SAND2022-2597C

Sandia National Laboratories

Towards Cyber-Physical Special Protection Schemes: Design and Development of a Co-Simulation Testbed Leveraging SCEPTRE™

Adam Summers[1], Christopher Goes[1], Daniel Calzada[1], Nicholas Jacobs[1], Shamina Hossain-McKenzie[1] and Zeyu Mao[2]

Sandia National Laboratories[1] Texas A&M University[2]

Power and Energy Conference at Illinois (PECI) 2022

U.S. DEPARTMENT OF ENERGY NNSA

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

Special Protection /Remedial Action Schemes

What do they do?

Special Protection(SPS) /Remedial Action Schemes(RAS)

- Respond to disturbances
  - Weather disturbances
    - Hurricanes Sandy, Texas Winter Storm of 2021
  - Malicious disturbances
    - Cyber attacks
    - EMPs
- Typically deployed at the transmission level
  - Starting to be deployed at the distribution level
- Challenges with traditional SPSs and RASs
  - Becoming more complex with inverter-based resources
    - Time consuming to design and test
  - Communications to devices presents a high value, low effort target to adversaries

The Need For a Cyber-Physical Testbed

Physical SPS

Typically designed to operate under physical system triggering conditions

- Load Shedding
  - Load > Generation
  - Demand due to changes in weather
- Generation Tripping
  - Adjusting MW and Mvar output
- Line Tripping
  - Excessive Line Loading
  - Topology Changes

