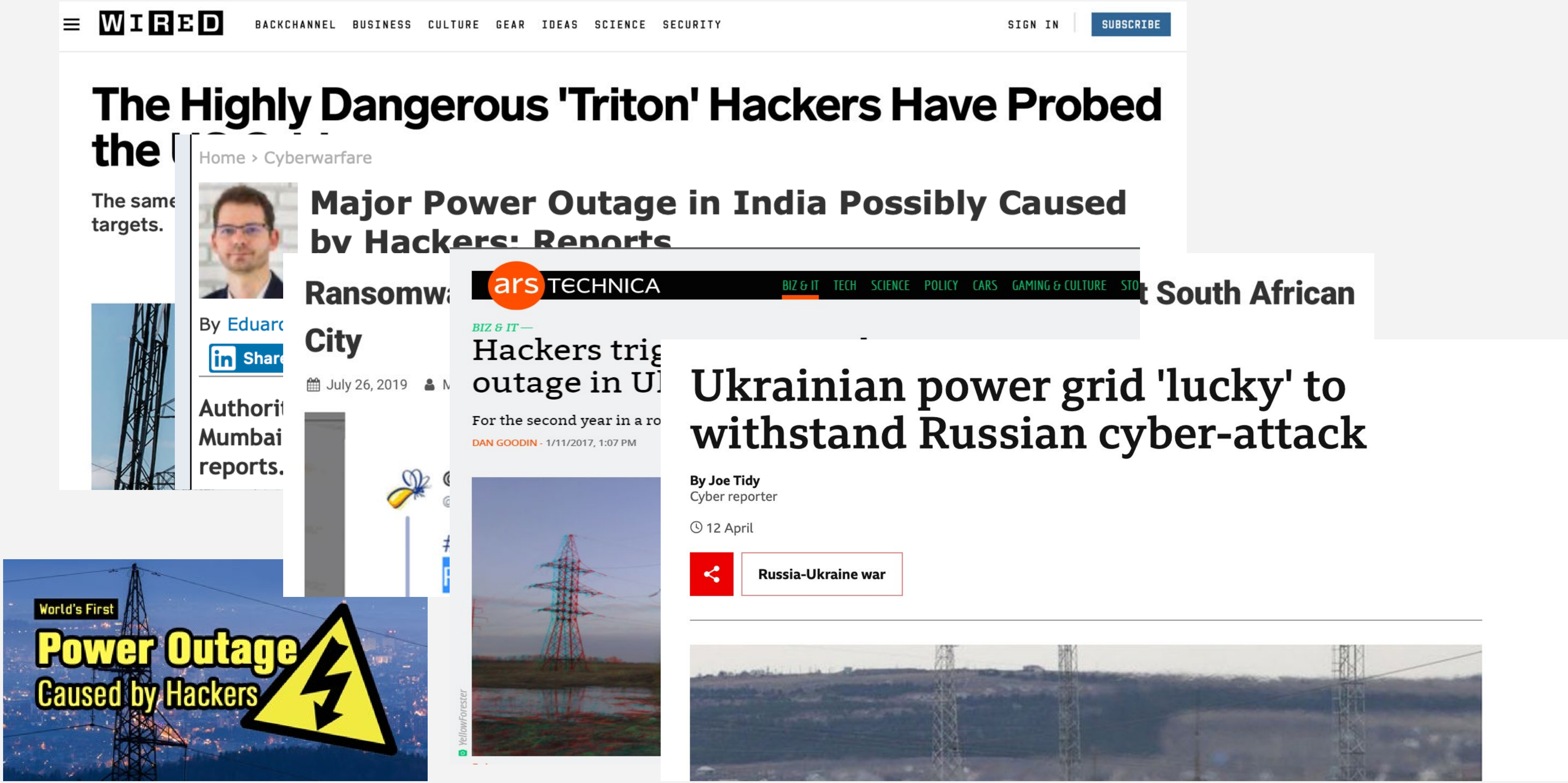
# CYBER POWER TEST-BED DEVELOPMENT & CYBER SECURITY ANALYTICS FOR SMART GRID RESILIENCY

**MOHAMMED MUSTAFA HUSSAIN, SAGNIK BASUMALLIK AND ANURAG K SRIVASTAVA**

Smart Grid REsiliency and Analytics Lab (SG-REAL), West Virginia University, Morgantown, WV, USA

**USER SPOTLIGHT SERIES 2.0 BY RTDS Technologies**


WIRED
BACKCHANNEL BUSINESS CULTURE GEAR IDEAS SCIENCE SECURITY
SIGN IN
SUBSCRIBE
The Highly Dangerous 'Triton' Hackers Have Probed
the
The same
targets.
Home › Cyberwarfare
Major Power Outage in India Possibly Caused
by Hackers: Reports
By Eduar
Share
Authori
Mumbai
reports.
Ransomw
City
July 26, 2019
t South African
ars TECHNICA
BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTURE
BIZ & IT —
Hackers trig
outage in U
For the second year in a ro
DAN GOODIN - 1/11/2017, 1:07 PM
Ukrainian power grid 'lucky' to withstand Russian cyber-attack
By Joe Tidy
Cyber reporter
12 April
Russia-Ukraine war
World's First
Power Outage
Caused by Hackers

# WHAT CAN WE DO ABOUT IT?

## Tools

1

### Tools for Cyber Resiliency

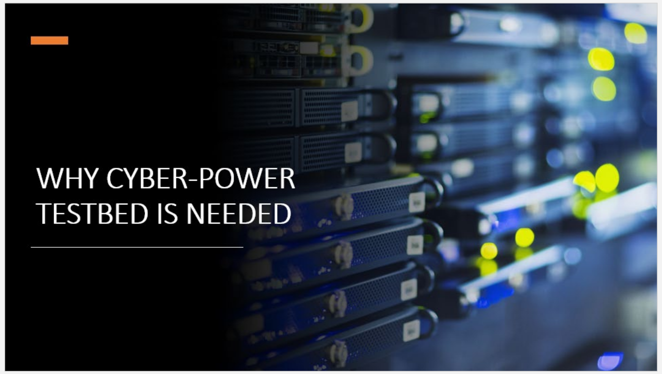
Algorithms and tools for cyber anomaly detection, classification, localization, root cause analytics and resiliency analysis

## Testbed

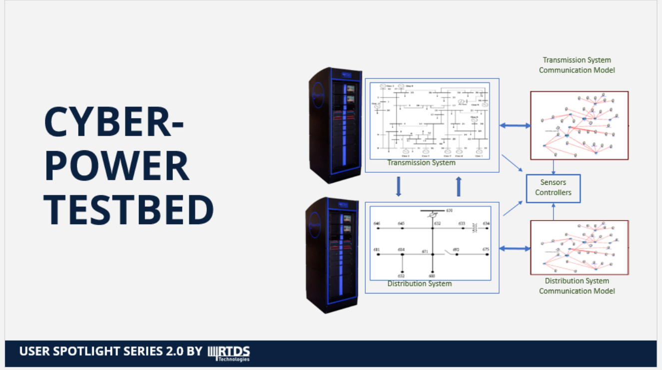
2

### Testbed for Validation

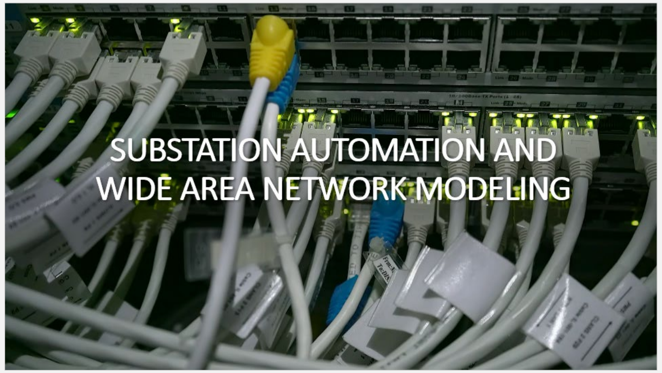
Validate algorithms and tools for deployment


WHY CYBER-POWER TESTBED IS NEEDED


CHALLENGES IN DEVELOPING CYBER-POWER TESTBED


CYBER-POWER TESTBED
Transmission System Communication Model
Transmission System
Sensors Controllers
Distribution System
Distribution System Communication Model
USER SPOTLIGHT SERIES 2.0 BY RTDS


