Power Grid OT Simulation System

Mini OT-Energy-System Cyber Security Digital Twin

Service Introduction

Version: V_0.1.5

By NCL Development Team

07 Feb 2025

National Cybersecurity R&D Laboratory

Power Grid Simulation System [Mini OT-Energy-System Cyber Security Digital Twin]

Power Substation

High Tension Power Transmission towers

Railway

Industry

City House

Solar Photovoltaic Farm

Wind Turbine Farm

Natural Gas Power Plant

Power Grid Simulation System Physical World Simulator

Power Generation

Power Transmission

Power Customers

Power Distribution

Human-Machine Interface

Power Grid HQ Center

Gas Motor

Generator

Transformer

Power Storage

MU

PLC

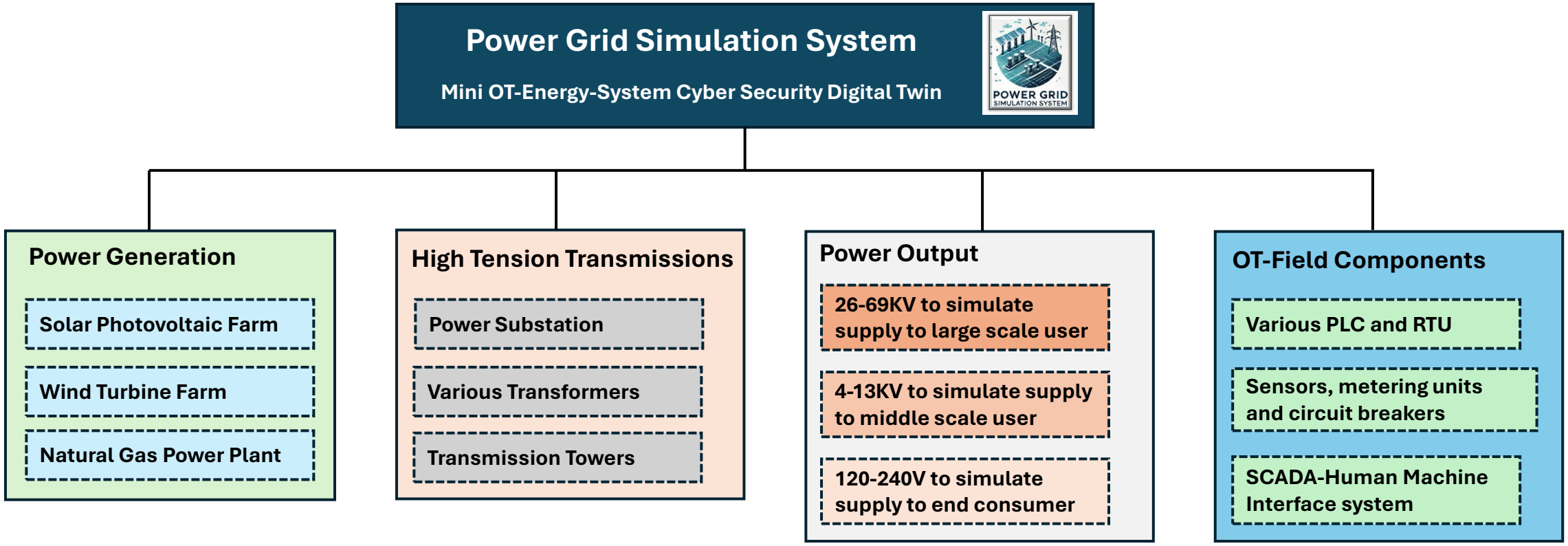
RTU

POWER GRID SIMULATION SYSTEM

National Cybersecurity R&D Laboratory

Introduction

The objective of this project is to simulate a Power Grid OT digital system that can be used for cyber-security related activities. The system is a comprehensive software platform designed to simulate the essential operations of a typical small-scale hybrid power grid. The simulated Power Grid have the following:



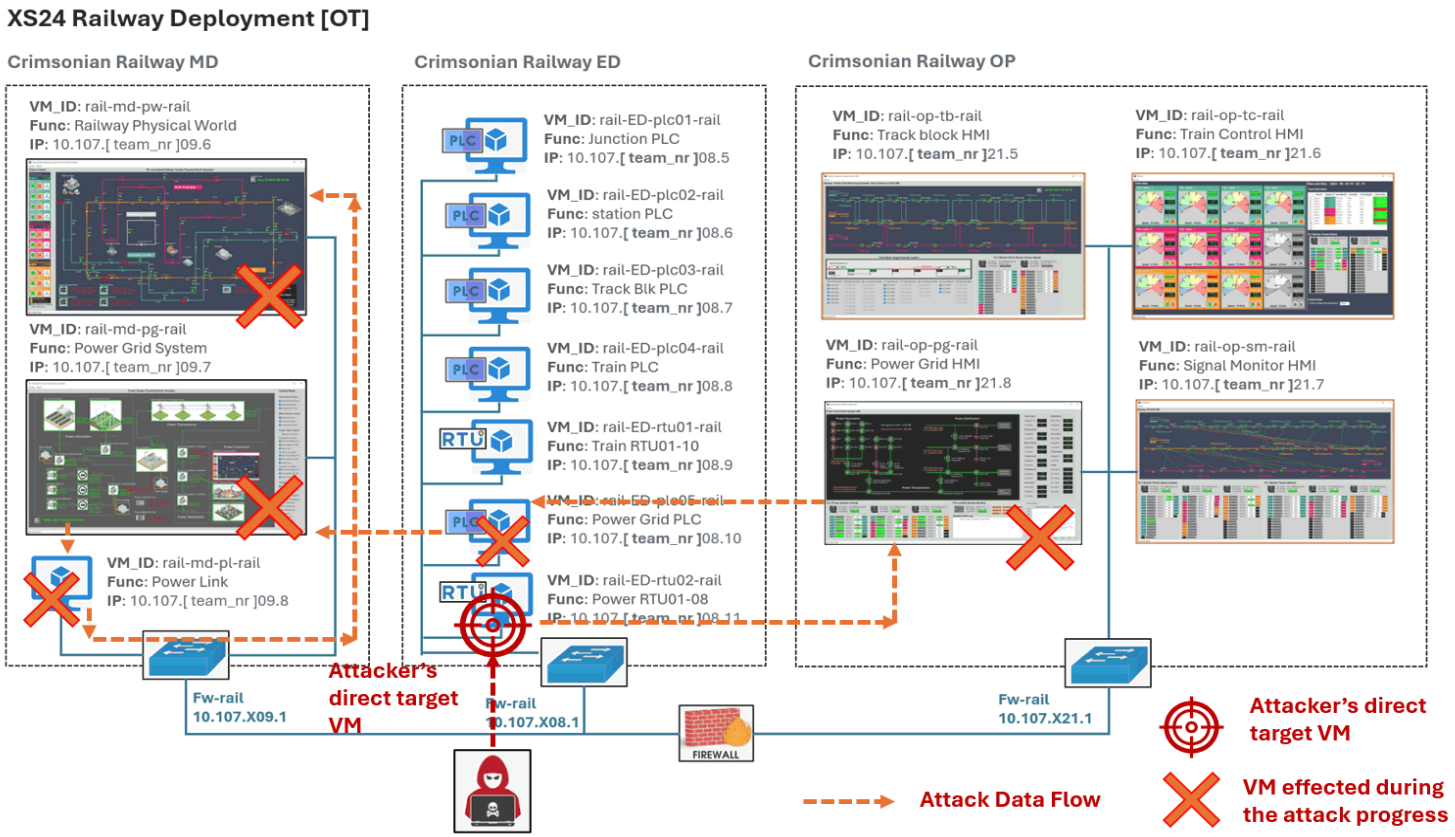
Power_Grid_Simulation_System [Project Use Case]

National Cybersecurity R&D Laboratory

Crossed Swords 2024 (Dec 2024):