Cyber SPS

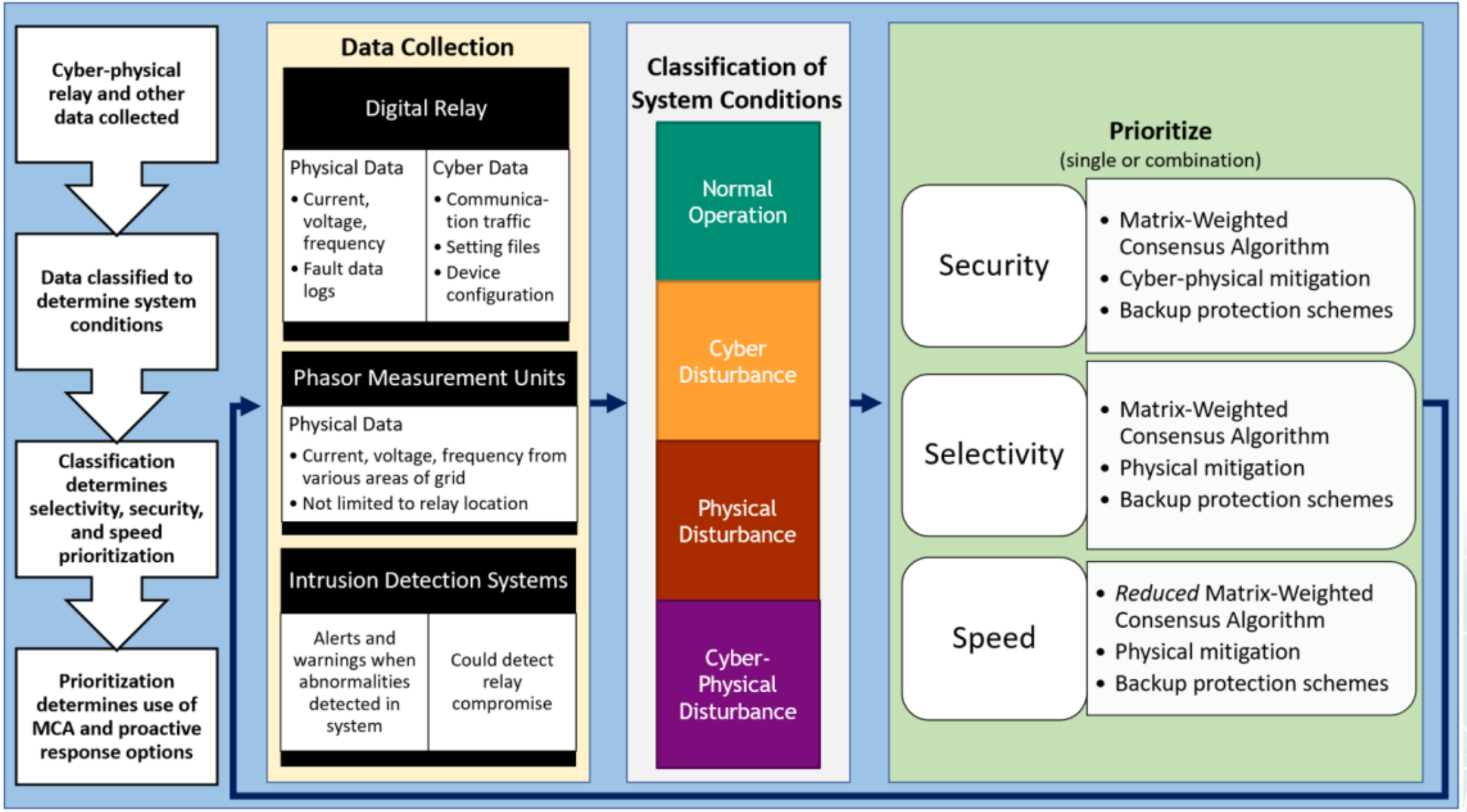
At present, cyber SPSs do not exist

- Depend on intrusion detection or prevention systems

Cyber-Physical SPS

- SPS that can adapt to unpredictable, cyber-physical events
