file which configures the input and output pins of the Solver Block. Note that the PowerFactory option must be selected from the ”Input file format” drop down options menu, all in the ”Network data” tab, as shown in the figure.

The DGS-XML file imported here is that of the GB Transmission System Reduced Model exported from PowerFactory. The process for preparing and executing the model in real-time using the RT-LAB environment is shown in Figure 4.8.

The first step is to open the model by clicking on the ”Edit the model.”. This opens the Simulink model as seen in Figure 4.7 and enables the editing of the model blocks and parameters as well as configuring the necessary input files, such as the DGS-XML file, and selecting suitable settings. A model must first be able to run offline

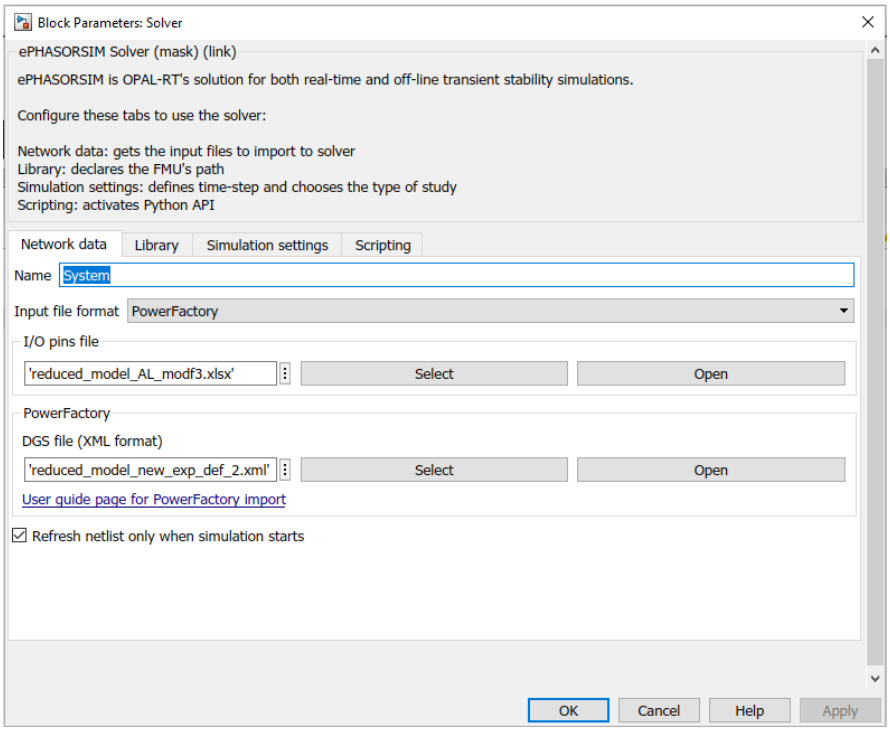

Figure 4.7: The ePHASORSIM solver's options menu in RT-LAB

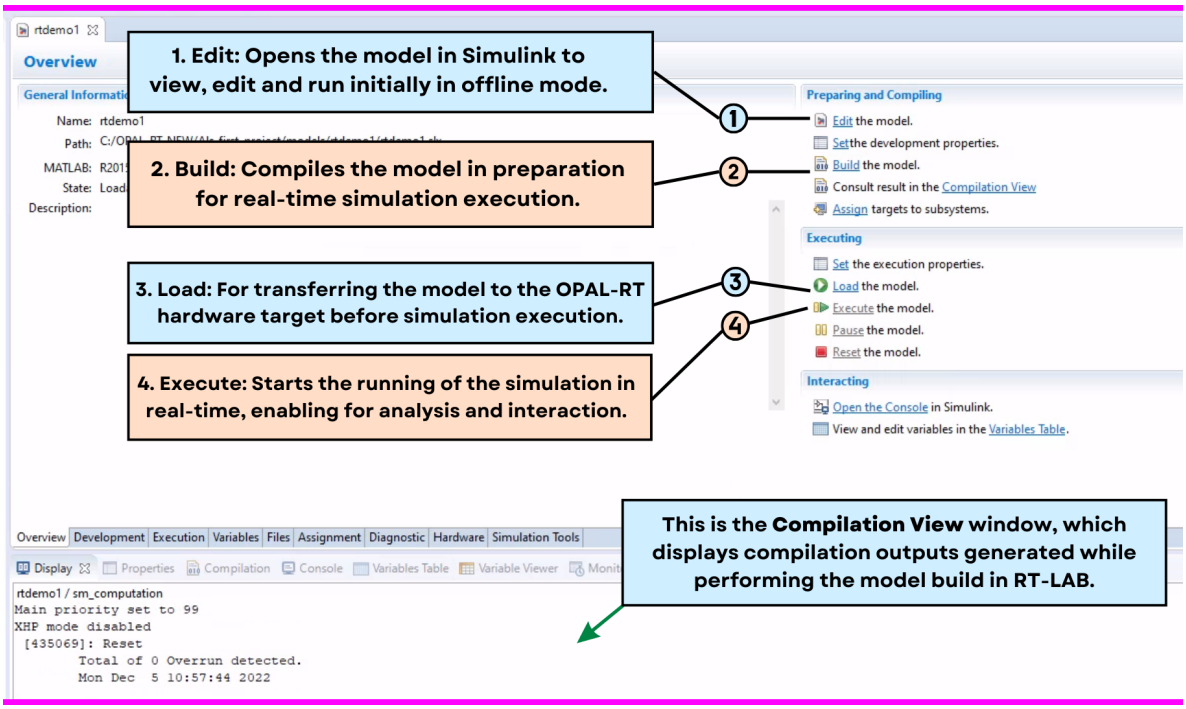

Figure 4.8: The model preparation and execution process in RT-LAB

successfully prior to real-time simulation. This first step is concluded by saving the model once all editing and configurations are complete. Then, the model needs to

be compiled to allow for preparation before real-time simulation execution. This is done by clicking on "Build the model.". Once the model is built successfully, It can be loaded onto the actual physical OPAL-RT hardware target, since it is this powerful computer that enables for the model to be executed in real-time. This is initiated by clicking on "Load the model.". After the model has been loaded onto the OPAL-RT hardware target, the model can finally be executed in real-time to allow for analysis and interaction with the model. This is done by clicking on "Execute the model."

Also shown towards the bottom of Figure 4.8, is the compilation window which displays compilation outputs generated while performing the model build in RT-LAB. Errors and warning messages are highlighted with red and orange colours respectively. A model that is not properly built is not executable on the target nodes.

4.4.4 Model Debugging Workflow

Several issues were faced with importing and executing the GB TSRM model in both in offline and real-time mode. For major issues, where significant time and effort was required, a systematic workflow was developed to aid in the determination of the root-causes and help develop solutions in a documented and managed approach. This would also help as a significant reference piece for future works and other researchers working on the same or similar projects.

Firstly, it is worth mentioning relevant changes in software and file formats in RT-LAB, ePHASORSIM and the PowerFactory import feature which were significant to this project. Up until version v2020.4 of RT-LAB (excluding), the PowerFactory file (the DGS-XML file) was a plain-text file encoded using ASCII and had a proprietary .dgs extension. In the updated workflow, this format was replaced by a structured .xml format based on the XML markup language, which is typically encoded in UTF-8 and allows for better parsing, validation, and integration with other tools. Also, the I/O pins file was saved in XLS format and after the RT-LAB update this was now required to be in XLSX format. The RT-LAB was updated because the PowerFactory import feature was disabled between version v2020.4 of RT-LAB to version v2021.3, where it was reworked and enabled [89]. Since the previous RT-LAB version used for this project was v2019, and the newer was v2022, the updates were necessary to

consider during the simulations in order to comply with the updated settings requirements and ensure the smooth running of software files and model execution. The relevant and important technical details are summarised in Table 4.1 with details for other software and hardware components of the study also included. Regarding the transition from .xls to .xlsx file formats for the I/O pins file, the significance lies not only in the updated content (I/O pin definitions, parameter data...etc.) but importantly in the change of file structure itself. The .xls format is a proprietary binary file format with limited flexibility and increased susceptibility to compatibility issues with contemporary software tools. In contrast, .xlsx is an open-standard, XML-based spreadsheet format, offering enhanced compatibility, easier parsing, and greater robustness in data handling processes. Furthermore, while software that supports .xlsx can typically read .xls files, the reverse is not true; older tools limited to .xls formats cannot read .xlsx files, making this change significant for ensuring forward compatibility and future-proofing simulation workflows. This transition, therefore, was technically significant for ensuring smoother integration, fewer import errors, and enhanced overall reliability in the simulation environment.

Table 4.1: Specifications of study hardware and software components

Component	Updated Setup	Previously
OPAL-RT Hardware Target	OP5700 S/N: OPT900064	same
Host Desktop	i7-3770 @ 3.40GHz 16GB RAM Windows 10 Enterprise 21H2	8GB RAM
RT-LAB	v2022.1.0.405	v2019
DGS-XML file format/extension	Structured XML /.xml (UTF-8)	Proprietary plain-text /.dgs (ASCII-encoded)
I/O pins file format/extension	XLSX/.xlsx	XLS/.xls
PowerFactory	2019 SP3 (x64)	same
MATLAB	R2021b Update 2 64-bit (9.11)	2015b 32-bit

Upon first errors with the offline running of the GB TSRM model, contact was made with the technical support team of OPAL-RT (OPAL-RT TS). Initially, the Unified Data Base (UDB) of RT-LAB was suspected as the issue, so subsequently OPAL-RT

TS opened an internal request with experts of the UDB and PowerFactory import feature in their Canada HQs. After identifying problems with ePHASORSIM's import tool, they started technical investigations whilst the OPAL-RT TS suggested modifications to the DGS-XML file including suggestions that the governor TGOV1 parameter "At" value has different expected values which blocked the importation process. The TGOV1 turbine-governor model in PowerFactory is a more generalized version of the one implemented inePHASORSIM. To make sure both of them are equivalent, the "At" constant of the internal additional gain block in the PowerFactory TGOV1 must be set to 1. Subsequently, the DGS-XML file was modified to act on this suggestion as shown in Figure 4.9, however this did not solve the issues.

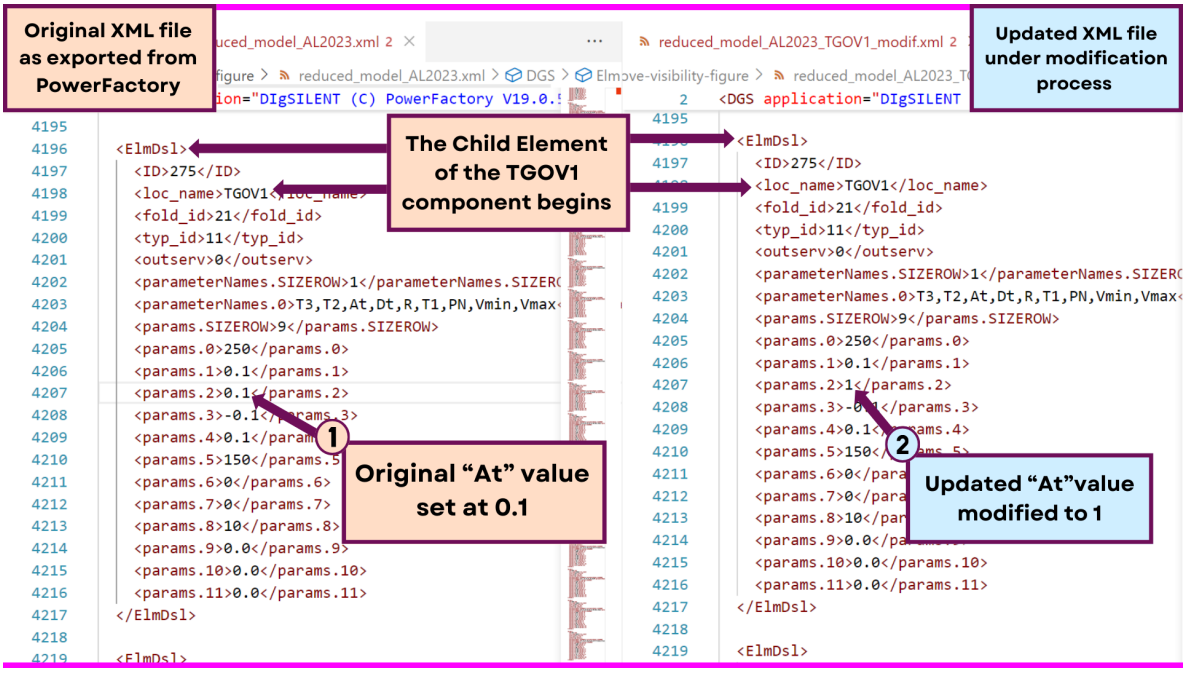

Figure 4.9: Modification of the XML file

The overview of the workflow for determining the root-cause and finding a solution via successful debugging is illustrated in Figure 4.10, showing the stages from initial parameter or component selection through to executing the power system model in Simulink and RT-LAB via the stage of modifying any values of the parameter or component.