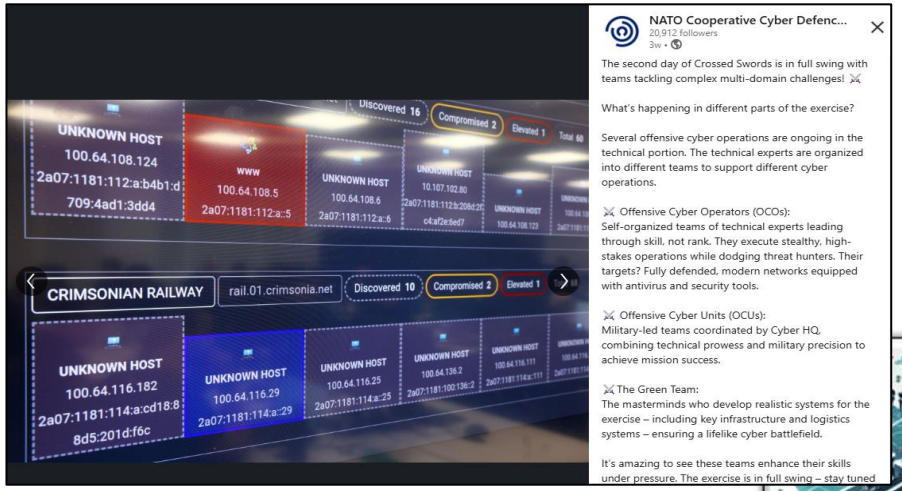
The Power Grid Simulation System with its substation power customer Railway System is used as one attack target critical infrastructure system in the Crossed Swords (XS) 2024 exercise in Estonia Tallinn, conducted by the NATO Cooperative Cyber Defense Centre of Excellence (CCDCOE)

