OPAL-RT TECHNOLOGIES

FROM IMAGINATION TO REAL-TIME

Power Grid Cybersecurity Webinar

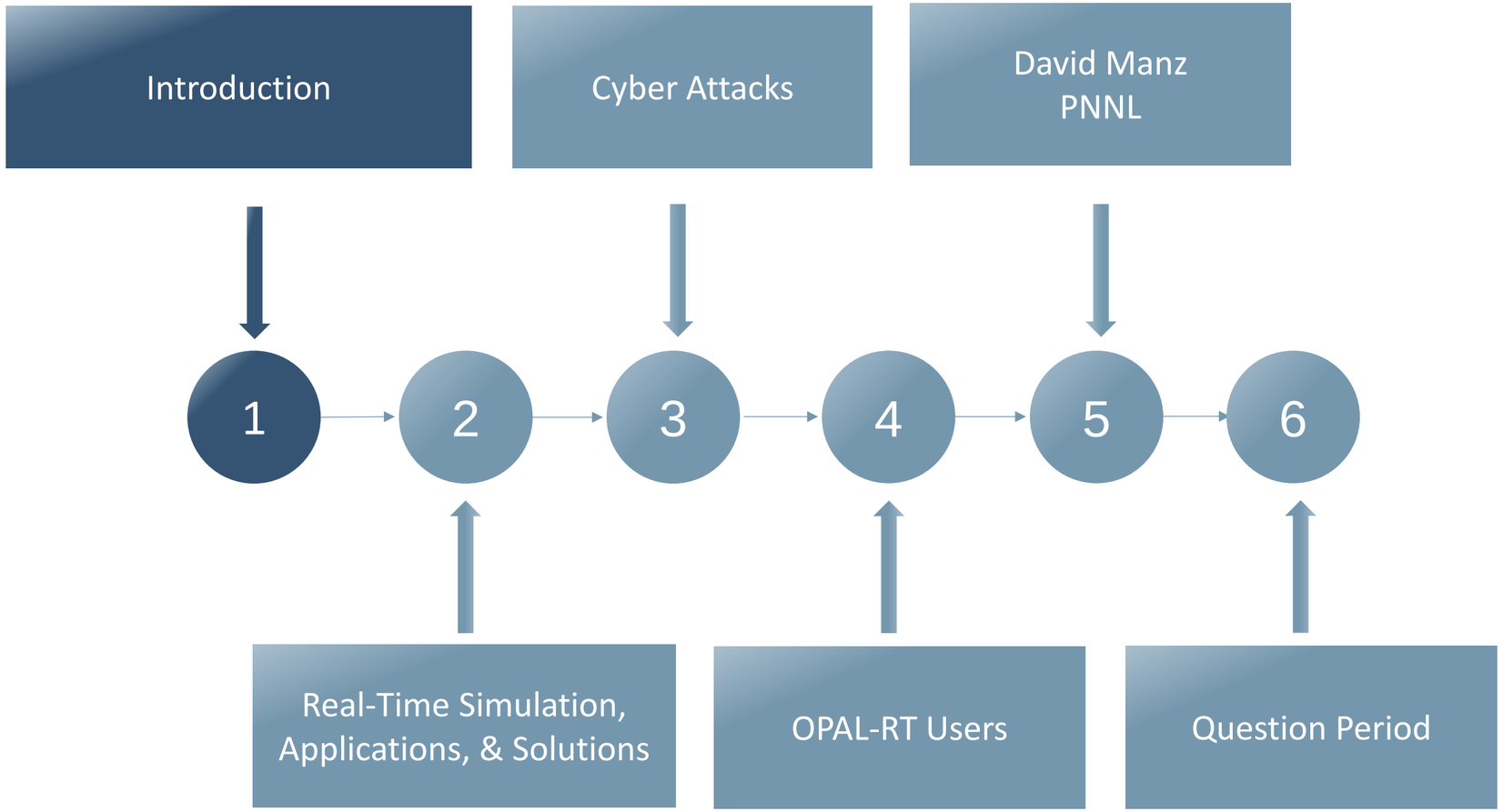
Jan. 29, 2016

Your Hosts

Introduction &
Real-Time Applications
Thomas Kirk
Sales Engineer
OPAL-RT Technologies

Keynote Speaker
David Manz
Cybersecurity Research Scientist
Pacific Northwest National Laboratory

Presentation Outline



Introduction

The **electric power grid** is evolving quickly with the introduction of new **“intelligent” technologies**, which will improve its efficiency and performance. However, these technologies have the potential to make the grid more **vulnerable** to **cyberattacks**, which has motivated a new set of **standards (NERC CIP)**.[1]

OPAL-RT is **dedicated** to providing **open** power system **real-time digital simulators** that meets the new requirements of **power system professionals** as the industry focus on **cybersecurity** increases.

1 R. J. Campbell, Cybersecurity Issues for the Bulk Power System, Congressional Research Service, 2015

Introduction

DEFINITIONS:

The **activity** or **process**, **ability** or **capability**, or state whereby **information** and **communications systems** and the **information** contained therein are protected from and/or **defended** against **damage**, **unauthorized** use or **modification**, or **exploitation.**[1]

2 – Cybersecurity definition taken from National Initiative for Cybersecurity Careers and Studies (NICCS)

The art of ensuring the **existence** and **continuity** of the **information** society of a nation, guaranteeing and protecting, in **Cyberspace**, its information, **assets** and **critical infrastructure**. [2]

3 – Canongia, C., & Mandarino, R. 2014. *Cybersecurity: The New Challenge of the Information Society*. In Crisis Management: Concepts, Methodologies, Tools and Applications: 60-80. Hershey, PA: IGI Global.

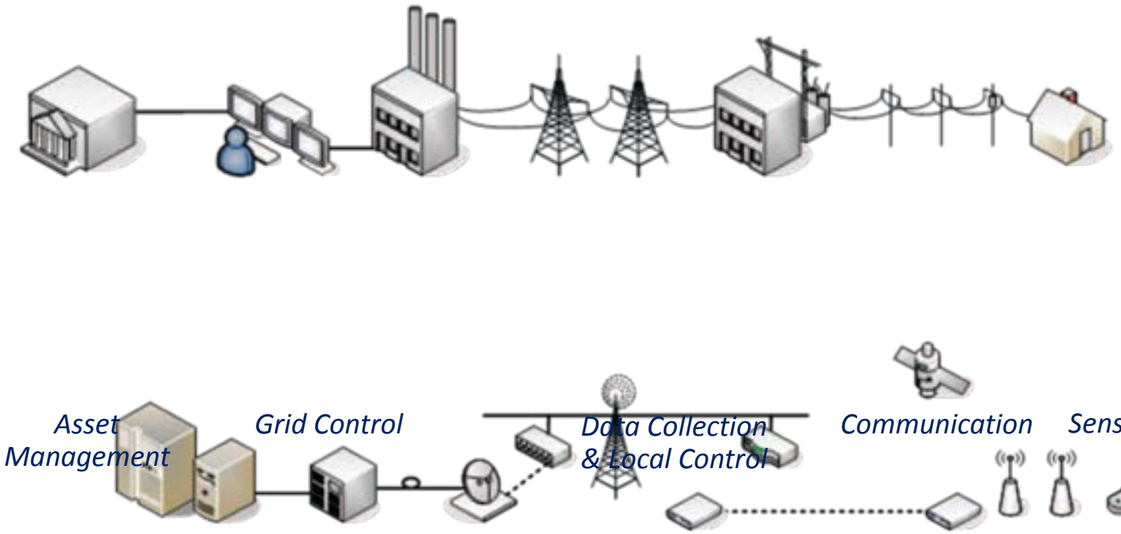
Introduction: Grid Modernization

- Modern power grids are Cyber-Physical System (CPS) composed of electrical and information infrastructure

- The grid is becoming “intelligent” through:
  - Wide deployment of new technologies
  - Substation, transmission and distribution automation
  - Increased distributed Energy Resource (DER) integration
  - Advanced two-way communication networks
  - Development of synchrophasor systems

- But… as newer technologies are adopted, the grid is becoming more vulnerable to cybersecurity threats both:

Malicious and **Accidental**[4]



Source: EPRI 2007

4 See NIST (http://www.nist.gov/el/smartgrid/cybersg.cfm)

Introduction: Threats and Scenarios

- Dozens of industrial-level cybersecurity incidents since 1999 (Source: Lloyd's):
  - 2001: Cal-ISO hacking incident (15 days)
  - 2007: Idaho National Laboratory Aurora experiment
  - 2010: Iran nuclear Stuxnet incident
  - 2012: German utility DoS attack (5 days)

- FERC analysis: The loss of 9 out of 55k+ US substations could lead to an extended (1+ year) national blackout (Source: WSJ)

- 2014 NESCOR failure scenarios report includes failures due to:
  - Compromised equipment functionality
  - Data integrity attacks
  - Communication failures
  - Human Error
  - Natural Disasters

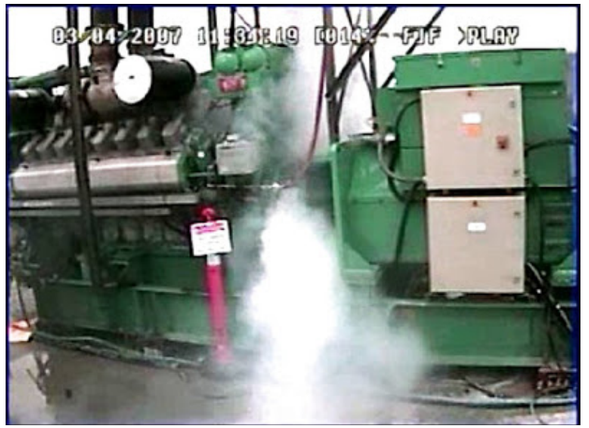


Table 4 - Draft Top Ranked Failure Scenarios from document version 0.7

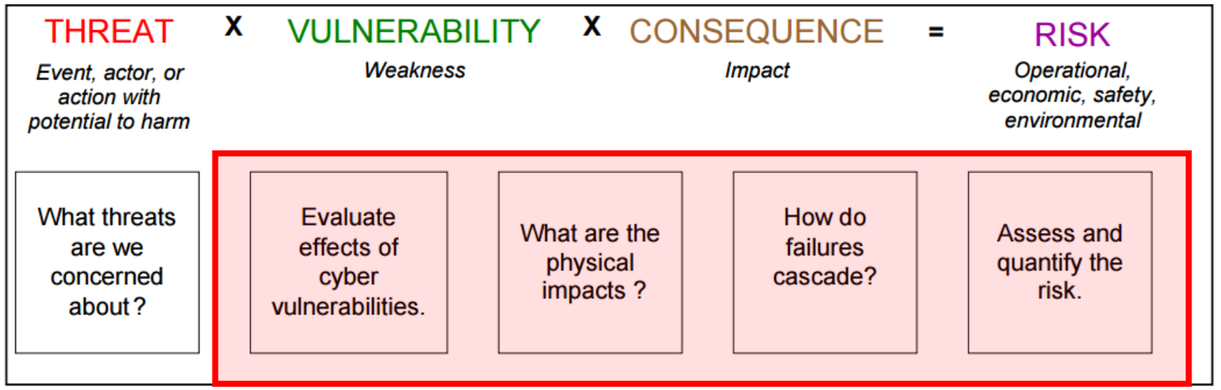
AMI.1	Authorized Employee Issues Invalid Mass Remote Disconnect
AMI.3	Invalid Access Used to Install Malware Enabling Remote Internet Control
AMI.23	Meter Authentication Credentials are Compromised and Posted on Internet
AMI.24	Weak Encryption Exposes AMI Device Communication
AMI.25	Known but Unpatched Vulnerability Exposes AMI Infrastructure
DER.1	Inadequate Access Control of DER Systems Causes Electrocution
DER.16	DER SCADA System Issues Invalid Commands
WAMPAC.1	Denial of Service Attack Impairs NTP Service
WAMPAC.2	Networking Equipment used to Spoof WAMPAC Messages
WAMPAC.3	Improper PDC Configuration Interferes with Relay of Measurement Data
WAMPAC.4	Measurement Data Compromised due to PDC Authentication Compromise
WAMPAC.5	Improper Phasor Gateway Configuration Obscures Cascading Failures
WAMPAC.6	Communications Compromised between PMUs and Control Center
DR.1	Blocked DR Messages Result in Increased Prices or Outages
DR.4	Improper DRAS Configuration Causes Inappropriate DR Messages
DGM.3	Malicious Code Injected into Substation Equipment via Physical Access
DGM.5	Remote Access used to Compromise DMS
DGM.13	Poor Account Management Compromises DMS and Causes Power Loss
Generic.1	Malicious and Non-malicious Insiders Pose Range of Threats
Generic.2	Inadequate Network Segregation Enables Access for Threat Agents
Generic.3	Portable Media Enables Access Despite Network Controls