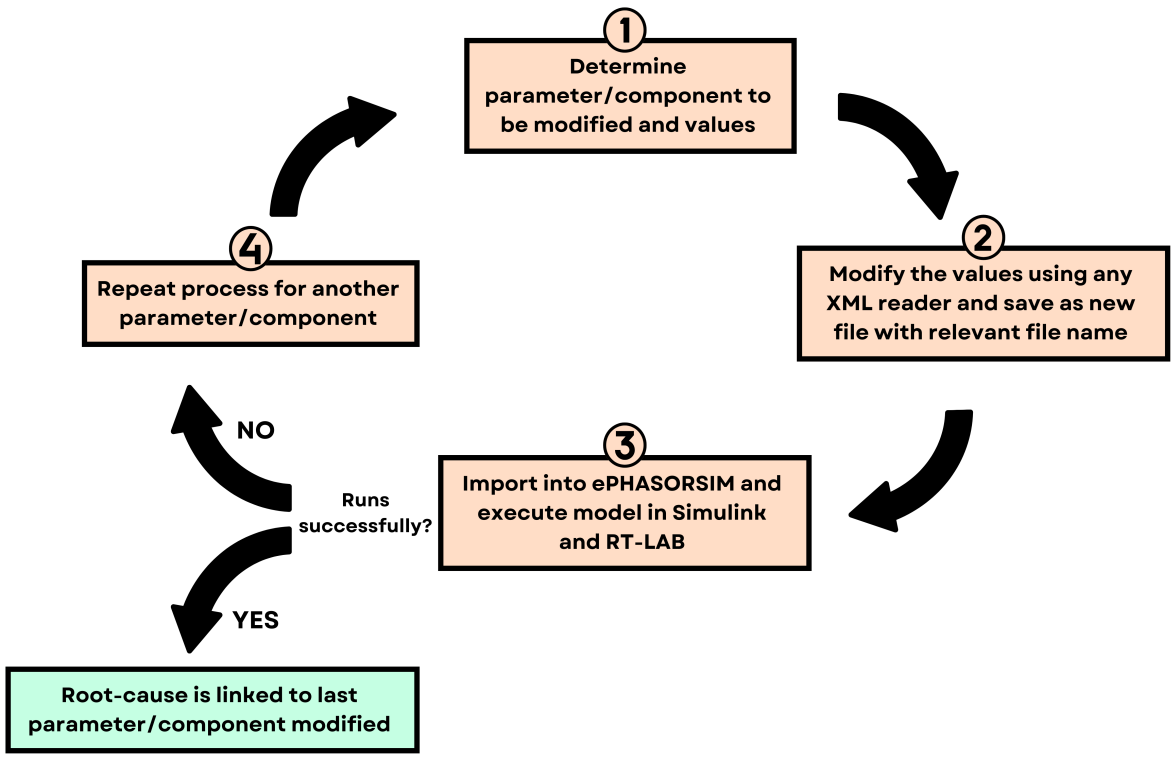

Figure 4.10: Overview of the XML root-cause analysis workflow

Eventually, the UDB and PowerFactory import tool experts fixed the issues by updating the UDB and sending a patch to the team at Brunel. After successful installation and setting up of the patch, the GB TSRM model runs successfully offline.

4.5 Results and Discussion

4.5.1 Simulating GB Interconnector Faults in Real-Time

For the previously discussed GB TSRM model, which was exported from PowerFactory and imported into the ePHASORSIM module of RT-LAB, the model is run in real-time. A disconnection fault (also known as trip or tripping) of HVDC interconnector is set at 3 seconds for each case seperately, of which there are ffour; 1) IFA1, 2) Viking Link, 3) BritNed, and 4) NSL. Then, for each interconnector trip (simulated seperately), the system frequency is observed at three selected areas, called zones which are; 1) Zone 3-Sellindge, 2) Zone 17-Staythorpe, and 3) Zone 28-Dalmally.

These were selected because they are three dispered zones, one from the south of GB, one from the central areas of GB and and one from the North, respectively. Selecting such dispersed zones will allow to observe how the interconnector faults affects system frequency differently in different areas of GB.

4.5.2 Observations across all Four Interconnector Cases

The system frequency across all four interconnector cases, shown in Fig. 4.11, Fig. 4.12, Fig. 4.13, and Fig. 4.14, starts with normal expected operation, maintaining a system frequency of 50 Hz from the instant of running the model in real-time. Then, the effect of the interconnector fault can clearly be seen at 3s, again this is true for all the cases. This is shown by the sudden and instantaneous decrease in system frequency for all three zones of each interconnector, which occurs due to the in-feed loss of generation, and according to first-princicples; when generation decreases, so does the system frequency, provided the system load remains constant. The extent of the decrease, i.e. the magnitude, differs for every zone of each interconnector, and this will be discussed further, describing the frequency reponse for each interconnector. This difference in magnitude indicates a difference in sensitivity of each zone to the fault of different interconnectors, which could arise, for example, due to the distance between the zones and the interconnector. After the frequency drop, the GB system attempts to return the frequency back towards normal operation of 50 Hz, achieving varying results between 49.9 Hz (Zone 3–Sellindge of the IFA1 disconnection fault) to a close 49.99 Hz (Zone 3–Sellindge of the NSL disconnection fault). Following such attempt to increase the frequency, for all four cases, the frequency of all zones begins to decline constantly, either in an oscillatory form or steadily, indicating a state of instability for the GB power system. In practicality, the system operator would substitute the power infeed loss with power from elsewhere, for example by calling upon fast-acting generators to supply power, increasing the frequency back to normal conditions. NESO refers to various such responses as dynamic and non-dynamic frequency response services (FRS).

4.5.3 Observations for each Interconnector Case

IFA1 Interconnector Fault

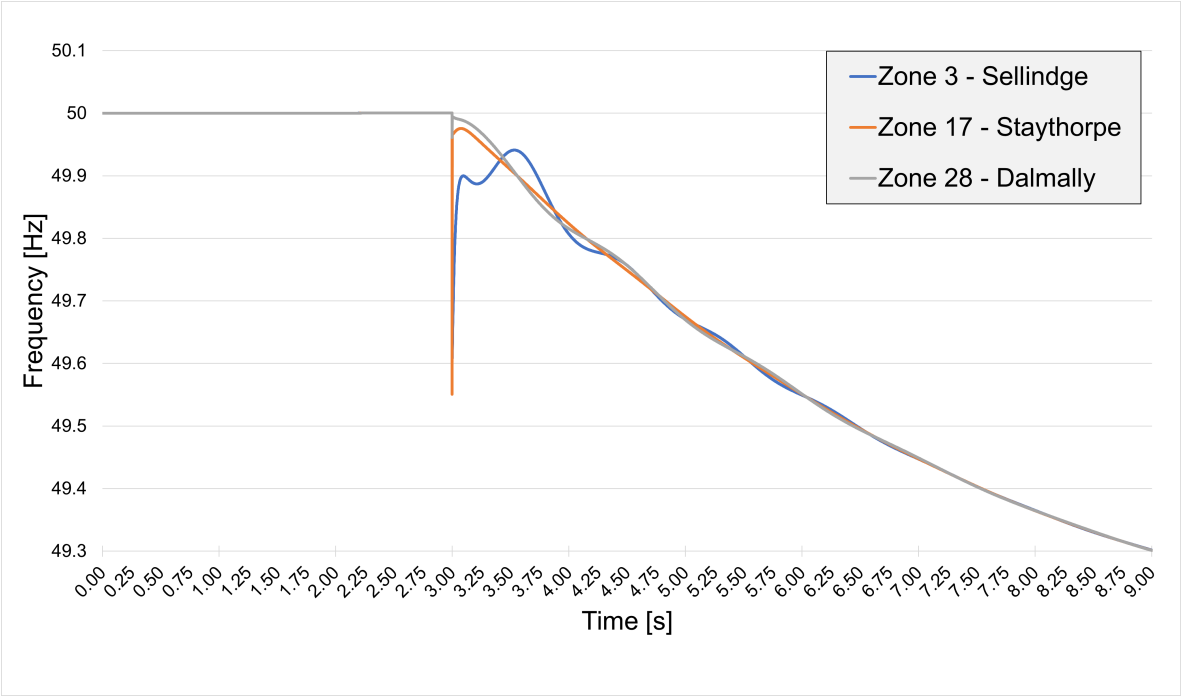

Figure 4.11: Frequency response of a disconnection fault (at 3 seconds) of the IFA1 HVDC interconnector

For the case of the disconnection fault of the IFA1 interconnector, the frequency response is shown in Fig. 4.11. At the fault time (of 3.00s) Zone 17–Staythorpe experiences the largest decrease to 49.55 Hz, followed by Zone 3–Sellidge which decreases to 49.64 Hz and the minimum drop is experienced by Zone 28–Dalmally which decreases to a frequency of 49.96 Hz. This response is the largest out of the other interconnector cases. Between the primary response reaction (of attempting to return the frequency back to 50 Hz normal operation) and the point where all zones meet and continue together at around the 4.50s mark, only Zone 3–Sellindge experiences clear oscillatory reponse, which could be because it is close to the fault location. Then from 4.50s to 6.50s those oscillations become smaller in amplitude, eventually ceasing. The frequency of all zones continue in gradual decline as shown in the figure, with no sign of return to normal system frequency indicating a state of instability due to the disturbance of the IFA1 interconnector disconnection.

Viking Link Interconnector Fault

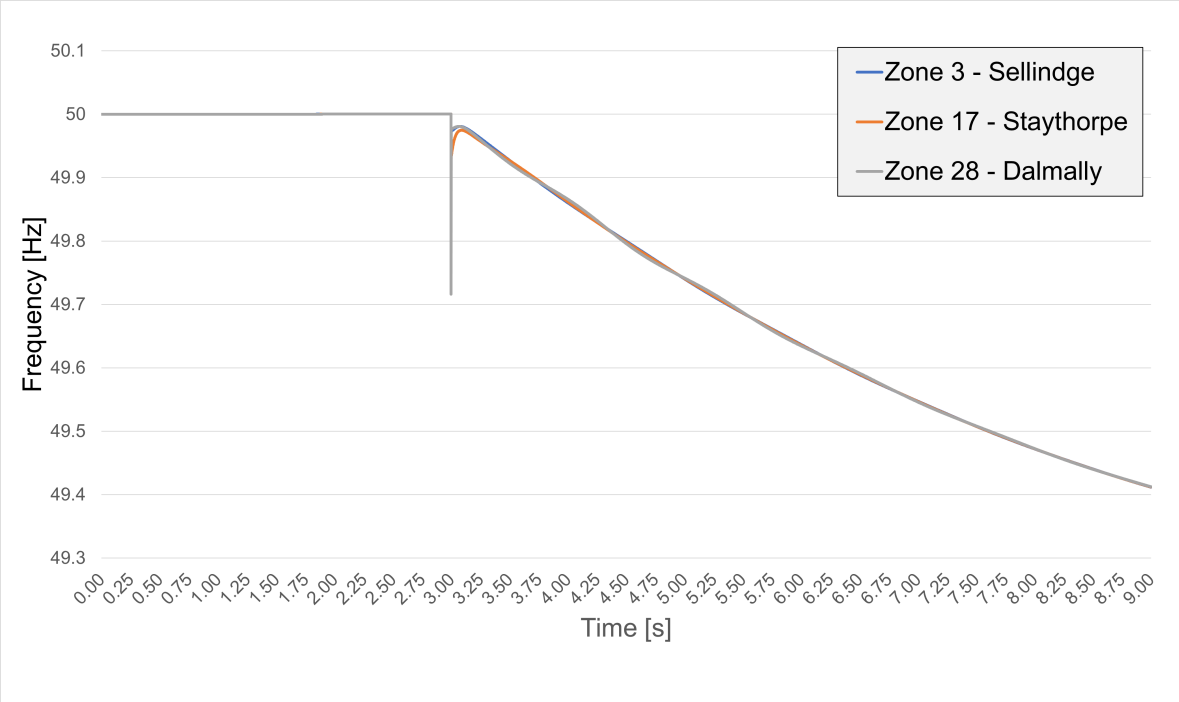

Figure 4.12: Frequency response of a disconnection fault (at 3 seconds) of the Viking Link HVDC interconnector

Whereas in IFA 1, where the largest frequency nadir was in Zone 17–Staythorpe (49.55 Hz), in the case of the Viking Link interconnector, shown in Fig. 4.12, the largest frequency nadir is 49.72 Hz by Zone 28–Dalmally. This is the second largest response after IFA1. All zones experience a similar and very short primary frequency response, meeting and continuing together at around 3.20s, and then gradually decreasing, again with no sign of return to steady-state system conditions indicating a state of instability for the system.