- Cyber-physical in analyzing collected data and taking response actions
- Extends the use of protective relays to adaptively learn system conditions

HARMONIE-SPS: Cyber-Physical, Adaptive SPS



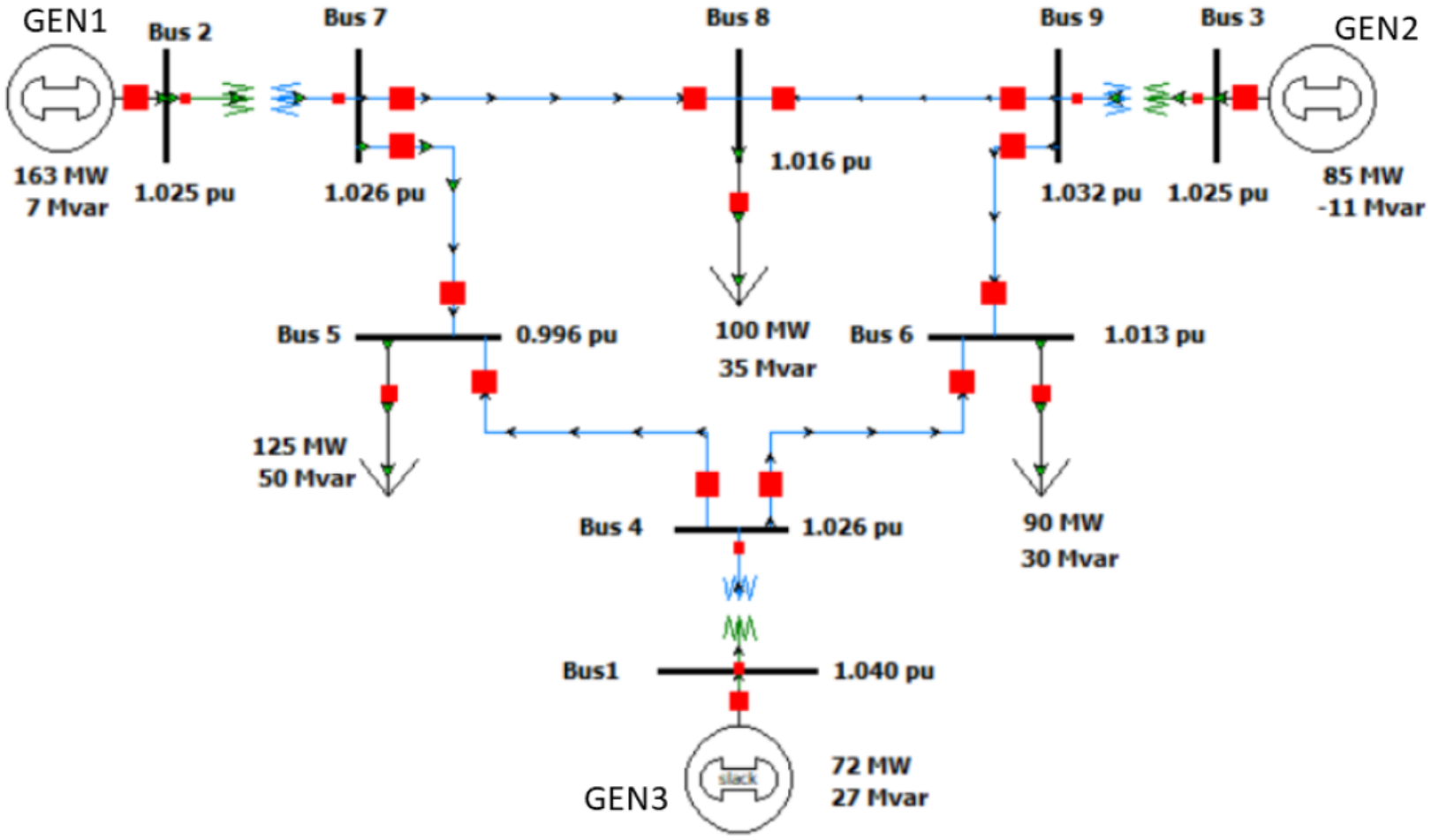
Need For A Real-Time Cyber-Physical Testbed

