CYPRESS

CYPRESS : Report D2.2 – Co Simulation of cyber-physical transmission systems

Task 2.2 – Project Report

Authors: Sami Ben Mariem*, Adrien Leerschool, Adrien Godfraind, Alireza Bahmanyar, Laurine Duchesne

Date: 2024-12-28

Table of Contents

Executive Summary

This document is a deliverable of the "*Cyber-Physical Risk of the bulk Electric Energy Supply System*" (CYPRESS) project. The work presented in this document has been performed in the frame of the second task (T2.2) of the second work package WP2, titled "*Co-simulation of cyber-physical transmission systems*". The objective of CYPRESS WP2 is to develop a coherent methodology for the ex ante assessment of cyber-physical risks. It is based on i) the development of the mathematical and computational models of both the physical and the cyber parts of the system, ii) the design of a co-simulation platform where simulators of the electric power system physical behavior and of the ICT software and hardware layers are coupled, and iii) the development of an assessment methodology able to screen and identify the most important cyber-physical threats and compute the most informative performance indicators for reliability, resilience and cyber-security as defined in Task 1 of WP1.

Within this framework, T2.2 seeks at presenting the design and implementation of a co-simulation platform aimed at analyzing cyber-physical interactions within electrical power systems. The work addresses the critical challenge of understanding how cyber contingencies, such as network delays, packet losses, and cyber-attacks, can impact the stability and security of modern power grids.

The increasing integration of cyber components, including communication networks, control systems, and intelligent devices, introduces new vulnerabilities, making it essential to develop tools that capture the interplay between physical and cyber domains. Task 2.2 addresses this need by providing a unified framework that integrates key simulation tools and methodologies.

Chapter 2 introduces the context of cyber-physical systems and highlights the challenges of understanding the interactions between power system dynamics and cyber infrastructures. It provides a detailed analysis of the problem and describes the overall architecture of the co-simulation platform.

The platform integrates HELICS to synchronize the **time-driven power system simulation**, Dynawo, with our **event-driven network simulations**, OMNeT++. This synchronization ensures accurate modeling of interactions between the power and cyber domains. The platform also incorporates **libiec61850**, which emulates substation communication protocols like GOOSE and MMS. Furthermore, libiec61850 replicates the internal logic of smart substation devices, supporting configuration utilities based on real-world practices, such as parsing and using Substation Configuration Description (SCD) files.

Chapter 3 focuses on the implementation and validation of the co-simulation platform. The platform has been developed up to the level of simulating the **process bus**, enabling the relay of measurements and real-time control data between simulated substation components. A single validation scenario has been implemented to demonstrate the platform's functionality, focusing on the accurate synchronization of

simulations and the seamless exchange of data between power system and communication domains. While comprehensive cyber-physical scenarios, such as cyber-attacks or extensive communication disruptions, have not yet been implemented, this validation confirms the core principles of co-simulation and establishes a foundation for future extensions.

The final chapter reflects on the outcomes of Task 2.2, emphasizing that while the current implementation focuses on the process bus, the principles and methodologies established provide a pathway for further development. Future work could extend the platform to encompass the **station bus** and beyond, enabling a more complete analysis of cyber-physical interactions across all layers of the power system. Additional efforts could also incorporate advanced validation scenarios, such as cyber-attack simulations or probabilistic risk assessments.

Chapter 1: Introduction

The modernization of electrical power grids has introduced a significant reliance on cyber components, including communication networks, intelligent devices, and automation systems. While these advancements enable enhanced functionalities like real-time monitoring, adaptive control, and automated protection, they also expose the grid to new risks. Cyber-contingencies, such as delays, packet losses, or cyber-attacks, can propagate through the system, disrupting grid operations and stability.

For instance, a cyber-attack targeting substation communication can delay critical protection actions, introduce incorrect measurements, or disable control functionalities. These disruptions can escalate, affecting system reliability, voltage regulation, or even leading to cascading failures. Such vulnerabilities pose significant challenges to the operation and security of modern power systems, where timely and accurate information exchange is crucial for stability and resilience.

Traditional simulation tools are not well-equipped to address these challenges. Power system simulators, like Dynawo, excel at modeling physical grid behavior, such as voltage stability, frequency regulation, and fault recovery, but they do not account for the underlying communication and cyber infrastructure. On the other hand, network simulators like OMNeT++ focus on modeling communication systems, including packet flows, delays, and network topologies, but they overlook the interaction of these communication systems with the grid's physical dynamics. Furthermore, an additional complexity lies in accurately modeling the **internal logic of critical devices**, such as:

- **Intelligent Electronic Devices (IEDs):** Devices used for protection and control, such as relays, which process real-time measurement data and execute critical grid operations like tripping breakers during faults.
- **SCADA Devices:** Systems that aggregate and relay information between substations and control centers, enabling remote monitoring and control actions.
- **Merging Units (MUs) and Remote Terminal Units (RTUs):** Devices that digitize measurements or interface between legacy and modern systems.

These devices often implement proprietary algorithms and logic, making their behavior difficult to replicate in a simulation environment. Emulating this internal logic, including decision-making processes for protection, control, and data aggregation, requires specialized tools that can mimic real-world configurations, such as those based on Substation Configuration Description (SCD) files.

To address these challenges, Task 2.2 of the CYPRESS project focuses on developing a co-simulation platform capable of simulating both the physical and cyber domains of power systems. The platform integrates specialized tools:

- **Dynawo** models the physical behavior of the grid, capturing system dynamics like voltage stability and the response to faults.

- **OMNeT++** simulates the behavior of communication networks, such as data transfer between substations and control centers, and internal communication within substations (e.g., GOOSE messages and Sampled Values).
- **libiec61850** emulates the communication logic of substation devices, including IEDs and MUs, based on the IEC 61850 standard. It also supports the use of SCD files to replicate real-world device configurations and communication flows.

- **HELICS** orchestrates the co-simulation by synchronizing the time-driven simulations in Dynawo with the event-driven processes in OMNeT++.