BritNed Interconnector Fault

In the case of the disconnection fault of the BritNed interconnector as shown in Fig. 4.13, the frequency nadir experienced across all zones are significantly smaller compared to IFA1 and the Viking Link. The largest frequency nadir for BritNed is 49.94 Hz experienced by Zone 3–Sellindge. The three zones's frequencies meet and blend at around 4.75s due to some minor oscilatory response between this and the fault

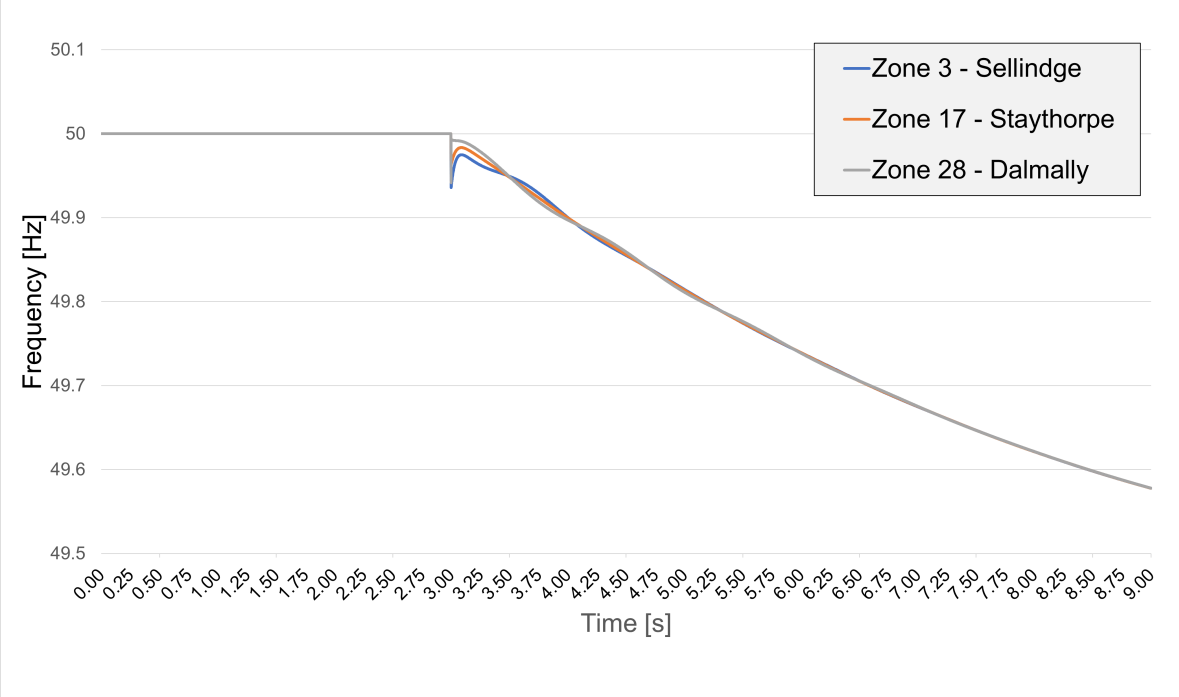

Figure 4.13: Frequency response of a disconnection fault (at 3 seconds) of the BritNed interconnector

time. A state of system instability is also applicable for the case of BritNed.

NSL Interconnector Fault

The frequency response shown in Fig. 4.14 is that of the fault trip of the NSL interconnector, of which the largest frequency nadir is 49.88 Hz experienced by Zone 28–Dalmally, and it is the only one with an oscillatory response in this case, that is at the same time the largest reaction of all interconnector cases since it meets stably with the frequency of the other two zones only after the 6.84s mark, representing the longest time to do so. A state of system instability is also applicable for the final case of the NSL interconnector.

4.6 Chapter Summary

In this chapter, an interfacing methodology between the offline simulator PowerFactory (by the company DIgSILENT), and the real-time simulator ePHASORSIM

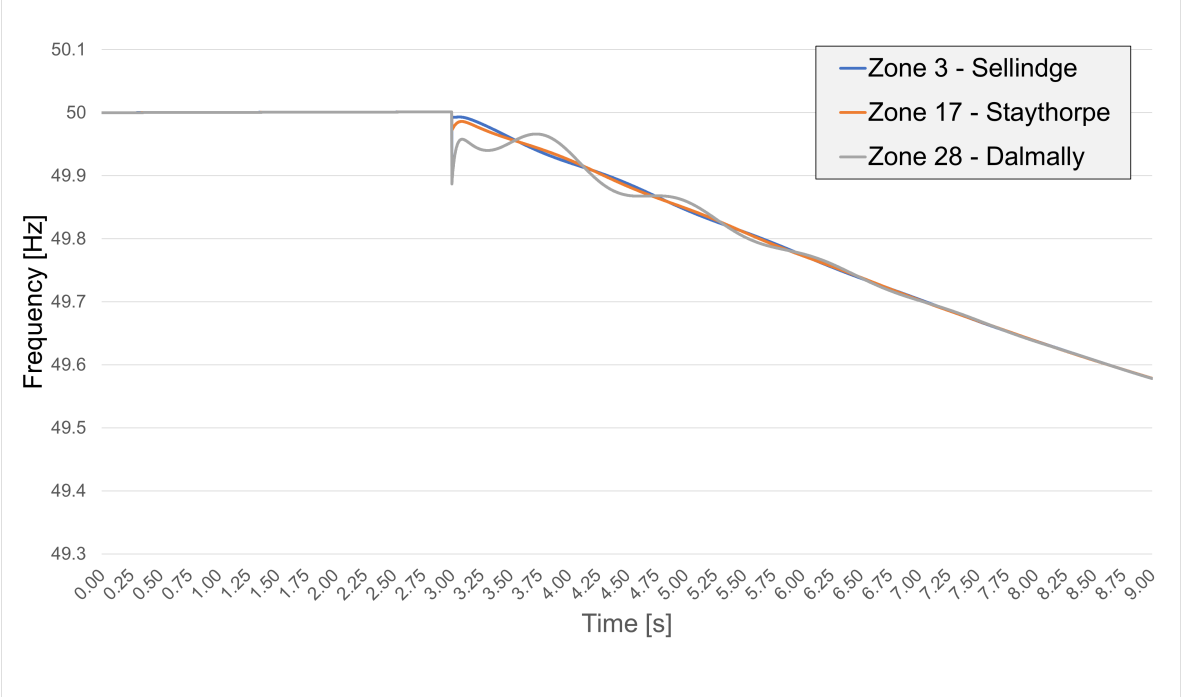

Figure 4.14: Frequency response of a disconnection fault (at 3 seconds) of the NSL HVDC interconnector

(by the company OPAL-RT) was presented. The interfacing methodology allows for large power system models designed in PowerFactory to be exported, including their netlist and power system components, imported into ePHASORSIM and then executed in real-time. This contributes to power system analysis using closed-loop HIL approaches for hardware testing, development and validation in specially designed power system models.

The methodology combines readily-available exporting tools in PowerFactory, specifically the XML file feature, which is a flexible and human/machine readable type of file format. Issues arising from ePHASORSIM's software updates regarding the exported file format have successfully been addressed and presented with detailed explanations and discussions. The GB TSRM, which was the power system model selected as an example, was utilised throughout the interfacing workflow until successful execution and interaction with hardware in a HIL laboratory setup. The setup consisted of a real RoCoF relay and the simulation of HVDC tripping events, system studies of which are becoming increasingly important in current times, particularly after the various recent incidents in the UK which saw the unexplained dis-

connecting of HVDC interconnectors which raises grid stability concerns, especially with the decrease in grid inertia and the uptake of IBRs.

The work in this chapter marks an advancement in interfacing offline and real-time simulators which is of vital importance to research efforts, such as smart grid labs in academic and research institutions around the globe employing the same industry-standard tools, as well as for use in practical engineering environments. Most importantly this work is advantageous for streamlining transmission system analysis processes since this approach reduces the need for duplicated efforts of redesigning power networks in real-time software platforms and hence reduces the overall lead times.

Chapter 5

Real-Time CPPS Testbed for Software-in-the-Loop Studies

5.1 Introduction

Real-time ITL simulators play a crucial role in CPPS research by allowing researchers to test, validate, and optimise the interaction between the cyber layer and the power layer components of the system. These simulators enable realistic testing environments where hardware, software and simulations interact closely, providing valuable insights into the behaviour and resilience of modern power systems. There are several types of ITL simulation setups and variations thereof such as HIL, SIL, Power-Hardware-in-the-Loop (PHIL) and Controller-in-the-Loop (CIL).

This chapter details the architecture of a real-time SIL CPPS testbed with the capability and application of investigating grid and control resilience to cyber-contingencies. The testbed enables for the investigation of the effects of communication contingencies on volt-var control schemes. The architecture consists of HYPERSIM, a power systems and power electronics simulator by the company OPAL-RT, with both the communication network and the control scheme modelled in MATLAB on an external PC allowing for real-time data exchange. The interfacing involves the use of the Modbus protocol over Ethernet, known as Modbus TCP/IP, which connects the OPAL-RT hardware target to the external PC. The platform's uniqueness lies in combining a high-fidelity power system simulator with a flexible, accessible modelling environment, enabling robust testing of various communication and control technologies, schemes, and configurations. This setup is invaluable for researchers aiming to explore the complex interactions between power systems and communication networks, assess control scheme resilience, and develop strategies for enhancing the robustness of grid operations against cyber threats.

5.2 Architecture and Design of Proposed Testbed

5.2.1 Design Overview

The real-time CPPS testbed's architecture features three main hardware components and four main systems, and is depicted in Figure 5.1.

The three hardware components are two PC workstations and the OPAL-RT hard-

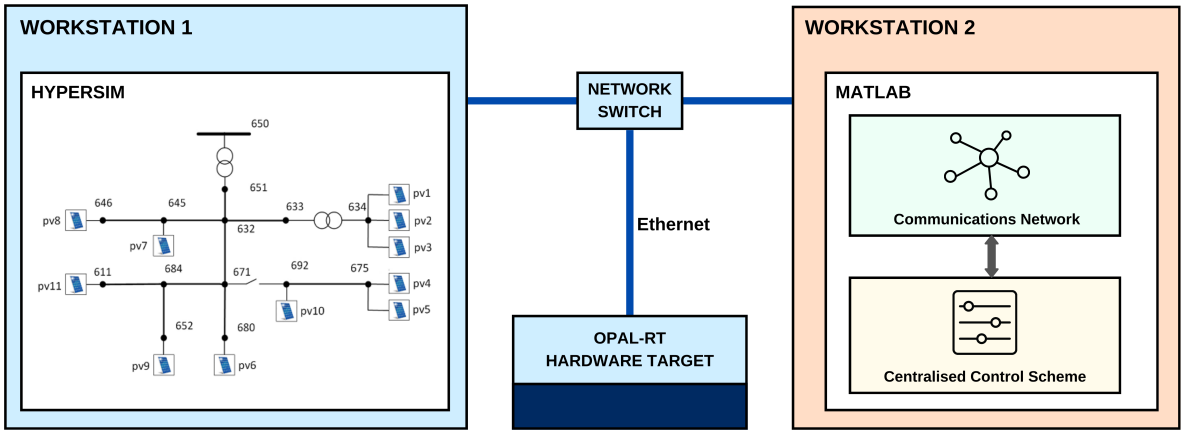

Figure 5.1: Testbed design of real-time CPPS testbed

ware target. The first PC workstation is used as a platform to design and analyse the power system model using the HYPERSIM software. Various models can be designed and compared, for example the readily available IEEE test feeders. The OPAL-RT hardware target provides the necessary computing power to execute the designed power system in real-time. The second workstation is used for designing and modelling the communication and the centralised control scheme (CCS) and for those two systems to communicate with each other. To enable data transfer, all three aforementioned hardware parts are linked via Ethernet cables and a network switch. The four main systems are the power distribution system, the communication network, the control scheme and the interfacing protocol. An element list of the real-time CPPS testbed is shown in Table 5.1 alongside the functions of each element and the selected option of this testbed.

5.2.2 Main Components and Interfacing Connections

For the electrical distribution network, the chosen network is a PV-modified version of the well known IEEE 13 Node Test Feeder (IEEE 13 NTF), which is commonly used to test common features of distribution analysis software. The original network is relatively small and simple, having a standard operating voltage of 4.16 kV. It is characterised by being short, comparatively highly loaded and contains a single voltage regulator at the substation. It also contains cables that are both overhead and

Table 5.1: Element list of real-time CPPS testbed

Element	Function	Selected System/Technology
PC Workstation 1	To design power system model	i7-3770 @ 3.40GHz 16GB RAM Windows 10 Enterprise 21H2
PC Workstation 2	To design and simulate communication network and control scheme	Same as above or similar
Hardware Target	To execute designed power system model in real-time	OPAL-RT
Distribution Network	To model physical (power) domain through various configurations	PV-Modified IEEE 13-Node Test Feeder
Communication Network	To model cyber (communications and control) domain	13-Node IP over WDM
Control Scheme	To regulate and maintain feeder voltages within specified limits	Centralised Volt/Var control
Interfacing Protocol	To interface and transfer data between physical and cyber domain	Modbus protocol

underground, shunt capacitors, an in-line transformer, and has unbalanced loading.

For the corresponding communications network, a 13-node communications network is used to model the communication infrastructure which, in the real field, the whole system relies on to transmit system information and device control commands between the centralised controller and the different power devices. The Internet protocol over wavelength division multiplexing (IPoWDM) was selected due to its high data rate capability, which is provided by carrying multiple wavelengths on a single fibre. This suits the high communications requirement demanded by modern power grids, though only latency and packet loss are configurable in simulation. It is acknowledged that the actual Modbus-over-Ethernet (explained below) hardware in the testbed will dominate observed communication effects. However, the IPoWDM model was retained for broader applicability beyond the immediate experimental setup.

For the control system, a centralised Volt/Var control scheme (CCS) will be used to maintain feeder voltages between certain limits and to coordinate between voltage

regulation devices and the PV devices.