2014 NESCOR failure scenarios report

Introduction: Risk Assessment

- NERC CIP Standards focus largely on risk assessment and identification of:
  - Critical Assets
  - Critical Cyber Assets

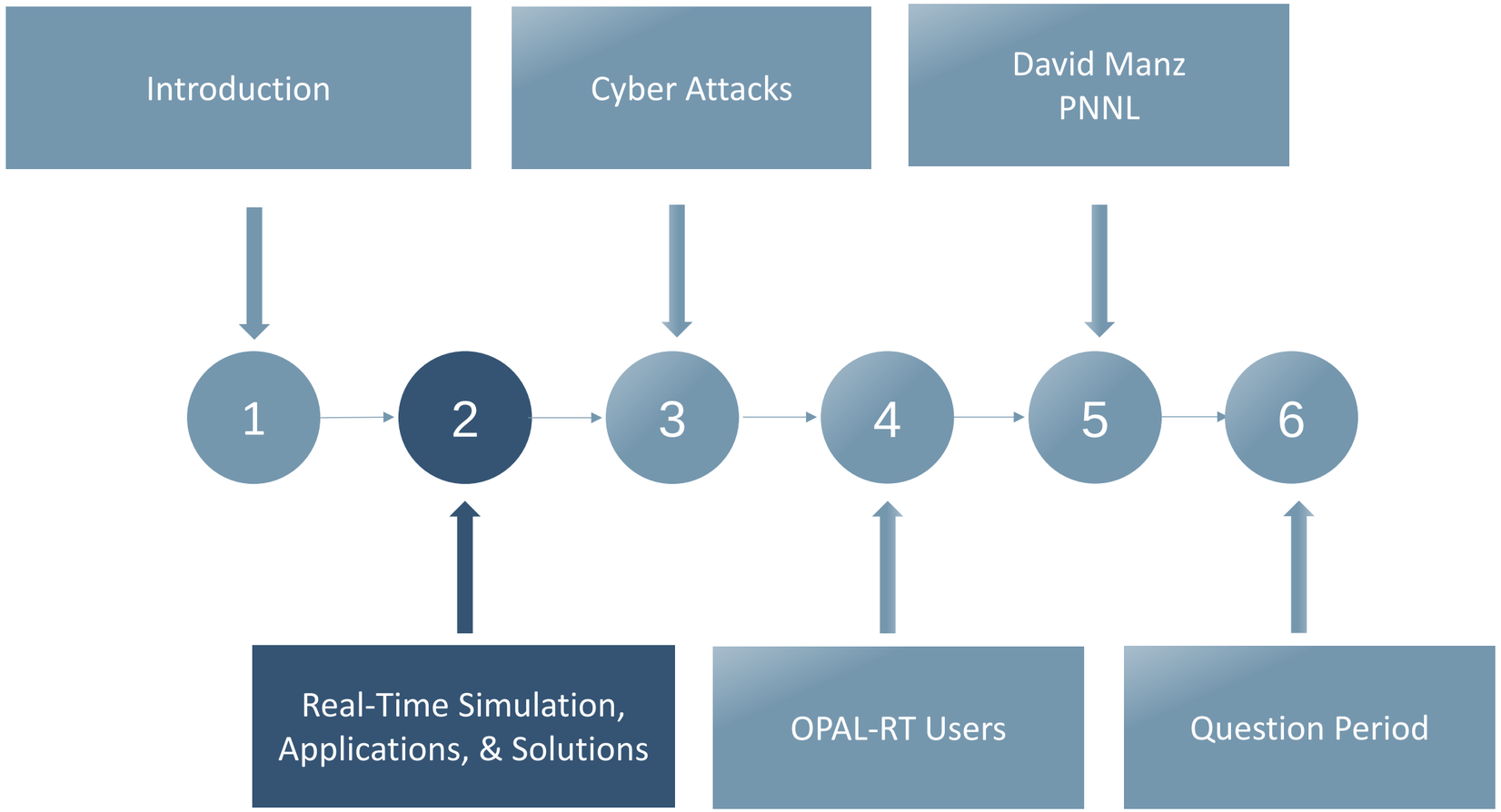
- SGIP Cyber Security Guidelines (NISTIR 7628) are also based on risk assessment:



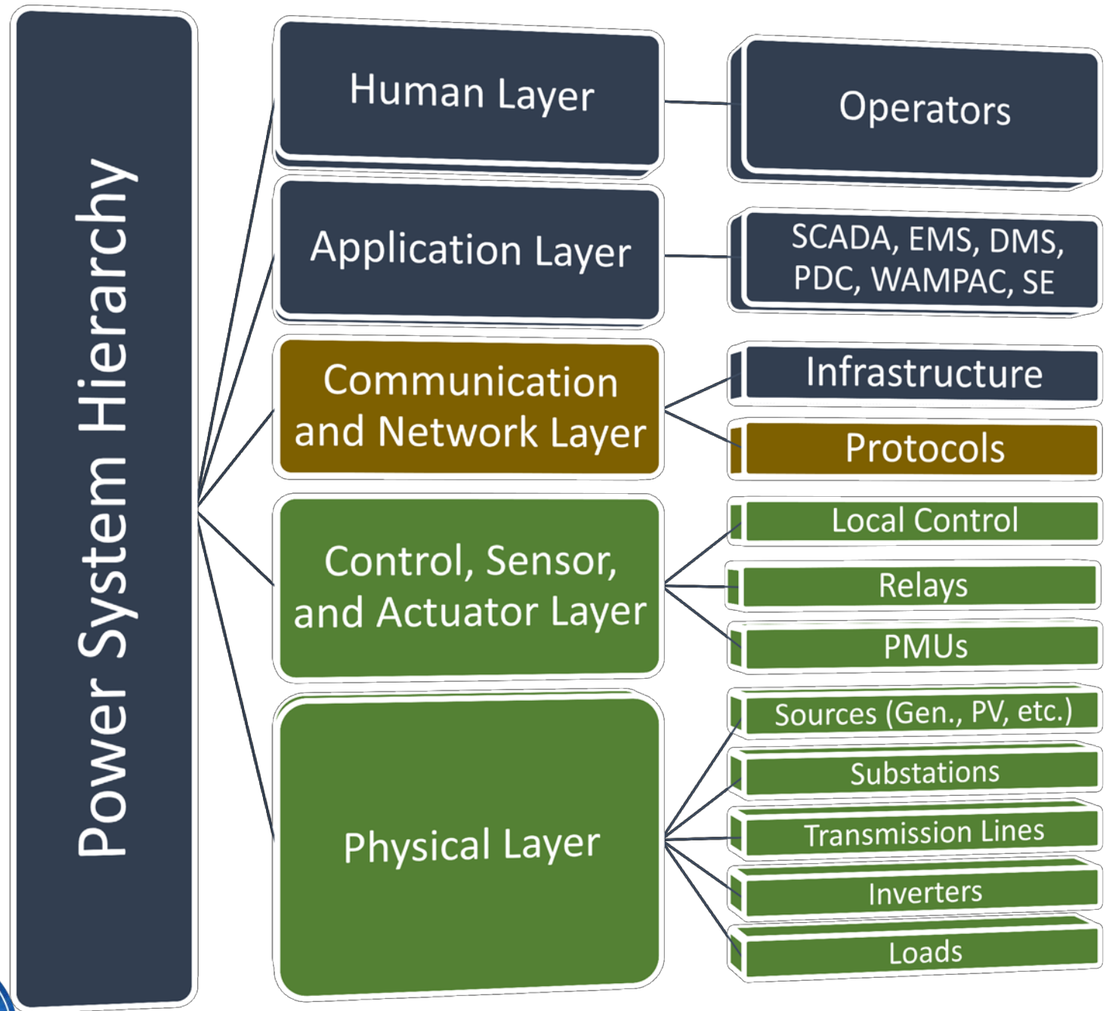
From Introduction to NISTIR 7628 Guidelines for Smart Grid Cyber Security