POWER SYSTEM MODELING


SUBSTATION AUTOMATION AND WIDE AREA NETWORK MODELING


CONTROL CENTER MODELING AND CYBER LOG MONITORING


INTEGRATION WITH RESILIENCY ANALYSIS TOOLS

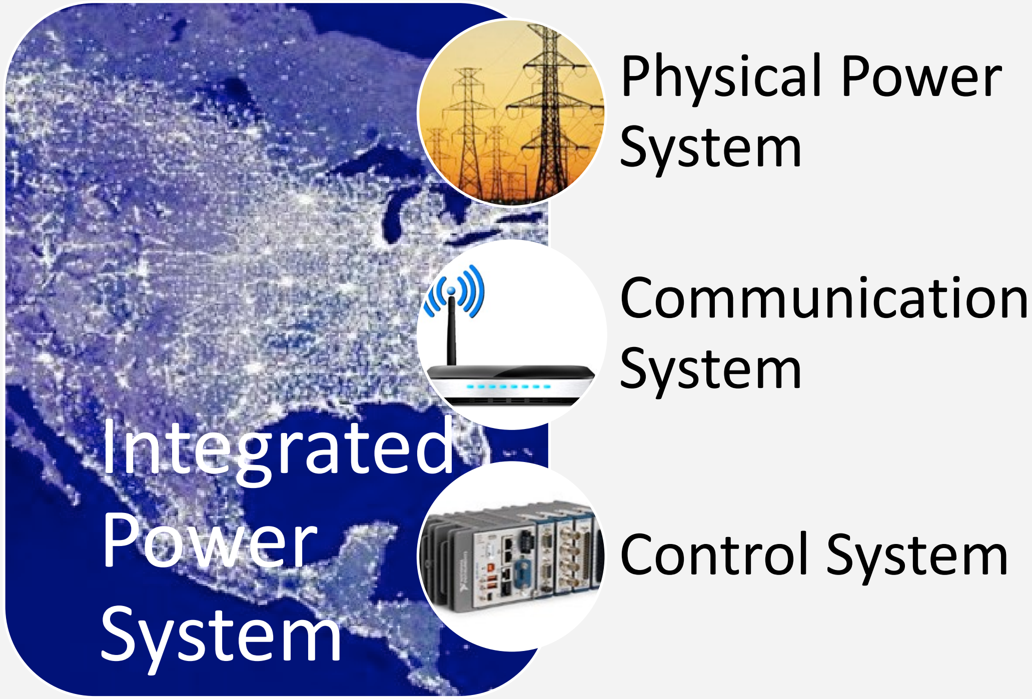

SUMMARY

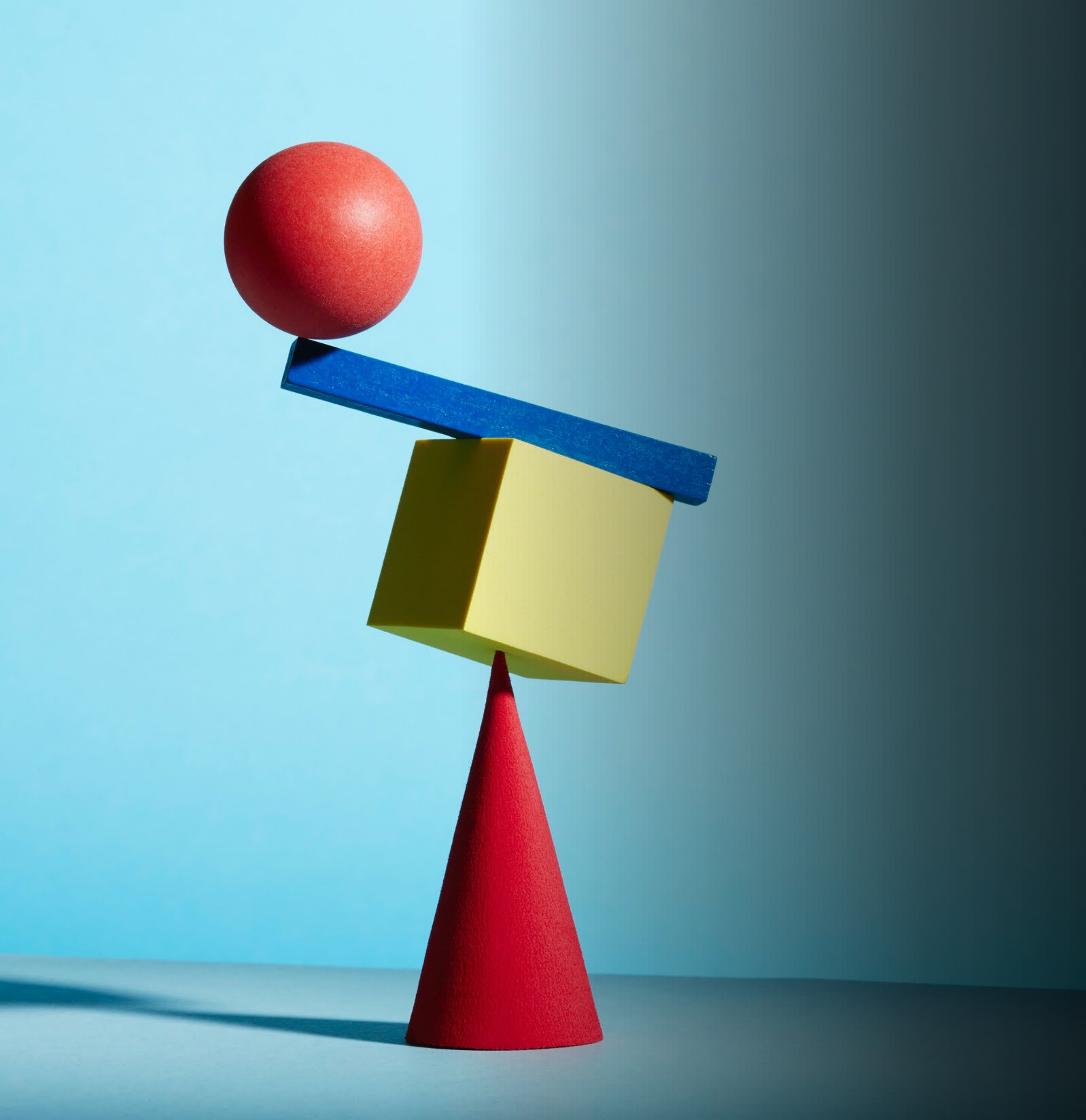
# WHY CYBER-POWER TESTBED IS NEEDED

# WHY REAL-TIME TESTBED WITH CO-SIMULATION

- The Electric Grid is becoming increasingly complex with the new technologies and services such as,
  - Distributed Energy Resources (DERs).
  - Internet of Thing (IoT) devices.
  - Communication network technologies.
- Prone to Cyber Attacks (Stuxnet malware, Ukraine attack)
- Deploying new technologies needs extensive testing and validation
- Not realistic to test new cyber-physical algorithms on an actual power system
- Testbeds provide confidence in solution!

- Co-Simulation of increasingly complex power system with communication systems, control systems help accurately test new applications
- Need to determine if time sensitive applications perform as required in this integrated environment



