OPAL-RT TECHNOLOGIES

TESTING CYBER-PHYSICAL RESILENCY ON A MICROGRID

University of Vaasa

Application

- Substation Automation
- Cybersecurity

Related Products

- HYPERSIM
- EXata CPS

Type of Simulation

- Hardware-in-the-Loop (HIL)
- Software-in-the-Loop (SIL)

SUCCESS STORY

INTRODUCTION

Safeguarding the Future of Smart Grid Systems

Microgrids, as small-scale power networks, can operate independently or collaboratively with the main grid. However, their online connectivity—as illustrated in this case study—exposes significant security vulnerabilities. Microgrids rely centrally on communication and control systems to manage Distributed Energy Resources (DERs) like solar panels, wind turbines, batteries, etc. Unfortunately, these very systems are also susceptible to cyberattacks, jeopardizing microgrid functionality and performance. A recent report from the International Energy Agency found the average number of cyberattacks against utilities each week **more than doubled between 2020 and 2022 worldwide—with 1,101 weekly attacks registered last year.**

Cyberthreats, such as false data injection, denial-of-service, and malicious control commands—sometimes even including state-sponsored data terrorism—pose severe risks; the consequences including power outages, equipment damage, and frequency and voltage instability. Given the integral role of these mini networks in daily operations, enhanced security measures—such as **dedicated and vigilant specialized software**—emerge as imperative necessities. Simulation of cyberattacks on microgrids consequently becomes paramount to understanding the potential impacts of such attacks, and developing or testing detection and mitigation strategies. Most importantly, **simulation offers a safe and cost-effective means to assess diverse scenarios and attack vectors, without affecting the actual power system**. Various simulation tools and testbeds—employing techniques like Hardware-in-the-Loop (HIL), digital real-time simulators, and cyber-physical emulators—have been devised for this purpose: These tools can model the physical and cyber layers of microgrids, enabling the simulation of various cyberattacks and their effects on microgrid operations.

In this case, we delve into the design of a microgrid controller subject to cyberattacks using the HIL development process and platforms. This case study illuminates the intricate processes involved in fortifying microgrid controllers against potential cyberthreats, contributing to the overall resilience of Smart Grid systems.

Meet the Team

VEBIC (Vaasa Energy Business Innovation Center) is a multidisciplinary research platform at the University of Vaasa. Serving as a base of knowledge exchange, it brings together expertise from both research and business communities, addressing the global need of efficient energy production, energy business, and sustainable societal development.

FREESI is one of the laboratories operated by VEBIC, utilized for various research activities related to Smart Grids and flexible energy resources. Their primary focus revolves around grid integration of inverter-based DERs and protection of power systems, also utilizing the facilities at the Internal Combustion Engine (ICE) laboratory of VEBIC.

The Smart Grid Laboratory (housed at FREESI) is a collection of related facilities at the Technobothnia joint laboratory, hosted by three collaborating higher education institutes. The name FREESI comes from the words **Future, Reliable, Electricity and Energy Systems Integration**, which communicates the laboratory's commitment to exploring innovative avenues in the mentioned research domains.

THE PROBLEM

Microgrid Controllers Subject to Attack

The research group engaged in the HIL development initiative drew on two decades of shared power system simulation expertise and the core facilities of the laboratory had recently been upgraded to enable real-time HIL simulations.

Essential for diverse studies, the HIL facilities focus on relay protection systems, featuring a distinctive setup of Protection, Automation, and Communication (PAC) equipment for IEC 61850-based system testing. The laboratory also houses power electronic facilities for in-depth studies on inverter-based DER control. Moreover, the high voltage laboratory conducts critical tests such as dielectric insulation breakdown, partial discharge investigations, and impulse testing.

The groundbreaking security lab in Vaasa, Finland, establishes itself as the first of its kind in Northern Europe, pioneering the use of **HYPERSIM** power system simulation platform, from OPAL-RT, and **EXata CPS** network simulation platform, from Keysight. EXata CPS, with its library of simulated cyber-attacks on vulnerabilities and cyber-defenses, is used to analyze and test the resilience of critical communication networks effectively. Tools like EXata CPS allow customers to visualize their specific environments in a manageable laboratory setting and quickly evaluate a range of 'what if' scenarios to determine the impact on their systems if subjected to cyberattack.