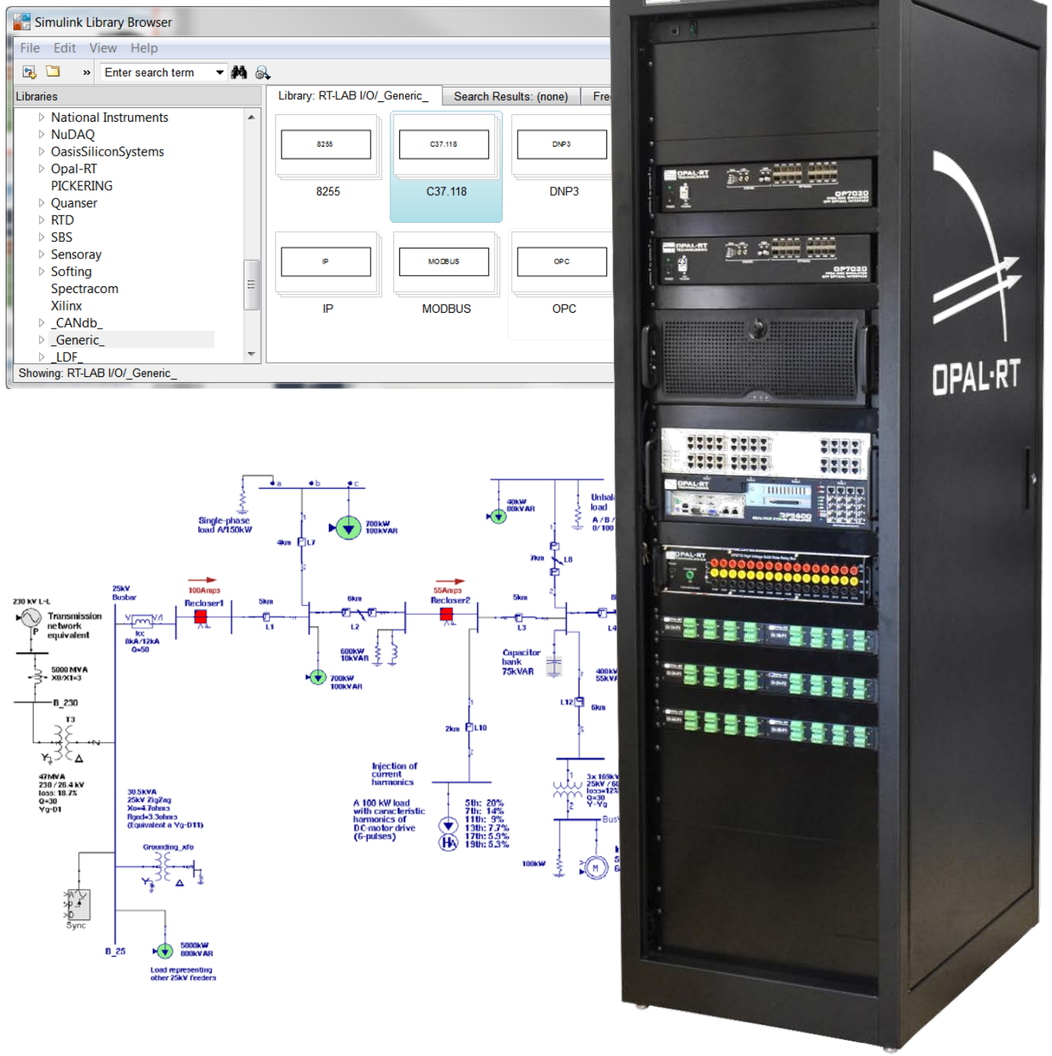
- Simulation can be used to answer these questions and assess risk
- What about real-time simulation?

Presentation Outline



Real-Time Simulation





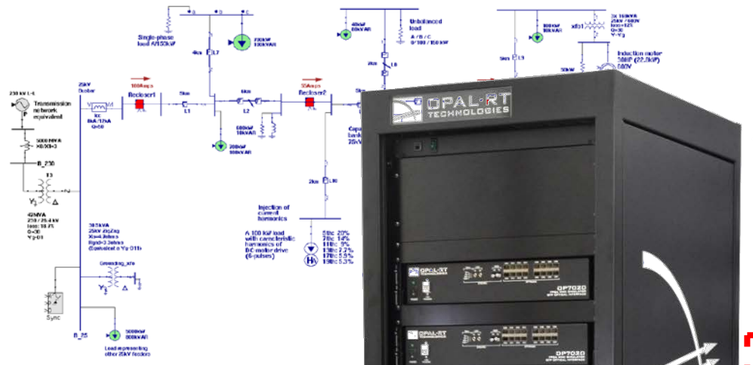
Real-Time Cybersecurity Applications

- Risk assessment studies including penetration testing, & cyber-critical asset and vulnerability identification

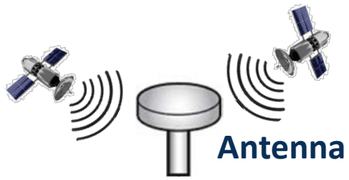
- Research & development, design and testing of:
  - Situational awareness, anomaly detection and cyber-attack mitigation systems
  - Network/communication systems
  - Control and monitoring systems (e.g. SCADA, DMS, EMS, WAMPAC)
  - Synchrophasor systems
  - State Estimators

- Meeting standards specific and related to cybersecurity, following smart grid guidelines
  - e.g. NERC CIP, NIST SGIP-CSWG, IEEE C37.118

Typical Real-Time Simulation Setup



Virtual Devices



Antenna

RF

GPS Clock

Time sync

Time sync

PMU

Analog out

C37.118

Communication Network

IEC61850 SV, GOOSE

Analog out

Relay

Digital Comm

Analog, Digital IO

Controller

Modbus, DNP3, etc.

To & From Virtual Devices
Commands, Status

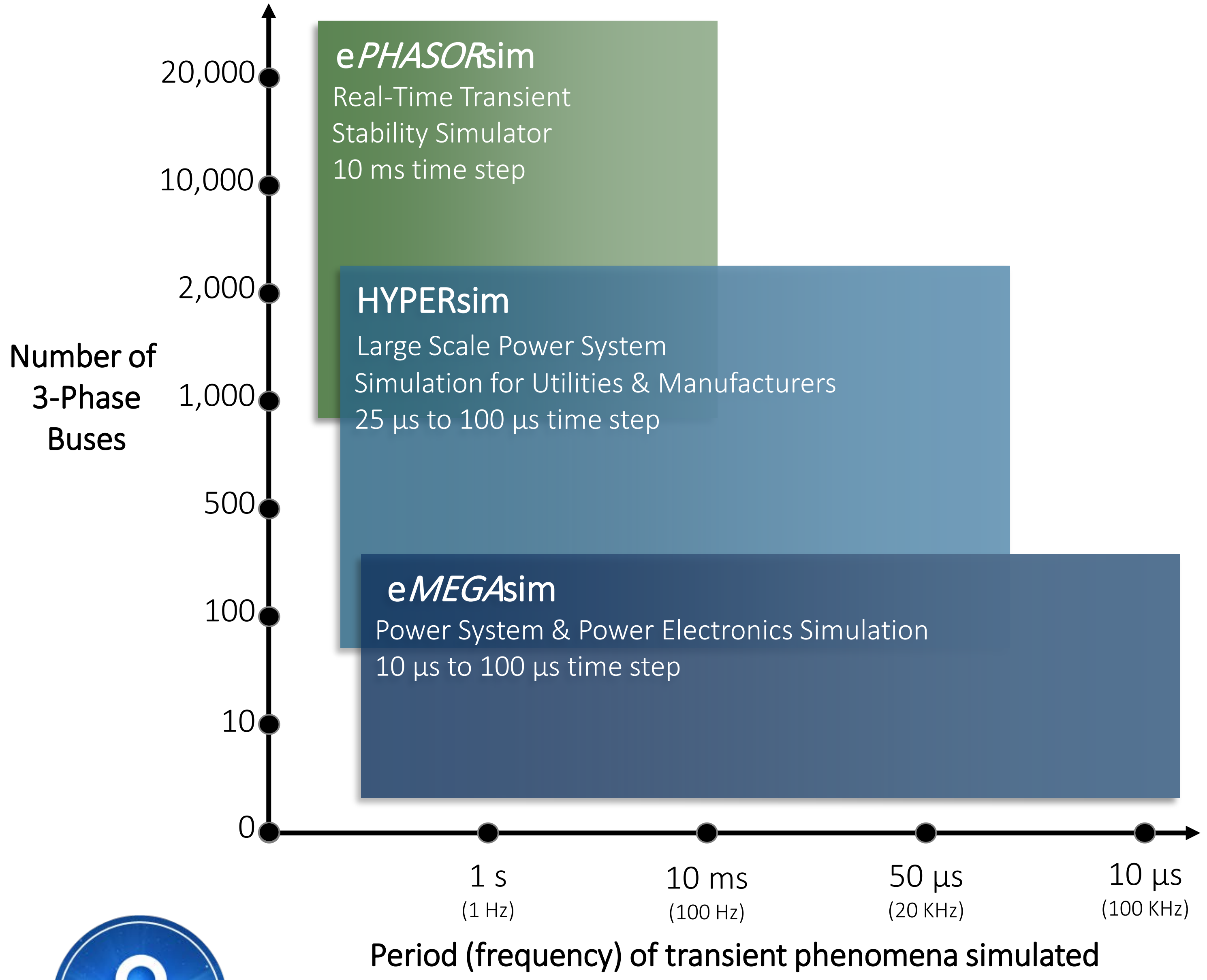
Power Amplifier

Synchropasors

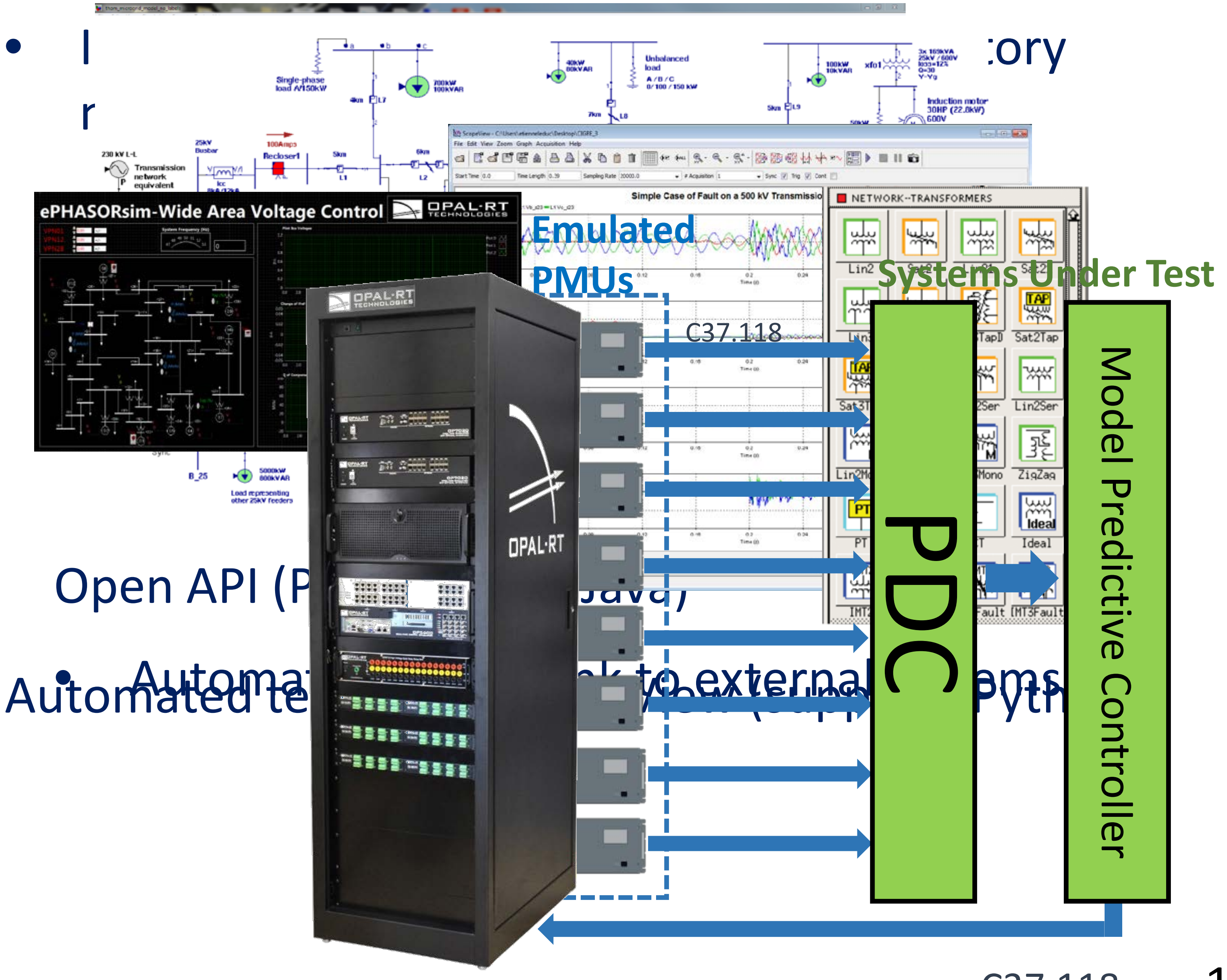
Phasor Data Concentrator(PDC)

