Energy Systems
Innovation Center

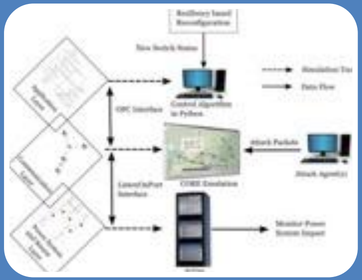
Cyber-Physical Resiliency Experimentation using RTDS

Venkatesh Venkataramanan,
Anurag Srivastava, and Adam Hahn
Smart Grid Demonstration and Research Investigation Lab (SGDRIL)
Energy System Innovation Center
Washington State University
Contact: anurag.k.srivastava@wsu.edu

WASHINGTON STATE UNIVERSITY
World Class. Face to Face.

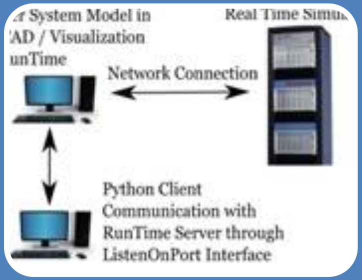
SGDRIL
Smart Grid Demonstration & Research Investigation Lab, Washington State University, Pullman

Outline



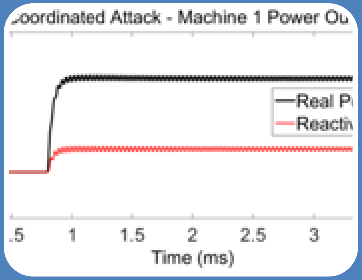
Challenges with Cyber-Physical Testbed

- Why Ad-hoc testbeds?
- Interfacing challenges



Interfacing Techniques

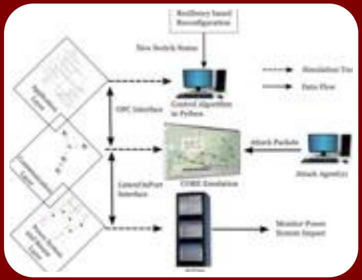
- Power – Cyber Interface
- Communication – Security Interface



Case Studies

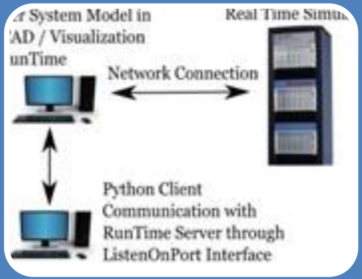
- Simulation Cases and Discussion

Outline



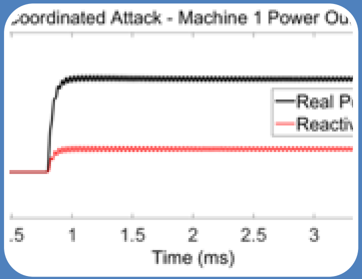
Challenges with Cyber-Physical Testbed

- Why Ad-hoc testbeds?
- Interfacing challenges



Interfacing Techniques

- Power – Cyber Interface
- Communication – Security Interface



Case Studies

- Simulation Cases and Discussion

Why Cyber-Physical Security?

THE WALL STREET JOURNAL.

Home World U.S. Politics Economy Business Tech Markets Opinion Arts Life Real Estate

U.S.

Cyberattacks Raise Alarm for U.S. Power Grid

Experts believe Russian hackers linked to the DNC breach are also behind attacks on utilities in Ukraine and U.S., leaving domestic power grid exposed

By Rebecca Smith

Dec. 30, 2016 12:58 p.m. ET

Bloomberg Markets Markets Tech Pursuits

U.S. Grid in 'Imminent Danger' From Cyber-Attack, Study Says

by **Ari Natter** and **Mark Chediak**

January 6, 2017, 7:40 AM PST *Updated on* January 6, 2017, 12:37 PM PST

fedscoop

DEFENSE ACQUISITION WATCH LISTEN

TECH

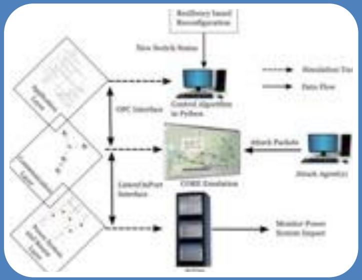
Energy Department warns of 'imminent' cyberattack on power grid

Don't trust the news?
Even DOE says it's true!