The integration of these tools enables the platform to analyze cyber-physical interactions comprehensively. It captures the propagation of cyber contingencies, such as communication delays or faults, through the grid and evaluates their impact on both the physical and cyber domains. For example:

- A delay in a GOOSE message relayed by an IED can affect the tripping of a breaker, leading to prolonged fault conditions and potential cascading failures.
- SCADA communication delays or packet losses may result in stale data at the control center, causing operators to act on outdated information.

By focusing on the interaction between physical system dynamics and supporting cyber infrastructure, the co-simulation platform allows for deeper analysis of vulnerabilities and the testing of mitigation strategies. The platform provides a foundation for studying immediate impacts of cyber-contingencies, such as operational disruptions, and for exploring long-term strategies to enhance the resilience of power grids. This deliverable documents the design, implementation, and validation of the platform, demonstrating its potential to address critical challenges in securing modern power systems.

Chapter 2: Co-Simulation Platform Architecture and Framework

This chapter presents the architecture and design of the co-simulation platform developed under Task 2.2, focusing on how the power system and communication network simulators are integrated to study cyber-physical interactions. It begins with an overview of the platform, describing its modular design and the key components involved, including Dynawo for power system dynamics, OMNeT++ for communication network modeling, libiec61850 for substation communication emulation, and HELICS for synchronization.

The chapter elaborates on the synchronization mechanisms that bridge the time-driven and event-driven paradigms of the power and cyber domains, ensuring consistent and accurate data exchange. The internal logic of devices such as Intelligent Electronic Devices (IEDs) and Merging Units (MUs) is also discussed, emphasizing how libiec61850 replicates real-world configurations and behaviors.

Problem Statement

The increasing integration of advanced communication networks and intelligent devices into power systems has transformed traditional grids into complex cyber-physical systems (CPS). While this integration enhances monitoring, control, and efficiency, it also introduces new challenges, particularly concerning the interactions between the cyber and physical components. Disruptions in the communication network—such as delays, data losses, or cyber-attacks—can adversely affect power system operations, potentially leading to instability or failures [1].

Traditional simulation tools often address either the physical power system or the communication network in isolation, lacking the capability to capture the intricate interdependencies between these domains. This limitation hampers the ability to analyze how cyber events impact physical grid stability and vice versa. To bridge this gap, co-simulation platforms have been developed to enable integrated analysis of both domains, providing a more comprehensive understanding of CPS behavior [2].

Existing platforms for simulating cyber-physical power systems (CPPS) often encounter challenges in providing both scalable and detailed simulations of complex CPPS behaviors. Many rely on hardware-in-the-loop (HIL) mechanisms to achieve detailed, real-time simulations, which can be limited by the need for specialized hardware and may not scale effectively for large systems. For instance, a co-simulation platform utilizing RT-LAB and OPNET software offers real-time HIL capabilities but may face scalability constraints when applied to extensive power grids [3]. Conversely, some platforms employ custom implementations tailored to specific CPPS scenarios, potentially lacking the flexibility to encompass the complex behaviors of the system as a whole. These limitations highlight the need for more versatile simulation platforms capable of balancing detail and scalability across diverse CPPS applications. Conversely, some platforms employ custom implementations tailored to specific CPPS scenarios, potentially lacking the flexibility to encompass the complex behaviors of the system as a whole. For example, the co-simulation platform presented in [4] integrates control function layers, communication layers, and the physical power

system layer to enhance CPPS security. However, it simplifies the cyber component to basic communication network aspects, primarily focusing on latencies and packet drop policies, without incorporating more intricate cyber elements such as device logic, firewall rules, or database interactions. This reduction limits its ability to fully represent the complexities of cyber-physical interactions within power systems. On the other hand, [5] employs a highly customized setup utilizing virtual hosts configured for specific use cases. This static configuration, based on a network emulation layer, poses challenges when adapting to different scenarios, particularly those involving wide-area networks (WANs). The reliance on emulated network environments limits scalability and flexibility, making it difficult to accurately represent the complexities and dynamics of diverse CPPS applications.

The primary objective of the co-simulation platform developed in Task 2.2 is to address the limitations observed in existing platforms by enabling a more versatile and comprehensive analysis of cyber-physical interactions within power systems. Building on the need for scalability and adaptability, the platform bridges the gap by integrating power system simulators with communication network simulators in a unified and flexible framework. Unlike hardware-in-the-loop (HIL) setups constrained by specialized hardware, the platform eliminates the dependency on physical components while preserving the capability to emulate detailed device behaviors, such as IED logic, firewall configurations, and communication protocols. In contrast to custom implementations that focus on narrow use cases with rigid configurations, it employs a modular and dynamic architecture, allowing for the seamless adaptation of simulations to diverse CPPS scenarios, including wide-area network interactions and cascading grid failures. By avoiding simplifications such as reducing cyber-physical interactions to network latency and packet loss metrics, the platform provides a detailed and realistic representation of the cyber domain, including the ability to simulate complex cyber-attacks, data corruption, and their propagation through the grid. Through these innovations, the Task 2.2 platform addresses the challenges of existing solutions, delivering a robust tool that enhances the understanding of CPPS behaviors and supports the development of strategies to improve grid resilience and security.

Platform Architecture & Design

The architecture of the co-simulation platform developed under Task 2.2 integrates components from both power system simulation and cyber domain modeling to provide a comprehensive framework for analyzing cyber-physical power systems (CPPS). This section details the platform's design, emphasizing its modular structure, synchronization mechanisms, and the interaction between its various components.