Control Center: Control, Applications and HMI

Software Solutions

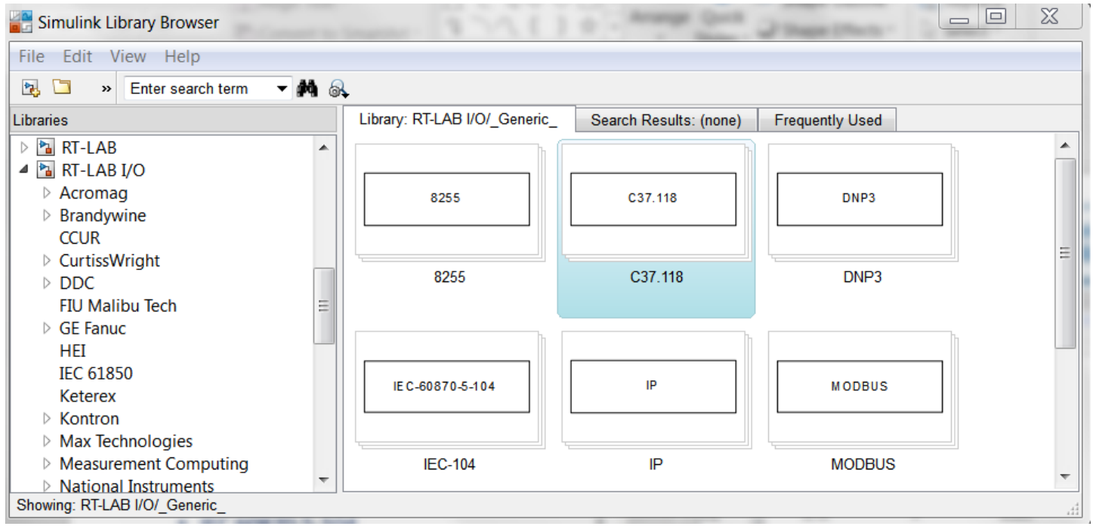


- Detailed Large-Scale Power System software developed by Hydro-Québec
- Phasor-based real-time simulation software for very large
- Based on MATLAB/Simulink & SimPowerSystems
- I ... tory r
- Open API (P... Java)
- Automated te...
- Automat... k to external ... ems

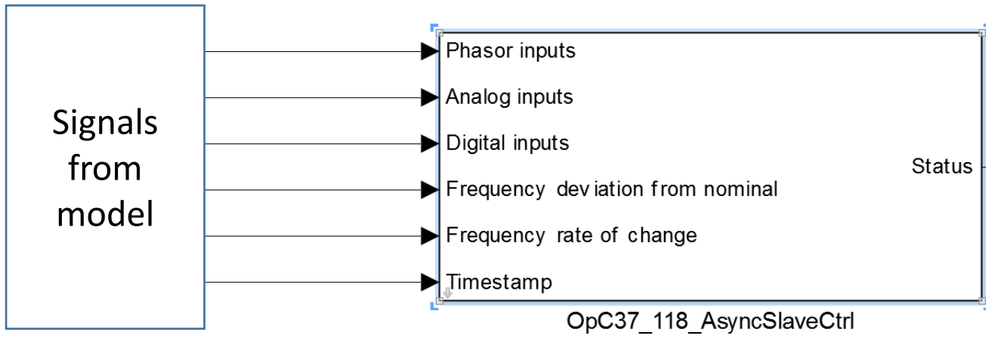


Communication Protocols

- Protocol support for smart grid applications:
  - IEC61850-8-1 GOOSE
  - IEC61850-9-2 Sampled Values
  - C37.118
  - MODBUS
  - DNP3
  - IRIG-B and 1 PPS Sync
  - IEC 60870-5-104
  - OPC UA Server
  - TCP/IP
  - UDP
  - RS-232, RS-422, RS-485
  - IEEE 1588

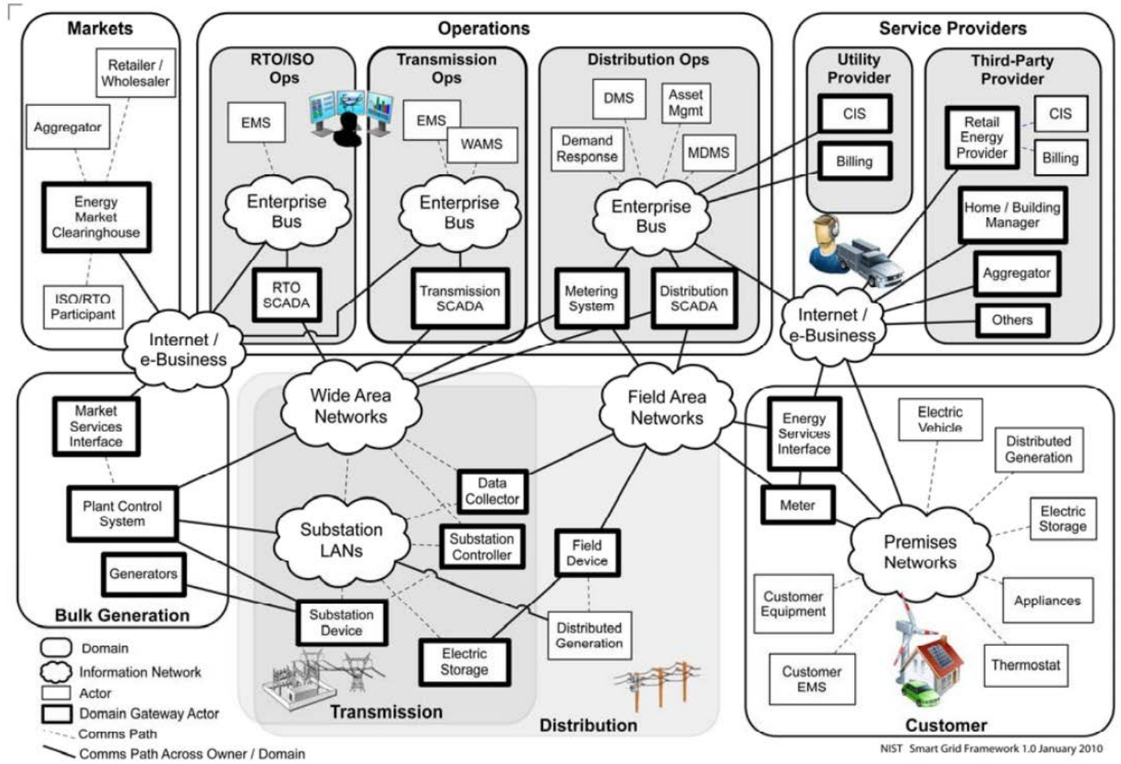


- Permits for some attacks/faults to be emulated directly within a model



Network Simulators

- Communication becoming critical component of grid along with new considerations (NISTIR 7628):
  - Cybersecurity
  - Performance: Latency, Bandwith, Processing Speed
  - Added cost



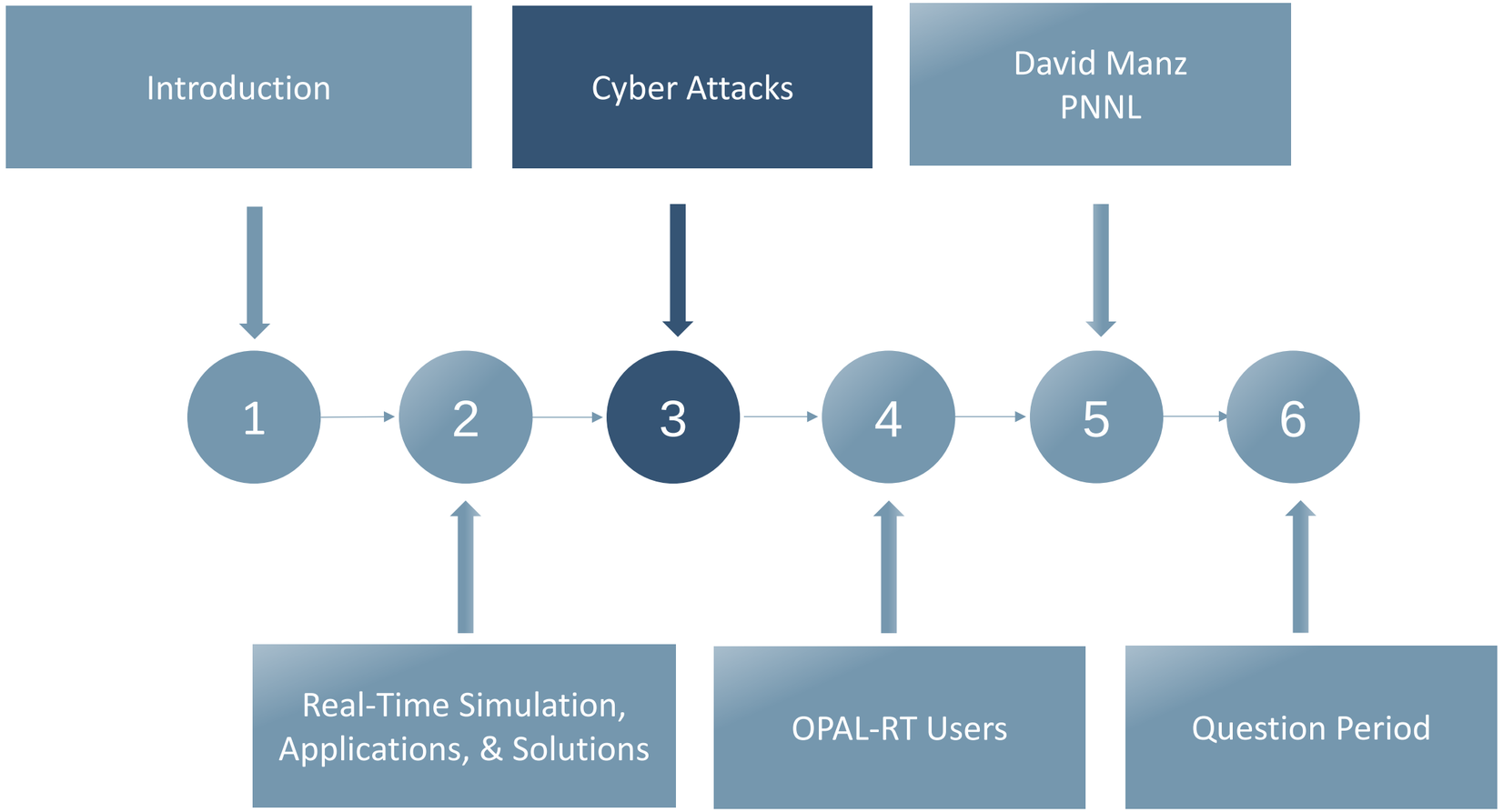
Source: NISTIR 1100

- Network simulators have been used towards real-time co-simulation of power and communication systems