- https://ccdcoe.org/exercises/crossed-swords/



CCDCOE NATO COOPERATIVE CYBER DEFENCE CENTRE OF EXCELLENCE

CROSSED SWORDS 2024

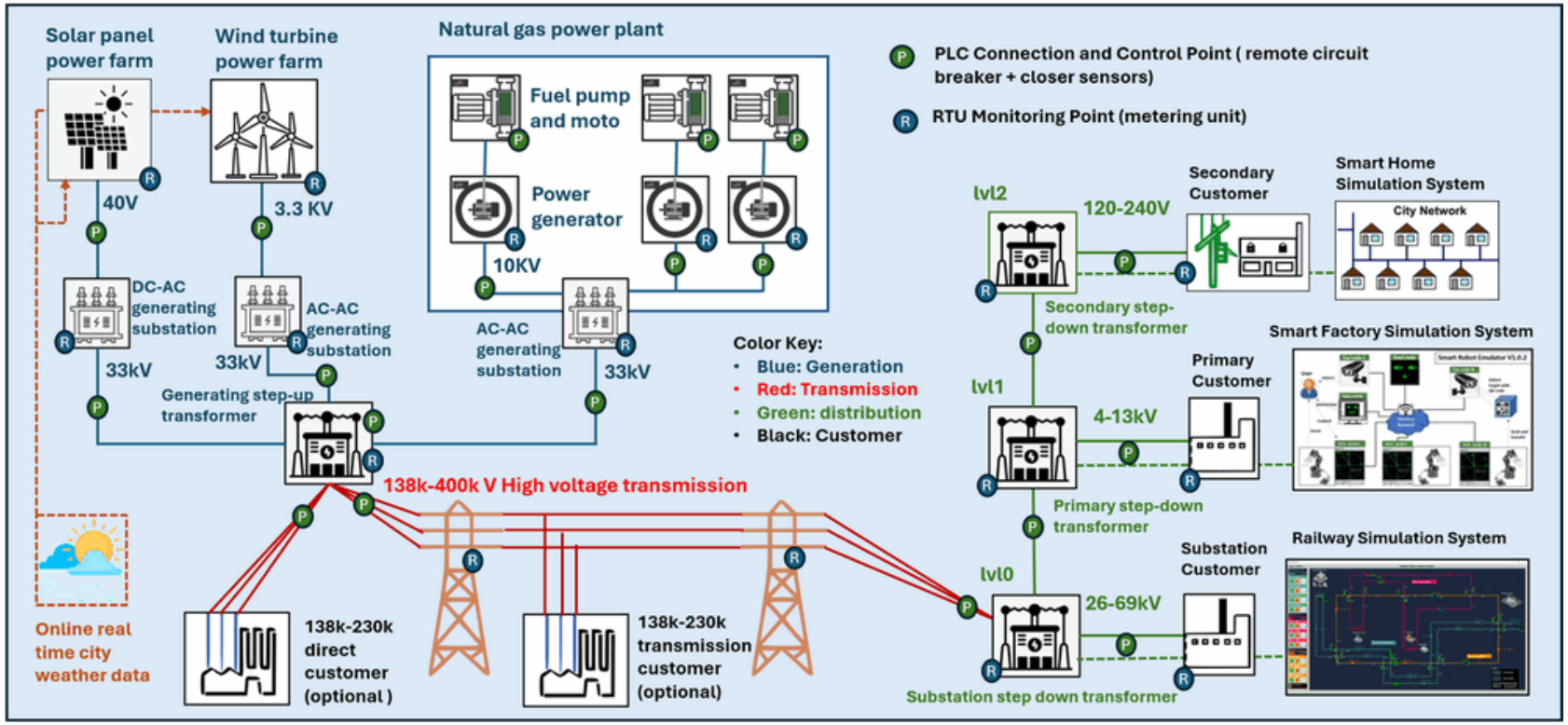


POWER GRID SIMULATION SYSTEM

National Cybersecurity R&D Laboratory

System Overview

The **Mini OT Power Grid Simulation System** is a digital equivalent software platform designed to simulate the core operations of a hybrid power grid system, including hybrid power generation (natural gas power plants, solar power plants, and wind turbine farms), high-voltage power transmission and a three-level step-down power distribution system. The simulation integrates a SCADA system that incorporates PLCs for remote system control, RTUs and MUs for real-time data monitoring, and an HMI interface for operators to manage the grid.