The Modbus protocol is employed over the Ethernet link connecting the OPAL-RT target and the two workstations. OPAL-RT has the capability to model several communication protocols such as the newer IEC 61850 protocol and the traditional, albeit still common, DNP3 and Modbus protocols. This allows for researchers to develop and test different control and protection schemes considering different communication issues such as delays, outages, missing or tempered data.

5.3 Electrical Network

5.3.1 Technical Background on Distribution Networks and Effects of DERs

Distribution networks are composed of various configurations and topologies according to planning and operational requirements. Typical voltages of distribution systems range from 6.6kV to 33kV in the UK and from 2.4kV to 34.5kV in the US [90]. Common distribution system topologies include radial, ring/loop and meshed topologies and can vary depending on unique requirements of different areas.

DERs such as PVs are continually being installed at the edge of power networks in distribution systems. From the transmission level down to the consumer level, TSOs and DNOs have decreasing amounts of:

1. Visibility - e.g. measurements and models
2. Controllability - e.g. voltage and protection
3. Flexibility and automation

Hence grid changes are occurring at places where utilities have the least amount of information, posing a challenge for distribution network planning.

In traditional distribution network planning and expansion, voltage regulation schemes are designed with the assumption that power flows in a single direction: from the substation to the feeder ends. The goal is to ensure that voltage levels across the

lines from the distribution substations down to the furthest customers remain within acceptable limits, often set by standards like ANSI C84.1 [91]–[93].

In this conventional approach, planners account for voltage drops caused by the resistance and reactance of the distribution lines as electrical power flows from the distribution substation to loads. The voltage drop is typically highest during peak demand periods, when current flow is maximum. To prevent the voltage from dropping below acceptable levels, planners install capacitor banks and voltage regulators along the feeder. These devices help maintain the voltage within the required range by adding reactive power or by dynamically adjusting the voltage level, respectively.

However, with the integration of DERs, such as solar PV systems, wind farms, and battery storage, the planning process becomes more complex. Unlike traditional loads, DERs inject power into the grid, which can cause voltage rise, especially near the points where these DERs are connected. During periods of high DER output, power may flow backward from the DERs toward the substation, known as reverse power flow. This reverse flow can lead to voltage levels rising above acceptable limits, creating operational issues such as overvoltage at certain points on the feeder.

As a result, planners must now design voltage regulation schemes that consider both voltage drop during high demand and voltage rise during high DER output. This requires a dynamic approach to simulations, where planners analyse the feeder's voltage profile over time to capture variations due to changes in both load and DER output. They must account for day-night cycles, seasonal variations, and cloud cover impacts on solar generation, as these factors influence the DER power injection and thus the voltage profile throughout the day.

To manage these fluctuations, planners may need to implement advanced voltage control schemes such as smart inverters for DERs, which can provide voltage regulation by absorbing or injecting reactive power as needed. They may also use real-time monitoring and control systems or automated voltage regulators capable of adjusting settings based on real-time conditions. These advanced schemes help maintain voltage within standard limits, balancing the impact of both traditional loads and DERs on feeder voltage stability.

5.3.2 PV-Modified IEEE 13-Node Test Feeder

The electrical distribution system selected is a PV-modified version of the IEEE 13 NTF which is available in ePHASORSIM examples. The original IEEE 13 NTF was produced by the IEEE PES AMPS DSAS Test Feeder Working Group as part of a series of test feeders designed to provide standardised models that allow researchers and engineers to simulate, investigate, and optimise power distribution systems under various scenarios [94], [95].

Table 5.2: Technical network components and specifications of the IEEE 13-Node Test Feeder

Aspect	Modified IEEE 13 NTF	Original IEEE 13 NTF
Nominal Voltage	4.16kV	4.16kV
No. of PVs	11	N/a
PV Phase	Single-phase	N/a
Converter Model	PVGU1	-
Controller Model	PVEU1	-
Solar panel Model	PANELU1	-
Irradiance Profile Model	IRRADU1	-

The modified 4.16kV IEEE 13-NTF has 11 single-phase PV sources and is based on PSS/e's photovoltaic system model. Each of the units includes a converter model of type PVGU1, a controller of type PVEU1, a solar panel model of type PANELU1 and an irradiance profile model of type IRRADU1. Table 5.2 compares the original and modified IEEE 13 NTF. In ePHASORSIM's example project, these components were originally modelled in Modelica and interfaced with ePHASORSIM as an FMU using the FMI standard. However, in this work, HYPERSIM has been employed to take advantage of its capabilities of including the models internally rather than relying on external simulators and interfacing. To observe an example of this, see figure 5.2 which depicts the option to insert the irradiance profile model of the PVs.

Compared to the original test feeder [94], the following modifications were performed by ePHASHORSIM for this example network:

1. 11 PV units are connected to the buses as shown in Figure 5.3.

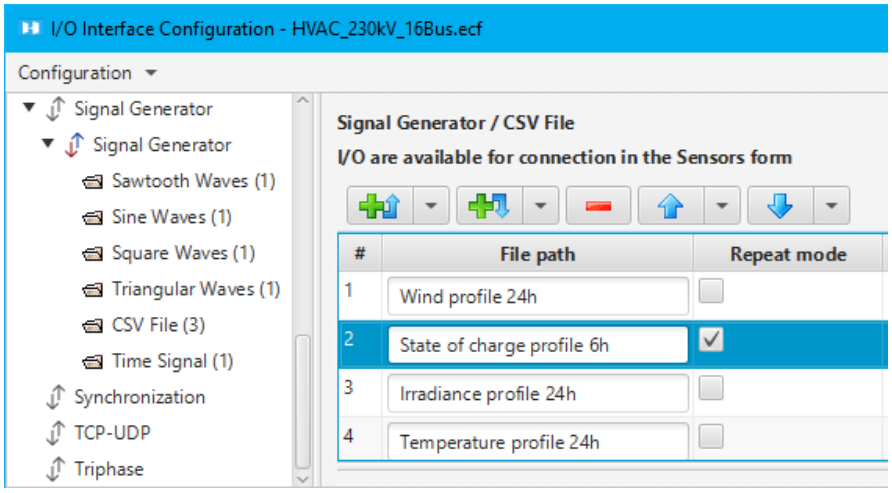

Figure 5.2: Irradiance profile option in HYPERSIM

2. The distributed load along the line 632 to 671 is replaced by a spot load located at bus 632.

3. The voltage regulator between nodes 632 and 650 is substituted by a transformer (Yg-Yg), and a new node 651 is inserted.

4. All loads have Yg concoction.

5.4 Communication Network

5.4.1 IP over WDM Communication Protocol

The preferred architecture for the core networks is the IP over WDM network [96], which supports high data rates by carrying multiple wavelengths on a single fibre. The IP layer and the optical layer make up the IP over WDM network (Fig. 6). Every node's IP router is used in the IP layer to combine traffic from access networks that link end users. The large bandwidth needed to facilitate data communication between IP routers is provided by the optical layer. An optical switch connects the IP router to the optical layer.

The optical switch is connected to the fibre links. OEO (optical-electronic-optical) conversion is provided by the transponders. The optical signals can be transmitted over long distances as a result of the erbium-doped fibre amplifiers (EDFAs), which

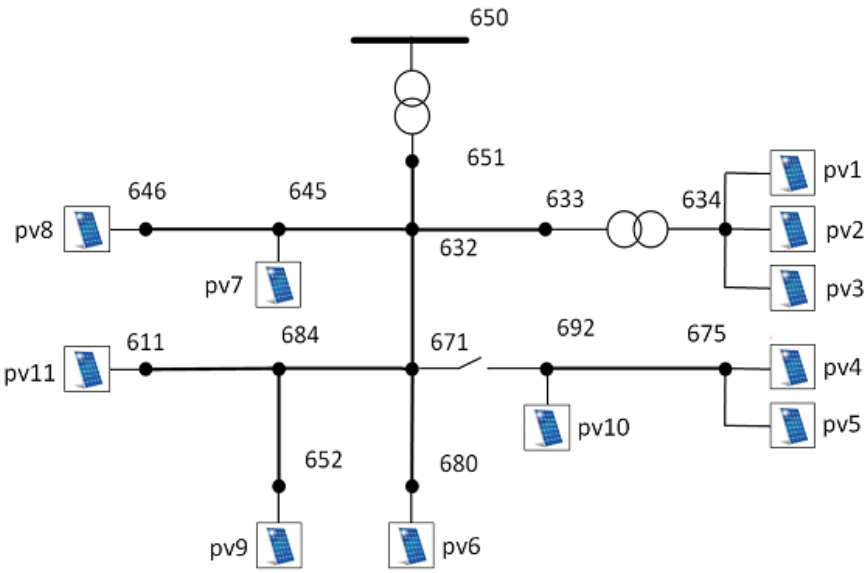

Figure 5.3: PV-Modified IEEE 13 Node Test Feeder

are installed in the fibre links. In the current implementation of IP over WDM networks, IP traffic is processed and forwarded by IP routers at all intermediate nodes of its path, in addition to optical switching and OEO conversion.

5.4.2 Network Delays and Latencies

There are various places at which traffic flows in communication networks encounter delays. Transmission delay is the amount of time needed to fit every bit of a packet into the transmission link. Delays are caused by several aspects of the network. Traffic in the IP over WDM architecture will encounter switching delays at optical switches, amplification delays at EDFAs, and processing delays at routers and transponders. When traffic packets are in buffers awaiting processing or transmission, they also experience queuing delays. The propagation delay is the amount of time it takes for information to move across the transmission medium. The propagation delay in optical fibre networks is limited by the speed of light. Only propagation delay and component delay is taken into account in this work.

5.5 Interface

5.5.1 OPAL-RT's ICS Capabilities

The OPAL-RT simulator is connected to an external PC via an Ethernet link, see Figure 5.4, which can be used to simulate multiple communication protocols. OPAL-RT can replicate a number of communication protocols, including the more recent IEC 61850 standard as well as the more established but still widely used DNP3 and Modbus protocols. This makes it possible for researchers to create and evaluate various control and protection schemes that take into account various communication problems including tempered or missing data, delays, or outages.

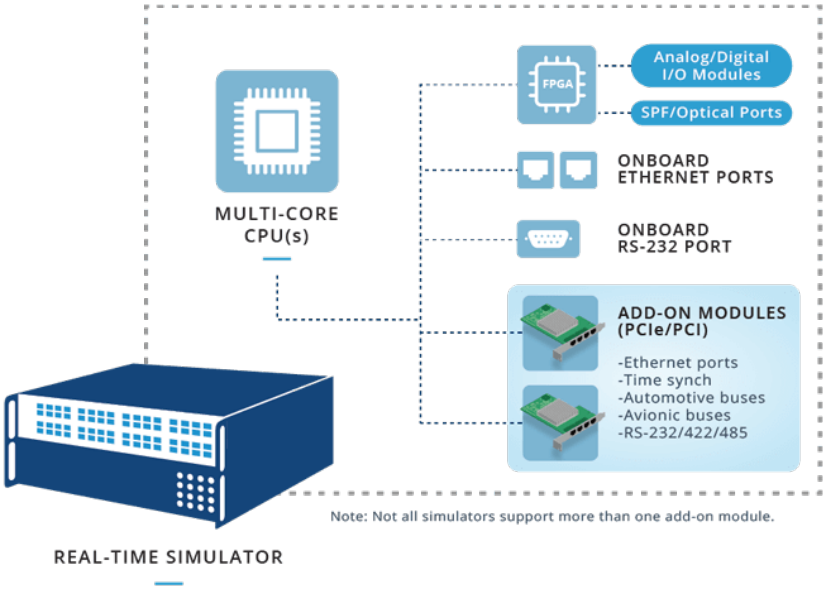

Figure 5.4: Communication Protocols for interfacing with OPAL-RT hardware [97]

5.5.2 OSI and TCP/IP Model and Layers

Regarding the detailed developmental interfacing methodology, the OSI and TCP/IP layers need to be taken into account for understanding the approach commonly employed by CPPS researchers to interface communication networks simulators, or even real communication hardware devices, with external real-time power simulators. See Figure 5.5 which shows the comparison between the OSI basic reference model and the TCP/IP stack, and Figure 5.6 which shows the seven layers of the OSI

model with examples. The main layers of concern in this work are the application, transport and network interface layers, of which the specific types of communication protocols required are Modbus, TCP/IP sockets and Ethernet respectively. These layers and specific communication technologies are emphasised in blue in Figure 5.5 and will be further detailed in the following subsections.