Design Philosophy

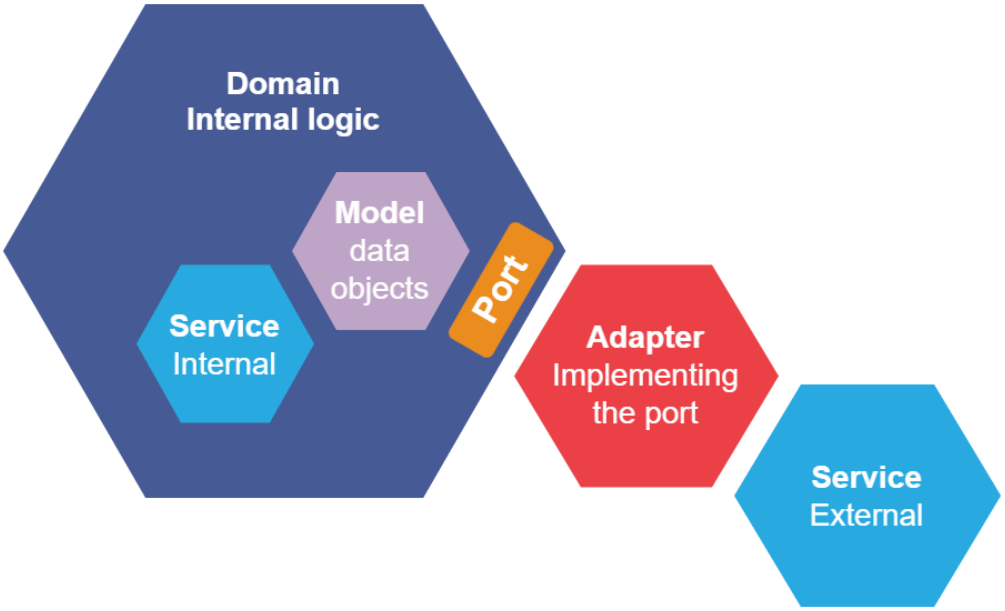

Figure 1: *Hexagonal Architecture*

The co-simulation platform is built upon a **Hexagonal Architecture** to ensure modularity, flexibility, and adaptability. This architectural principle organizes the platform into a central **Domain Engine**, surrounded by independent modules responsible for scenario management, ICT network simulation, power system simulation, and output processing.

The **core idea** of the hexagonal design is to separate functionality into distinct components that interact through well-defined **ports** and **adapters**. Ports provide standardized interfaces for communication, while adapters handle data translation and integration, ensuring seamless interoperability between heterogeneous systems.

This architecture supports the independent development and integration of components, allowing researchers to plug in new tools or replace existing ones without disrupting the overall framework. By maintaining a clear boundary between the core engine and external modules, the hexagonal design enhances scalability and facilitates collaboration across diverse CPPS studies.

Overview

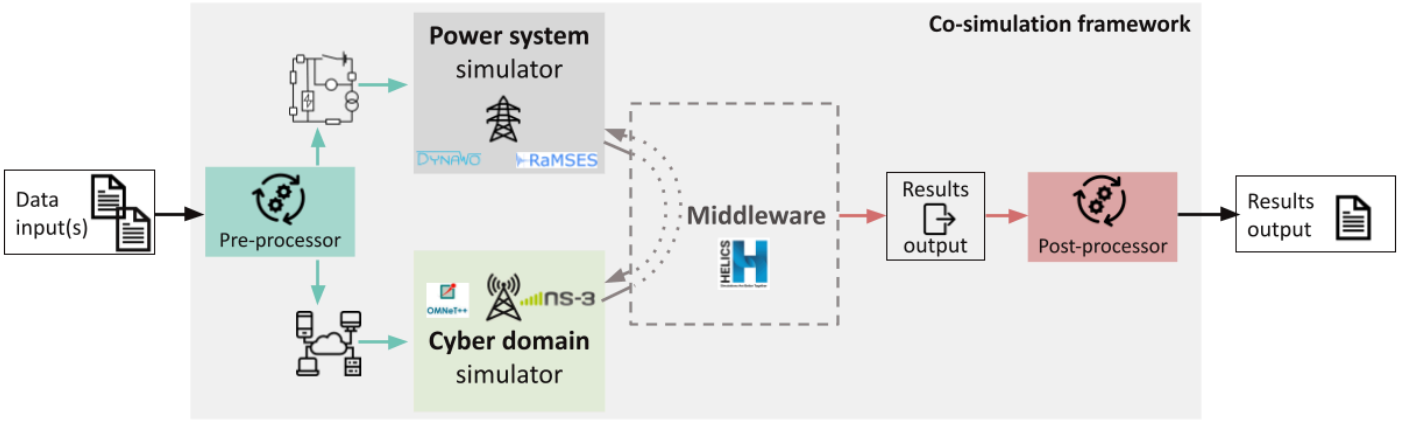

Figure 2: *Architecture Overview*

Core Components of the Architecture

At the heart of the platform lies the **Domain Engine**, which serves as the central integration point for the power system simulation, the ICT network simulation, scenario management, and the processing of simulation outputs. The architecture can be broken down into the following key elements:

1. **Scenario Management**:
    - The **Scenario Creator** defines the events, conditions, and configurations required for a simulation.
    - It supports both JSON and CSV formats for flexible scenario input. These are parsed through respective loaders to populate the necessary simulation parameters.

2. **ICT Network Simulation**:
    - This component represents the cyber domain of the platform, where network interactions such as communication delays, data packet losses, and routing decisions are modeled.
    - ICT Network configurations are ingested via a **Network Loader** and parsed from dedicated configuration files. These files define the topology, protocols, and behavior of the communication infrastructure.

3. **Power System Simulation**:
    - The physical power grid is modeled in this component, which supports time-driven simulations of power flows, fault conditions, and system stability.
    - The power system inputs are provided through pre-configured files, parsed and loaded into the platform to ensure realistic grid behavior.

4. **Simulation Output**:
    - As the simulation runs, outputs from both the cyber and power system domains are collected, processed, and passed through post-processing utilities.

    - These outputs enable detailed analysis of the system behavior under the simulated scenarios, such as fault propagation or the impact of cyber-attacks.

Coordination and Synchronization

The co-simulation platform employs HELICS as the middleware to coordinate the interactions between the various simulators and synchronize their operations. HELICS acts as the backbone of the framework, facilitating data exchange and temporal alignment between:

- **Dynawo** for power system simulations.
- **OMNeT++** as network simulators for ICT modeling.

The HELICS input and output adapters enable seamless communication between the simulators and the co-simulation framework. These adapters act as bridges, ensuring data consistency and efficient synchronization between different domains.

Simulation Workflow

The simulation process begins with the preparation of input files:

- **Power System Configuration Files** describe the physical grid layout, component properties, and operational parameters.
- **ICT Network Files** define the communication infrastructure.
- **Scenario Files** specify the sequence of events and conditions to be analyzed.