To test cyber-physical SPSs such as HARMONIE-SPS and evaluate disturbance impacts in a dynamic grid, we need a real-time cyber-physical testbed to:

- Assess physical changes to system conditions that have not been seen before
  - Fire or Weather conditions
- Not solely rely on intrusion detection methods for grid cybersecurity; incorporate into RAS/SPS implementations
- Allow the creation and testing of cyber-physical SPS that can be rapidly tested to protect the grid

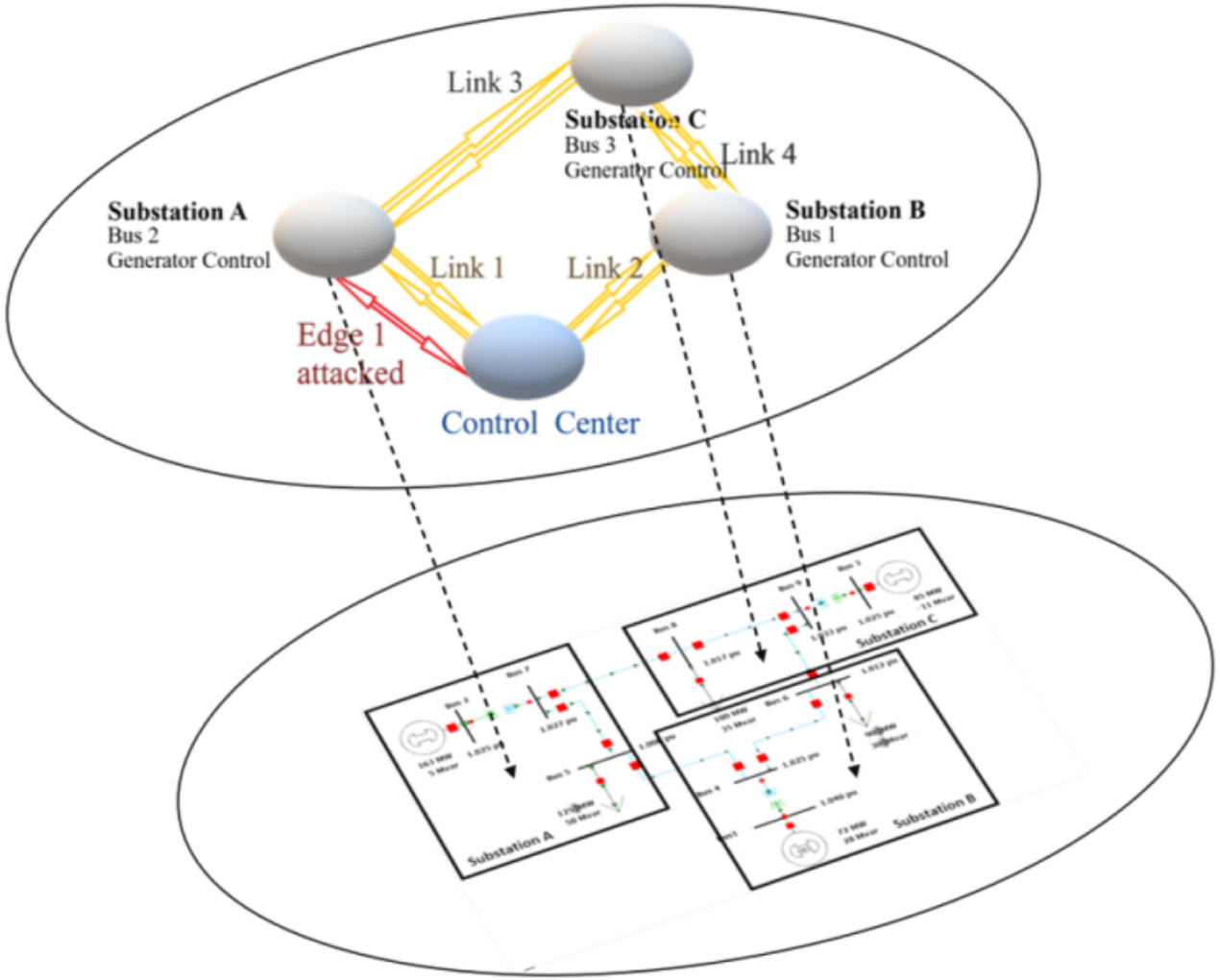
The HARMONIE-SPS CYBER-PHYSICAL TESTBED DESIGN and DEVELOPEMENT