Partners Driving This Research

Vipuvoimaa EU:lta 2014–2020
Euroopan unioni
Euroopan aluekehitysrahasto

University of Vaasa

Österbottens förbund
Pohjanmaan liitto

ABB

Arcteq

VAASAN SÄHKÖ

VASEK

Wapice

WÄRTSILÄ

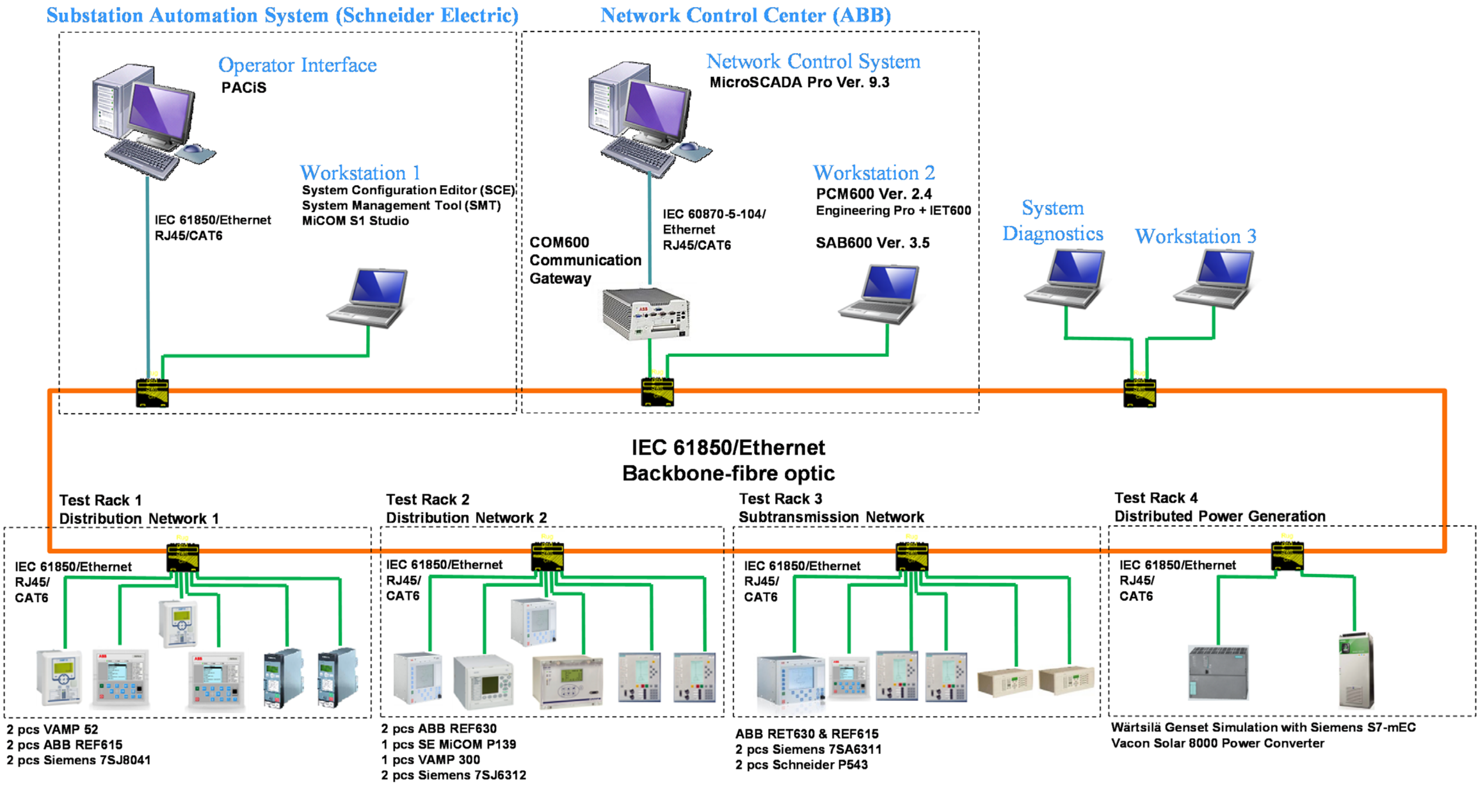
CONFIGURATION

In their advanced laboratory setting, they have established a distinctive multi-vendor environment dedicated to educational, testing, and training purposes for IEC 61850 based protection systems. The IEC 61850 standard plays a pivotal role, facilitating the seamless integration of devices from various vendors and their custom-designed lightweight Intelligent Electronic Devices (IEDs).