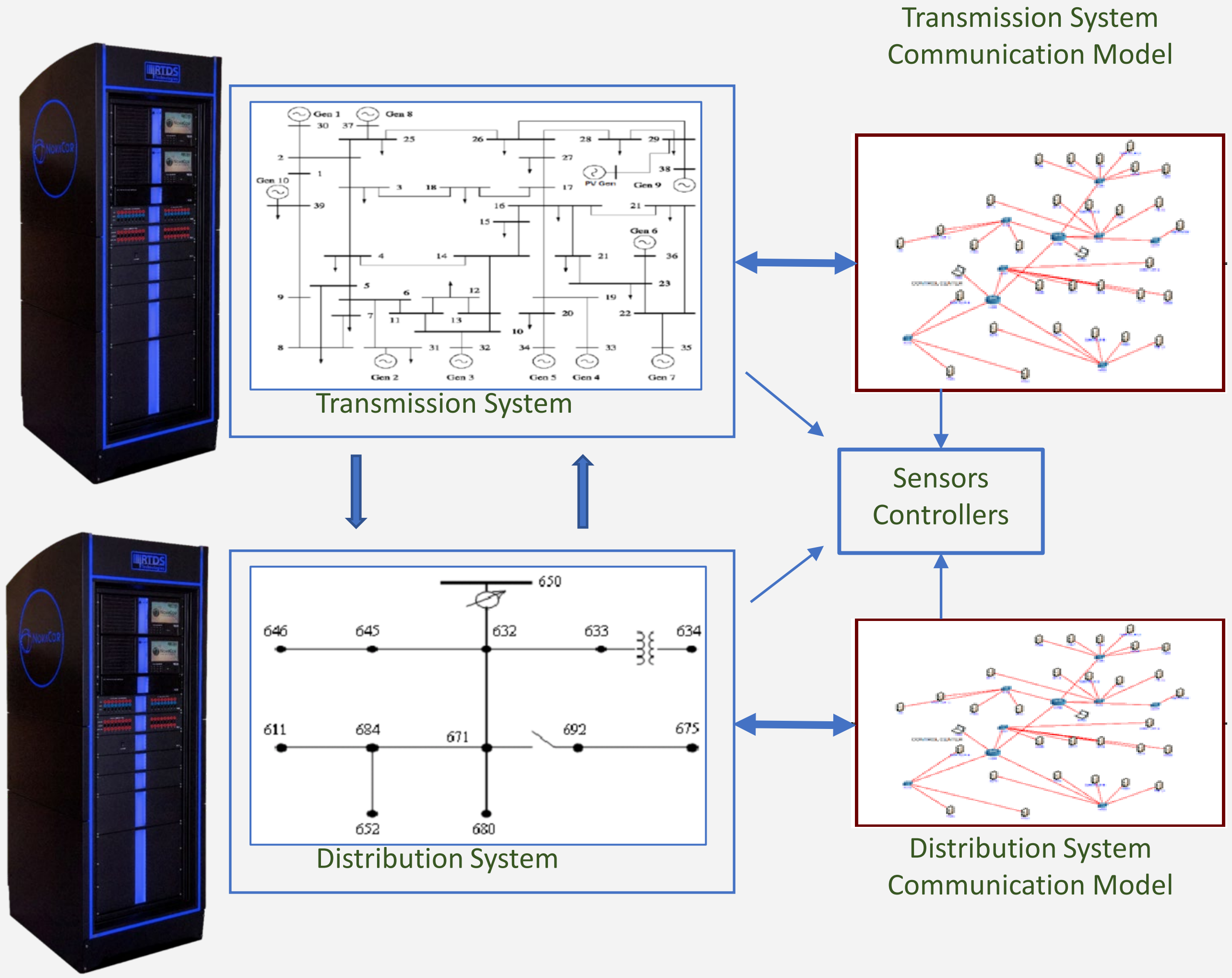


# CHALLENGES IN DEVELOPING CYBER-POWER TESTBED

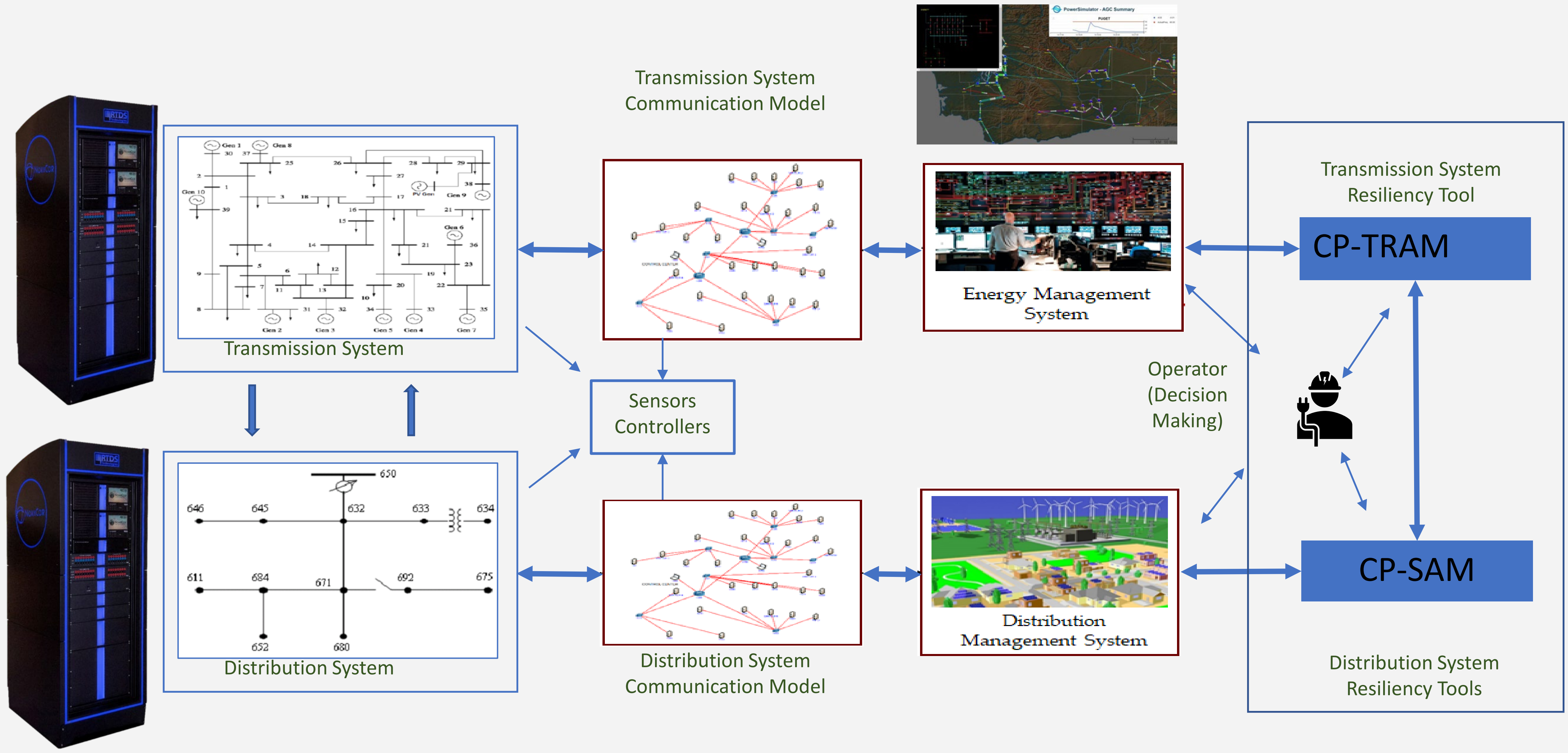
# CHALLENGES AND POSSIBLE SOLUTIONS

| Challenge | Solution |
|---|---|
| Synchronization between dynamic power system and discreet cyber network system | Developed Hardware-In-The-Loop testbed using NS3 & SEL SDN switches to exchange data in real time |
| Interfacing multi vendor hardware & software components | Worked with SEL, RTDS & GPA products to come up with common supporting standards and protocol |
| Developing logging & data storage system involoving both power and cyber data | Used a combination of MySQL and Cloud Database along with Splunk to create a real-time logging system |
| Creating real-time cyber-power scenarios to validate monitoring and control tools | Developing different cyber attack and power system events to create real-time cyber-power scenarios |