The system of study: WSCC 9 Bus that is deployed to the RTDS



The HARMONIE-SPS CYBER-PHYSICAL TESTBED DESIGN and DEVELOPEMENT

WSCC 9 bus and communication network



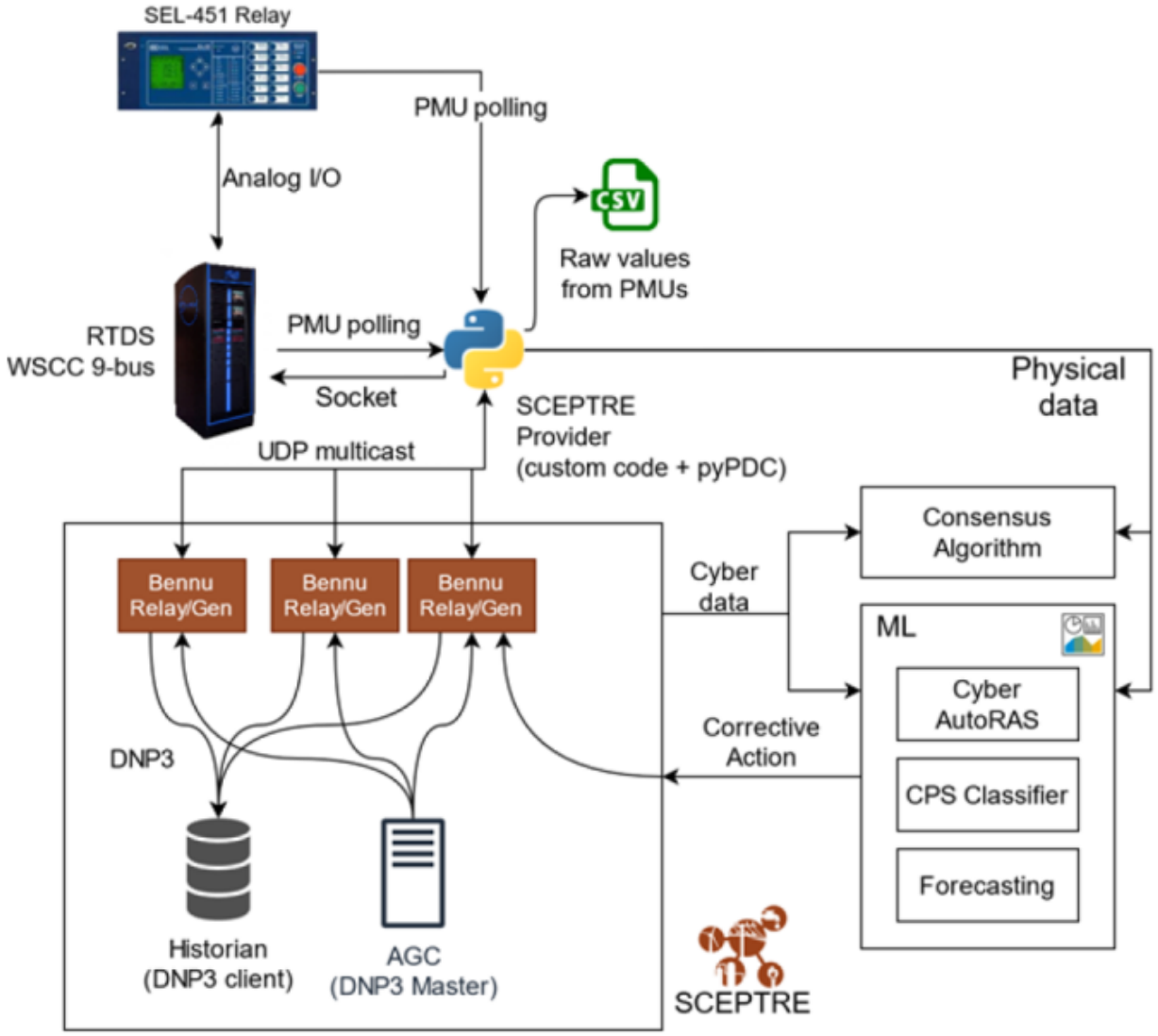
The HARMONIE-SPS CYBER-PHYSICAL TESTBED DESIGN and DEVELOPEMENT