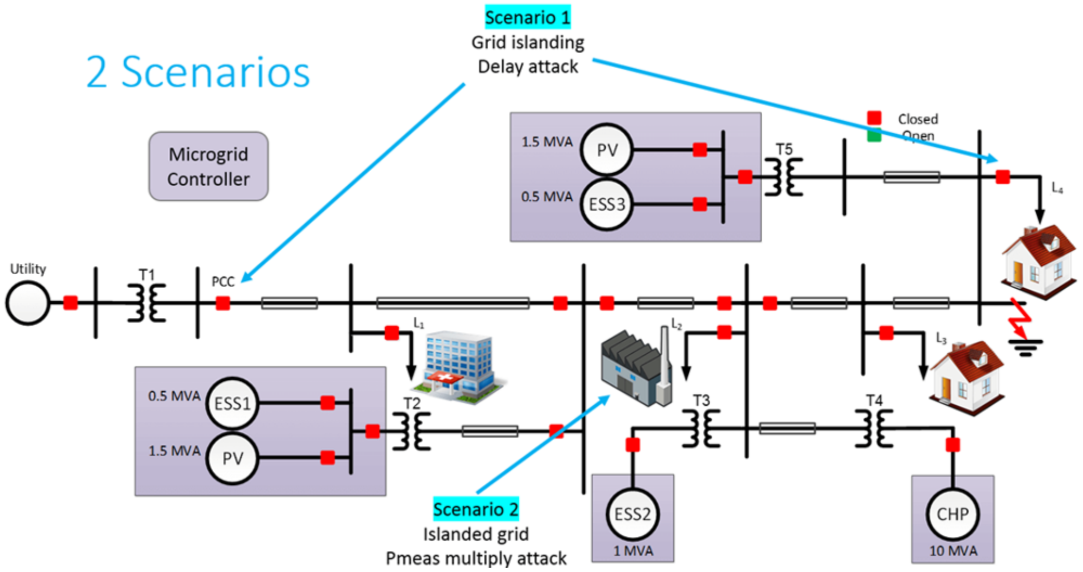
Their primary focus lies in the **development and validation of multi-agent hardware controllers**. This is meticulously assessed through Software-in-the-Loop (SIL) and Hardware-in-the-Loop (HIL) Real-time testing, utilizing the OPAL-RT simulator. Ongoing research is directed towards AI-enabled algorithms specifically tailored for the microgrid controller.

The laboratory actively engages in diverse testing scenarios, encompassing energy grid dynamics, cyber attacks, defender strategies, and intelligent agent interactions. This holistic approach allows them to evaluate the impacts on the efficient operation of power networks by monitoring both communication and physical energy grid characteristics.

Among their esteemed vendors are industry leaders such as ABB, Siemens, Schneider, VAMP, Vacon, and Wärtsilä. Leveraging this wealth of hardware, the laboratory serves as **a central hub for groundbreaking research** and remains **an invaluable resource for teaching and training sessions**, disseminating knowledge in the realm of Cyber-Physical Simulation (CPS) of Energy systems.



2 Scenarios



Scenario 1
Grid islanding
Delay attack

Scenario 2
Islanded grid
Pmeas multiply attack

SIMULATION OF CYBERATTACKS

SCENARIO #1: THE ONE SECOND DELAY

1

With Scenario #1, we experience microgrid islanding subject to "delay"-type cyber-attack:

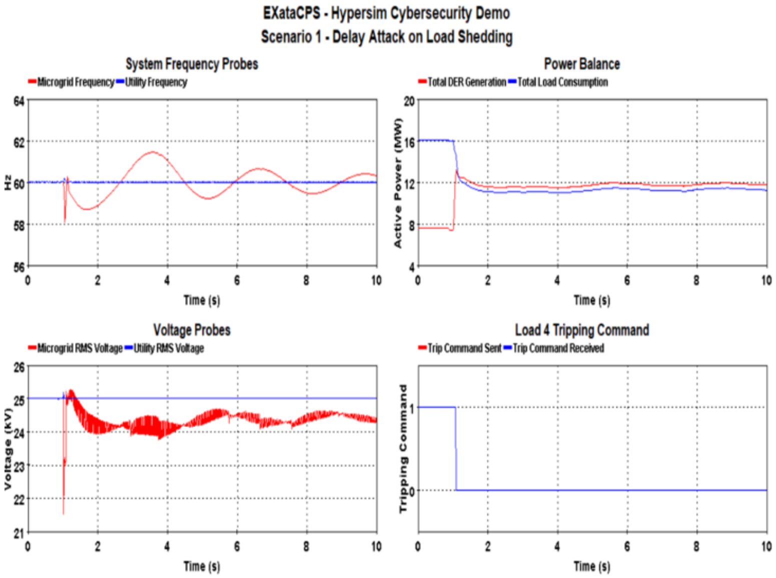
- Microgrid islanded at t = 1 second.
- Microgrid Central Controller (MGCC) sends a shedding command to Load 4.
- Figure shows matching power balance between supply and demand in islanded mode. Note a voltage dip occurs during islanding for a very short time until the load shedding occurs.