# CYBER-POWER TESTBED



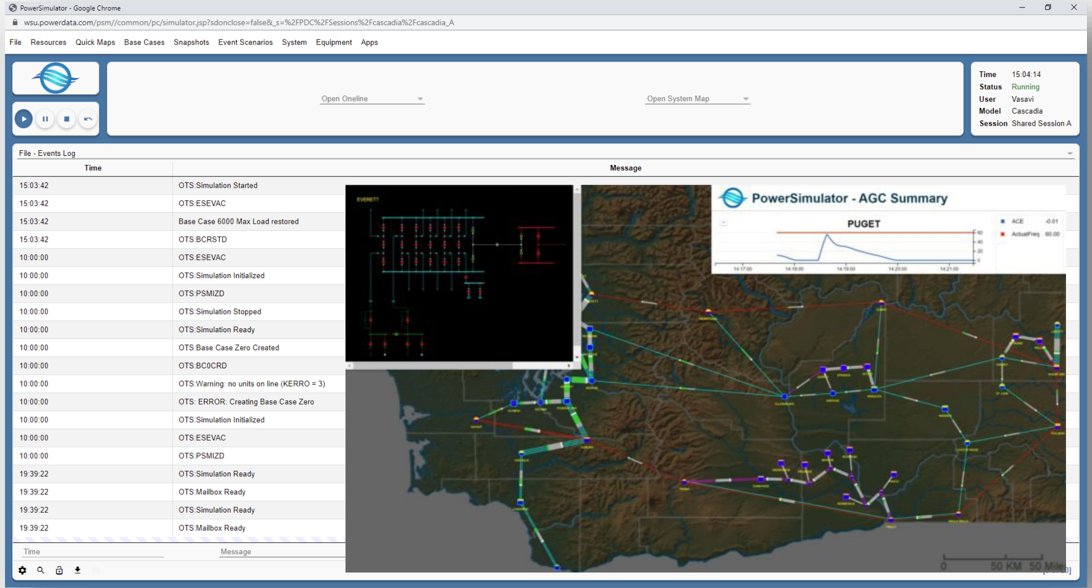
# CYBER-POWER TESTBED



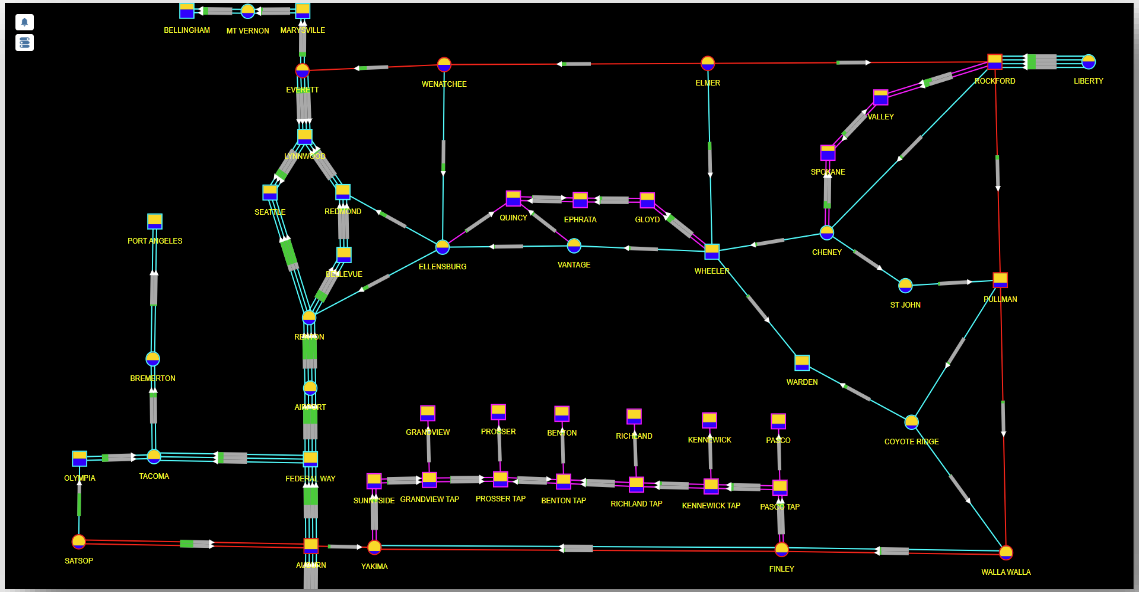
# POWER SYSTEM MODELING

# POWER SYSTEM MODELING

- Dynamic Model to Represent Field System: Electromagnetic model developed in RTDS
- Realistic Static Model in Control Room using PowerSimulator– A realistic platform for power system operation and control developed by IncSys and PowerData.
- About PowerSimulator: The Modeling and Simulation Solution with Dispatch training simulator.
- Cascadia Test System: A power system model in PowerSimulator also being developed in RTDS.




PowerSimulator web user interface

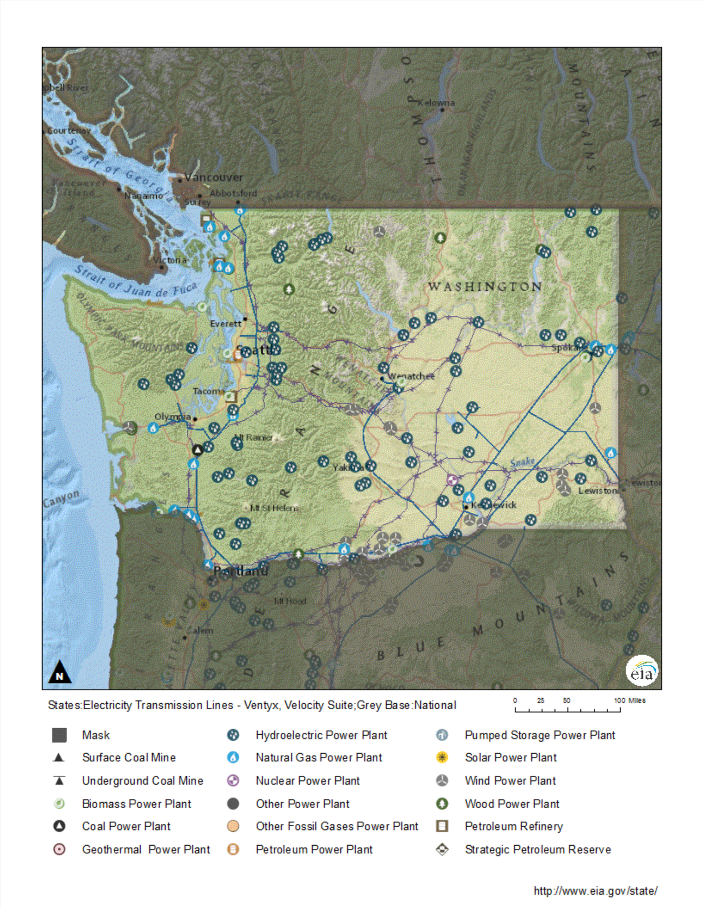



System Schematic-Cascadia power system model

# CASCADIA POWER SYSTEM

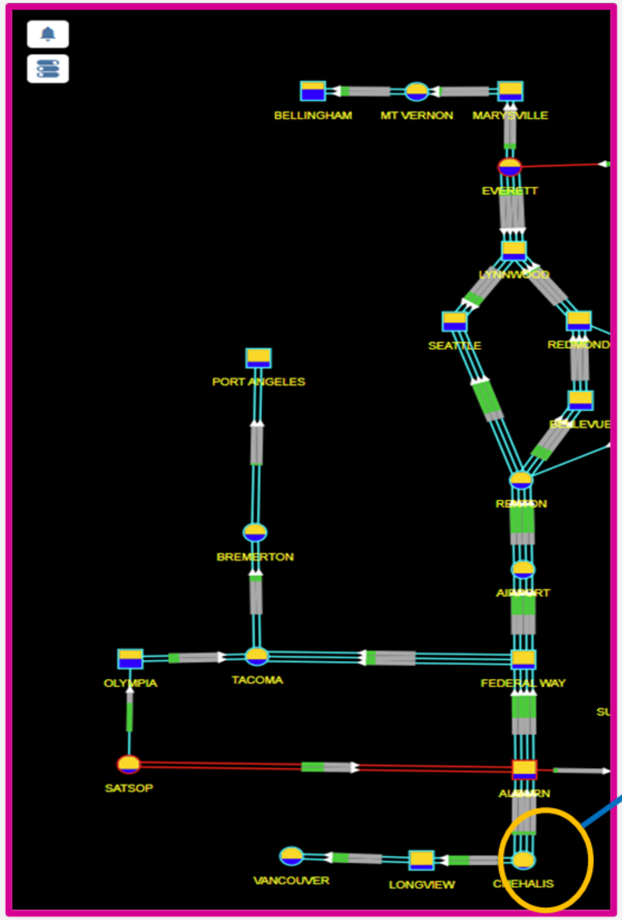
## HIGHLIGHTS

- Total number of sub stations: 54
- With an overall 21 generating stations (mainly Hydro, Thermal and Natural Gas)
- The Largest generator is at Chehalis with 1200 MW capacity.
- The Cascadia deals with power transfer through 115 KV, 230 KV and 525 KV lines.