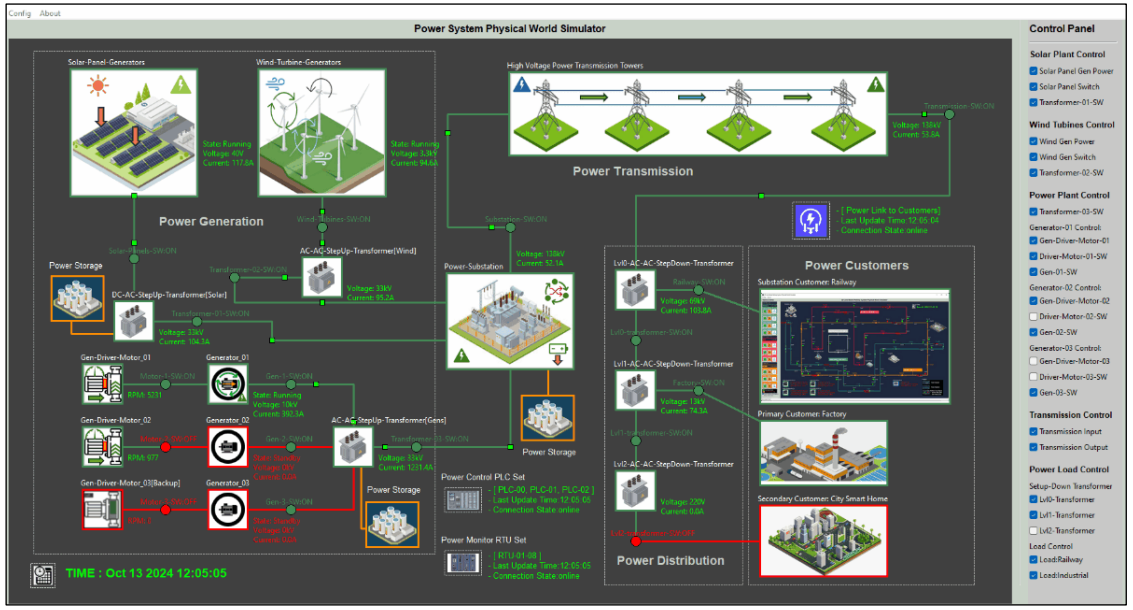
POWER GRID SIMULATION SYSTEM

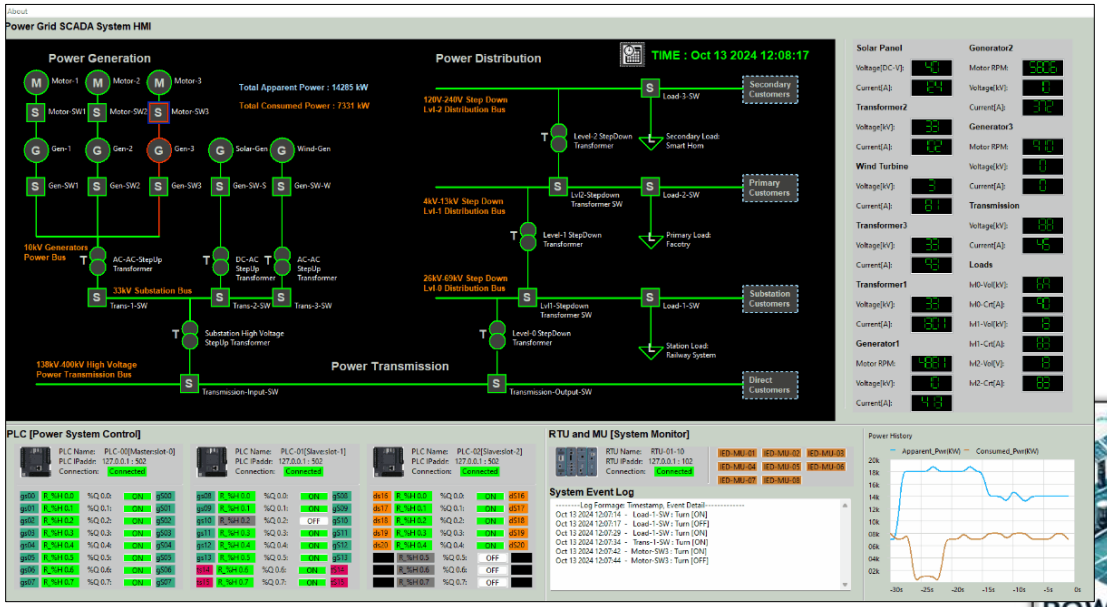
National Cybersecurity R&D Laboratory

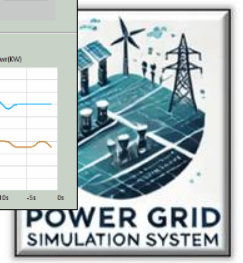
System Architecture

The system architecture consists of three primary modules:

- **2D Physical World Visualization Program:** Simulates the physical-world devices and components of the power grid, providing a clear visual representation of grid operations.
- **OT Field Controller Simulation:** Includes simulation programs for PLCs, sensors, Metering Units (MUs), and Remote Terminal Units (RTUs) that enable interaction between the grid's physical elements and the control systems.
- **SCADA and HMI System:** Provides supervisory control and real-time monitoring of the simulated power grid, allowing for detailed oversight of grid performance and operations.