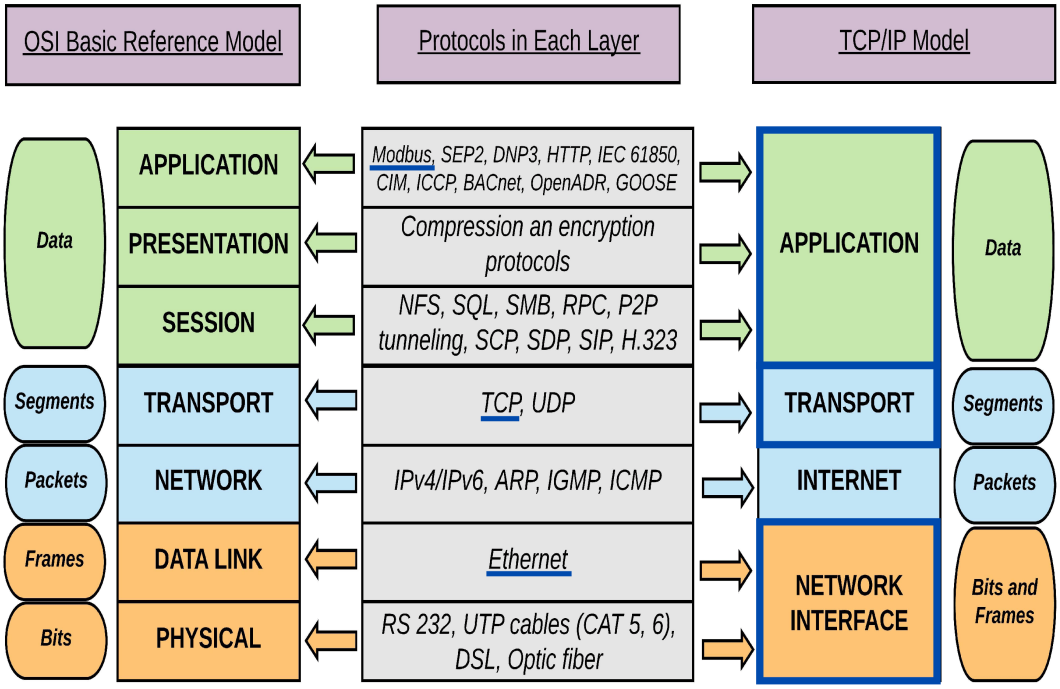

Figure 5.5: Comparison between OSI basic reference model and the TCP/IP stack [98]

5.5.3 MATLAB Implementation vs NS-3 and OMNeT++

Although MATLAB was used in this work to model the communications layer, NS-3 has also been employed in a significant number of research works as the DES to model the communication layer. The same can be said for OMNeT++ but it has been used less than NS-3. This is due to two main reasons. First, NS-3 is dedicated towards communications networks and systems, whereas OMNeT++ is a generic simulation framework used mostly towards simulating communication networks and systems. The second reason is NS-3's native capability to interface with external real-time simulators due to the availability of its "Real-time Scheduler" module which handles real-time synchronisation mechanisms and simulation events. Whilst the

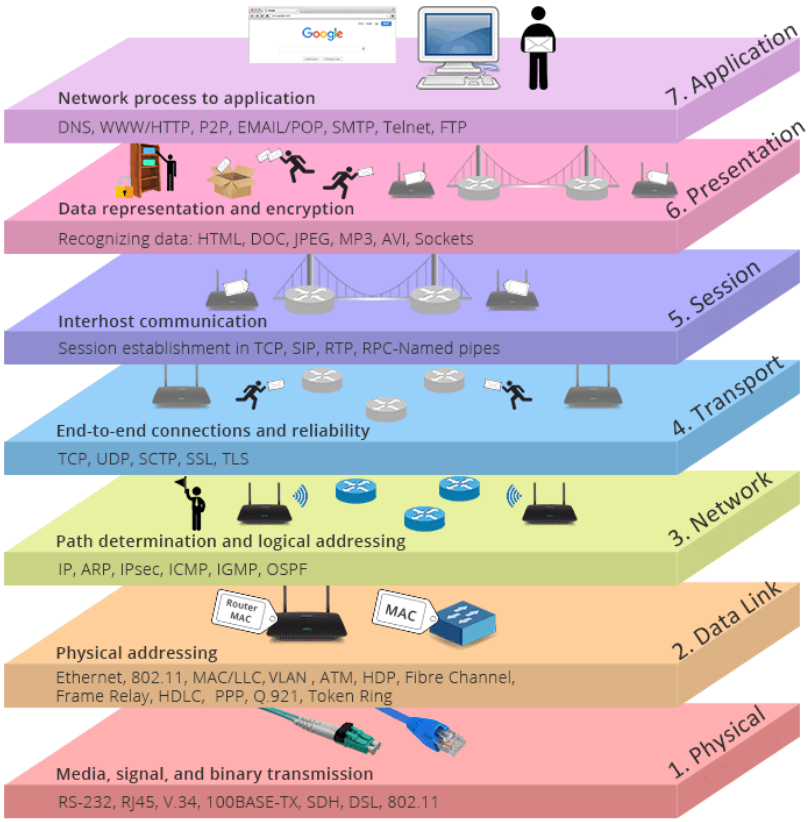

Figure 5.6: The Seven layers of the OSI model with examples [99]

interfacing of OMNeT++ with external real-time simulators is still possible, significant time and effort is required in developing event handling procedures, software communication channels and a real-time synchronisation implementation.

Interfacing NS-3 with OPAL-RT involves establishing a connection between the communication network simulation in NS-3 and the real-time power system simulation in OPAL-RT. The process begins by defining the simulation goals, such as analysing the impact of communication delays on grid stability. Communication is typically achieved through middleware or direct data exchange protocols, such as TCP/IP sockets, enabling real-time bidirectional data flow. Synchronisation between NS-3's discrete-event simulation and OPAL-RT's real-time operations is critical and can be managed using time-stepped coordination, where NS-3 pauses its event processing until OPAL-RT completes a time step. NS-3's real-time scheduler "RealtimeSimulatorImpl" must be enabled to ensure it operates within the real-time constraints dictated by OPAL-RT. The simulators exchange data such as network pa-

rameters from NS-3 and power system states from OPAL-RT, enabling integrated analysis. Finally, the setup requires extensive testing and validation to ensure accurate data exchange, synchronisation, and compatibility between the simulators for reliable co-simulation.

5.6 Control Scheme

5.6.1 Centralised Volt/Var Control Scheme

For the PV-modified IEEE 13 NTF, a centralised Volt/Var control scheme will be implemented to regulate and maintain voltages within specified limits across the feeder. This control system will coordinate the operation between the 11 PV sources, 2 transformers, 2 shunt devices and 3 switches to act in cohesion for the control objectives. The inputs and outputs of this can be seen in Figure 5.7.

The control strategy will focus on the following key objectives:

1. Voltage regulation: The central controller will continuously monitor voltages at all nodes to ensure they remain within predefined operational limits. This will involve dynamically adjusting the outputs of the transformers and shunt devices to correct voltage deviations.

2. Coordination of PV sources: The 11 distributed PV sources will be actively integrated into the Volt/Var control scheme. These PV sources will be instructed to either inject or absorb reactive power, depending on the voltage levels at nearby nodes, to assist in voltage stabilisation.

3. Transformers and shunt devices: The two transformers and two shunt devices will be managed to support voltage regulation. The transformers will adjust tap positions based on the central controller's signals, while the shunt devices, such as capacitor banks and reactors, will be engaged to either supply or absorb reactive power as needed to control voltage levels.

4. Switching coordination: The 3 switches will be strategically operated as part of the control system to reconfigure the network, if necessary, to isolate sec-

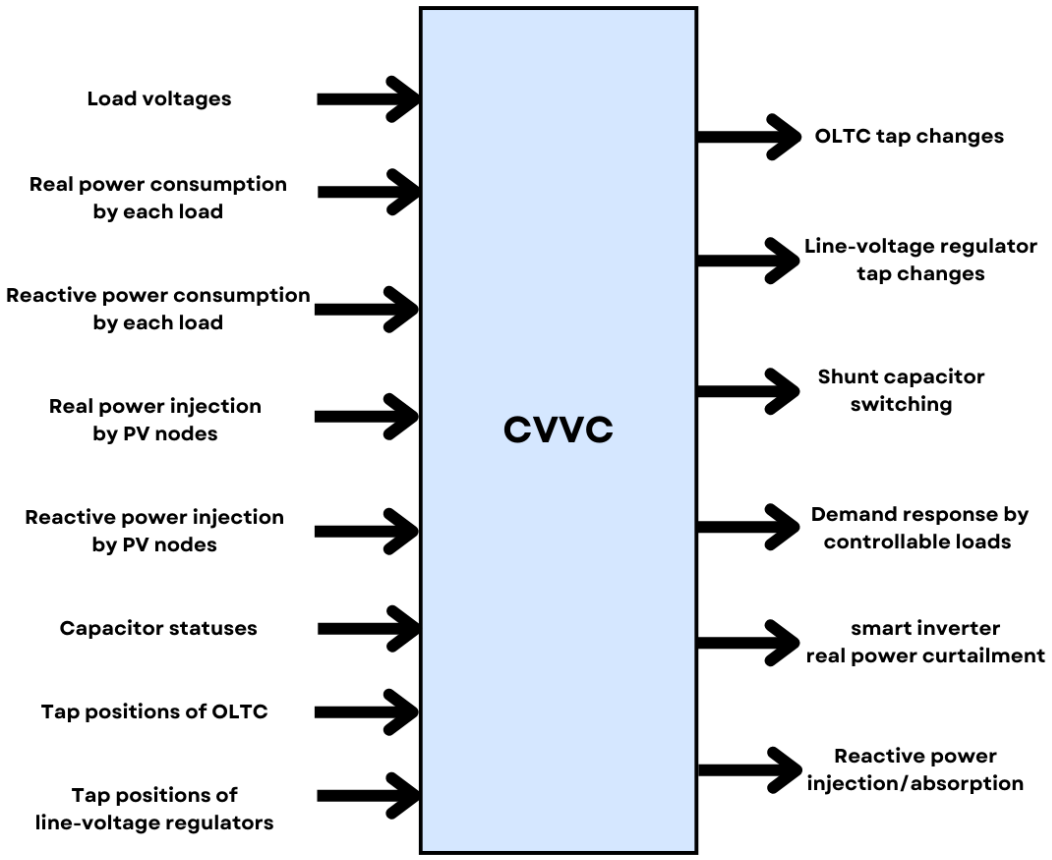

Figure 5.7: Centralised volt-var controller illustrating inputs and outputs

tions or optimise power flows, ensuring voltage stability across the feeder. This could include altering power flow paths to balance the load and reduce voltage imbalances.

By using this centralised Volt/Var control scheme, the IEEE 13 NTF will maintain voltage stability, ensure optimal reactive power coordination, and facilitate the smooth integration of its PV systems. The centralised control will dynamically adjust the settings of all controllable devices to react to real-time voltage fluctuations, maintaining the power quality across the network.

5.7 Chapter Summary

This chapter presented the architecture of a real-time CPPS SIL testbed, a critical tool for advancing CPPS analysis and an example of a key approach. The testbed integrates four primary components: the power system, the corresponding communication network, the control scheme, and the interfacing methodology. The IEEE 13 NTF was selected as the power system model to be simulated using OPAL-RT's HYPERSIM. MATLAB was employed for the development and modelling of both the communication network and the control scheme, with the Modbus protocol facilitating the integration between the two seperate PC environments.

The testbed was designed to enable the exploration of interactions between power systems and communication networks, particularly in scenarios involving communication errors and their impact on Volt/Var control schemes. By utilising a high-fidelity power system simulator alongside a flexible and customisable modelling platform, the testbed provides researchers with a powerful environment to investigate grid resilience, validate control strategies, and analyse advanced communication challenges. Its ability to simulate real-time scenarios makes it a valuable resource for testing the dynamic behaviour of CPPS under various conditions.

Additionally, the testbed offers significant potential for furthering the understanding of CPPS operation and optimisation. It is particularly relevant in the context of modern power systems, where the integration of distributed energy resources and the increasing reliance on communication technologies demand robust frameworks for analysis. By bridging the gap between theoretical modelling and practical application, the testbed lays the groundwork for future research into enhancing the stability, reliability, and efficiency of CPPS.

Chapter 6

Conclusion and Future Research

6.1 Conclusion

This thesis has presented several contributions focusing on a niche area of cross-domain analysis, aiming to bridge the continuous simulation domain of power systems with the discrete-event domain of communications. The thesis began with an organised literature review, structured around a novel taxonomy of three main classifications for CPPS modelling and simulation approaches. While the studies under each classification may not differ substantially, the proposed taxonomy provides improved nomenclature for future research in the field of CPPS. The new taxonomy consists of:

1. Model-based approaches
2. Co-simulation approaches
3. Real-time in-the-loop approaches

Following the literature review, a contribution was made to the first category (model-based approaches), specifically in vulnerability assessment. Here, the CNII successfully identified critical nodes in a graph-based CPPS model. This metric proved effective in analysing the resilience of the GB TSRM infrastructure, revealing vulnerabilities and guiding mitigation strategies. Additionally, by evaluating both centralised and distributed communication topologies, this chapter demonstrated how these configurations influence CPPS stability and stress response. Key limitations and assumptions of the CNII were detailed, including the lack of modelling of last-mile communications between the power station nodes and the communication nodes, providing a base to improve this study in future works as discussed in the next section.

Another key contribution of this research, which contributed to the second and third categories of approaches (co-simulation approaches and real-time in-the-loop approaches), was the development of methodologies for converting power system models from offline to real-time simulations. By interfacing two industry-standard tools, PowerFactory and OPAL-RT's ePHASORSIM, this work addressed compatibility and synchronisation challenges between offline and real-time environments. This

enables an improved workflow for power system studies, where models developed in familiar offline software can be transferred and executed in real-time. The methodology was validated through a case study on the GB TSRM, conducting frequency response analysis for interconnector infeed loss, which confirmed the model's successful operation. This achievement facilitates further high-fidelity real-time studies.