What is SCEPTRE™ and What Can IT DO?

- An application that uses underlying network Emulytics™ technologies to run
- ICS devices(simulated, emulated, real) communication and interact via high-fidelity protocols
- All ICS devices are able to interact with the simulation
- Bridge multiple infrastructures into the same experiment
- Provides a cyber-physical interface to show how cyber-initiated events affect the physical system and vice versa

The HARMONIE-SPS CYBER-PHYSICAL TESTBED DESIGN and DEVELOPEMENT

Testbed configuration



The HARMONIE-SPS CYBER-PHYSICAL TESTBED CASE STUDIES

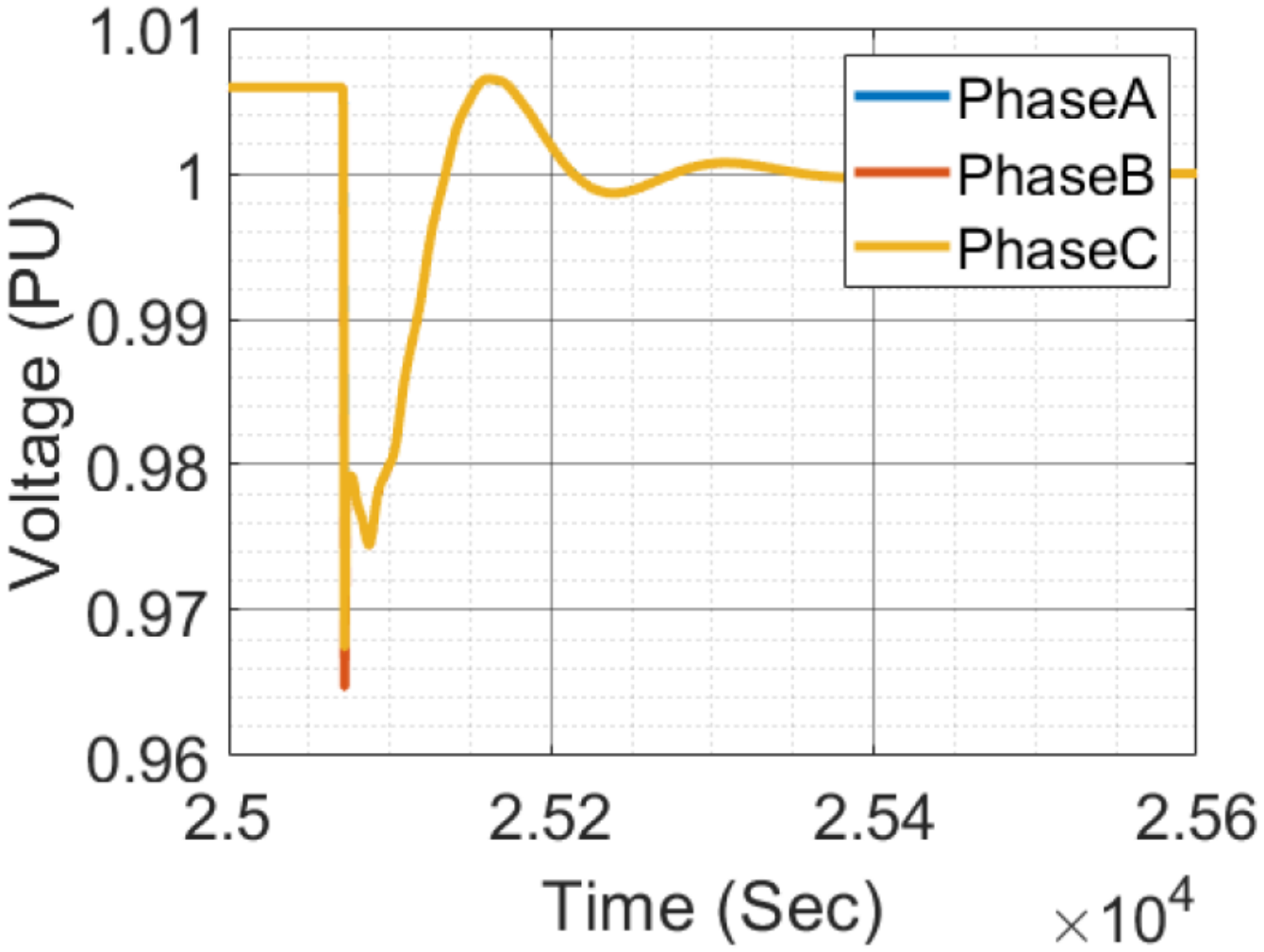
For all the case studies we focused on Bus 8 in the WSCC 9 Bus system

- The load is remotely controlled from the HARMONIE-SPS.

Case 1: Test the closed loop connection between RTDS and SCEPTRE by issuing a breaker trip command simulating a load drop

Result:

- RTDS C37.118 data for Bus 6 voltage data is collected and processed
- The resulting load drop can be observed in either the RTDS or SCEPTRE environment