Challenges in CPS Testbed

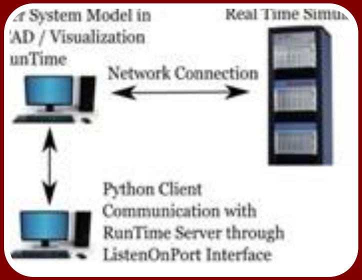
- Simulators talk different languages
- Operating in real time – coordination between simulators
- Mimic real system – or use real or
    - substation protocols
    - controller designs
    - data flow paths
- Flexible to test diverse set of applications
- Include all layers – power system, communication system, and control system
- Testbed must allow end to end testing meeting time requirement
- Ability to model cyber security

Outline



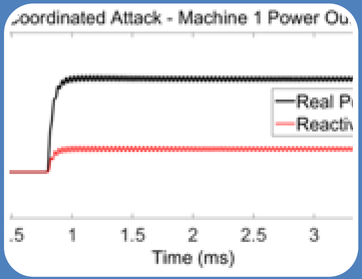
Challenges with Cyber-Physical Testbed

- Why Ad-hoc testbeds?
- Interfacing challenges



Interfacing Techniques

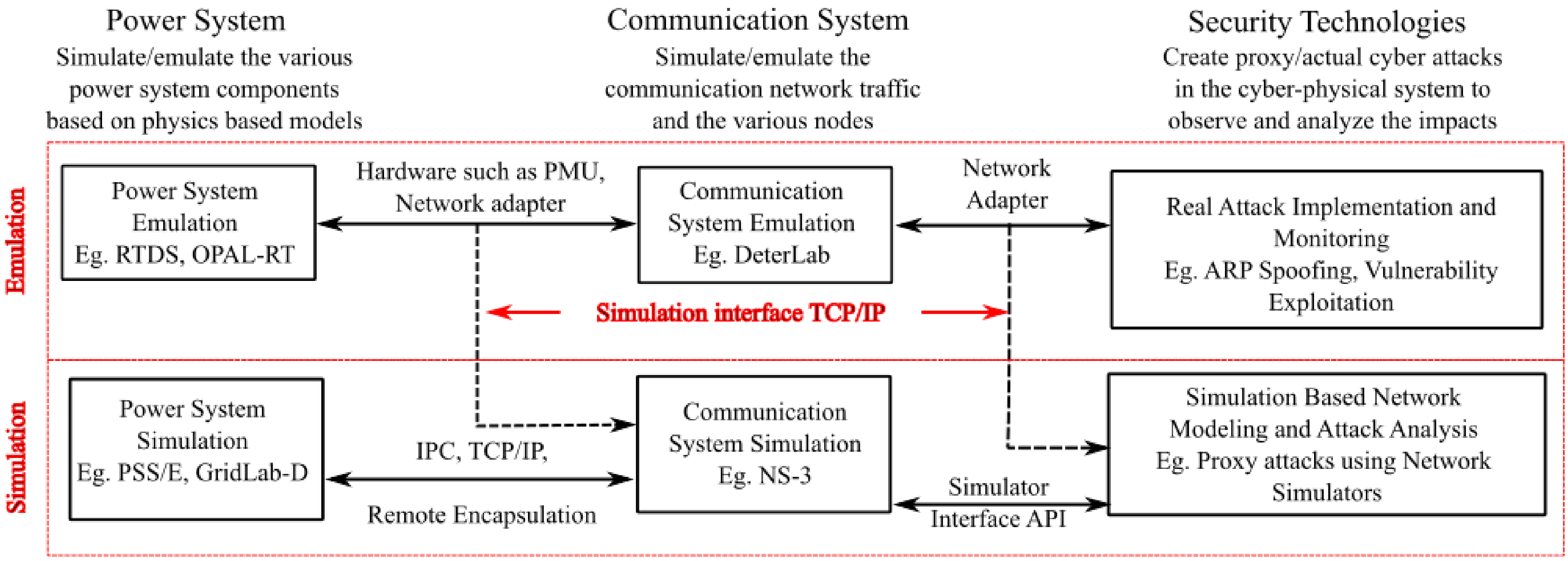
- Power – Cyber Interface
- Communication – Security Interface