Once inputs are loaded, the co-simulation framework coordinates the execution of the simulations across the cyber and power system domains. Data is exchanged through defined ports, enabling bidirectional interaction. For instance:

- Fault data from the power system simulation triggers network responses in the ICT domain.
- Communication delays or losses simulated in the ICT network affect control signals sent to the power system.

Finally, the simulation outputs are processed to generate results, which can be analyzed for insights into CPPS behavior.

Input & Output Data Processing

The co-simulation platform incorporates a well-defined architecture for input and output data processing, enabling streamlined scenario management, ICT network configuration, and power system simulation. Although the data processing framework has been designed, its implementation is still a work in progress. This section outlines the planned functionalities and the envisioned workflows for handling input and output data.

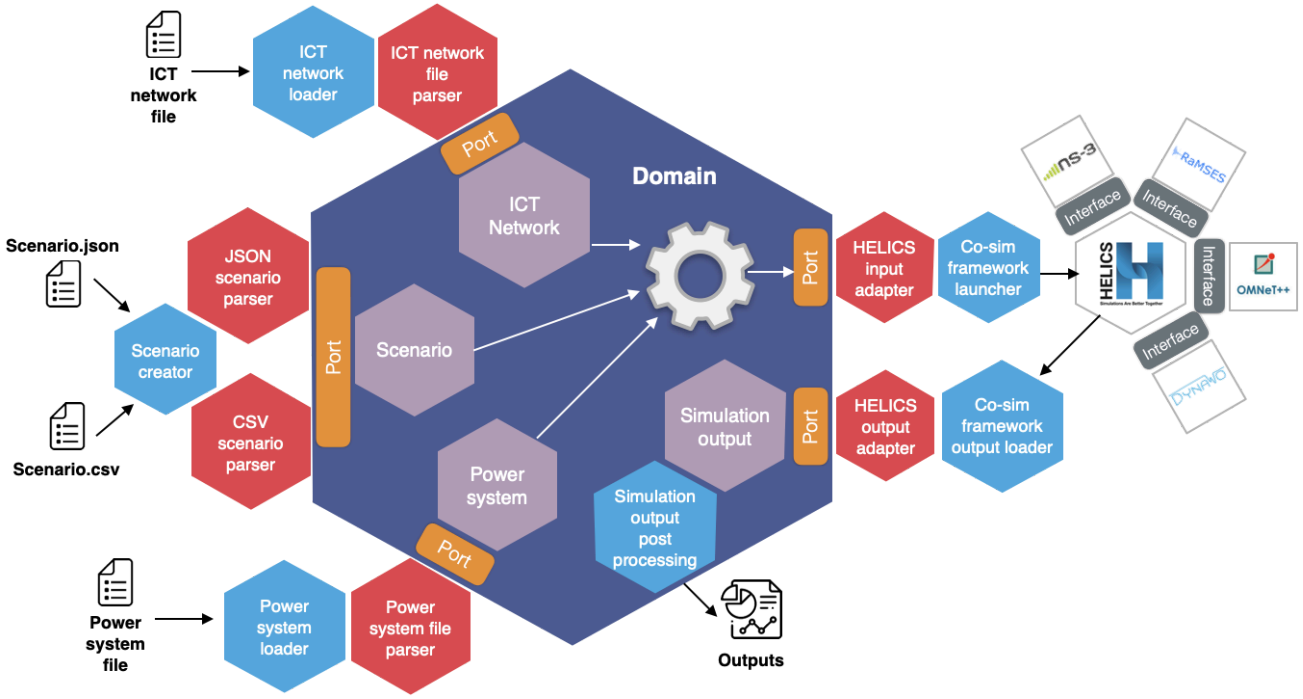

Figure 3: Input and Output Data Processing

Scenario Management

Scenario management is a cornerstone of the platform's architecture, providing the ability to define and execute complex CPPS scenarios. The design includes:

- **Scenario Input Files:** Support for JSON and CSV formats to specify scenarios. These formats are intended to allow users to define:
  - Event triggers such as cyber-attacks or power system faults.
  - Timelines and dependencies for event execution.
  - Dynamic interactions between cyber and physical domains.
- **Scenario Creator:** A module designed to parse and validate input files and load scenario data into the simulation framework.

ICT Network Configuration

The ICT network configuration defines the behavior of the cyber domain, focusing on communication networks and device interactions. The proposed architecture includes:

- **ICT Network Input Files:** These files will specify network topology, communication protocols, and device behaviors, including:
    - Parameters for IEC 61850, MMS, and other protocols.
    - Network-specific characteristics such as delays and packet loss.
- **Network File Parser and Loader:** Designed to validate and process input files for integration into the OMNeT++ simulator. This module will enable the simulation of network interactions, including the propagation of control signals and data packets.

Power System Configuration

The power system simulation layer models the physical grid's behavior, with the architecture designed to handle both static and dynamic data inputs. Key components include:

- **Power System Input Files:** Defined formats for specifying grid topology, operational parameters, and component behavior.
- **Power System File Parser and Loader:** A module intended to process and validate input data before integration into the Dynawo simulator.

Output Post-Processing

The post-processing stage is crucial for analyzing the results generated by the simulation. The design includes:

- **Simulation Output Loader:** A component to aggregate simulation results from the power and cyber domains.
- **Output Processing Tools:** Tools for converting raw data into formats suitable for visualization and reporting.

Implementation Status

While the input and output data processing framework has been conceptually defined, its implementation is pending. The design provides a strong foundation for integrating scenario management, network configuration, and power system simulation into a cohesive pipeline. Future development will focus on implementing these modules to realize the platform's full potential.

Co-Simulation Architecture and Workflow

The co-simulation framework integrates the time-driven power system simulator, the event-driven network simulator, and the emulated IEC 61850 components to provide a holistic view of cyber-physical interactions. This section details the interaction mechanisms and synchronization processes within the co-simulation framework, facilitated by the HELICS middleware.