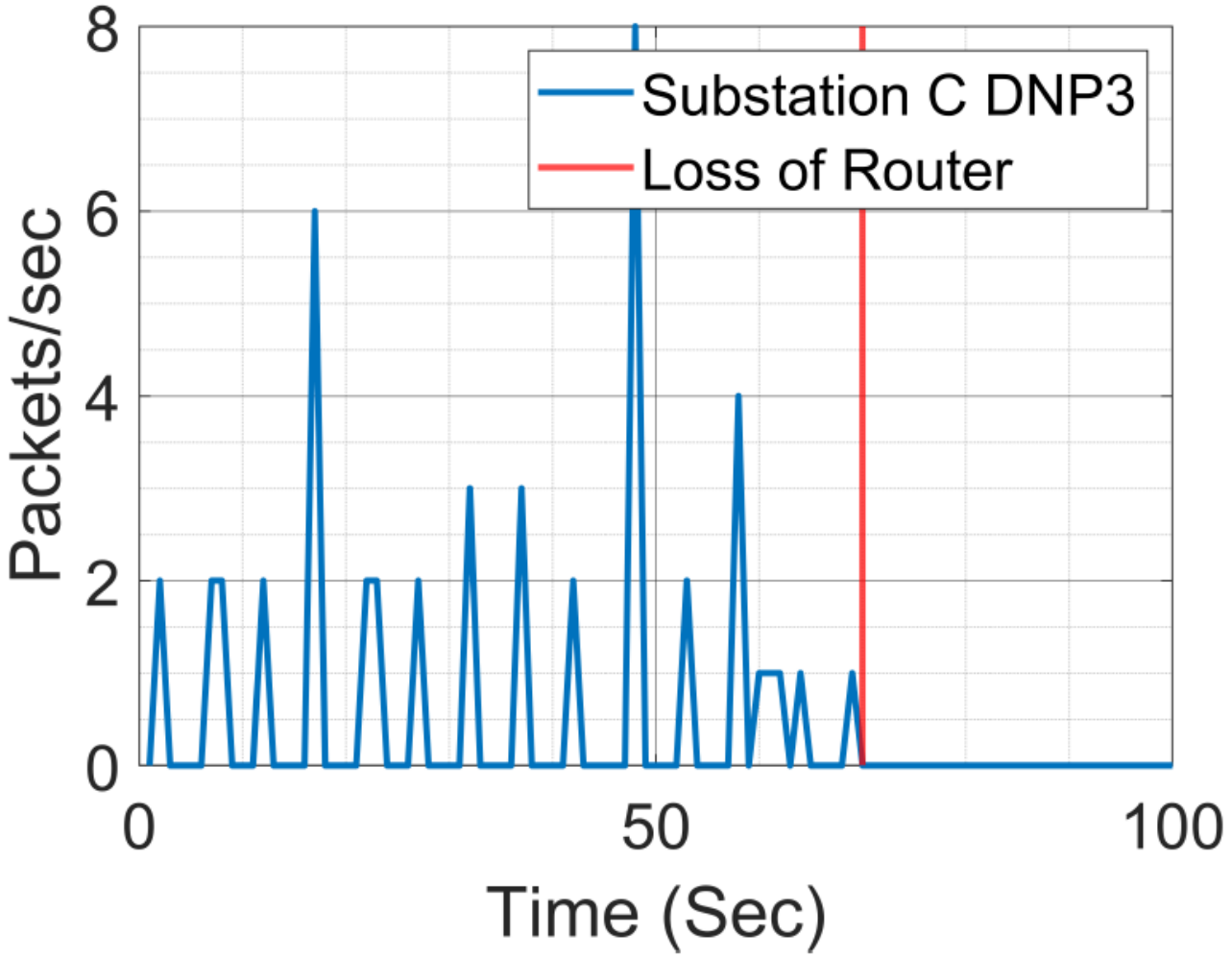
The HARMONIE-SPS CYBER-PHYSICAL TESTBED CASE STUDIES

Cyber Event: Loss of C37.118 data at Substation C

Using the SCEPTRE platform to drop several of the PMU connections at a virtual router

This could represent equipment failure or a malicious event

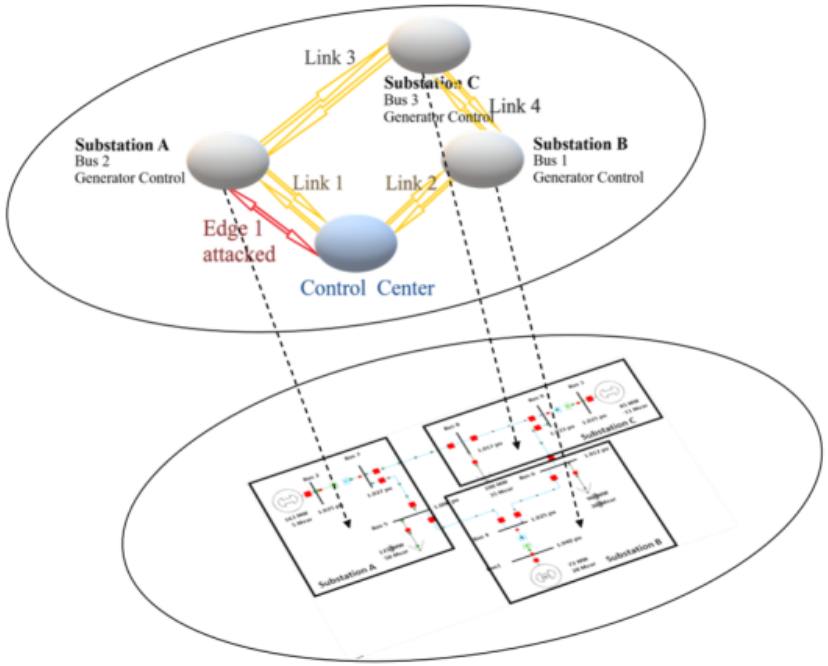
The loss of system visibility could prevent a SPS from operating correctly