Case Studies

- Simulation Cases and Discussion

Overview of Interfacing Techniques and Tools



Tools

Power System

- Real-Time emulation tools including RTDS and OPAL-RT

Communication System

- Emulation tools such as CORE, DeterLab

Security Tools

- Device and host level attack implementation and analysis

TCP/IP, Remote Encapsulation, Hardware

TCP/IP, libpcap, attack libraries

- Offline simulation tools

- Simulation tools such as NS-3, Mininet

- Network level simulation of attacks

IPC, TCP/IP, Remote Encapsulation

Proxy interface, attack implementations

Power – Cyber Interface

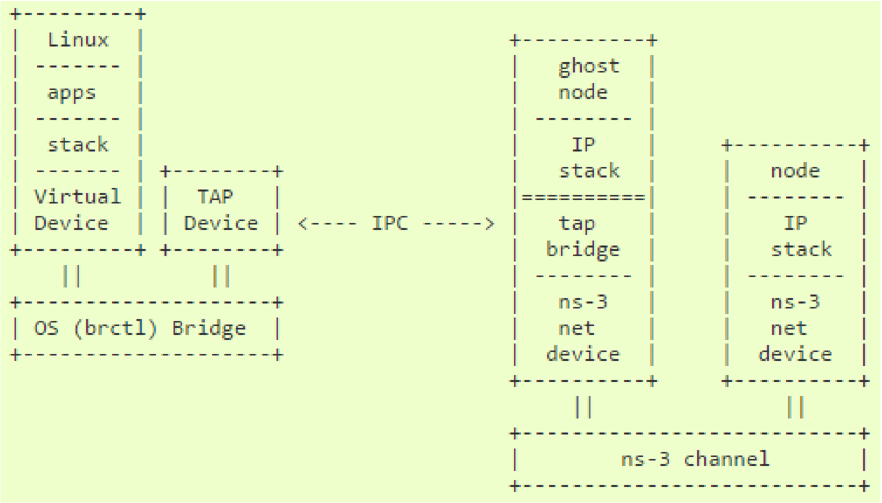
- Interfaces can be broadly classified into simulation and emulation interfaces
- Emulation interfaces tries to mimic the real system by using actual devices wherever possible – which enables the test to be more accurate
- Simulation interfaces hardware based methods are not typically used, but they are easier to set up, and data transfer methods enable to test various cyber-attack scenarios

Power – Cyber Interface

- Emulation using Power System Hardware
  – Devices such as PMUs are used by exporting analog signals from power system simulator
  – Signal sent to CT/PT → PMU → PDC
- Emulation using Network Card
  – RTDS offers GTNET cards, which samples the analog waveforms generated
  – Phasors are estimated similar to actual PMU devices