The co-simulation platform couples three main components to enable detailed analysis of CPPS:

1. **Power System Simulator (Dynawo):**
    - Simulates the physical grid using a variable time-step method.
    - Models grid elements, including generators, transformers, and loads.
    - Incorporates fault conditions and system dynamics.
2. **Cyber Domain Simulator (OMNeT++):**
    - Emulates network behavior using an event-driven simulation paradigm.
    - Models communication delays, packet losses, and protocol-specific interactions (e.g., GOOSE, MMS).
    - Incorporates a process bus for detailed communication modeling.
3. **Emulated IEC 61850 Components (libiec61850):**
    - Implements device-specific logic, such as protection relays and RTUs.
    - Supports server and client functionalities for GOOSE, MMS, and Sampled Values (SV).
    - Configured using industry-standard ICD files for realistic substation emulation.

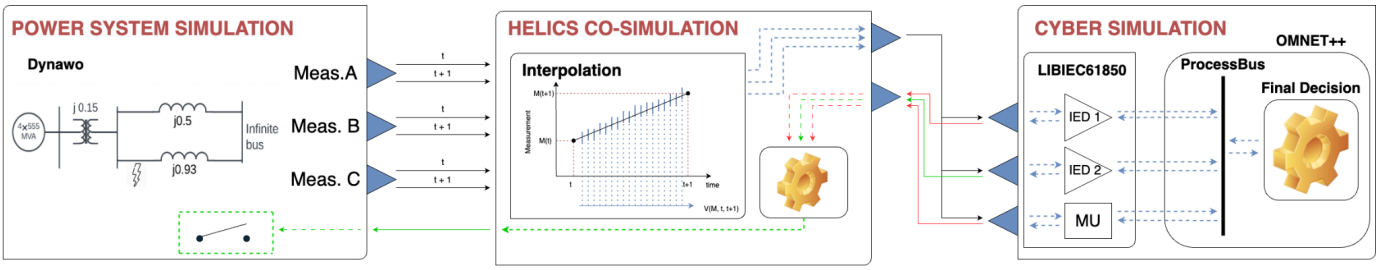

Figure 4: Co-Simulation Workflow

Time Synchronization

Time synchronization is a critical aspect of the co-simulation framework, ensuring accurate interaction between the time-driven power system simulator, the event-driven cyber simulator, and the emulated IEC 61850 components. Given the differing time management paradigms of these simulators, a robust synchronization mechanism is required to maintain consistency across the simulation domains.

Challenges of Synchronization

- **Variable Time-Step in Power System Simulations:**
    - The power system simulator, such as Dynawo, employs a variable time-step method to optimize computational efficiency.
    - Time-steps vary depending on grid dynamics, with smaller steps during rapid transients (e.g., fault events) and larger steps during steady-state operation.

- **Event-Driven Nature of Cyber Simulations:**
    - The cyber simulator, like OMNeT++, processes events asynchronously, focusing only on specific communication actions.
    - Time advances only when events occur, which contrasts with the continuous time progression of power system simulations.
- **Synchronization Between Domains:**
    - A mismatch in time management can lead to inconsistencies, such as outdated power system states in the cyber simulator or missed events due to delayed synchronization.

HELICS as the Synchronization Engine

HELICS plays a central role in achieving synchronization across the simulators:

- **Time-Management Coordination:**
    - HELICS implements a federated time-management mechanism to align the clocks of all participating simulators. Each federate (simulator) communicates its time requests and constraints to HELICS, which determines the global time advancement.
- **Discrete-Time Coordination:**
    - The event-driven nature of OMNeT++ is aligned with the discrete-time events in Dynawo by synchronizing the HELICS federation at the smallest common time-step required for accurate interaction.
- **Dynamic Time Adjustment:**
    - HELICS dynamically adjusts time synchronization based on the complexity of ongoing events. For instance, during rapid transient conditions, synchronization intervals are reduced to capture high-resolution interactions.

Interpolation of Missing Values

Interpolation of missing values is essential in the co-simulation platform to address the temporal mismatches between the time-driven power system simulator and the event-driven cyber simulator. The power system simulator, such as Dynawo, uses a variable time-step approach to optimize computational resources, employing smaller steps during transients and larger ones during stability. Conversely, the cyber simulator processes events asynchronously, often requesting power system states at times not covered by the simulator's steps, leading to data gaps. While forcing the power system simulator to adopt tiny fixed time steps could theoretically align the two simulators, this approach would introduce excessive computational overhead, redundant state updates, and inefficiencies, especially in large-scale grid simulations. Instead, the platform uses interpolation to estimate missing intermediate values, ensuring the cyber simulator receives accurate data without imposing unnecessary computational demands on the power system simulator.

HELICS facilitates this process by detecting discrepancies in time requirements and invoking an interpolation module to generate values using techniques like linear or spline interpolation, tailored to the system's behavior. This method preserves the power simulator's efficiency while enabling seamless interaction, ensuring robust and accurate modeling of cyber-physical power system dynamics.

OMNeT++ Scheduler for Interacting with Emulated libIEC61850 Devices

A custom scheduler has been implemented within OMNeT++ to facilitate interaction with the emulated libIEC61850 devices, ensuring precise synchronization and efficient handling of time-sensitive operations. This scheduler is central to bridging the event-driven cyber simulator with the real-time emulation of IEC 61850 devices, which include functionalities such as GOOSE messaging, MMS interactions, and Sampled Values (SV) publishing. The OMNeT++ scheduler is tailored to meet the following requirements:

- **Synchronization with Emulated Devices**:
  - The scheduler coordinates with the emulated libIEC61850 software to ensure all device interactions occur at the correct simulation time.
  - It queries the state of the emulated devices based on the simulator's current time-step and processes the output as needed.
- **Dynamic Time Management**:
  - The scheduler dynamically advances the simulated time within OMNeT++ based on the computational requirements of the emulated devices.
  - It determines how much time has elapsed in the emulation and uses this information to align with the broader simulation timeline managed by HELICS.
- **Output Handling**:
  - At each step, the scheduler collects output data from the emulated devices, such as GOOSE messages or control responses, and forwards it to the appropriate modules within the cyber simulator.
  - These outputs are then processed or sent to other parts of the co-simulation, such as the process bus or power system simulator.