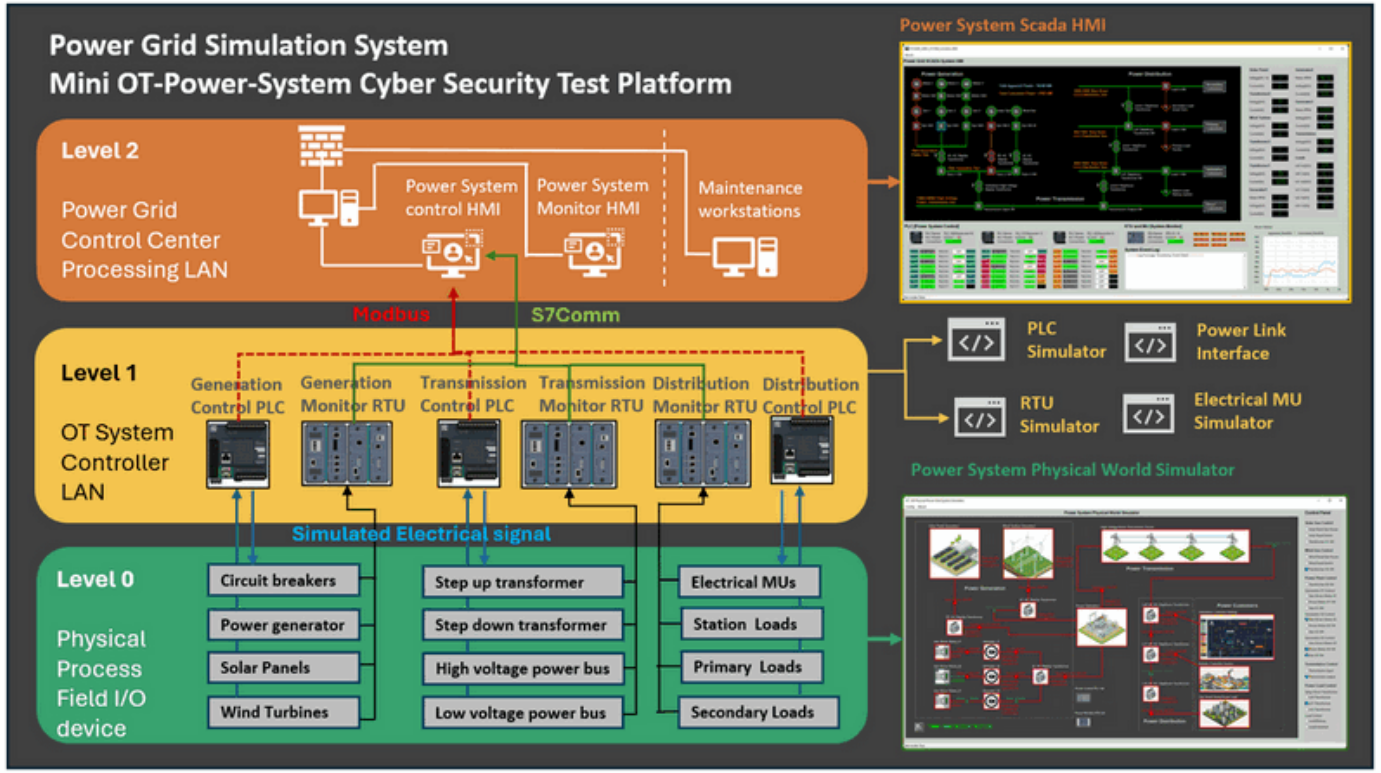




National Cybersecurity R&D Laboratory

System Design

The simulation provides a modular, comprehensive approach to replicating the functionality of a real-world small sized 18KW (560+MkWh/year) hybrid power grid with power generation, transmission, and distribution processes. It will integrate physical-world simulation with various control and monitoring units, including electrical metering units (MUs), programmable logic controllers (PLCs), remote terminal units (RTUs), and a SCADA-HMI interface. By offering full-spectrum emulation from Level 0 (physical field devices and sensors) to Level 2 (control center operations) to full fill the requirements for cybersecurity training, exercises, and research in OT-Energy-System-Security field.



Provide three Levels OT Environment Simulation:

Level 0 : 2D Power Grid Physical-world Simulation.

Level 1:Power System Controller Simulation (MU, PLC & RTU).

Level 2 : Power Grid Supervisory Control and Data Acquisition (SCADA) System.