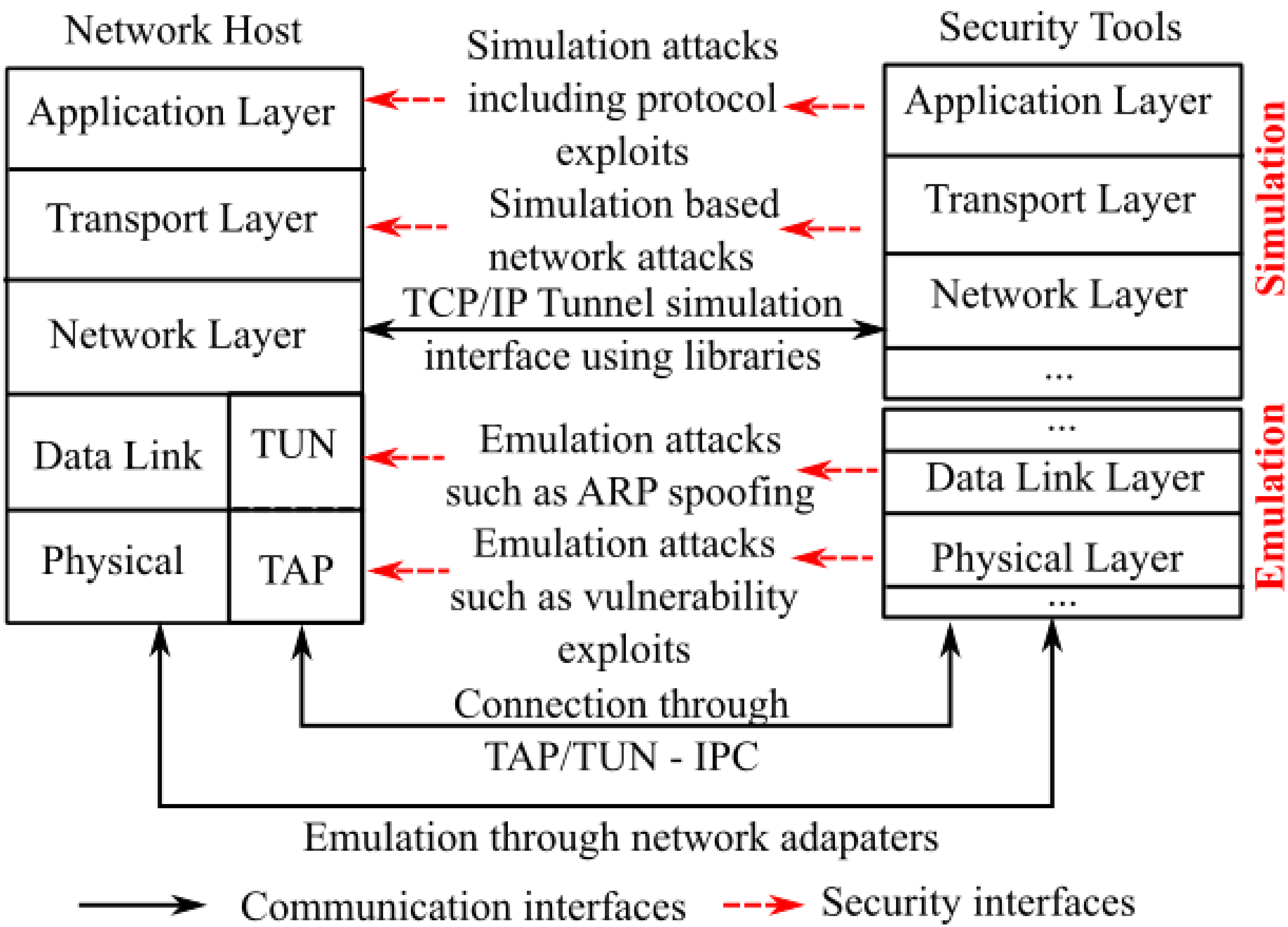
Power – Cyber Interface

- Simulation based interface using IPC
  - Virtual devices called Tap/Tun are used
  - Signal is sent from power simulator to these virtual devices



- Simulation based interface using TCP/IP
  - TCP/IP can be used for both local and remote connections to exchange data between simulators
  - Data can be wrapped in protocol of choice (ex. CORE), or transferred via SSH for remote connections (ex. DeterLab)

Communication – Security Interface



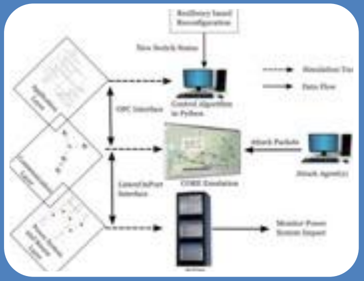
Communication – Security Interface

- Emulation Environment Attack Implementation and Analysis
  - Model closely resembles actual field – provides increased attack surface to study various attacks
  - Various network monitoring tools such as Wireshark can be used, as well IDS tools such as Bro and Snort
  - Detailed attack implementations require exploiting vulnerabilities to gain access to the network, and then using security tools such as those offered by Kali Linux, or etttercap to implement cyber-attacks

Communication – Security Interface

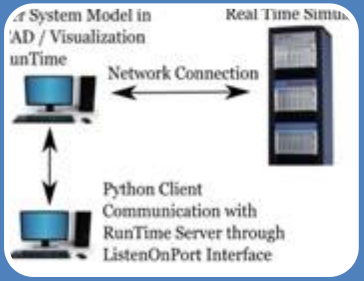
- Simulation Environment Attack Implementation and Analysis
  - Modeling is focused on determining the effect of the cyber attack on the power system
  - Measurements from the power system tool is transferred to the communication layer using TCP/IP
  - Detailed implementations are not present, such as device kernels, memory management for the network hosts etc.
  - Simulation provides convenience for studying common network scenarios such as latency, dropped or missed packets, etc.