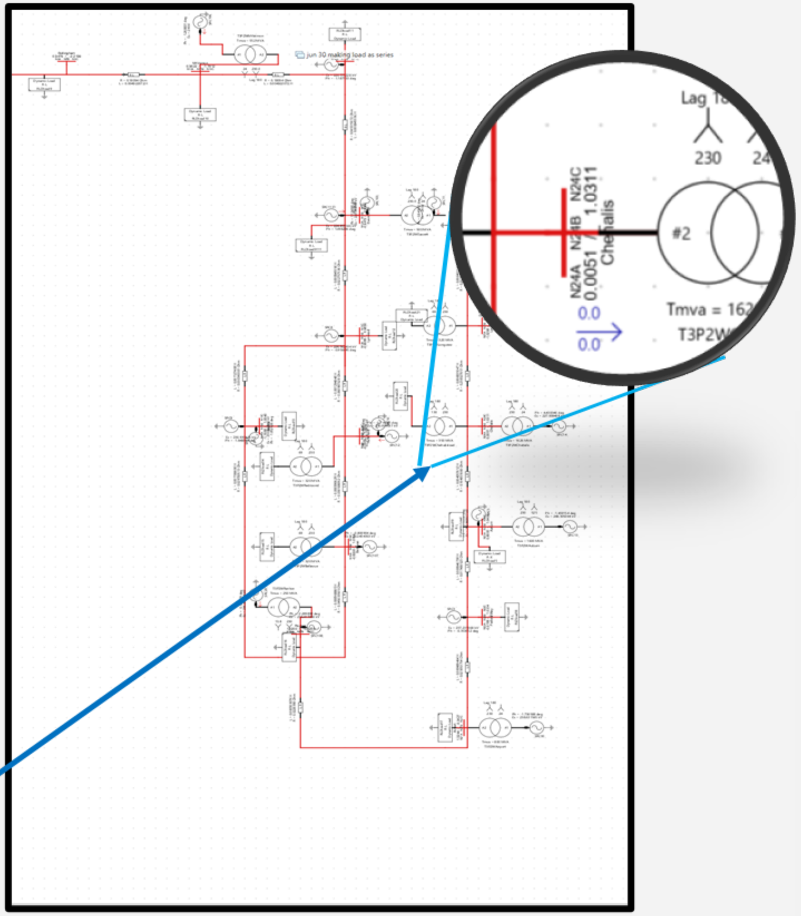



Test System Representing Washington State Area

# WESTERN REGION(PUGET) OF CASCADIA MODELLED IN RTDS



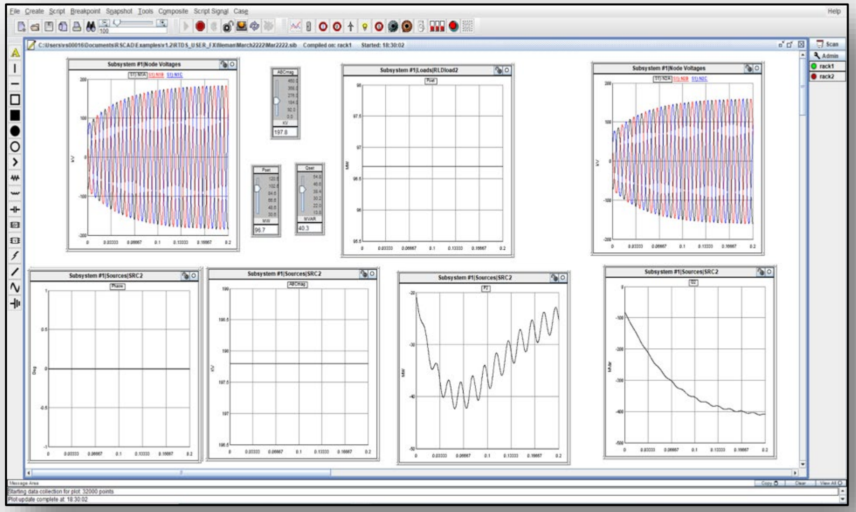

Puget Region of Cascadia on PowerSimulator




Cascadia(Puget) on RTDS via RsCad Fx

The Power Flow converges after 6 iterations

Real Power flow achieved identical to PowerSimulator



Voltage and Power wave forms from Mt Vernon substation in PUGET model on RTDS

# SUBSTATION CYBER NETWORK MODELING


Real-Time Digital Simulator Running Cascadia Model

Real Time Automation & Controller (RTAC), Working as Local PDC and local historian