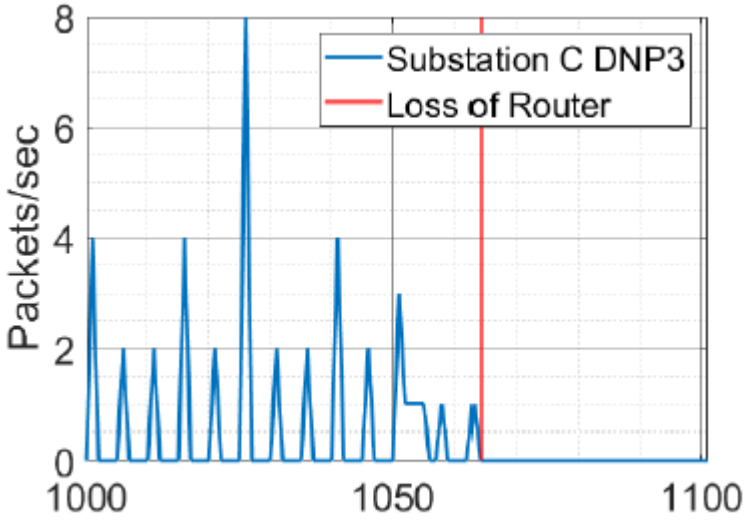


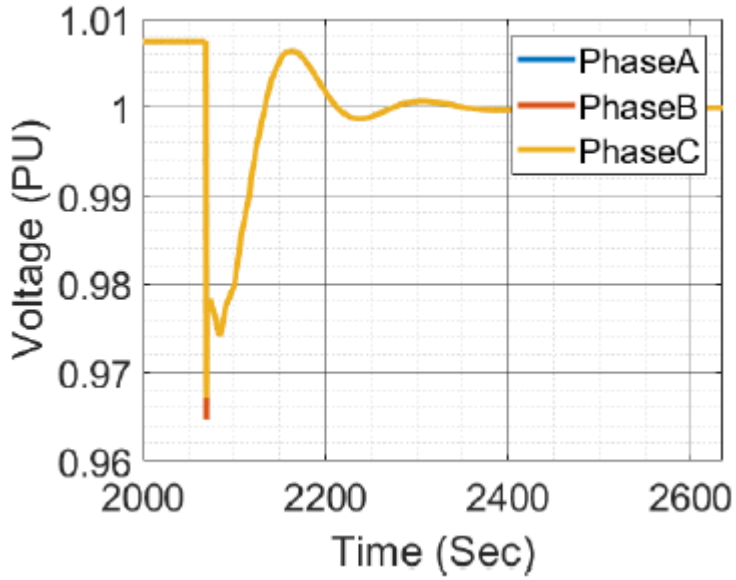
The HARMONIE-SPS CYBER-PHYSICAL TESTBED CASE STUDIES

Cyber-Physical Event: Loss of Critical Cyber Equipment At Substation C and with Load Drop

Joining the two previous cases together, a load drop command is sent from the 'Edge 1' attacker







The HARMONIE-SPS CYBER-PHYSICAL TESTBED CONCLUSION AND FUTURE WORK

CONCLUSION

The HARMONIE-SPS cyber-physical emulation testbed approach for testing an adaptive, cyber-physical SPS has been completed.

3 different use cases were successful deployed and demonstrated 1) cyber disturbance, 2) physical disturbance, and 3) cyber-physical disturbance

With the successful implementation of these disturbances in the cyber-physical testbed, we can test the HARMONIE-SPS methodology using both cyber and physical metrics and model a wide range of disturbances

FUTURE WORK

Continuing implementing different disturbances for training and testing HARMONIE-SPS and incorporating additional hardware-in-the-loop