Outline



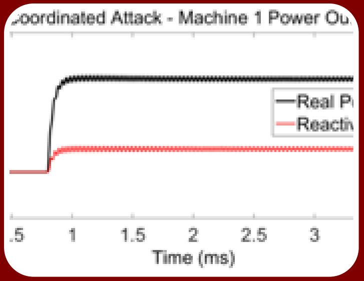
Challenges with Cyber-Physical Testbed

- Why Ad-hoc testbeds?
- Interfacing challenges



Interfacing Techniques

- Power – Cyber Interface
- Communication – Security Interface



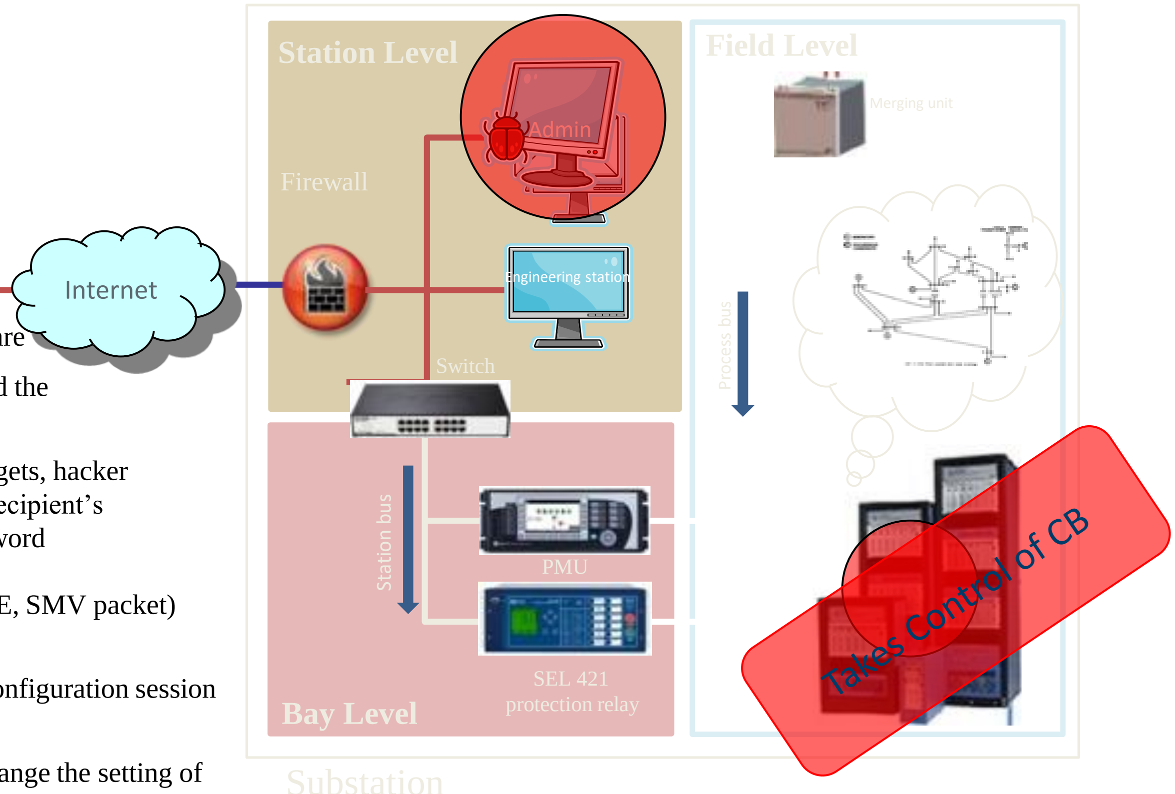
Case Studies

- Simulation Cases and Discussion

Example Case Studies

- Case Study#1: Cyber-physical analysis for failure diagnosis in protection system
- Case Study#2: Cyber-Physical analysis for distributed control and optimization
- Case Study#3: Cyber-Physical Resiliency Analysis for Microgrid