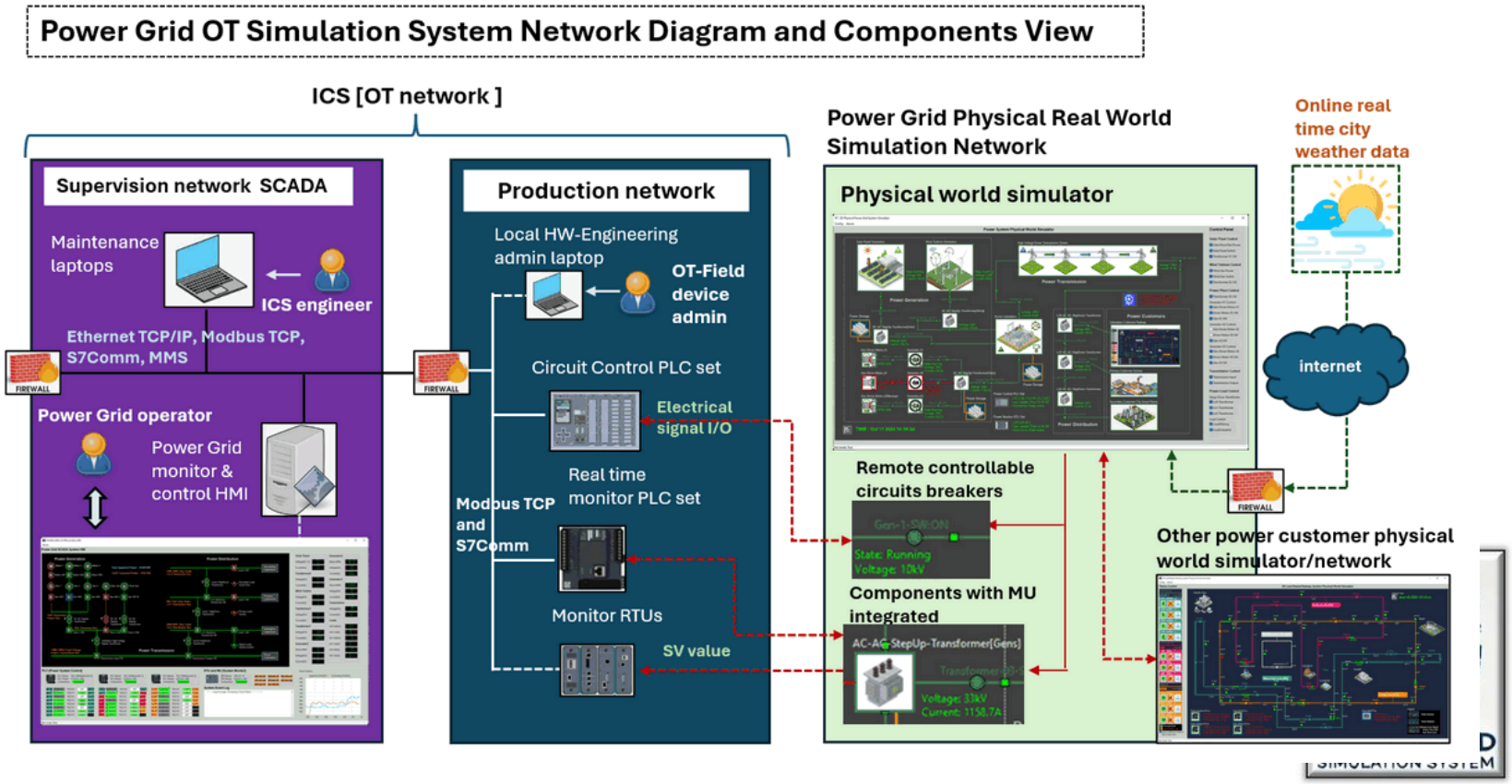
POWER GRID SIMULATION SYSTEM

National Cybersecurity R&D Laboratory

Technical Specification

The Power Grid Simulation System is a POC project and provides a fully digital simulation of an OT environment without the needs for additional physical OT devices. The main program's development follows the International Electrotechnical Commission IEC 61850, IEC 60617 standard. The system supports both all-in-one deployment mode and multi-VM cluster deployment mode, making it suitable for diverse use cases such as professional training and cybersecurity exercises. Below are some technical details:

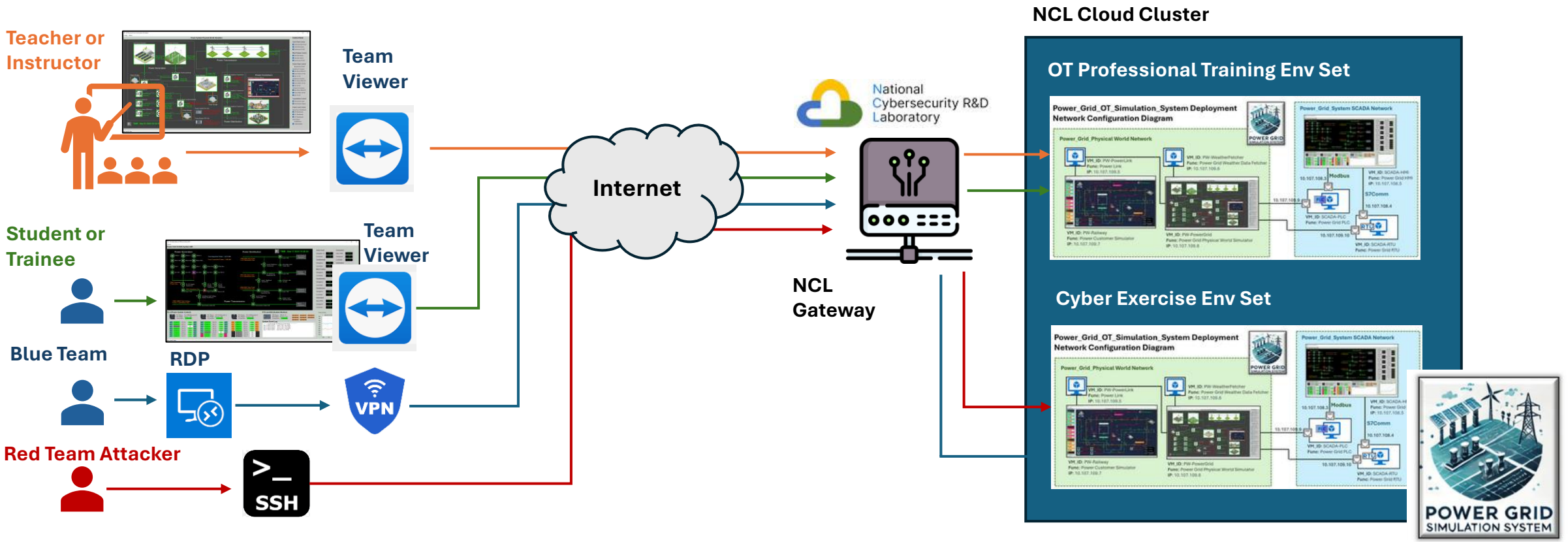
- One 2D UI physical world simulation program.
- Two types of OT protocol in SCADA network: Modbus-TCP and Siemens-S7Comm
- Three PLC simulation module.
- One or multiple RTU + eight Metering Units(MU) simulation module.
- Flexible deployment mode (1 ~ 11 Vms)
- Real time weather impacts for renewable power generation.
- Integrable API for link to other OT system.
- Compatible for different IT system.



National Cybersecurity R&D Laboratory

Service Usage

Currently we provide the hosting service within the NUS-NCL infrastructure, enabling users to access it remotely. Multiple instances of the system can be deployed based on specific user requirements for cybersecurity exercises or training sessions. To facilitate remote access, we offer multiple connectivity options to suit user preferences: TeamViewer or VPN + RDP for accessing VMs with a user interface, SSH Connection for lightweight and terminal-based access to standard VMs. The remote access diagram is shown below :



Power_Grid_Simulation_System [Summary]

National Cybersecurity R&D Laboratory

The Mini OT-Energy-System Cyber Security Test Platform is a comprehensive software platform designed to simulate the essential operations of a small-scale hybrid power grid. The key objectives of this project will cover:

- **Cybersecurity Training & Exercises**: The platform will enable hands-on cybersecurity exercises, allowing professionals to explore and mitigate the effects of various cyber-attacks on OT systems.

- **OT System Simulation**: Simulating power grid operations with components that follow the [International Electrotechnical Commission](https://iec.ch/) standards, particularly IEC 61850 (communication networks and systems for power utility automation) and IEC 60617 (graphical symbols for diagrams), ensuring adherence to industry protocols.

- **Research & Development (R&D):** Providing a research platform to explore and develop novel cybersecurity strategies, protocols, and solutions specifically for OT systems in the energy sector.

- **Training for ICS Professionals**: Offering a realistic environment for industrial control system (ICS) professionals to enhance their understanding of OT operations and cyber-attack scenarios in a controlled, risk-free setting.

- **R&D and Testing**: Facilitating the testing of new OT security tools and protocols, as well as demonstrating the impact of cyber-attacks on critical infrastructures, such as power generation and distribution networks.