Software Defined Networking (SDN) Switches connecting substation network

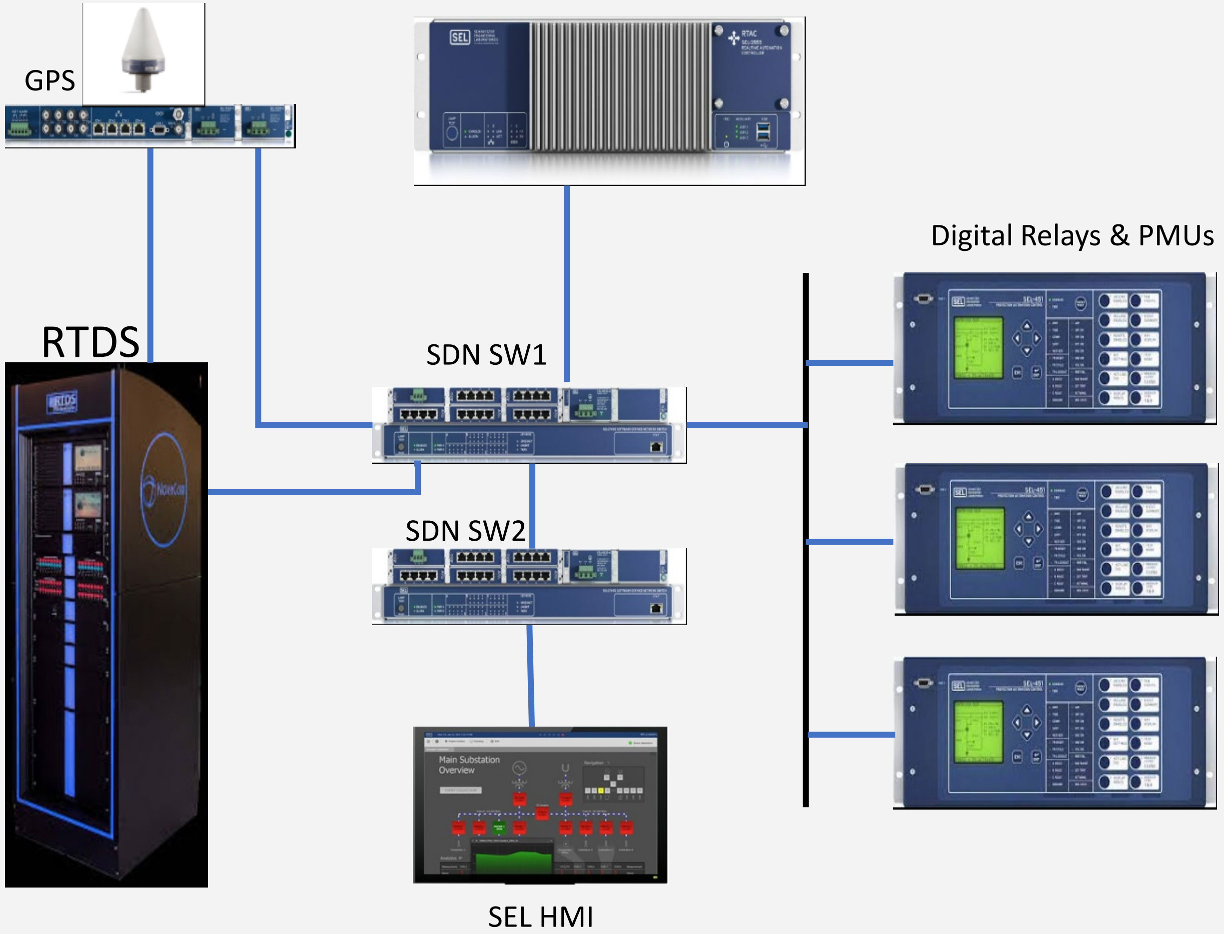
Substation Workstation and local HMI

SEL Relays and PMUs connecting RTDS

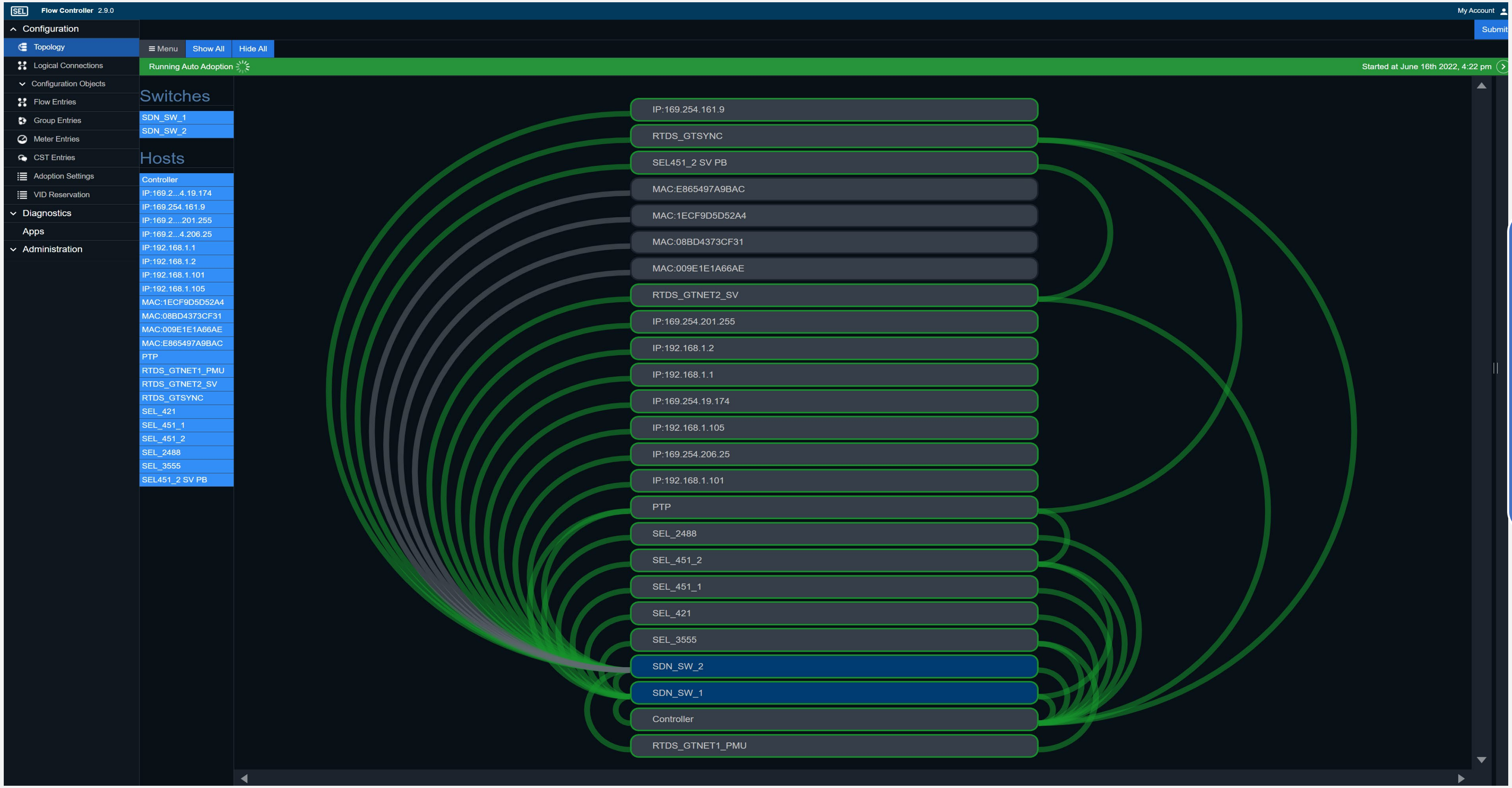
SEL GPS for time synchronization

Substation communication is developed using a combination of both RTDS software PMU/Relay and SEL hardware PMU/relays

# SUBSTATION CYBER NETWORK MODELING, CONNECTIVITY



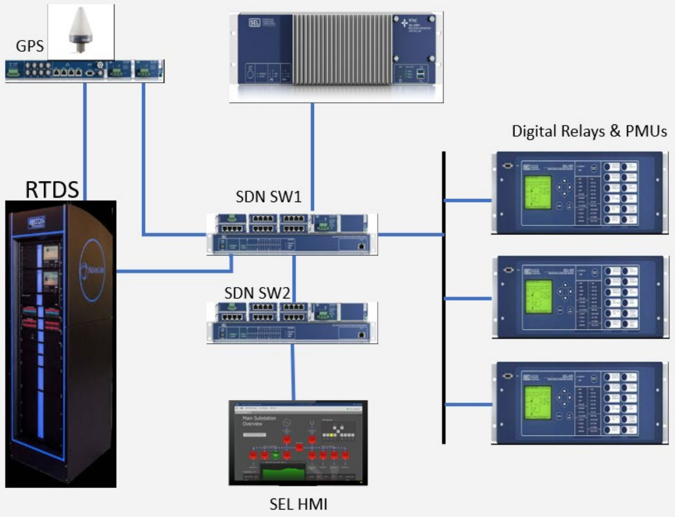
# SOFTWARE DEFINED NETWORK TOPOLOGY FOR SUBSTATION NETWORK, HMI VIEW



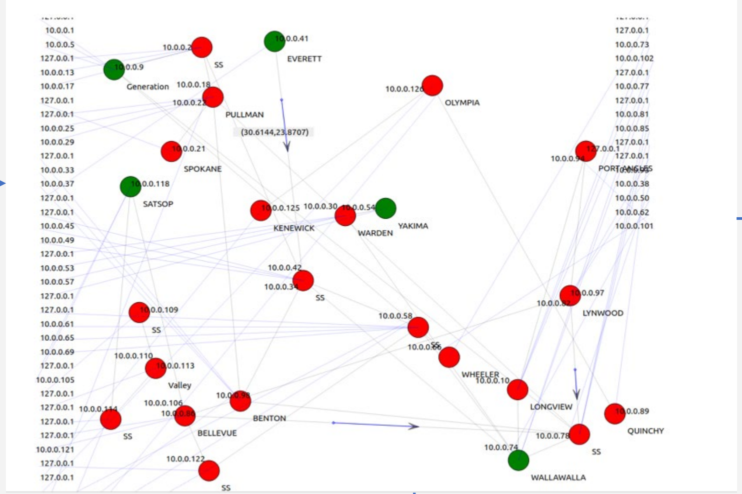

**SDN Advantages:**

- Greater Reliability via Automation
- More Efficient Network Management
- Improved Security