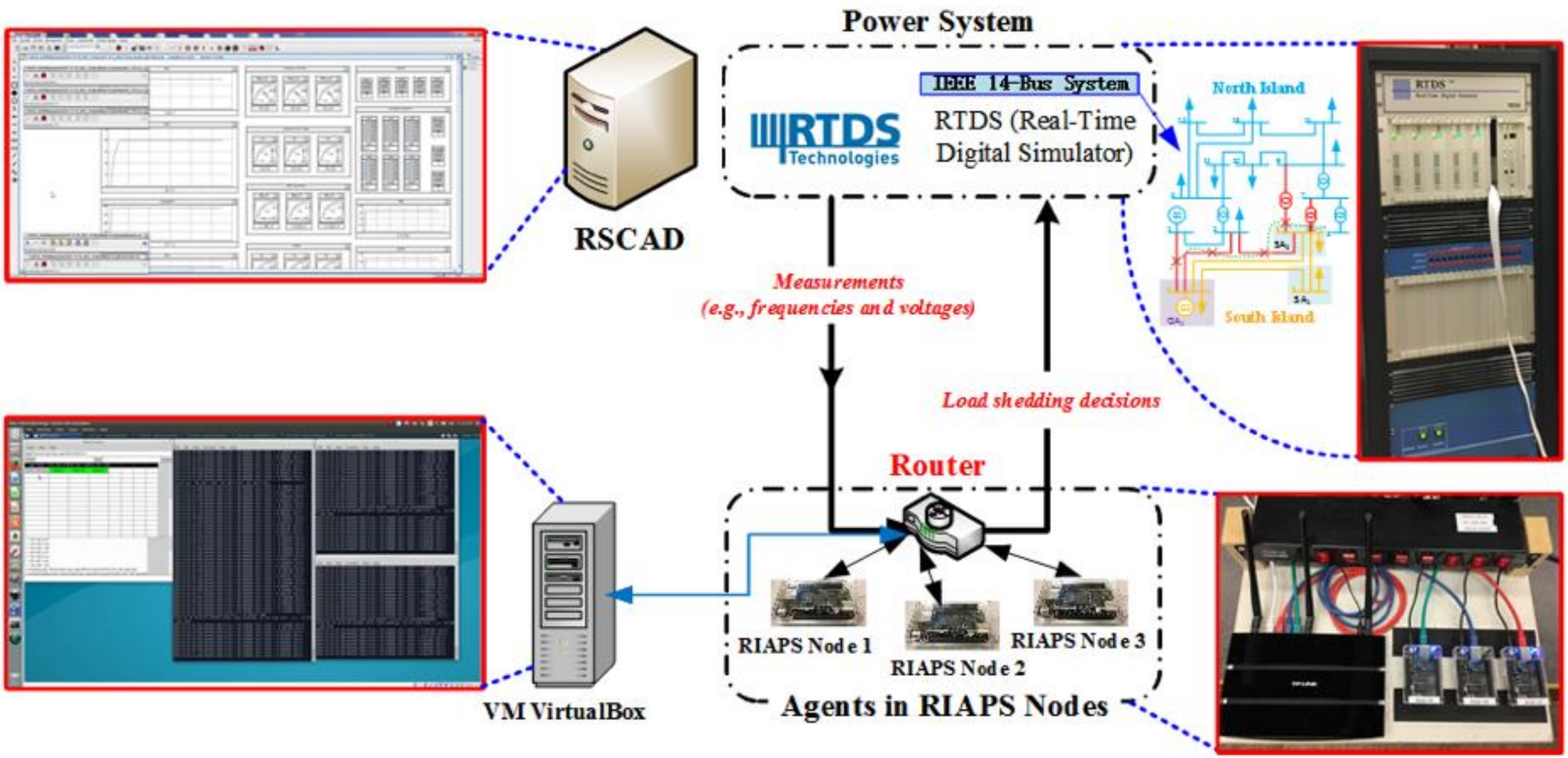
Use Case#1: Simulating data spoofing attack in Protection System



1. Attacker sends an e-mail with malware
2. E-mail recipient opens the e-mail and the malware gets installed quietly
3. Using the information that malware gets, hacker is able to take control of the e-mail recipient's PC and get access of two-level password
4. Analysis IEC 61850 protocol(GOOSE, SMV packet) information and relay setting file
5. Manipulate MMS packet and relay configuration session information
6. Takes control of circuit breaker or change the setting of relay

Objective of the project is to identify set of failures based on the observed alarms and cyber-power measurements using multiple hypothesis and machine learning approaches.