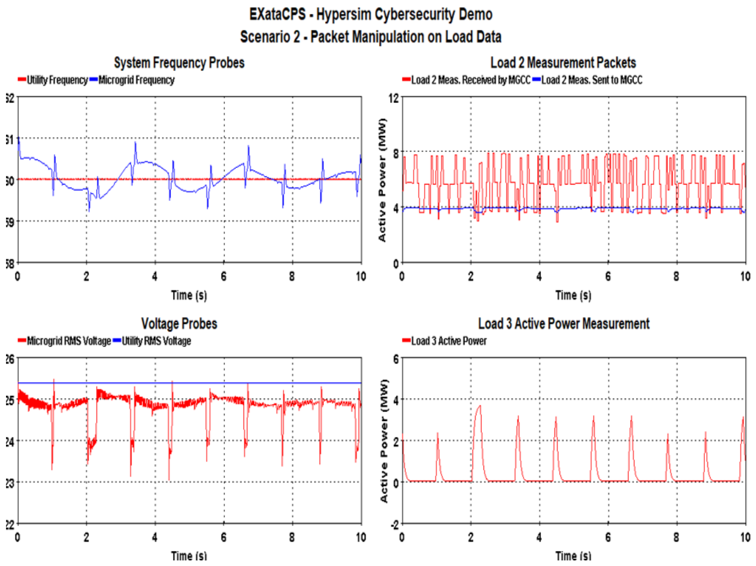
SCENARIO #2: THE SO-CALLED 'MAN IN THE MIDDLE' ATTACK

2

With Scenario #2, we experience islanded microgrid subject to "packet modification"-type cyber-attack:

- Load 2 measurements are manipulated before they are received by the MGCC.
- MGCC periodically trips and reconnects Load 3 since it is programmed to shed the priority Load 3 if the mismatch between generation and load exceeds 3 MW.
- Figure shows the microgrid suffers from a decline in power quality, including high frequency and voltage oscillations.





We work across borders in the project
CPS Security Lab

IMPROVING CYBERSECURITY OF CRITICAL INFRASTRUCTURES

Want to know more?
www.interregaurora.eu

Interreg Aurora
Co-funded by the European Union

Cyber-Physical Systems Lab - Development of a Roadmap & Project Plan (12/31/23 - 10/30/24)

Discover a collaborative project between the University of Vaasa and Lule University of Technology, focusing on enhancing cyber physical system (CPS) security in the energy sector. This small-scale project, operating under the Aurora program, aims to address common territorial challenges by creating a robust CPS security Laboratory Network. Through cross-border cooperation, the project leverages the expertise of both universities to develop innovative solutions and provide a real-time simulation-based environment for testing and designing cybersecurity measures.

CONCLUSION

Mitigating Risks: Thorough Testing of Microgrid Controllers in Action

Microgrid controllers play a crucial role in orchestrating the generation, storage, and consumption of electricity from diverse distributed energy resources, including solar panels, wind turbines, batteries, and diesel generators. These controllers interface with the main grid and other microgrids through communication protocols such as IEC 61850, a standard for data exchange and control of electrical substation equipment.

However, microgrid controllers introduce significant challenges and risks to the security and reliability of both the network and microgrid. **Malfunctions or failures in these controllers can lead to severe disruptions in power supply, equipment damage, and even pose risks to human lives.** Thus, it is imperative to subject microgrid controllers to thorough testing before deployment to ensure they can effectively manage the network and microgrid.

Testing should encompass not only the functionality and performance of the microgrid controller itself but also its compatibility and interoperability with other devices and systems employing IEC 61850 or other communication protocols. Various scenarios and conditions, including grid-connected and islanded modes, load changes, faults, and potential cyberattacks, must be considered in testing.

Comprehensive testing of microgrid controllers, incorporating communication protocols like IEC 61850, ensures their safe, efficient, and resilient operation in diverse situations and environments. This rigorous testing approach not only safeguards the security of the network and microgrid but also optimizes the benefits of microgrids in terms of reducing carbon emissions, lowering energy costs, and enhancing power quality and availability.

Mike Mekkanen, *Associate Professor & Senior Researcher at University of Vaasa - School of Technology and Innovations, Information Systems Science*

mike.mekkanen@uwasa.fi
+358294498285

tero.vartiainen@uwasa.fi
+358294498588