Finally, the thesis proposed an RT CPPS testbed architecture for investigating communication-based faults in electrical distribution networks, further advancing the field by unifying both domains into an integrated testing framework. This contributed to the third category of approaches (Real-time in-the-loop Approaches). Applications included assessing CPPS resilience under various conditions, such as cyberattacks and system disturbances, while also providing a platform for testing innovative control strategies. The testbed's flexible architecture supports diverse applications, including renewable energy integration and advanced grid management techniques.

In conclusion, this thesis contributes to CPPS research by enhancing theoretical understanding, including through a new taxonomy while addressing key challenges in modelling, vulnerability assessment, real-time tool integration, and RT CPPS testbed design. These contributions establish a methodological foundation for advancing cross-domain CPPS research, facilitating more rigorous analysis of complex cyber-physical interdependencies in modern power systems. Furthermore, the developed frameworks and tools provide actionable insights and improved workflows for industry practitioners to enhance critical smart grid infrastructure against emerging cyber-physical threats.

6.2 Future Research

While this research has made a significant contribution in CPPS modelling and cross-domain analysis, several areas warrant further exploration to address the evolving challenges in smart grids.

First, regarding the CNII metric, additional parameters and variations could be developed to enhance its effectiveness. Incorporating loss-of-load considerations and real-world risk data, such as historical system performance metrics, would improve

the CNII's ability to accurately determine node criticality by building upon established measures. Furthermore, developing a dedicated tool to streamline the workflow from model development to node importance visualisation, as demonstrated by the colour-coded graphs in Figure 3.12 in Chapter 3, could significantly improve usability and better guide mitigation strategies. With regards to the theoretical underpinnings, lessons could be derived from attempts to simulate CPS in other domains, and apply those in this context and for the other category of approaches.

Second, concerning the PowerFactory and ePHASORSIM interface, the increasing penetration of RES, particularly inverter-based resources, necessitates a shift from RMS-type to EMT-type studies. While ePHASORSIM provided adequate fidelity for the frequency response analysis presented in Chapter 4 in Section 4.5, more advanced studies may require higher precision. Future work could therefore focus on developing interfaces between industry-standard offline tools and specialised EMT simulation platforms like HYPERSIM, enabling more sophisticated smart grid analyses for current and future needs.

Also as part of the future work, studies yielding data could be conducted on the components of the designed real-time testbed. This could be done individually initially, with the aim of simulating the whole CPPS network. Furthermore, this research could be extended to support new functionalities and broader applications. Future work could focus on integrating emerging technologies, such as 5G communication networks, AI-driven controllers, and virtual power plants, into real-time testbeds for CPPS. Expanding the testbed to simulate combined effects of natural disasters and cyberattacks would help develop robust response strategies. Investigating the interoperability of the testbed with different hardware platforms and software tools would also enhance its versatility and ensure its applicability in diverse scenarios.

Cross-disciplinary collaboration between professionals across industries will be essential to address the multifaceted nature of CPPS challenges. Engaging with policymakers could align technical advancements with regulatory requirements and societal goals, ensuring a smooth pathway for implementation. Future research must tackle the dual challenges of increasing complexity in power systems and growing threats to their stability. By advancing modelling and simulation techniques, cyber-

security measures, and testbed capabilities, while integrating emerging technologies and fostering interdisciplinary collaboration, the next generation of CPPS research can pave the way for resilient, efficient, and sustainable energy systems.

References

[1] National Grid, *How much of the uk's energy is renewable?* [Online]. Available: https://www.nationalgrid.com/stories/energy-explained/how-much-uks-energy-renewable, (Last accessed: 12.08.2025).

[2] R. Alur, *Principles of Cyber-Physical Systems*. The MIT Press, 1981, ISBN: 0262029111.

[3] 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*, 2020. DOI: 10.1109/ACCESS.2020.3016826.

[4] Department for Business, Energy and Industrial Strategy, Government of the United Kingdom, *Energy trends: Uk renewables*. [Online]. Available: https://www.gov.uk/government/statistics/energy-trends-section-6-renewables, (Last accessed: 11.09.2024).

[5] Our World in Data, *Electricity production in the United Kingdom*. [Online]. Available: https://ourworldindata.org/grapher/electricity-mix-uk, (Last accessed: 11.05.2025).

[6] T. McGarry, "Uk electricity capacity and generation by fuel between 1920 and 2020," Department for Energy Security & Net Zero, Jun. 2023.

[7] V. C. Gungor *et al.*, "Smart grid technologies: Communication technologies and standards," *IEEE Transactions on Industrial Informatics*, vol. 7, no. 4, pp. 529–539, 2011. DOI: 10.1109/TII.2011.2166794.

[8] X. Fang, S. Misra, G. Xue, and D. Yang, "Smart grid — the new and improved power grid: A survey," *IEEE Communications Surveys & Tutorials*, vol. 14, no. 4, pp. 944–980, 2012. DOI: 10.1109/SURV.2011.101911.00087.

[9] "Capacity market: Five-year review (2014 to 2019)," Department for Business, Energy & Industrial Strategy, Jul. 2019.

[10] National Energy Action, *Timeline of the energy crisis*. [Online]. Available: https://www.nea.org.uk/energy-crisis/energy-crisis-timeline/, (Last accessed: 28.10.2024).

[11] M. Mersch, C. N. Markides, and N. Mac Dowell, "The impact of the energy crisis on the uk's net-zero transition," *iScience*, vol. 26, no. 4, p. 106 491, 2023, ISSN: 2589-0042. DOI: https://doi.org/10.1016/j.isci.2023.106491. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2589004223005680.

[12] ICAEW Insights, *Energy supplier collapses highlight bigger sector crisis*. [Online]. Available: https://www.icaew.com/insights/viewpoints-on-the-news/2022/aug-2022/energy-supplier-collapses-highlight-bigger-sector-crisis#:~:text=But%20then%20from%20mid%2D2021,July%202021%20and%20May%202022., (Last accessed: 28.10.2024).

[13] F. S. Candiece Cyrus, *Failed UK Energy Suppliers Update*. [Online]. Available: https://www.forbes.com/uk/advisor/energy/failed-uk-energy-suppliers-update/, (Last accessed: 28.10.2024).

[14] NESO, *Great Britain's Monthly Energy Stats*. [Online]. Available: https://www.neso.energy/energy-101/great-britains-monthly-energy-stats, (Last accessed: 25.11.2024).

[15] 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, no. 5, pp. 2375–2385, 2015. DOI: 10.1109/TSG.2014.2387381.

[16] R. H. Khan and J. Y. Khan, “A comprehensive review of the application characteristics and traffic requirements of a smart grid communications network,” *Computer Networks*, vol. 57, no. 3, pp. 825–845, 2013.

[17] D. M. Laverty, D. J. Morrow, R. Best, and P. A. Crossley, “Performance of phasor measurement units for wide area real-time control,” in *2009 IEEE Power & Energy Society General Meeting*, IEEE, 2009, pp. 1–5.

[18] H. Kirkham, J.-P. Kitzig, D. Laverty, A. Riepnieks, D. Strickland, and R. White, “Improving the pmu standard,” in *2023 IEEE 13th International Workshop on Applied Measurements for Power Systems (AMPS)*, IEEE, 2023, pp. 01–06.

[19] G. Cheng, Y. Lin, A. Abur, A. Gómez-Expósito, and W. Wu, “A survey of power system state estimation using multiple data sources: Pmus, scada, ami, and beyond,” *IEEE Transactions on Smart Grid*, vol. 15, no. 1, pp. 1129–1151, 2023.

[20] R. E. Shannon, *Systems simulation: The Art and Science*. Prentice-Hall, 1975, ISBN: 0138818398.

[21] National Grid, *National Grid Transmission: TPCR4 Rollover*. [Online]. Available: https://www.ofgem.gov.uk/sites/default/files/docs/2011/06/national-grid-response_1.pdf, (Last accessed: 14.10.2024).

[22] IEEE Task Force on Interfacing Techniques for Simulation Tools, “Interfacing Power System and ICT Simulators: Challenges, State-of-the-Art, and Case Studies,” *IEEE Transactions on Smart Grid*, vol. 9, no. 1, pp. 14–24, 2018. DOI: 10.1109/TSG.2016.2542824.

[23] D. Kundur, X. Feng, S. Mashayekh, S. Liu, T. Zourntos, and K. Butler-Purry, *Towards modelling the impact of cyber attacks on a smart grid*, 2011.

[24] X. Liu, D. Wang, L. Xu, Q. Guo, Y. Huang, and Z. Wu, “Graph Database and Graph Computing for Cyber-Physical Power Systems,” *2018 2nd IEEE Conference on Energy Internet and Energy System Integration (EI2)*, pp. 1–5, 2018. DOI: 10.1109/EI2.2018.8581924.

[25] G. Liu, K. Liu, D. Shi, W. Zhu, Z. Wang, and X. Chen, “Graph Computation and Its Applications in Smart Grid,” *2017 IEEE International Congress on Big Data (BigData Congress)*, pp. 507–510, 2017. DOI: 10.1109/BigDataCongress.2017.75.

[26] J. Dai *et al.*, “Cyber physical power system modeling and simulation based on graph computing,” *2017 IEEE Conference on Energy Internet and Energy System Integration (EI2)*, pp. 1–6, 2017. DOI: 10.1109/EI2.2017.8245745.

[27] D. Wang, Q. Guo, and Z. Su, “Feasibility Analysis and Application of Graph Processing in Gauss and Newton-Raphson Power Flow Calculation,” *2017 IEEE Conference on Energy Internet and Energy System Integration (EI2)*, pp. 1–6, 2017. DOI: 10.1109/EI2.2017.8245600.

[28] S. F. Myhre, O. Bjarte Fosso, P. E. Heegaard, O. Gjerde, and G. H. Kjølle, “Modeling Interdependencies with Complex Network Theory in a Combined Electrical Power and ICT System,” *2020 International Conference on Probabilistic Methods Applied to Power Systems (PMAPS)*, pp. 1–6, 2020. DOI: 10.1109/PMAPS47429.2020.9183667.

[29] M. Li, Y. Xue, M. Ni, and X. Li, “Modeling and hybrid calculation architecture for cyber physical power systems,” *IEEE Access*, vol. 8, pp. 138 251–138 263, 2020. DOI: 10.1109/ACCESS.2020.3011213.

[30] S. Xin, Q. Guo, H. Sun, C. Chen, J. Wang, and B. Zhang, “Information-Energy Flow Computation and Cyber-Physical Sensitivity Analysis for Power Systems,” *IEEE Journal on Emerging and Selected Topics in Circuits and Systems*, vol. 7, no. 2, pp. 329–341, 2017. DOI: 10.1109/JETCAS.2017.2700618.

[31] I. O. Datyev, A. A. Pavlov, M. V. Ashkadov, and M. G. Shishaev, “Analysis of causes for differences in modeling results of multi-hop wireless networks using various network simulators,” in *Software Engineering and Algorithms in Intelligent Systems*, R. Silhavy, Ed., Cham: Springer International Publishing, 2019, pp. 249–258, ISBN: 978-3-319-91186-1.

[32] A. Zarrad and I. Alsmadi, "Evaluating network test scenarios for network simulators systems," *International Journal of Distributed Sensor Networks*, vol. 13, no. 10, p. 1 550 147 717 738 216, 2017. DOI: 10.1177/1550147717738216. eprint: https://doi.org/10.1177/1550147717738216. [Online]. Available: https://doi.org/10.1177/1550147717738216.

[33] C. Steinbrink *et al.*, "Cpes testing with mosaik: Co-simulation planning, execution and analysis," *Applied Sciences*, vol. 9, no. 5, 2019, ISSN: 2076-3417. DOI: 10.3390/app9050923. [Online]. Available: https://www.mdpi.com/2076-3417/9/5/923.

[34] T. D. Hardy, B. Palmintier, P. L. Top, D. Krishnamurthy, and J. C. Fuller, "Helics: A co-simulation framework for scalable multi-domain modeling and analysis," *IEEE Access*, vol. 12, pp. 24 325–24 347, 2024, ISSN: 21693536. DOI: 10.1109/ACCESS.2024.3363615.

[35] J. G. R. VÁSQUEZ, "Comparison between two co-simulation frameworks, mosaik and helics," M.S. thesis, POLITECNICO DI TORINO, 2022.

[36] S. T. Watt, S. Achanta, H. Abubakari, E. Sagen, Z. Korkmaz, and H. Ahmed, "Understanding and applying precision time protocol," in *2015 Saudi Arabia Smart Grid (SASG)*, IEEE, 2015, pp. 1–7.

[37] S. Borenius, J. Costa-Requena, M. Lehtonen, and R. Kantola, "Providing network time protocol based timing for smart grid measurement and control devices in 5g networks," in *2019 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm)*, IEEE, 2019, pp. 1–6.

[38] D. L. Mills, "Internet time synchronization: The network time protocol," *IEEE Transactions on communications*, vol. 39, no. 10, pp. 1482–1493, 2002.

[39] 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. DOI: 10.1109/TII.2014.2338740.