Use Case#2: Cyber-Physical analysis for distributed control and optimization



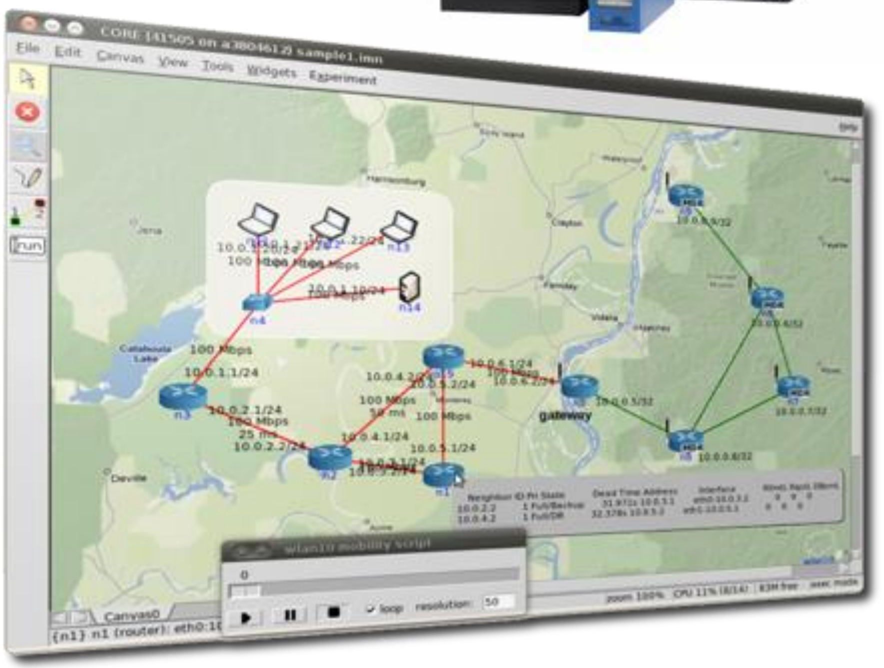
Objective of the project is to develop cyber-resilient distributed control and optimization for voltage and frequency control. Multiple cyber attacks has been modeled and analyzed.