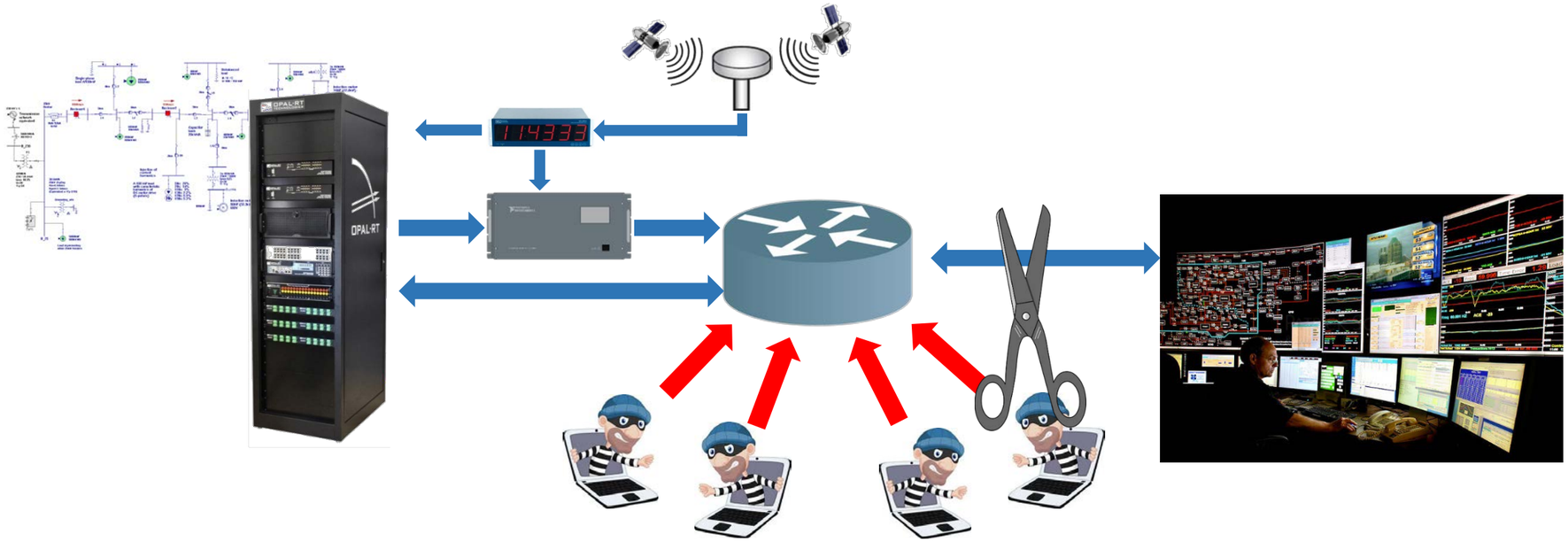
Network Simulation Tools with Real-Time Capabilities

Commercial	Free-for-use
• NetSim • Qualnet • Riverbed Modeler (formerly OPNET)	• NS2, NS3 • OMNeT++ • Kali Linux • J-Sim

Presentation Outline



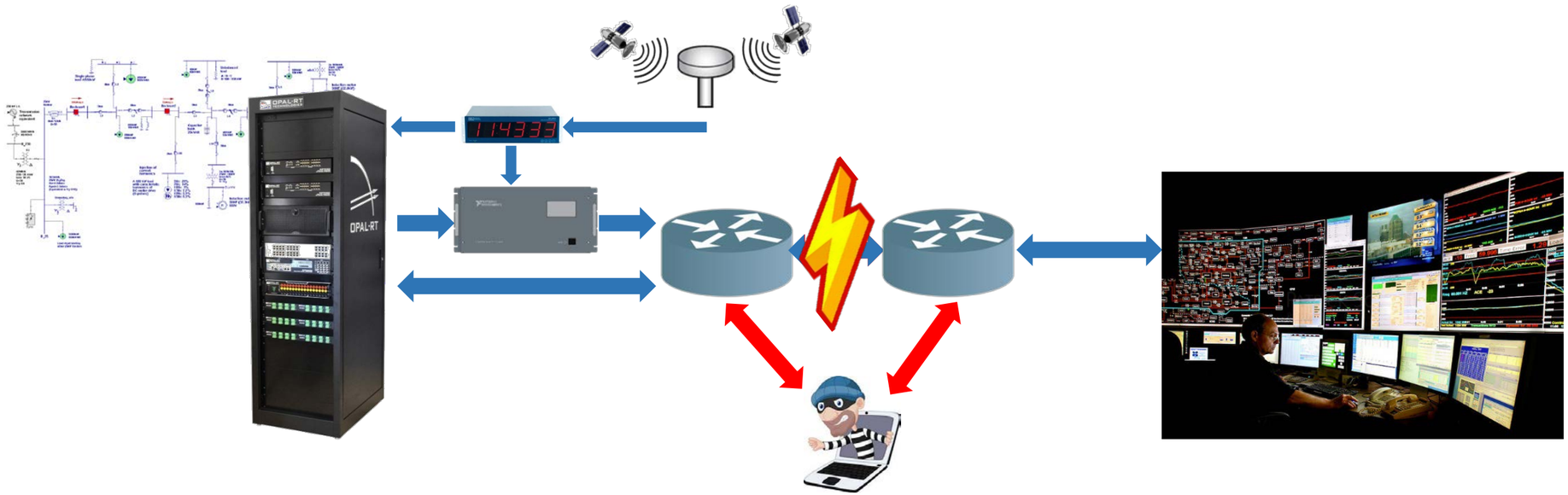
Cyberattacks: DoS



- Denial-of-Service (DoS) Attacks can render a service unavailable either through a direct or indirect attack
  - IEC61850 Goose identified as susceptible due to status numbers (Skopik & Smith 2015)
- Also refers to physical attacks on communication infrastructure
  - Cutting wires
  - Wireless jamming

Reference: Skopik F., Smith P.: Smart Grid Security - Innovative Solutions for a Modernized Grid, Elsevier Science Publishing, 2015, ISBN: 978-0-12-802122-4.

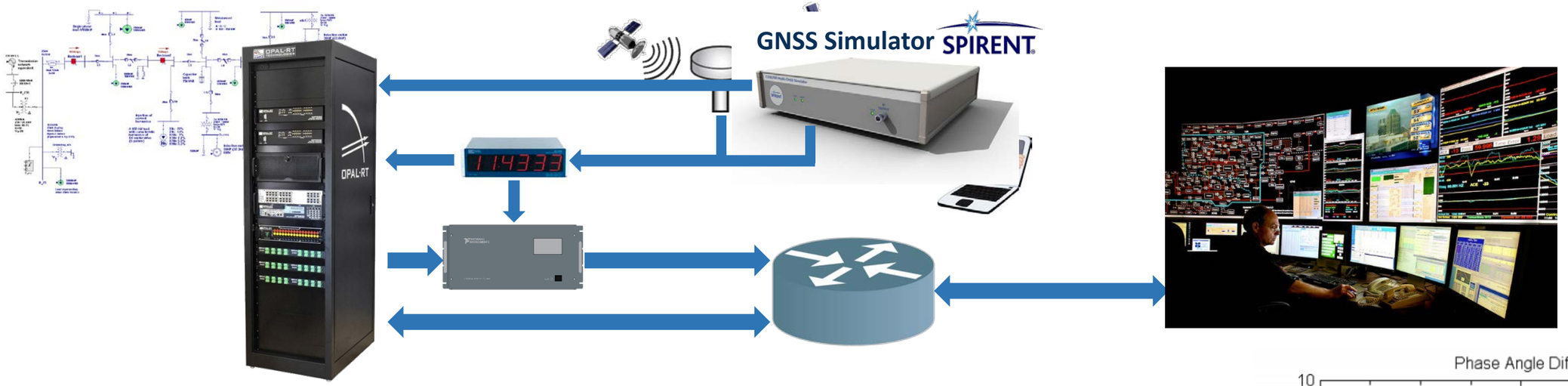
Cyberattacks : Man-in-the-Middle



- Man-in-the-middle (MitM) attacks “impersonate two communication nodes by making them believe that they are talking together” (Skopik & Smith 2015):
  - Packet injection/spoofing (IEC61850 Goose, DNP3, MODBUS),
  - Packet suppression,
  - Recording, replaying and modification of recorded packets

Reference: Skopik F., Smith P.: Smart Grid Security - Innovative Solutions for a Modernized Grid, Elsevier Science Publishing, 2015, ISBN: 978-0-12-802122-4.

Cyberattacks : GNSS Spoofing/Meaconing



- GNSS spoofing/meaconing is a threat to PMUs and synchrophasor systems, heavily reliant on time synchronization
  - For 60 Hz networks, IEEE C37.118-2014 Standard allows max 26.53 µs pure timing error