Interaction Workflow

1. **Call to Emulated Software:**
   a. The scheduler initiates a call to the libIEC61850 emulation at specific intervals, depending on the requirements of the simulation scenario.
   b. This call ensures that the emulated devices operate consistently with their real-world counterparts, providing outputs at expected intervals.

2. **Time Progression Management:**
   a. The scheduler calculates the time that should advance within the emulation based on the elapsed simulation time in OMNeT++.
   b. This mechanism ensures that the emulated devices respond to events in the correct temporal sequence, even when operating within an event-driven simulator.

3. **Output Collection and Processing:**
   a. Once the emulated devices complete their processing for a given interval, the scheduler collects all outputs, such as state changes or protocol-specific messages.
   b. These outputs are made available to other components of the simulation for further action, such as relaying commands or updating monitored states.

4. **Next Simulation Step:**
    a. The scheduler determines the next emulation step based on the input from OMNeT++ and the emulated software's internal logic, ensuring smooth continuity between events.

Benefits of the Custom Scheduler

- **High-Fidelity Emulation:**
    - By integrating libIEC61850 into the OMNeT++ environment, the scheduler ensures realistic behavior of IEC 61850 devices, preserving the fidelity of GOOSE, MMS, and SV communications.
- **Efficient Time Management:**
    - The dynamic adjustment of time progression minimizes unnecessary computation while ensuring that events occur at the correct simulated times.
- **Seamless Integration with HELICS:**
    - The scheduler operates in tandem with HELICS to align the emulation time with the overall co-simulation framework, maintaining consistency across all simulators.

<u>Synchronization Workflow</u>

The co-simulation workflow outlines how the power system simulator, cyber simulator, and middleware interact to ensure consistent and accurate modeling of cyber-physical power systems. The synchronization and data exchange processes are coordinated through HELICS, which facilitates smooth communication between the simulators and manages time alignment. The following steps detail the workflow:

1. **Power System Simulation Execution:** The power system simulator, such as Dynawo, begins its simulation for a given time interval t to $t+1$. During this interval, it computes the physical state of the grid, such as voltage, current, and frequency, based on its internal models and any applied operational conditions or faults.

2. **Data Subscription and Transmission:** At the end of the time step ($t+1$), the power system simulator forwards its computed state values to HELICS. These subscribed values represent the key parameters needed by the cyber domain for further processing and monitoring.

3. **Middleware Interpolation:** HELICS identifies any intermediate timestamps required by the event-driven cyber simulator that are not covered by the power system's variable time steps. The middleware uses an interpolation module to generate the missing values, ensuring that the data aligns with the cyber simulator's finer temporal resolution.

4. **Data Upsampling and Forwarding:** The interpolated and upsampled data is sent to the cyber simulator, where it becomes available for further processing by emulated devices. This ensures the cyber domain has continuous and temporally accurate data for making decisions.

5. **IED Monitoring and Decision-Making:** The emulated Intelligent Electronic Devices (IEDs) in the cyber simulator monitor the incoming data and use it to make decisions based on predefined logic. These decisions might include sending trip commands, adjusting control setpoints, or forwarding processed information to other components in the network via the process bus.

6. **Decision Feedback to Power System:**
    a. If no instructions are generated by the cyber simulator, the power system simulator advances to the next time step (t+1 to t+2) and repeats the process.
    b. If an instruction is issued (e.g., a breaker trip command or generator setpoint change), HELICS passes the command to the power system simulator. The simulator applies the changes to its operational state and then computes the next time step.

7. **Iterative Process:** This iterative workflow continues, allowing dynamic interaction between the power and cyber domains. The seamless synchronization provided by HELICS ensures that both simulators remain temporally aligned, capturing the bidirectional impact of cyber-physical interactions.

Chapter 3: Proof of Concept

In this chapter, we present the implementation and validation of a fully operational process bus within the co-simulation platform on the small test system represented in Figure 4. This proof of concept demonstrates the platform's ability to integrate power system and cyber domain simulations, focusing on Sampled Values (SV) for monitoring and GOOSE messaging for control processes. By showcasing the seamless interaction between the power system simulator (Dynawo), the cyber simulator (OMNeT++), and the emulated IEC 61850 components (libIEC61850), this chapter highlights the platform's capacity to model complex cyber-physical power system (CPPS) behaviors with high fidelity.

Implementation of the Process Bus

The process bus implementation aimed to emulate real-world substation communication. This included establishing a monitoring workflow through SV and a control workflow using GOOSE messages. These workflows were enabled by components designed within OMNeT++ and libIEC61850, synchronized with HELICS for consistent temporal alignment.

Sampled Value Workflow

- **Signal Acquisition and Interpolation:**
  - The **HelicsSensor** component in OMNeT++ periodically retrieved signal values from the **HelicsInterpolationFederate**, which interpolated data generated by Dynawo.
  - The interpolation accounted for the power system simulator's variable time steps and added minor noise to simulate realistic sensor behavior.
- **Sampled Values Publisher:**
  - The interpolated signals were forwarded to the **SV Publisher** component in OMNeT++, representing a Merging Unit (MU).
  - This component interfaced with libIEC61850 to generate SV messages formatted according to IEC 61850 standards.
- **Process Bus Communication:**
  - The SV messages were transmitted over the **ethernetBus** component in OMNeT++, simulating a real process bus environment within a substation.
- **Sampled Values Subscriber and HMI:**
  - The **SV Subscriber** component received the SV messages, which were parsed by libIEC61850 to extract the signal values.
  - These parsed values were returned to OMNeT++ and displayed on the OMNeT++ GUI, emulating the functionality of a Process Bus HMI.

Control Trigger Workflow

The control trigger workflow demonstrates how the co-simulation platform uses Sampled Values (SV) to detect voltage threshold violations and initiate a control action, such as tripping a breaker.