[40] 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, no. 2, pp. 548–558, 2006. DOI: 10.1109/TPWRS.2006.873129.

[41] J. Nutaro, P. T. Kuruganti, L. Miller, S. Mullen, and M. Shankar, "Integrated Hybrid-Simulation of Electric Power and Communications Systems," *2007 IEEE Power Engineering Society General Meeting*, pp. 1–8, 2007. DOI: 10.1109/PES.2007.386202.

[42] J. Bergmann, C. Glomb, J. Götz, J. Heuer, R. Kuntschke, and M. Winter, "Scalability of Smart Grid Protocols: Protocols and Their Simulative Evaluation for Massively Distributed DERs," *2010 First IEEE International Conference on Smart Grid Communications*, pp. 131–136, 2010. DOI: 10.1109/SMARTGRID.2010.5622032.

[43] W. Li, A. Monti, M. Luo, and R. A. Dougal, "VPNET: A co-simulation framework for analyzing communication channel effects on power systems," *2011 IEEE Electric Ship Technologies Symposium*, pp. 143–149, 2011. DOI: 10.1109/ESTS.2011.5770857.

[44] V. Liberatore and A. Al-Hammouri, "Smart grid communication and co-simulation," *IEEE 2011 EnergyTech*, pp. 1–5, 2011. DOI: 10.1109/EnergyTech.2011.5948542.

[45] H. Lin, S. S. Veda, S. S. Shukla, L. Mili, and J. Thorp, "GECO: Global Event-Driven Co-Simulation Framework for Interconnected Power System and Communication Network," *IEEE Transactions on Smart Grid*, vol. 3, no. 3, pp. 1444–1456, 2012. DOI: 10.1109/TSG.2012.2191805.

[46] H. Lin, Y. Deng, S. Shukla, J. Thorp, and L. Mili, "Cyber security impacts on all-PMU state estimator - a case study on co-simulation platform GECO," *2012 IEEE Third International Conference on Smart Grid Communications (SmartGridComm)*, vol. 3, no. 3, pp. 587–592, 2012. DOI: 10.1109/SmartGridComm.2012.6486049.

[47] D. Anderson, C. Zhao, C. Hauser, V. Venkatasubramanian, D. Bakken, and A. Bose, “Intelligent Design” Real-Time Simulation for Smart Grid Control and Communications Design,” *IEEE Power and Energy Magazine*, vol. 10, no. 1, pp. 49–57, 2012. DOI: 10.1109/MPE.2011.943205.

[48] H. Georg, S. C. Müller, N. Dorsch, C. Rehtanz, and C. Wietfeld, “INSPIRE: Integrated co-simulation of power and ICT systems for real-time evaluation,” *2013 IEEE International Conference on Smart Grid Communications (SmartGridComm)*, pp. 576–581, 2013. DOI: 10.1109/SmartGridComm.2013.6688020.

[49] H. Georg, S. C. Müller, C. Rehtanz, and C. Wietfeld, “Analyzing Cyber-Physical Energy Systems: The INSPIRE Cosimulation of Power and ICT Systems Using HLA,” *IEEE Transactions on Industrial Informatics*, vol. 10, no. 4, pp. 2364–2373, 2014. DOI: 10.1109/TII.2014.2332097.

[50] M. Wei and W. Wang, “Greenbench: A benchmark for observing power grid vulnerability under data-centric threats,” *IEEE INFOCOM 2014 - IEEE Conference on Computer Communications*, pp. 2625–2633, 2014. DOI: 10.1109/INFOCOM.2014.6848210.

[51] B. Choudhury *et al.*, “Control coordination in inverter-based microgrids using aoi-based 5g schedulers,” *IET Smart Grid*, vol. 7, pp. 38–50, 1 Feb. 2024, ISSN: 25152947. DOI: 10.1049/stg2.12136.

[52] I. Parvez, A. Rahmati, I. Guvenc, A. I. Sarwat, and H. Dai, “A survey on low latency towards 5g: Ran, core network and caching solutions,” *IEEE Communications Surveys & Tutorials*, vol. 20, no. 4, pp. 3098–3130, 2018.

[53] M. Boeding, P. Scalise, M. Hempel, H. Sharif, and J. Lopez Jr, “Toward wireless smart grid communications: An evaluation of protocol latencies in an open-source 5g testbed,” *Energies*, vol. 17, no. 2, p. 373, 2024.

[54] M. Rodríguez, J. Lazaro, U. Bidarte, J. Jimenez, and A. Astarloa, “A fixed-latency architecture to secure goose and sampled value messages in substation systems,” *IEEE Access*, vol. 9, pp. 51 646–51 658, 2021.

[55] S. Werner, L. Masing, F. Lesniak, and J. Becker, “Software-in-the-loop simulation of embedded control applications based on virtual platforms,” in *2015 25th International Conference on Field Programmable Logic and Applications (FPL)*, IEEE, 2015, pp. 1–8.

[56] C. S. B. Clausen, B. N. Jørgensen, and Z. G. Ma, “A scoping review of in-the-loop paradigms in the energy sector focusing on software-in-the-loop,” *Energy Informatics*, vol. 7, no. 1, p. 12, 2024.

[57] H. Tong, M. Ni, L. Zhao, and M. Li, “Flexible hardware-in-the-loop testbed for cyber physical power system simulation,” *IET Cyber-Physical Systems: Theory and Applications*, vol. 4, pp. 374–381, 4 Dec. 2019, ISSN: 23983396. DOI: 10.1049/iet-cps.2019.0001.

[58] “Real-time controller hardware-in-the-loop co-simulation testbed for cooperative control strategy for cyber-physical power system,” *Global Energy Interconnection*, vol. 4, pp. 214–224, 2021. [Online]. Available: www.sciencedirect.com/journal/global-energy-interconnection.

[59] Y. Tang *et al.*, “A hardware-in-the-loop based co-simulation platform of cyber-physical power systems for wide area protection applications,” *Applied Sciences (Switzerland)*, vol. 7, 12 Dec. 2017, ISSN: 20763417. DOI: 10.3390/app7121279.

[60] E. Ekomwenrenren, H. Alharbi, T. Elgorashi, J. Elmirghani, and P. Aristidou, “Stabilising control strategy for cyber-physical power systems,” *IET Cyber-Physical Systems: Theory and Applications*, vol. 4, pp. 265–275, 3 Sep. 2019, ISSN: 23983396. DOI: 10.1049/iet-cps.2018.5020.

[61] R. V. Yohanandhan, R. M. Elavarasan, R. Pugazhendhi, M. Premkumar, L. Mihet-Popa, and V. Terzija, *A holistic review on cyber-physical power system (cpps) testbeds for secure and sustainable electric power grid – part – ii: Classification, overview and assessment of cpps testbeds*, May 2022. DOI: 10.1016/j.ijepes.2021.107721.

[62] T. Becejac, C. Eppinger, A. Ashok, U. Agrawal, and J. O'Brien, "Prime: A real-time cyber-physical systems testbed: From wide-area monitoring, protection, and control prototyping to operator training and beyond," *IET Cyber-Physical Systems: Theory and Applications*, vol. 5, pp. 186–195, 2 Jun. 2020, ISSN: 23983396. DOI: 10.1049/iet-cps.2019.0049.

[63] V. P. Tran, S. Kamalasadan, and J. Enslin, *Real-time modeling and model validation of synchronous generator using synchrophasor measurements*. IEEE, 2013, ISBN: 9781479912551.

[64] G. Ravikumar and M. Govindarasu, "Anomaly detection and mitigation for wide-area damping control using machine learning," *IEEE Transactions on Smart Grid*, 2024, ISSN: 19493061. DOI: 10.1109/TSG.2020.2995313.

[65] R. Negi and S. K. Shukla, "Building india's first cyber-security test-bed for ci," in *Cyber Security in India: Education, Research and Training*, S. K. Shukla and M. Agrawal, Eds. Singapore: Springer Singapore, 2020, pp. 1–15. DOI: 10.1007/978-981-15-1675-7_1. [Online]. Available: https://doi.org/10.1007/978-981-15-1675-7_1.

[66] F. Mihalič, M. Truntič, and A. Hren, "Hardware-in-the-loop simulations: A historical overview of engineering challenges," *Electronics*, vol. 11, no. 15, p. 2462, 2022.

[67] F. Xie, C. McEntee, M. Zhang, B. Mather, and N. Lu, "Development of an encoding method on a co-simulation platform for mitigating the impact of unreliable communication," *IEEE Transactions on Smart Grid*, vol. 12, pp. 2496–2507, 3 May 2021, ISSN: 19493061. DOI: 10.1109/TSG.2020.3039949.

[68] M. A. Aftab, A. Chawla, P. P. Vergara, S. Ahmed, and C. Konstantinou, "Volt/var optimization in the presence of attacks: A real-time co-simulation study," *2023 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids, SmartGridComm 2023 - Proceedings*, 2023. DOI: 10.1109/SmartGridComm57358.2023.10333952.

[69] D. Babazadeh, M. Chenine, K. Zhu, L. Nordström, and A. Al-Hammouri, "A platform for wide area monitoring and control system ICT analysis and development," *2013 IEEE Grenoble Conference*, pp. 1–7, 2013. DOI: 10.1109/PTC.2013.6652202.

[70] D. Babazadeh and L. Nordström, "Agent-based control of VSC-HVDC transmission grid - A Cyber Physical System perspective," *2014 Workshop on Modeling and Simulation of Cyber-Physical Energy Systems (MSCPES)*, pp. 1–6, 2014. DOI: 10.1109/MSCPES.2014.6842398.

[71] 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. 60, no. 6, pp. 8329–8340, 2024. DOI: 10.1109/TIA.2024.3457877.

[72] L. Nam Hai Pham *et al.*, "Real-time cyber-physical power system testbed for optimal power flow study using co-simulation framework," *IEEE Access*, vol. 12, pp. 150 914–150 929, 2024. DOI: 10.1109/ACCESS.2024.3472748.

[73] D. Mishchenko, I. Oleinikova, L. Erdődi, and B. R. Pokhrel, "Multidomain cyber-physical testbed for power system vulnerability assessment," *IEEE Access*, vol. 12, pp. 38 135–38 149, 2024. DOI: 10.1109/ACCESS.2024.3375401.

[74] L. Chen, D. Yue, C. Dou, J. Chen, and Z. Cheng, "Evaluation of cyber-physical power systems in cascading failure: Node vulnerability and systems connectivity," *IET Generation, Transmission & Distribution*, vol. 14, 1197–1206(9), 2020. DOI: 10.1049/iet-gtd.2019.1286.

[75] *BT 21st Century Network*. [Online]. Available: https://kitz.co.uk/adsl/21cn_network.htm, (Last accessed: 23.05.2022).

[76] P. Imris, M. Bradley, G. Taylor, and Y. Li, "Development of a great britain transmission system reduced model for hardware-in-the-loop studies," pp. 1–6, 2020. DOI: 10.1109/UPEC49904.2020.9209888.

[77] A. Csoma, L. Toka, and A. Gulyás, "On lower estimating internet queuing delay," *2015 38th International Conference on Telecommunications and Signal Processing (TSP)*, 2015.

[78] W. Wang and C. Y. Tang, "Distributed estimation of betweenness centrality," pp. 250–257, 2015. DOI: 10.1109/ALLERTON.2015.7447012.

[79] P. Pantazopoulos, M. Karaliopoulos, and I. Stavrakakis, "Distributed placement of autonomic internet services," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 7, pp. 1702–1712, 2014. DOI: 10.1109/TPDS.2013.186.

[80] *Electricity Ten Year Statement (ETYS)*. [Online]. Available: https://www.nationalgrideso.com/research-and-publications/electricity-ten-year-statement-etys, (Last accessed: 26.09.2024).

[81] P. Imris, G. A. Taylor, M. E. Bradley, and Y. Li, "A novel hardware-in-the-loop approach to investigate the impact of low system inertia on rocof relay settings," *Energies*, vol. 15, 17 Sep. 2022, ISSN: 19961073. DOI: 10.3390/en15176386.

[82] *DIgSILENT PowerFactory*. [Online]. Available: https://www.digsilent.de/en/powerfactory.html, (Last accessed: 09.10.2024).

[83] *ePHASORSIM Guide on PowerFactory import*. [Online]. Available: https://opal-rt.atlassian.net/wiki/spaces/PEUD/pages/144439085/Network+data#PowerFactory, (Last accessed: 26.09.2024).

[84] *XML (eXtensible Markup Language)*. [Online]. Available: https://www.codelessplatforms.com/docs/knowledge-base/glossary-of-terms/what-is-xml/, (Last accessed: 26.09.2024).

[85] OPAL-RT, *Powerfactory Input File for ePHASORSIM*. [Online]. Available: https://opal-rt.atlassian.net/wiki/spaces/PEUD/pages/144506354/PowerFactory+Input+File, (Last accessed: 25.11.2024).

[86] S. M. OPAL-RT, *Supported Components in DGS-XML File Format*. [Online]. Available: https://opal-rt.atlassian.net/wiki/x/IoCeC, (Last accessed: 25.11.2024).

[87] S. Ménard, *General Elm Components*. [Online]. Available: https://opal-rt.atlassian.net/wiki/x/cQEFJg, (Last accessed: 25.11.2024).