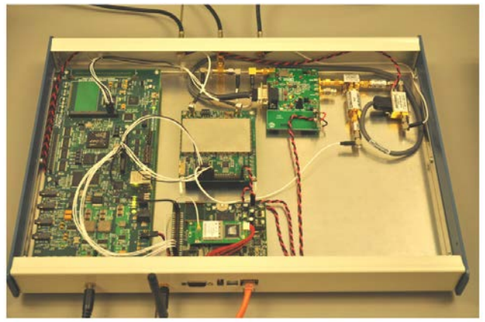
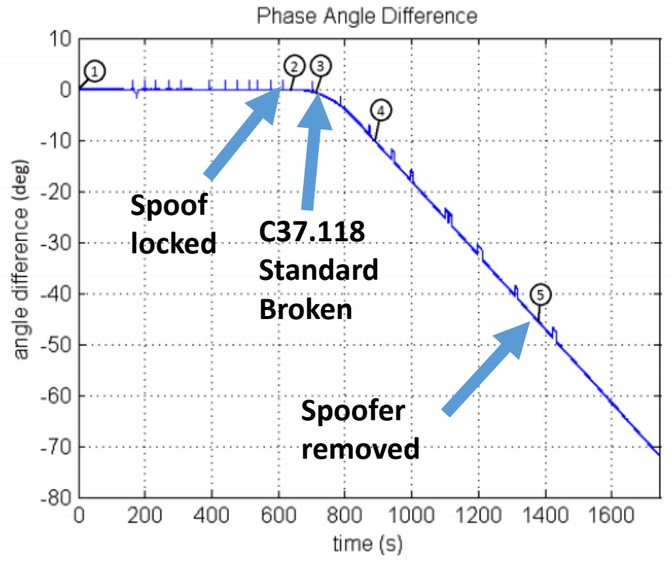
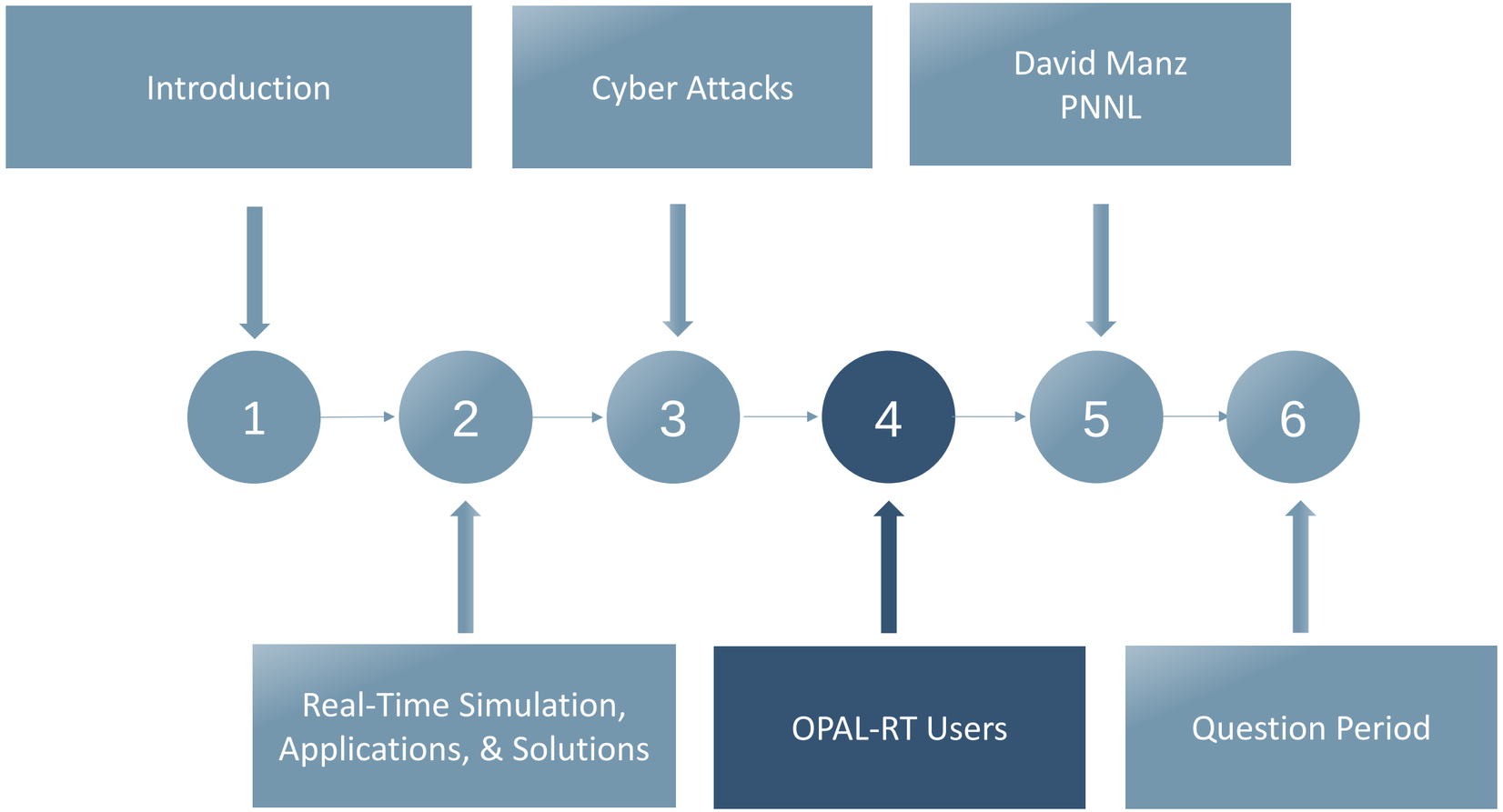


Fig. 1. The Civil GPS Spoofer.

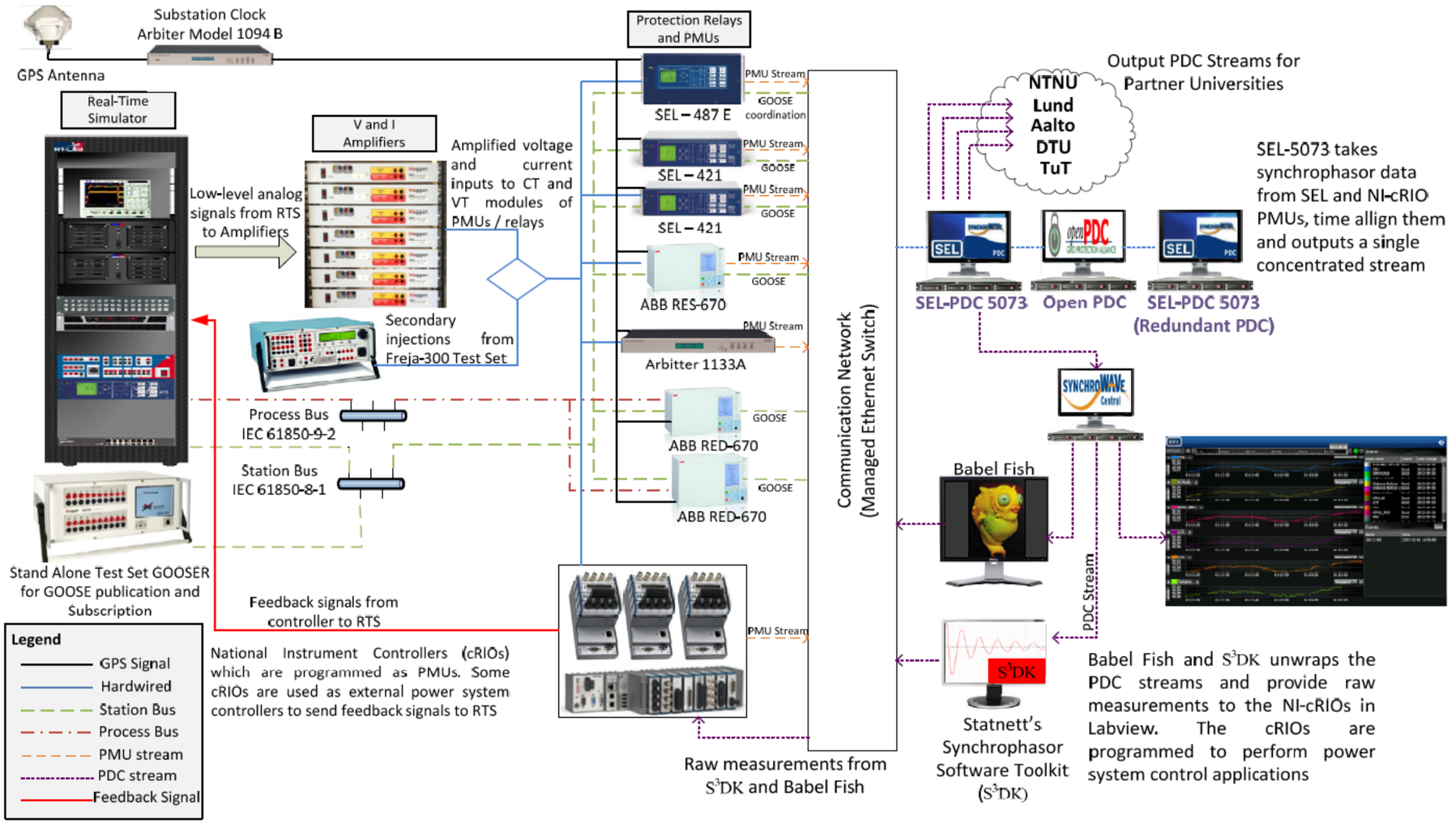


D. P. Shepard, T. E. Humphreys, and A. A. Fansler, "Evaluation of the vulnerability of phasor measurement units to GPS spoofing attacks," International Journal of Critical Infrastructure Protection, vol. 5, no. 34, pp. 146–153, 2012.

Presentation Outline

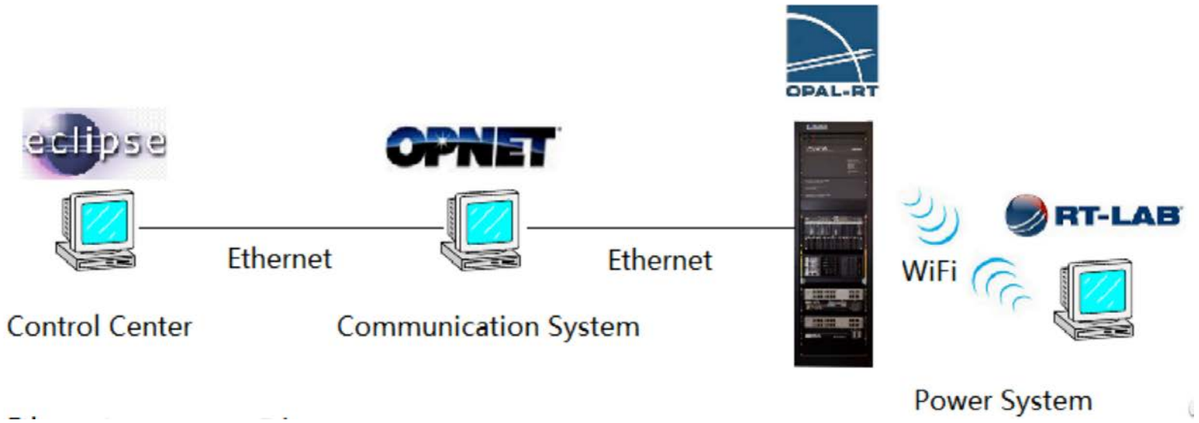


- Comprehensive WAMPAC Test Bench

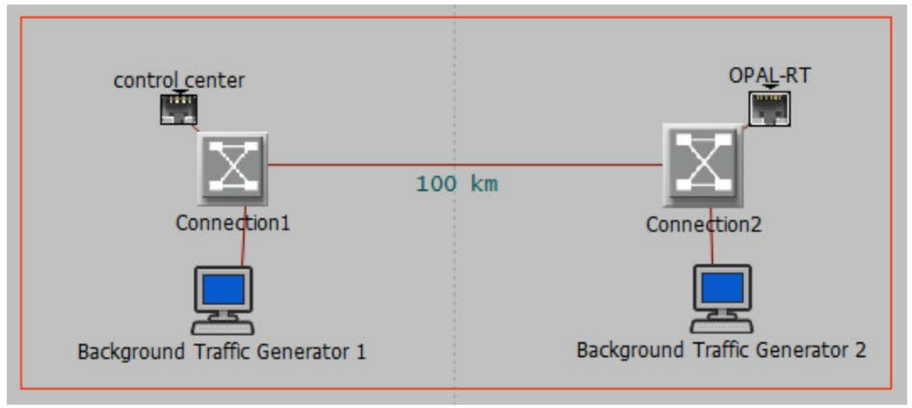


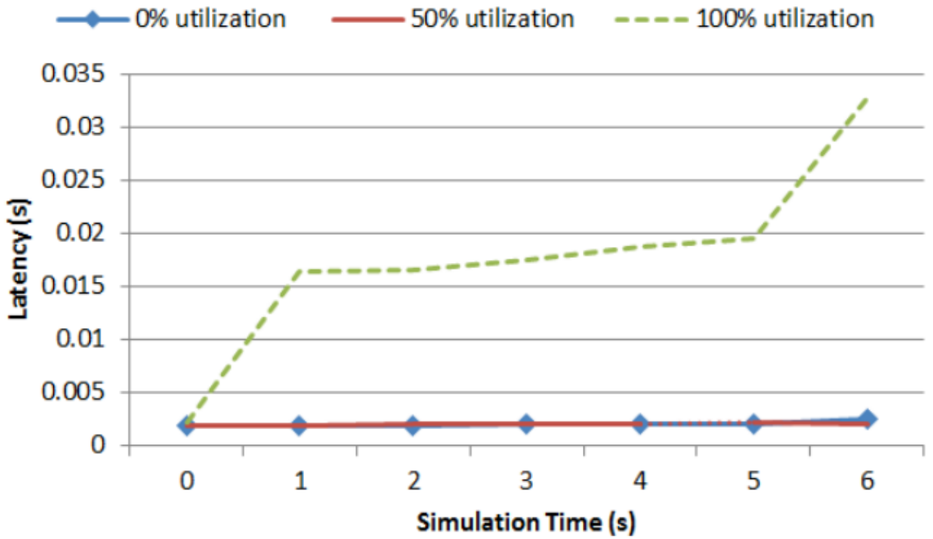
Almas, M.S.; Baudette, M.; Vanfretti, L; Lovlund, S; "Synchrophasor network, laboratory and software applications developed in the STRONg²rid project," 2014 PES General Meeting & Conference & Exposition, Wahsinton, USA, 27-31 July 2014