- **Signal Acquisition and SV Generation:**
  - Dynawo computes voltage values and sends them to the **HelicsInterpolationFederate** via HELICS.
  - The interpolated signal is retrieved by the **HelicsSensor** and passed to the **SV Publisher** to generate Sampled Value (SV) messages using libIEC61850.
- **Transmission over Process Bus:**
  - SV messages are transmitted over the **ethernetBus** in OMNeT++, simulating the process bus.
- **SV Reception and Threshold Monitoring:**
  - The **SV Subscriber** parses the messages using libIEC61850 and forwards voltage values to a **Threshold Monitoring Module**.
  - If the threshold is exceeded, a control action is triggered.
- **GOOSE Message Generation:**
  - The **GOOSE Publisher** generates a GOOSE message signaling the control action and sends it over the process bus.
- **Breaker Activation:**
  - The **Breaker Controller** receives and parses the GOOSE message, forwarding the command to HELICS.
  - HELICS sends the command to Dynawo, where the breaker is opened, updating the grid state.
- **System Feedback:**
  - The updated grid state is sent back to the cyber simulator, completing the workflow.

Results and Validation

The validation of the proof of concept focused on both the monitoring and control aspects of the implemented workflows, emphasizing accuracy and fidelity.

- **Signal Superposition for Sampled Values:**
  - Signals generated by Dynawo were directly compared to those displayed on the Process Bus HMI in OMNeT++ after undergoing SV digitalization, communication, and reconstruction.
  - Superposing the original and reconstructed signals demonstrated near-identical waveforms, confirming the accuracy of the SV workflow. Minor deviations introduced by interpolation noise were within acceptable limits and representative of real-world sensor behavior.
- **Control Action Verification for GOOSE:**
  - The control action initiated by the GOOSE message (e.g., a breaker trip) was tracked from generation to application.
  - Observations confirmed that the GOOSE message was generated correctly, transmitted through the process bus, parsed by libIEC61850, and relayed to Dynawo, where it triggered the intended state change.
  - The timing of the control action was consistent with real-world scenarios, demonstrating the platform's ability to model end-to-end control processes effectively.

Key Observations and Achievements

The implemented proof of concept highlighted the co-simulation platform's ability to accurately emulate cyber-physical interactions in power systems, integrating both real-time monitoring and control workflows. The key achievement lies in the seamless integration of Dynawo, OMNeT++, libIEC61850, and HELICS, enabling realistic and synchronized data exchange across the cyber and physical domains.

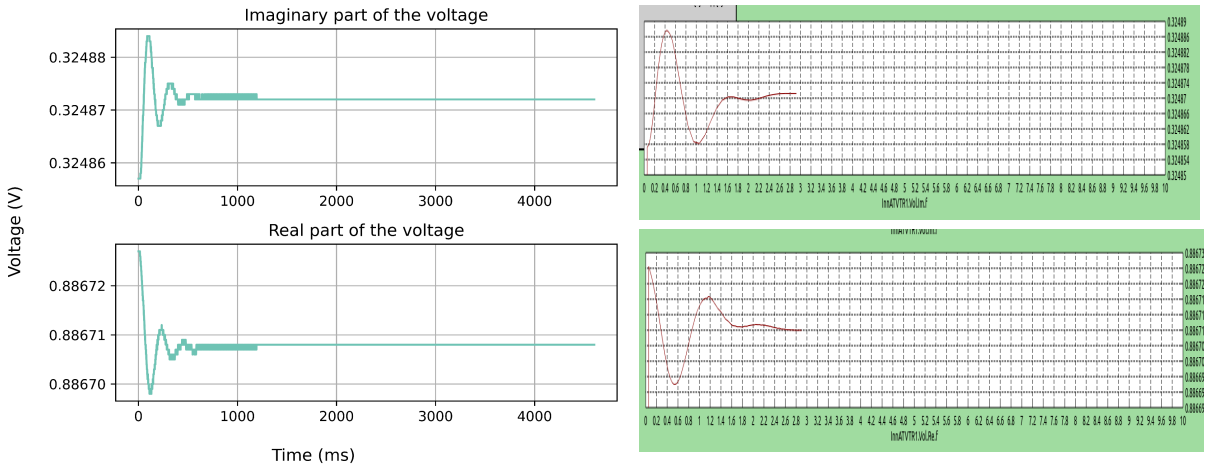

Figure 5: Co-Simulation Workflow

Figure 5 illustrates the validation of the workflow, where the voltage signals generated in the power system simulation (Dynawo) are superimposed with the signals displayed on the emulated Process Bus HMI in OMNeT++. Both the real and imaginary parts of the voltage show near-identical behavior in the simulated signals and the HMI output, demonstrating the fidelity of Sampled Value (SV) transmission, digitalization, and reconstruction. The minor discrepancies observed, mainly attributed to interpolation noise, fall within acceptable limits and are representative of real-world sensor variability.

Additionally, the platform effectively modeled control actions using GOOSE messaging, allowing a voltage threshold event to trigger a breaker operation. The end-to-end workflow, involving detection in the power system, communication over the process bus, and control application in Dynawo, validated the bidirectional interaction capability of the platform. These results confirm the platform's ability to accurately represent both the dynamic behavior of power systems and the intricacies of cyber communications, positioning it as a robust tool for analyzing complex cyber-physical power system scenarios. The flexibility demonstrated in adapting the platform for monitoring and control use cases further emphasizes its potential for studying diverse scenarios, such as cascading failures and cyber-attack impacts.

Chapter 4: Challenges, Contributions and Further Work

The co-simulation platform developed under Task 2.2 provides a robust foundation for studying the complex interactions within cyber-physical power systems (CPPS). However, the development process has revealed certain challenges that need to be addressed to further enhance its applicability and efficiency. In this chapter, we outline the main contributions of the platform, highlight the challenges encountered during its development, and propose directions for future work to expand its capabilities and usability.

Main Contributions

The platform delivers several innovations that address the limitations of existing co-simulation tools. Its modular and scalable design enables detailed and synchronized analysis of cyber-physical interactions:

- **Integration of Cyber and Physical Domains:**
  - The platform bridges the gap between time-driven power system simulations and event-driven network simulations, enabling detailed modeling of CPPS interactions. This integration captures the bidirectional dependencies between cyber and physical domains, including scenarios such as cyber-attacks affecting grid stability and physical faults propagating through communication networks.

- **Emulation of IEC 61850 Protocols:**
  - By integrating libIEC61850, the platform supports the emulation of Sampled Values (SV) and GOOSE messaging workflows, allowing realistic communication modeling at the substation level. This feature ensures compatibility with industry standards and replicates real-world substation behavior.