[88] S. Ménard, *Machine Controllers*. [Online]. Available: https://opal-rt.atlassian.net/wiki/x/cQEFJg, (Last accessed: 25.11.2024).

[89] S. Ménard, *RT-Lab Migration Notes*. [Online]. Available: https://opal-rt.atlassian.net/wiki/spaces/PEUD/pages/144472237/Migration+Notes, (Last accessed: 02.12.2024).

[90] J. D. Glover, T. J. Overbye, and M. S. Sarma, *Power System Analysis and Design 6th Edition*, Eng. Cengage Learning, 2017, ISBN: 978-1-305-88695-7. Accessed: Feb. 13, 2018.

[91] American National Standards Institute, *ANSI C84.1-2020*, 2020.

[92] American National Standards Institute, *ANSI C84.1-2020: Electric Power Systems Voltage Ratings (60 Hz)*. [Online]. Available: https://blog.ansi.org/2020/10/ansi-c84-1-2020-electric-voltage-ratings-60/, (Last accessed: 04.12.2024).

[93] American National Standards Institute, *ANSI C84.1-2020*. [Online]. Available: https://webstore.ansi.org/standards/nema/ansic842020?source=blog, (Last accessed: 04.12.2024).

[94] IEEE PES AMPS DSAS Test Feeder Working Group, *IEEE PES Test Feeder*. [Online]. Available: https://cmte.ieee.org/pes-testfeeders/resources/, (Last accessed: 05.11.2024).

[95] K. P. Schneider *et al.*, "Analytic considerations and design basis for the ieee distribution test feeders," *IEEE Transactions on Power Systems*, vol. 33, no. 3, pp. 3181–3188, 2018. DOI: 10.1109/TPWRS.2017.2760011.

[96] G. Shen and R. S. Tucker, "Energy-minimized design for ip over wdm networks," *Journal of Optical Communications and Networking*, vol. 1, pp. 176–186, 1 2009, ISSN: 19430620. DOI: 10.1364/JOCN.1.000176.

[97] *Our Approach to Communication Protocols*. [Online]. Available: https://www.opal-rt.com/software-communication-protocols/, (Last accessed: 12.09.2024).

[98] A. Sundararajan, A. Chavan, D. Saleem, and A. I. Sarwat, "A survey of protocol-level challenges and solutions for distributed energy resource cyber-physical security," *Energies*, vol. 11, no. 9, 2018, ISSN: 1996-1073. DOI: 10.3390/

en11092360. [Online]. Available: https://www.mdpi.com/1996-1073/11/9/2360.

[99] *TCP/IP vs. OSI: What's the Difference Between the Two Models?* [Online]. Available: https://community.fs.com/article/tcpip-vs-osi-whats-the-difference-between-the-two-models.html, (Last accessed: 09.12.2024).

Appendix A

Delays between City Nodes of the BT 21CN

Table A.1: Delays of every link between cities of the BT 21CN [60]

City A	Delay (μs)	City B
Leeds	60.445	Manchester
MiltonKeynes	61.130	Manchester
MiltonKeynes	61.099	Leeds
Docklands	61.621	Manchester
Docklands	61.447	Leeds
Docklands	60.592	MiltonKeynes
SouthBank	61.550	Manchester
SouthBank	61.412	Leeds
SouthBank	60.512	MiltonKeynes
SouthBank	60.194	Docklands
London	61.566	Manchester
London	61.471	Leeds
London	60.516	MiltonKeynes
London	60.190	Docklands
London	60.170	SouthBank
LondonNorthWest	61.546	Manchester

LondonNorthWest	61.408	Leeds
LondonNorthWest	60.497	MiltonKeynes
LondonNorthWest	60.212	Docklands
LondonNorthWest	60.188	SouthBank
LondonNorthWest	60.180	London
Birmingham	60.774	Manchester
Birmingham	60.916	Leeds
Birmingham	60.608	MiltonKeynes
Birmingham	61.035	Docklands
Birmingham	60.968	SouthBank
Birmingham	60.905	London
Birmingham	60.952	LondonNorthWest
Glasgow	61.522	Manchester
Glasgow	61.566	Leeds
ClydeValley	61.546	Manchester
ClydeValley	61.586	Leeds
ClydeValley	60.453	Glasgow
Newcastle	61.087	Manchester
Newcastle	60.806	Leeds
Newcastle	61.618	MiltonKeynes
Preston	60.370	Manchester
Preston	60.592	Leeds
Preston	61.265	MiltonKeynes
Preston	60.845	Birmingham
Sheffield	60.402	Manchester
Sheffield	60.382	Leeds
Sheffield	60.711	Birmingham
Derby	60.556	Manchester
Derby	60.683	MiltonKeynes
Derby	60.425	Birmingham

Peterborough	60.497	MiltonKeynes
Peterborough	60.687	SouthBank
Peterborough	60.695	LondonNorthWest
Guildford	60.445	Docklands
Guildford	60.370	SouthBank
Slough	60.326	Docklands
Slough	60.318	SouthBank
Slough	60.326	London
Slough	60.311	LondonNorthWest
Slough	60.322	Guildford
Bristol	60.920	SouthBank
Bristol	60.920	London
Bristol	60.734	Birmingham
Cardiff	61.130	London
Cardiff	61.118	LondonNorthWest
Cardiff	60.853	Birmingham
Cardiff	60.441	Bristol
Wolverhampton	60.703	Manchester
Wolverhampton	60.687	MiltonKeynes
Wolverhampton	60.976	LondonNorthWest
Wolverhampton	60.271	Birmingham

Appendix B

MATLAB Code for CNII Parameters: ASPTDD

```
1  function [t_d_delta, t_avg_normal] = calculatingDeltaT(
       matrix)
2  %calculatingDeltaT Analyze impact of node failures on
       network paths
3  %   [t_d_delta, t_avg_normal] = calculatingDeltaT(
       adjMtxPath)
4  %   calculates the impact of each node failure on average
       shortest path time.
5  %
6  %   Input:
7  %       matrix - adjacency matrix of network, elements
       represent delay
8  %       values
9  %
10 %   Outputs:
11 %       t_d_delta    - array of differences in average
       shortest path time when each node fails
12 %       t_avg_normal - average shortest path time during
       normal operation (no failures)
```

```
13
14 % Load adjacency matrix
15 numNodes = size(matrix, 1);
16
17 % Calculate normal operation statistics (no failures)
18 G_normal = graph(matrix);
19 D_normal = distances(G_normal);
20 validPaths_normal = D_normal(~isinf(D_normal) & D_normal >
      0);
21 t_avg_normal = mean(validPaths_normal);
22
23 % Preallocate array for results
24 t_d_delta = zeros(numNodes, 1);
25
26 % Calculate impact of each node failure
27 for node = 1:numNodes
28     % Create graph and remove current node
29     G = graph(matrix);
30     G = rmnode(G, node);
31
32     % Calculate shortest paths
33     D = distances(G);
34     validPaths = D(~isinf(D) & D > 0);
35
36     % Only calculate if there are valid paths remaining
37     if ~isempty(validPaths)
38         t_avg_failure = mean(validPaths);
39         t_d_delta(node) = t_avg_failure - t_avg_normal;
40     else
41         t_d_delta(node) = NaN; % No valid paths when this
              node fails
```

```
    end
end

% Display results
disp(['Normal average shortest path time: ', num2str(
    t_avg_normal), ' seconds']);
disp('Impact of each node failure (increase in average path
    time):');
for node = 1:numNodes
    disp(['Node ', num2str(node), ': ', num2str(t_d_delta(
        node)), ' seconds']);
end

end
```

Appendix C

MATLAB Code for CNII Parameters: Betweenness Centrality

```
function [t_d_delta, t_avg_normal] = calculatingDeltaT(
    matrix)

% Calculate betweenness centrality of nodes in centralised
    and distributed

load('comms_adj_mtx.mat')
global  comms_adj_mtx;

bc_nodes_distr = []; % Betweenness centrality of nodes in
    distributed mode
bc_nodes_centr = []; % Betweenness centrality of nodes in
    centralised mode

for N = 1:21
    bc_nodes_distr(N) = 0;
    for i = 1:size(comms_adj_mtx,1)
        for j = 1:size(comms_adj_mtx,1)
            [sp, spcost] = dijkstra(comms_adj_mtx, i, j);
```

```
            if ismember(N,sp)
                bc_nodes_distr(N) = bc_nodes_distr(N)+1;
            end
        end
    end
end

for N = 1:21
    bc_nodes_centr(N) = 0;
    for i = 1:size(comms_adj_mtx,1)
        for j= 1:size(comms_adj_mtx,1)
            [sp1, spcost1] = dijkstra(comms_adj_mtx, i, 21)
               ;
            [sp2, spcost2] = dijkstra(comms_adj_mtx, 21, j)
               ;
            if ismember(N,sp1) || ismember(N,sp2)
                bc_nodes_centr(N) = bc_nodes_centr(N)+1;
            end
        end
    end
end

disp(bc_nodes_distr)
disp(bc_nodes_centr)
```

Appendix D

GB Transmission System ETYS Zones

Figure A5: GB Transmission System ETYS Zones

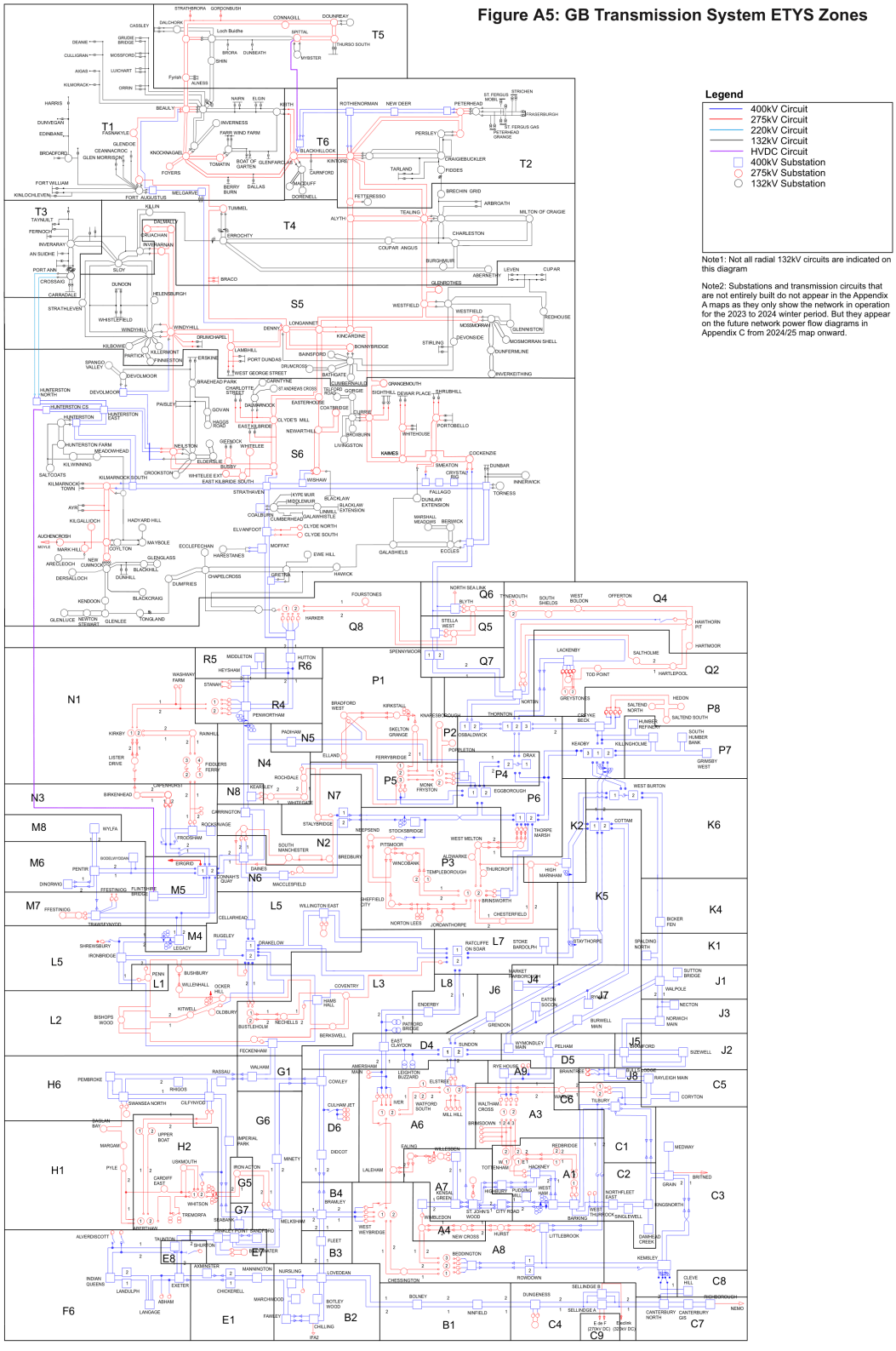

Figure D.1: GB Transmission System ETYS Zones

Appendix E

ePHASORSIM Workspace and Modelling Files

Figure E.1: ePHASORSIM workspace showing important modelling files 1

Figure E.2: ePHASORSIM workspace showing important modelling files 2