Virginia Tech University



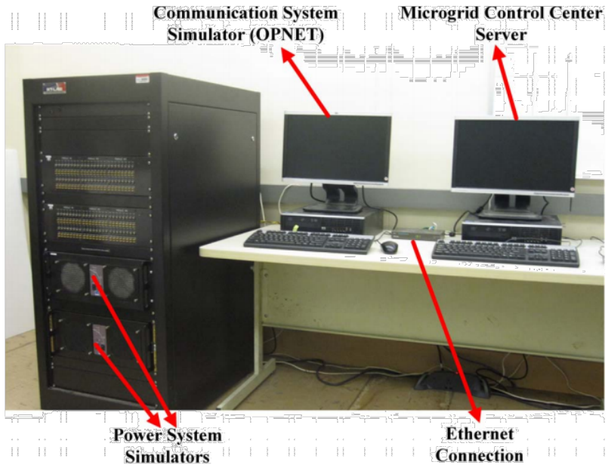
- Smart grid communication system performance testing
- OPNET uses to simulate smart grid traffic

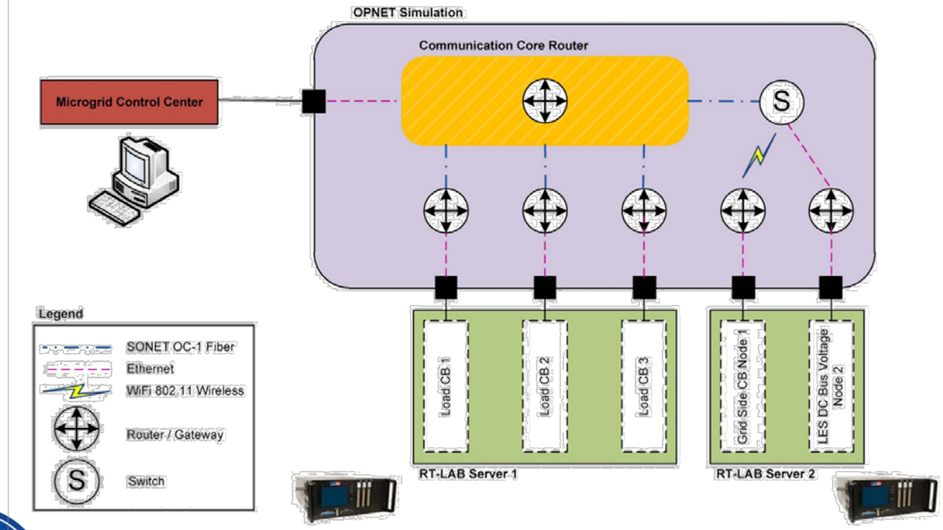




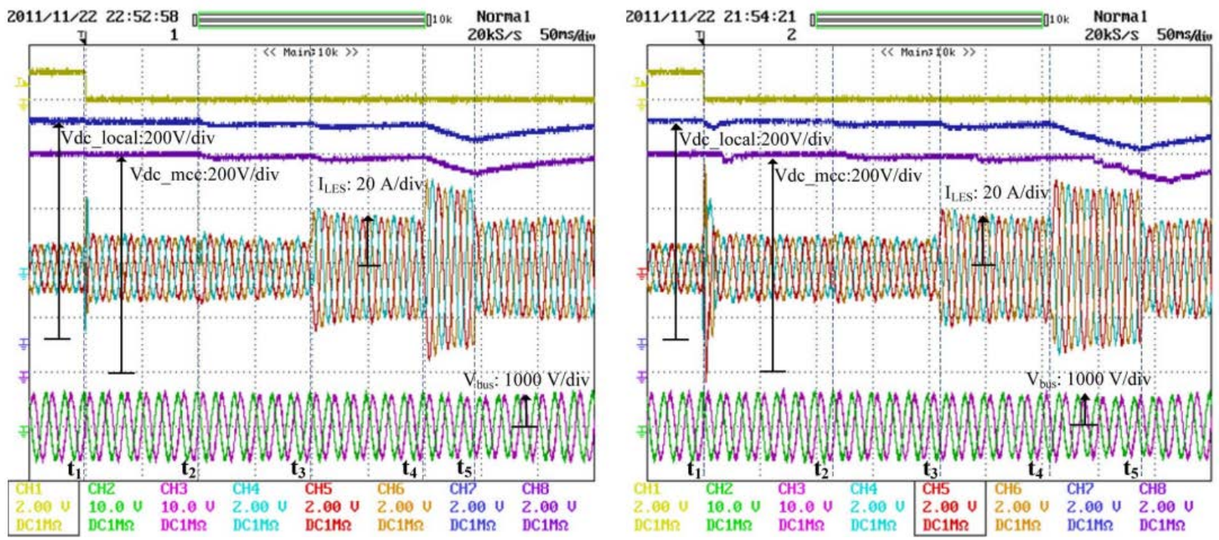
D. Bian, M. Kuzlu, M. Pipattanasomporn, S. Rahman, Y. Wu, Real-time co-simulation platform using OPAL-RT and OPNET for analyzing smart grid Performance, Power & Energy Society General Meeting, 2015 IEEE, 1-5

Ohio State University





- Microgrid power and communication systems co-simulation
- Results show that communications have a significant effect on system dynamics



F. Guo, L. Herrara, R. Murawski, E. Inoa, C. Wang, P. Beauchamp, E. Ekici, J. Wang. Comprehensive Real-Time Simulation of the Smart Grid, IEEE Transactions on Industry Applicatio, Vol. 49, No. 2, 2013

University of South Florida

- Smart Grid Power Systems Lab (SPS) uses OPAL-RT to model power grid and PMUs in SCADA Testbed for research validation:
  - Cybersecurity,
  - Communication,
  - Grid visualization,
  - Power system control and optimization

- Simulator connects to OSIsoft PI Server IEEE-C37.118 to PI Server to send data and receive commands

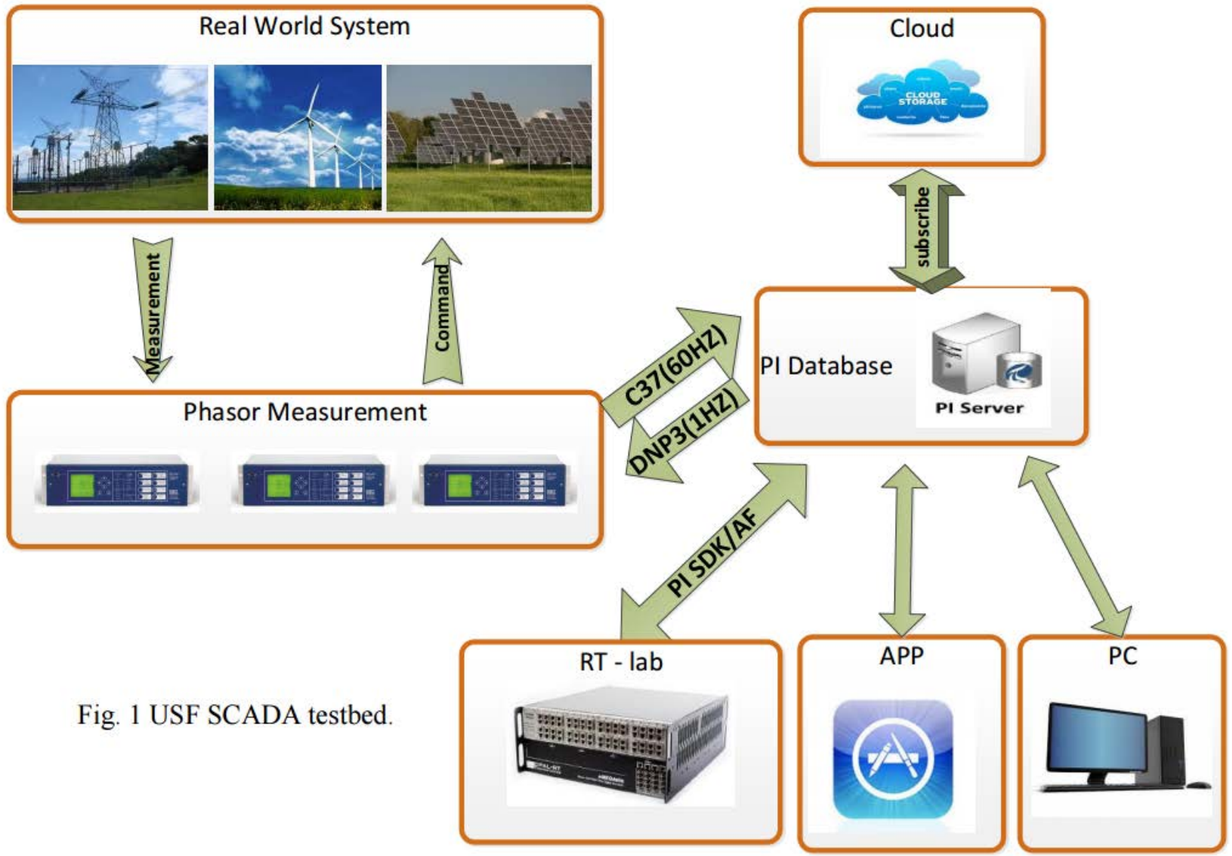
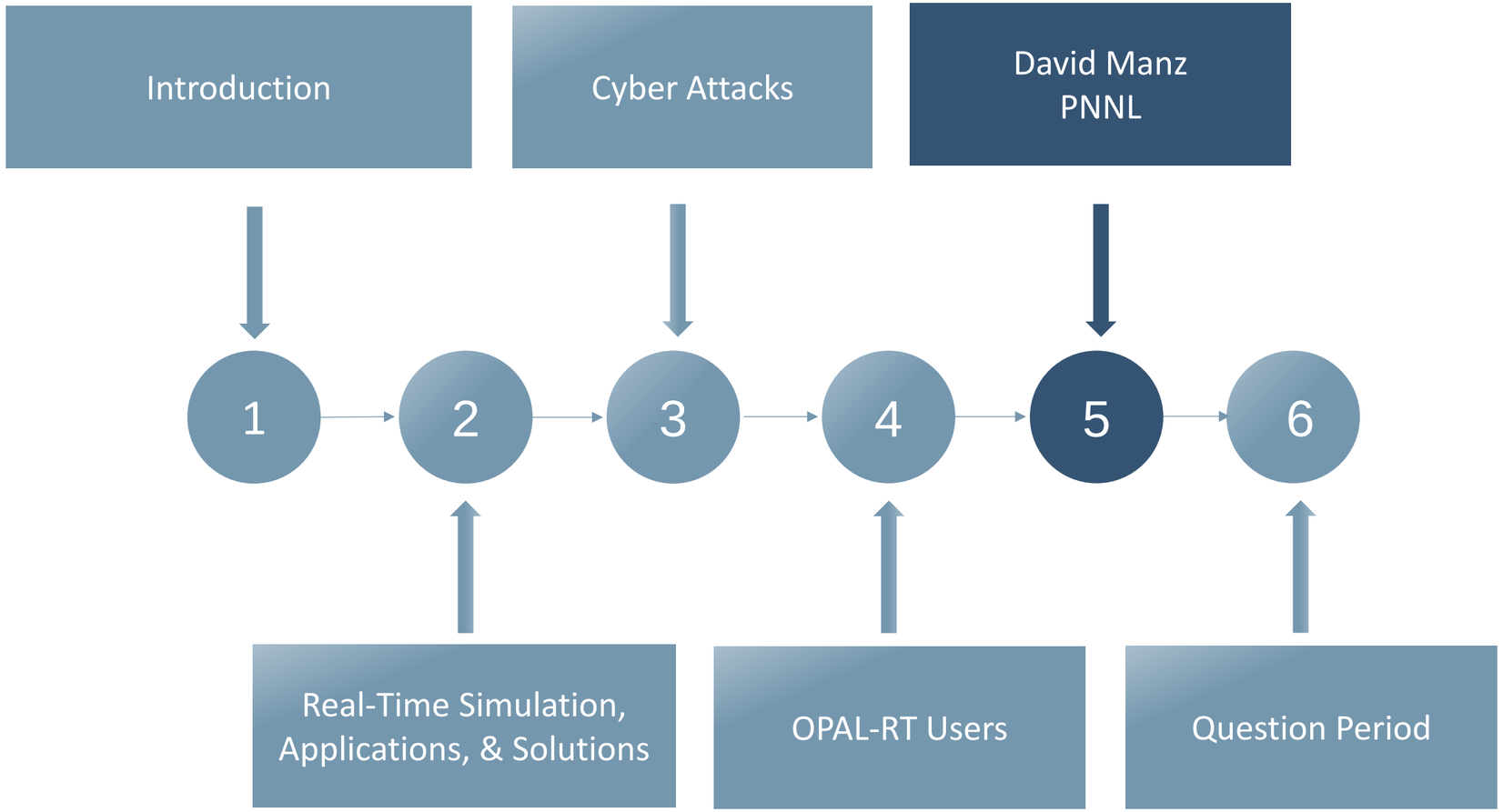