- **Flexible Synchronization Framework:**
  - The use of HELICS provides dynamic synchronization between the simulators, accommodating the differing time-management paradigms of time-driven and event-driven systems. The interpolation module ensures smooth data exchange without compromising efficiency or accuracy.

- **Validation Through Realistic Scenarios:**
  - The platform has been validated through a fully implemented process bus, demonstrating its ability to simulate monitoring (SV) and control workflows. These tests confirm the platform's capability to analyze cyber-physical interactions with high fidelity.

Encountered Challenges

The development of the platform highlighted several technical and design challenges, which provide valuable insights for future improvements:

- **Synchronization Complexity:**
    - Aligning the time-driven power system simulations with the event-driven cyber simulations posed significant challenges. Handling temporal mismatches required advanced interpolation techniques to generate intermediate values, ensuring accurate and consistent data exchange. Balancing accuracy with computational efficiency, especially during high-dynamics events, was a key focus area.

- **Unimplemented Input/Output Data Processing:**
    - While the input/output data processing architecture has been clearly defined, its implementation is yet to be completed. This includes developing tools for loading and validating input scenario files and post-processing simulation outputs. Without these functionalities, the workflow remains partially manual, limiting the platform's usability and efficiency.

- **Scenario Complexity:**
    - Designing and defining complex scenarios, such as cascading failures, multi-stage cyber-physical contingencies, and adaptive control strategies, proved to be challenging. These scenarios require detailed parameterization and dynamic adjustments during runtime to fully leverage the platform's capabilities. Enhancing the tools for scenario definition and runtime interaction will be crucial for future development.

- **Integration of Diverse Components:**
    - While the platform successfully integrates different simulators and emulated devices, ensuring seamless communication across varying data formats, protocols, and interfaces required extensive customization. Establishing robust mechanisms for compatibility between the cyber and physical components was particularly challenging, as it required significant development effort.
      Unlike many other co-simulation platforms, **scalability has not emerged as a limiting factor** for this platform. By leveraging virtualization for emulated devices and allowing parallelization of simulators, the platform inherently supports efficient scaling. With sufficient computational resources, the platform could manage large-scale simulations involving multiple substations and complex system-wide scenarios, ensuring its applicability to real-world CPPS challenges.

Future Works

To address the identified challenges and expand the platform's functionality, the following areas of further work are proposed:

- **Implementation of Input/Output Data Processing:**
    - Develop tools to parse JSON and CSV scenario files, enabling seamless loading of complex simulation parameters.
    - Implement post-processing utilities to align and visualize simulation outputs for comprehensive analysis.

- **Enhanced Device and Protocol Modeling:**
    - Extend support to additional protocols, such as DNP3 and IEC 60870-5-104, for representing legacy systems.
    - Introduce emulation of more advanced devices, such as wide-area monitoring systems (WAMS) and phasor measurement units (PMUs).

- **Expansion Beyond the Process Bus**
    - The proof of concept focuses on the process bus; however, extending the platform to model additional levels of the power system is crucial:
    - Integration of station-level communication, enabling interactions between multiple substations and control centers.
    - Modeling inter-substation communication protocols and their influence on grid-wide protection and control.

- **Dynamic Interaction Support:**
    - Enable dynamic scenario modifications during runtime, such as introducing faults or changing control logic, to support adaptive strategies and cascading event simulations.

- **Scalability Enhancements:**
    - Optimize HELICS synchronization for large-scale simulations involving multiple substations and control centers.
    - Introduce parallelization techniques in OMNeT++ and Dynawo to handle grid-wide models more efficiently.
- **Validation Against Real-World Data:**
    - Collaborate with industry stakeholders to test the platform using operational data, ensuring that its results align with practical CPPS behavior.

- **Definition of More Complex Scenarios:**
    - Leverage the configuration files (e.g., JSON and CSV) to define multi-stage and interdependent scenarios, such as cascading faults, evolving cyber-attacks, and system restoration processes.
    - Enhance the flexibility of the configuration schema to capture more nuanced interactions between cyber and physical components.

- **Enhanced Interpolation and Time Synchronization**
    - The current interpolation module effectively bridges the time-driven power system simulator and the event-driven cyber simulator. However:
        - Advanced interpolation techniques, such as machine learning-based prediction models, can be explored to improve accuracy and computational efficiency.
        - Optimization of HELICS synchronization mechanisms for large-scale simulations will ensure scalability without compromising performance.
- **User-Friendly Interfaces and Automation**
    - Developing graphical user interfaces (GUIs) for easier configuration of scenarios, network topologies, and power system models.

- Automating repetitive tasks, such as scenario generation and result analysis, to streamline the simulation process.

Bibliography

[1] Abdelmalak, M., & Macwan, R. (2022). A Survey of Cyber-Physical Power System Modeling Methods for Future Energy Systems; A Survey of Cyber-Physical Power System Modeling Methods for Future Energy Systems. *IEEE Access*, *10*. https://doi.org/10.1109/ACCESS.2022.3206830

[2] Fan, H., Wang, H., Xia, S., Li, X., Xu, P., & Gao, Y. (2021). Review of Modeling and Simulation Methods for Cyber Physical Power System. *Frontiers in Energy Research*, *9*. https://doi.org/10.3389/FENRG.2021.642997/FULL

[3] Liu, Z., Wang, Q., & Tang, Y. (2020). Design of a Cosimulation Platform with Hardware-in-the-Loop for Cyber-Attacks on Cyber-Physical Power Systems. *IEEE Access*, *8*, 95997–96005. https://doi.org/10.1109/ACCESS.2020.2995743

[4] Gao, X., Ali, M., Rahman, A., Rahman, M. M., & Sun, W. (2024). An Open Source Co-Simulation Test Platform for Cyber-Physical Power System Security Analysis. *North American Power Symposium*. https://doi.org/10.1109/NAPS61145.2024.10741832

[5] Cui, H., Li, F., & Tomsovic, K. (2020). Cyber-physical system testbed for power system monitoring and wide-area control verification. *IET Energy Systems Integration*, *2*(1), 32–39. https://doi.org/10.1049/IET-ESI.2019.0084