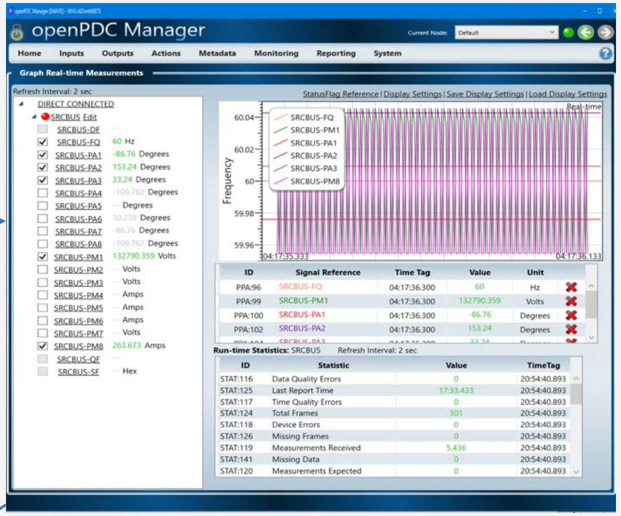
# END TO END DATA CONNECTIVITY, FROM SUBSTATION TO CONTROL CENTER USING NS3



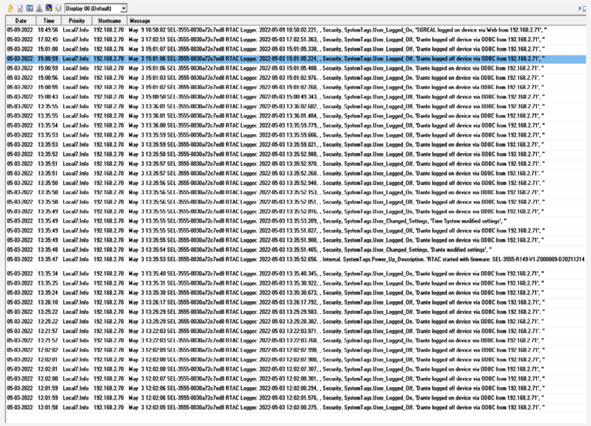

Substation Cyber Network Modeling




NS3 communication network for multiple substation




OpenPDC receiving data from substation to control center



Logging and Archiving from Substation, NS3 and Control center

# CONTROL CENTER MODELING AND CYBER LOG MONITORING

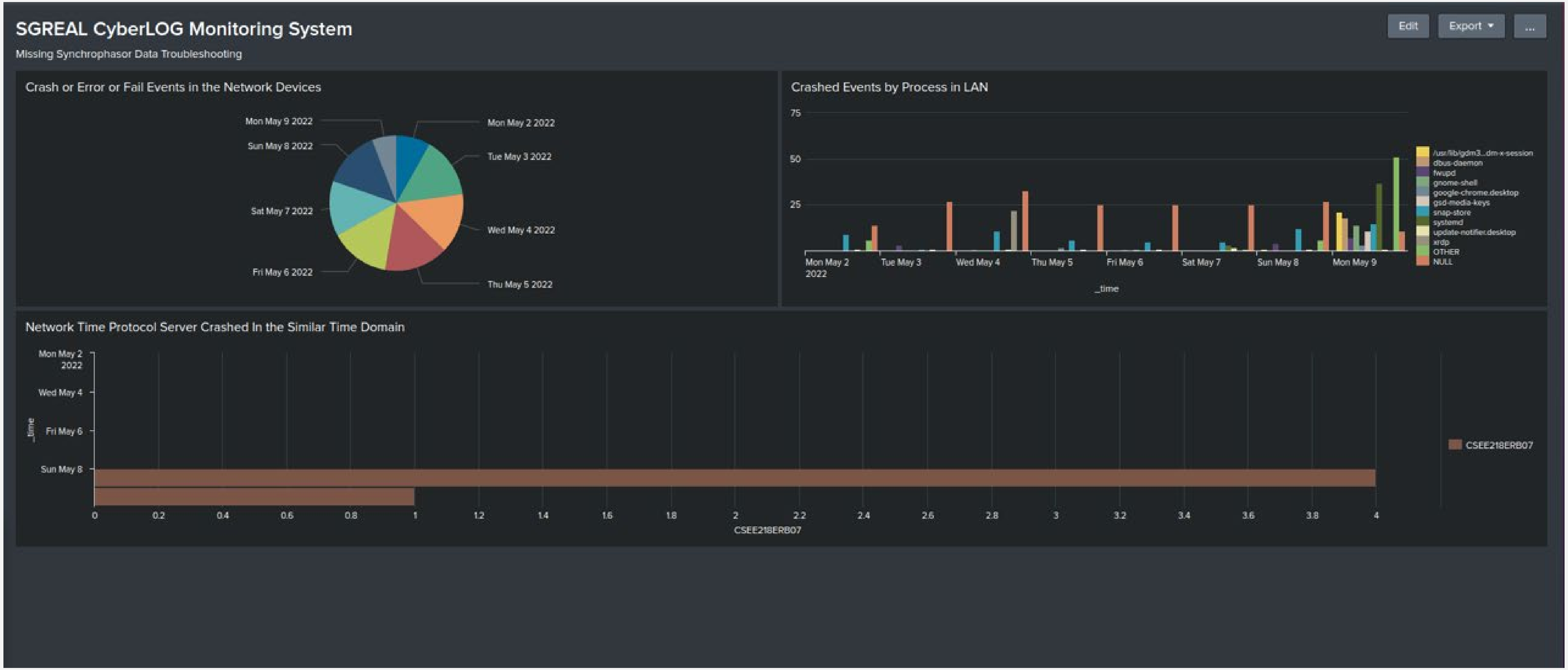
# SG-REAL CONTROL CENTER

Control Center is developed for:

- Power system operation center
- Network Operation center

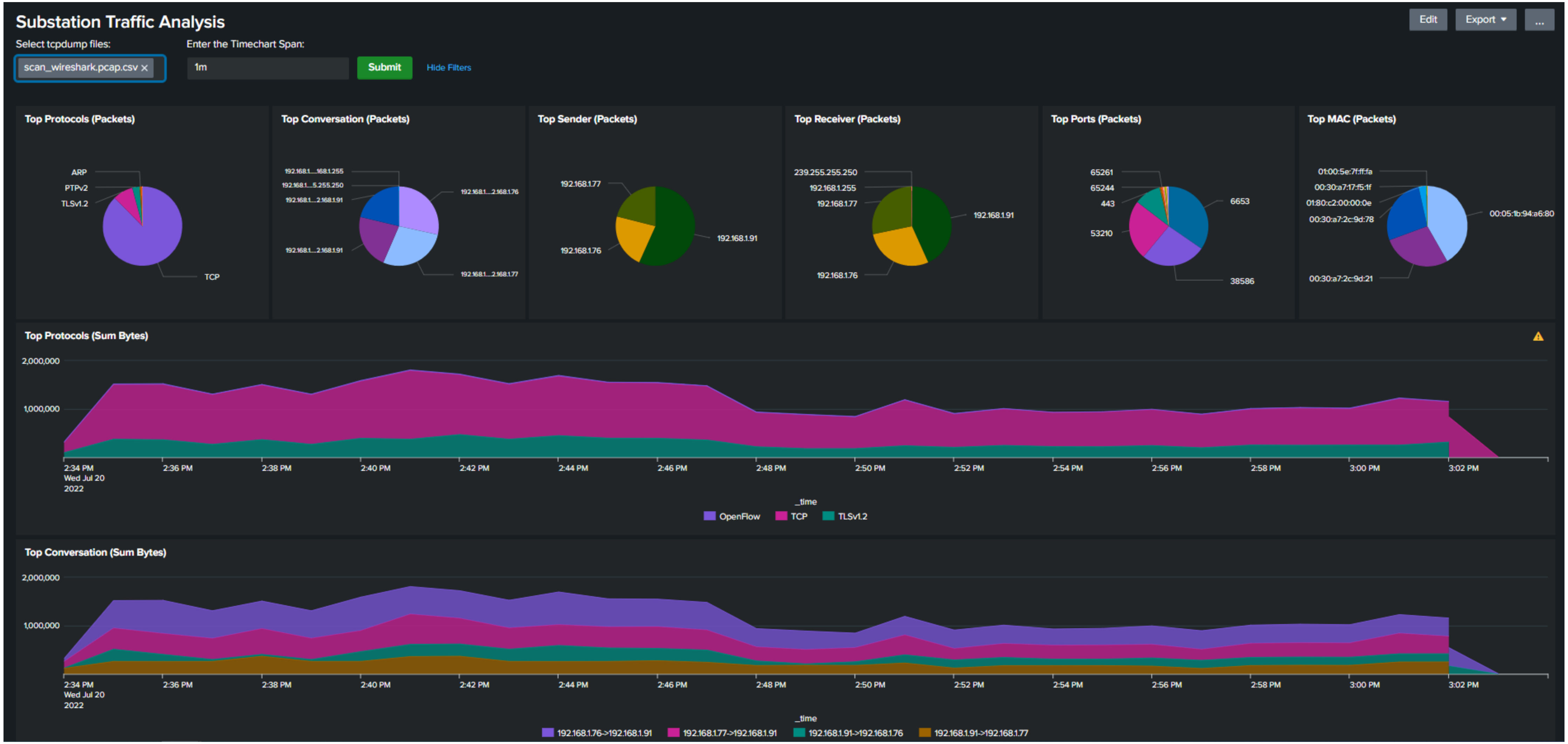
Dashboards from the screenshot shown in the slides is being shown here in the control center

# SG-REAL CYBER LOG MONITORING SYSTEM




Assisting operator to investigate missing Synchrophasor Data using dashboard and data logging