Fig. 1 USF SCADA testbed.

Fig. 1: USF SPS's SCADA testbed.

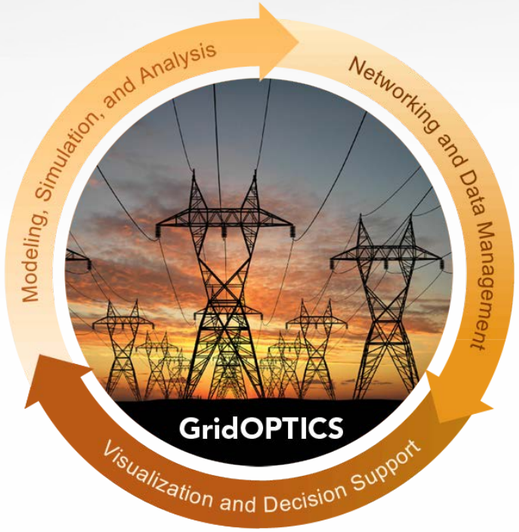
H.G. Aghamolki, Z. Miao, L. Fan. A Hardware-in-the-Loop SCADA Testbed, North American Power Symposium (NAPS), 2015

Presentation Outline



Pacific Northwest
NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965

Cyber-Physical Security Research, Experimentation and Applications



David Manz, PhD

Pacific Northwest National Laboratory

Richland, WA

powerNET
What is it?

Pacific Northwest NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965

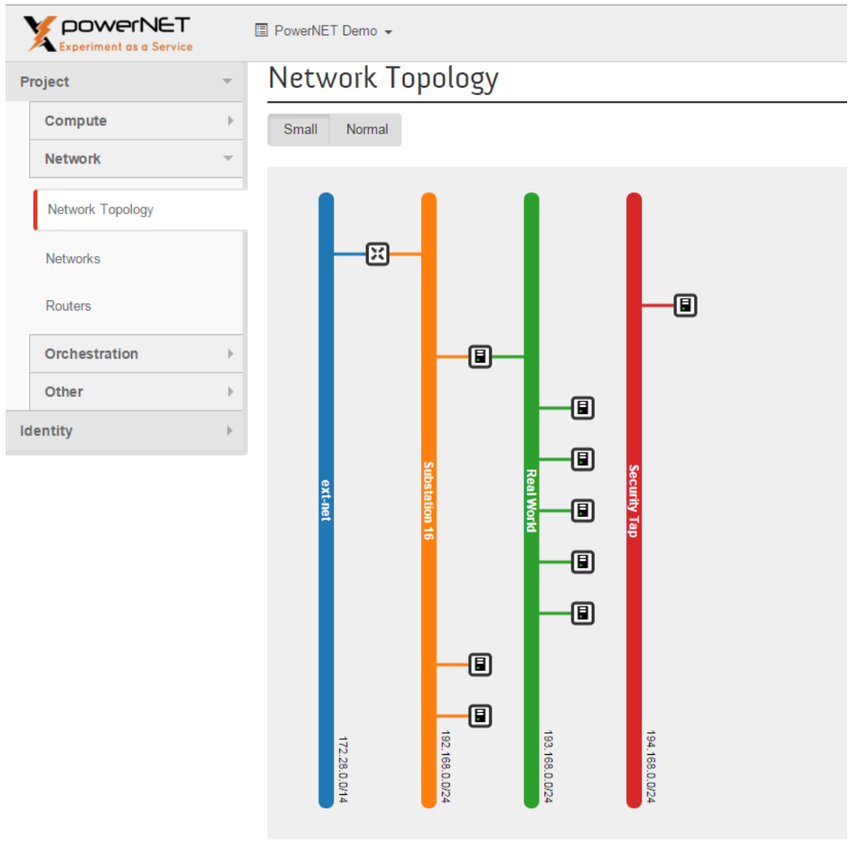
- Multi-user power system testbed
  - Sandbox environment
- Experiment based
  - Access controls by project/user
- Auto-configuration
  - Built upon cloud technology
- Remote access
- Scalable
  - Emulation and simulation
- User friendly
  - Configuration/monitoring portal
  - Common library of scenarios

What is it?

- Modular and extendable
  - Support for multiple cyber physical industries
  - Federation with internal and external testbeds and resources
- Current capacity
  - 2-3 projects at once
- Vision
  - National user facility

Facilities

- **Cloud technology based orchestration with web based user portal**
- **Network Emulation**
  - Emulate LAN/WAN communication characteristics. Examples:
    - Dedicated Line
    - Dial-up
    - Wireless
- **SCADA environments**
  - Real equipment to model ~2 substations
  - Software simulation of dozens of SCADA equipment
  - Support for legacy communications



Facilities Cont.

- **Physical Process Emulation** OPAL-RT
  - Hardware-in-the-loop modeling
  - Large scale simulation
- **Synchrophasors**
  - 9 PMU from variety of vendors
    - 1 PMU Development Platform
  - 1 Hardware PDC
    - (Many software PDC possible)
- **Up to ~1000 general purpose virtual nodes possible**
  - XenServer hypervisor
- **Energy Management System**

Testbed Uses

- Validation and verification
- Technology assessment and prototyping
- Simulation and modeling
- Training and education
- Demonstration (with PNNL EIOC)

Research Topics

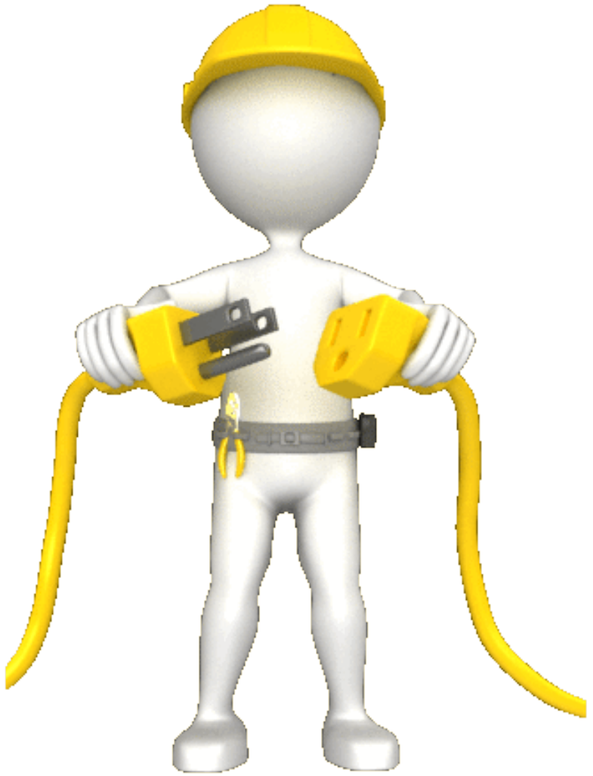
Pacific Northwest NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965

- Cyber security
- Cyber-physical system
  - Cyber impact/interaction on physical processes
- Distributed applications
  - Smart Grid
- Interoperability testing
- Application prototyping

powerNET Usage Examples

Pacific Northwest NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965

- Gridlab-D Analysis Project
- FPGI: A Distributed Systems Architecture for the Power Grid
- CEDS Digital Ants
- IEC 61850/62351 Interoperability Testing
- SCADA network determinism
- Cyber-Physical Training
- DHS Cyber-Physical Federation Demonstration



powerNET Testbed Benefits

Pacific Northwest NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965

- Multi-user shared facility and equipment
- Time and resource efficient
- Dynamically configurable
- Remote access
- Test wide scale federation of testbeds and understand associated management and security concerns
- User benefits:
  - Researchers: Efficiency, Realistic Sandbox
  - Industry: Conformance and Interoperability testing
  - Academia: Hands-on Education

cyberNET

- Peer Capability
- Model and emulation enterprise environments
  - Enterprise services
  - User modeling and simulation
- Federate resources for bigger experiments
  - IT and OT joint experiments

cyberNET

Experiment as a Service

powerNET Video

Question Period

Thomas Kirk
514-935-2323
thomas.Kirk@opal-rt.com

David Manz
509-372-5995
david@pnnl.gov

Thank you!

Our new Cybersecurity webpage is now online:

http://www.opal-rt.com/cybersecurity

For a one-on-one demo or any additional questions you might have:

http://www.opal-rt.com/contact-opal-rt

Visit our event page to view where to meet OPAL-RT Technologies:

http://opal-rt.com/events

The content of this webinar will be available shortly on:

http://opal-rt.com/events/past-webinars

Quick Survey as you leave!

Join the Conversation!
"Real-Time Simulation with OPAL-RT"