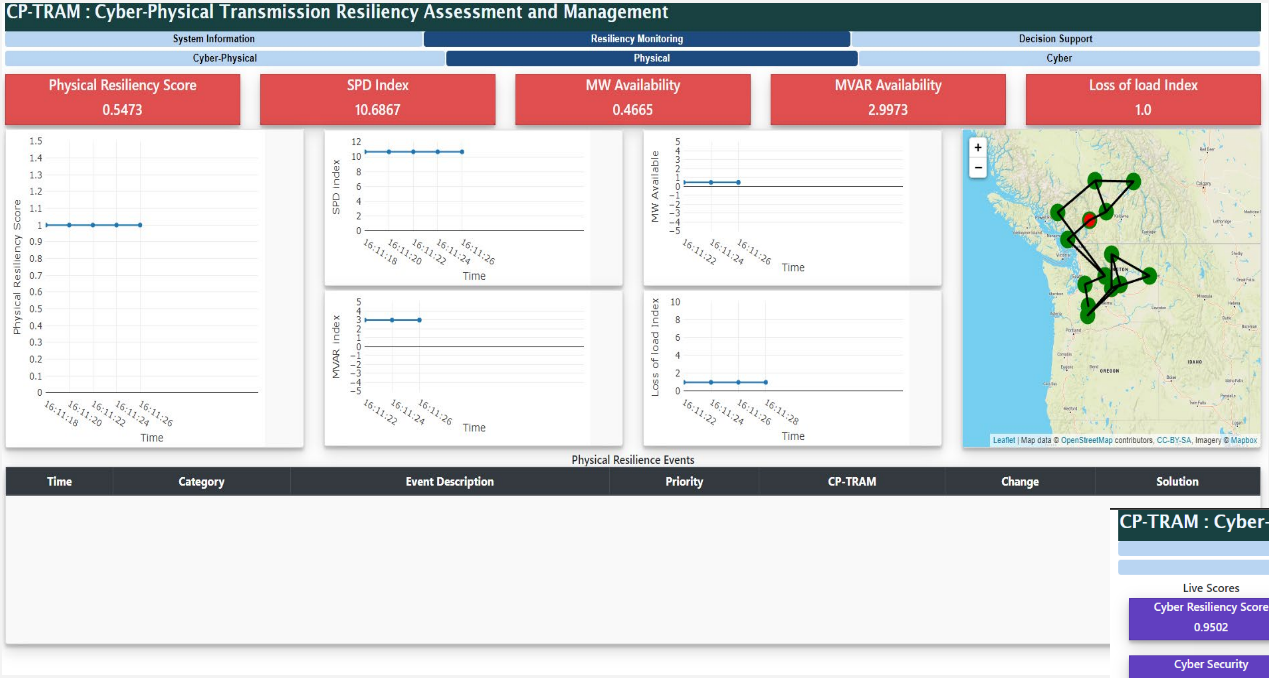
# SG-REAL CYBER LOG MONITORING SYSTEM



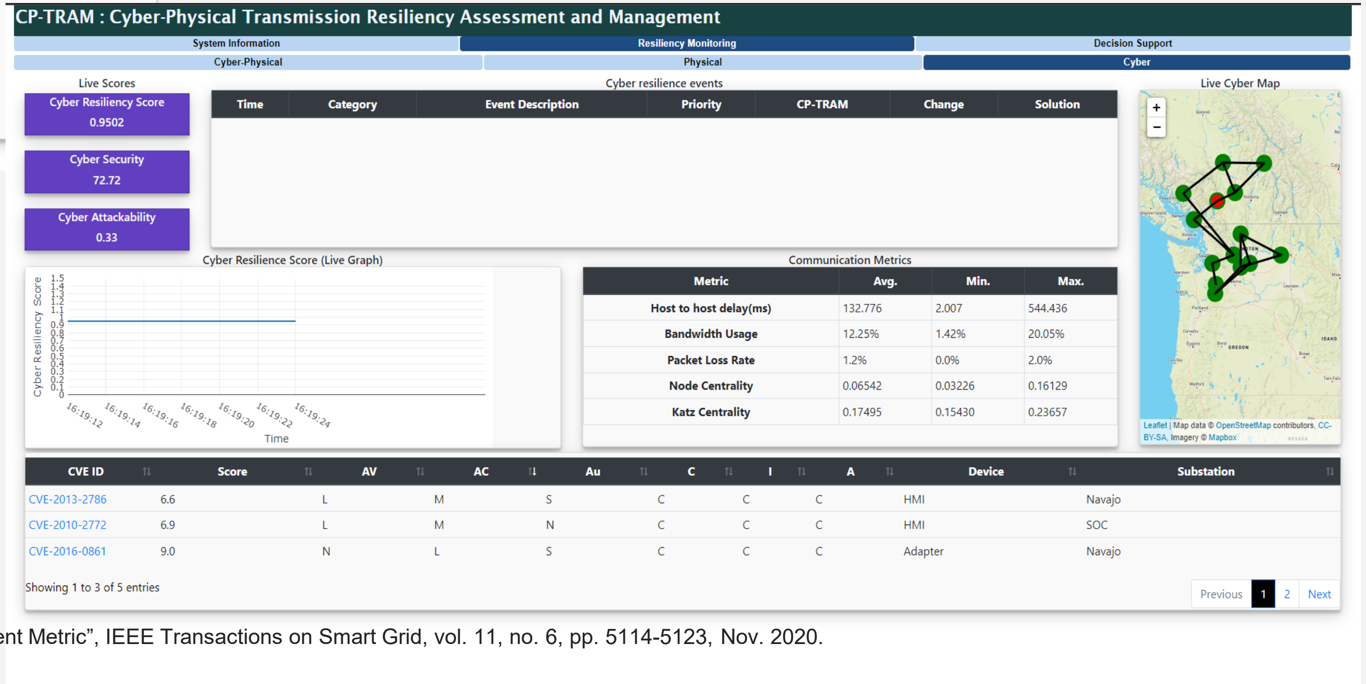

Assisting operator to investigate Network anomaly using dashboard and data logging

# INTEGRATION WITH RESILIENCY ANALYSIS TOOLS

# ADVANCED TOOLS, CP-TRAM



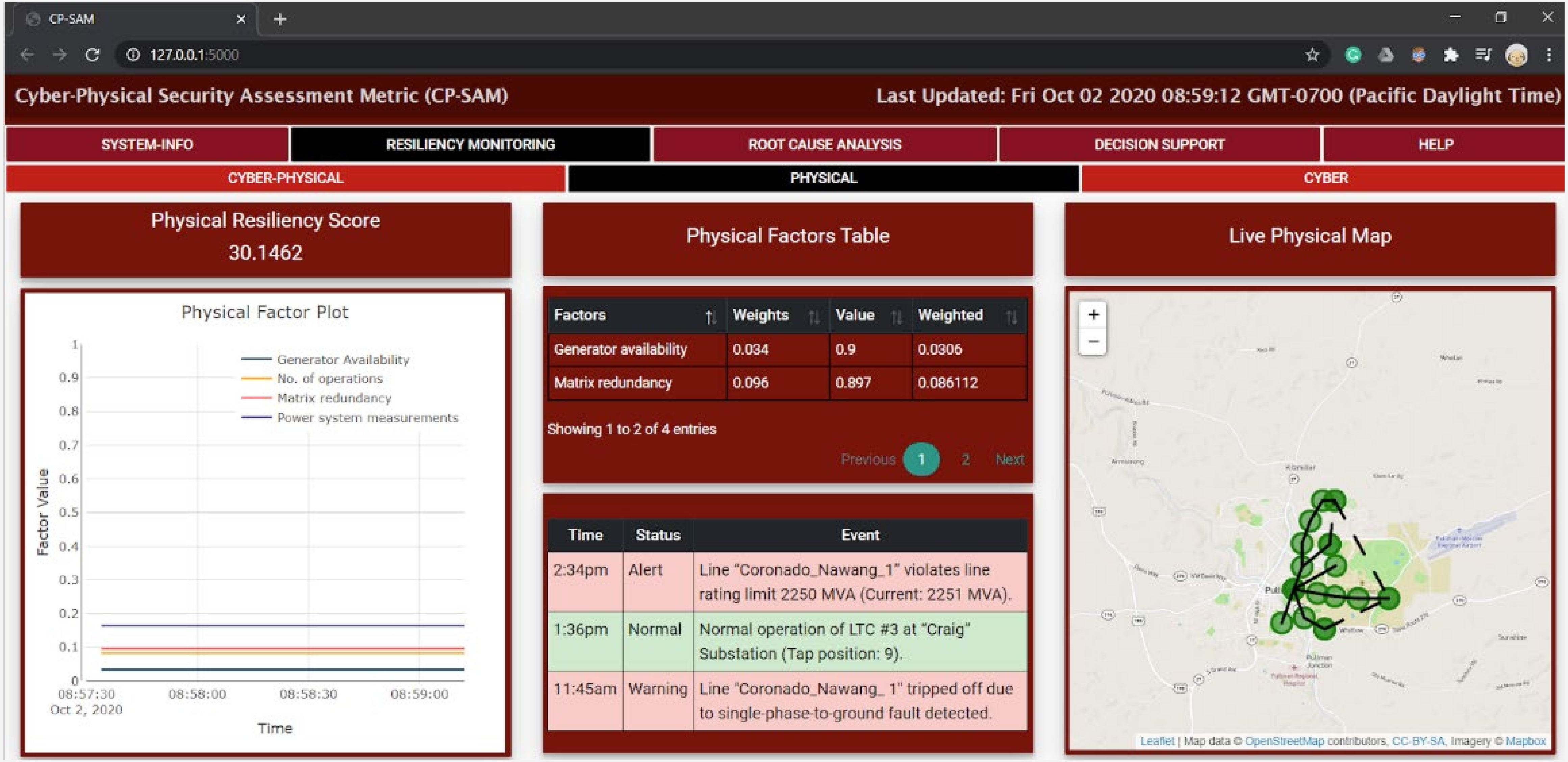

Physical Scenario, showing resiliency for Physical power system event such as tripping a breaker.




Cyber Scenario, showing resiliency in case of a cyber event such as network change or software update.

Tushar, V. Venkataramanan, A. K. Srivastava, A. Hahn, “CP-TRAM: Cyber-Physical Transmission Resiliency Assessment Metric”, IEEE Transactions on Smart Grid, vol. 11, no. 6, pp. 5114-5123, Nov. 2020.

# ADVANCED TOOLS, CP-SAM




Venkatesh Venkataramanan, Adam Hahn, and Anurag Srivastava. "CP-SAM: Cyber-physical security assessment metric for monitoring microgrid resiliency." *IEEE Transactions on Smart Grid* 11.2 (2019): 1055-1065.

# SUMMARY

# SUMMARY

## DEVELOPED A REAL-TIME, MULTI-LAYER CYBER–POWER TESTBED

Used Real-Time Digital Simulator (RTDS) as a dynamic power system simulator.

Used both software PMUs/RTUs as well as SEL Hardware Relays & RTAC for substation level Automation with software defined networking.

Used NS3 network emulator to create wide area communication network on top of the physical power system

Used MySQL database, Snort IDS and Splunk Logging system for real-time security alerts and log analysis.

Developing Advanced Tools to help operators with better decision making and situational awareness

Generating Synthetic but realistic data for validation of the algorithms/ tools

Performing Cyber attacks and creating power events to understand the nature of interdependency within cyber-power system.

We acknowledge technical support from other students, post-docs, RTDS, SEL and financial support from the US Department of Energy and National Science Foundation.