Use Case # 3: Cyber-Physical resiliency Analysis for Microgrid

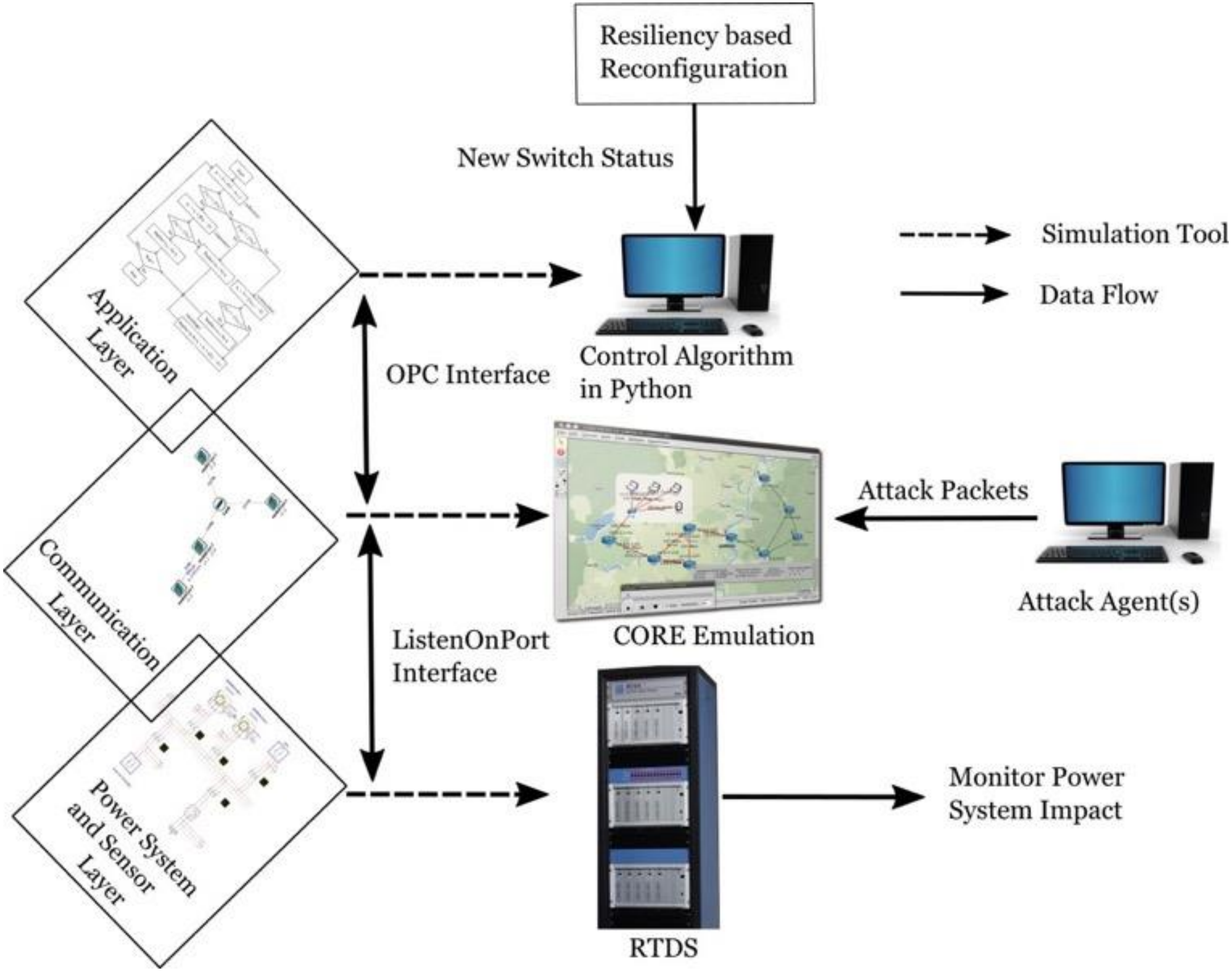
Testbed Components

- Power system simulation using Real Time Digital Simulator (RTDS)
- Simulation done in real time with a timestep of 50μs, and 2.5-5μs for power electronic components

- Communication emulation using Common Open Research Emulator (CORE)
- Socket based interface, allows connection to other devices
- Allows for packet manipulation, used to simulate various attacks



Cyber-Physical Testbed

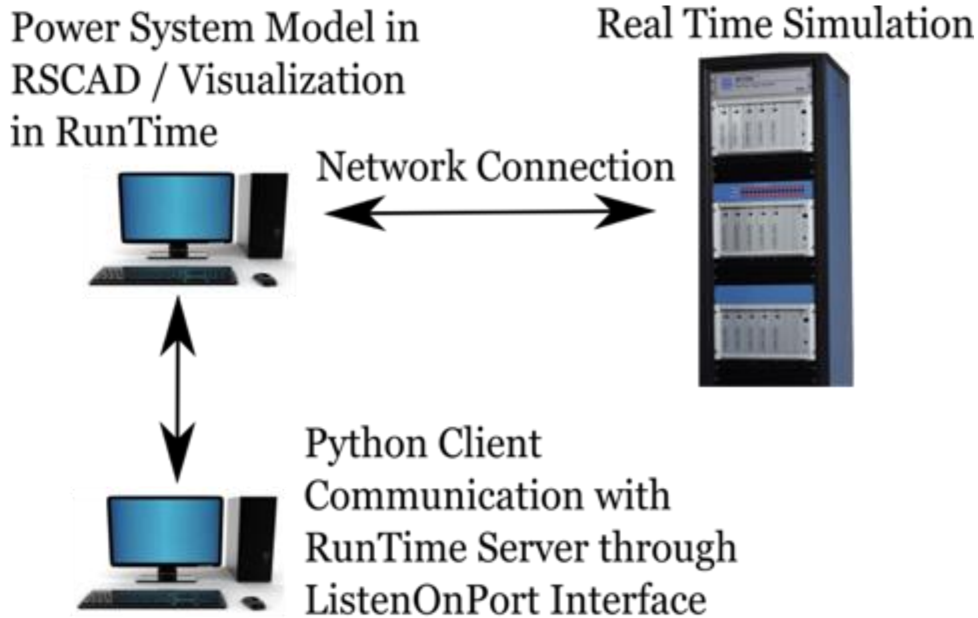


V. Venkataraman et. al, "Real-time co-simulation testbed for microgrid cyber-physical analysis," (MSCPES), April 2016.

Testbed Components - Interface

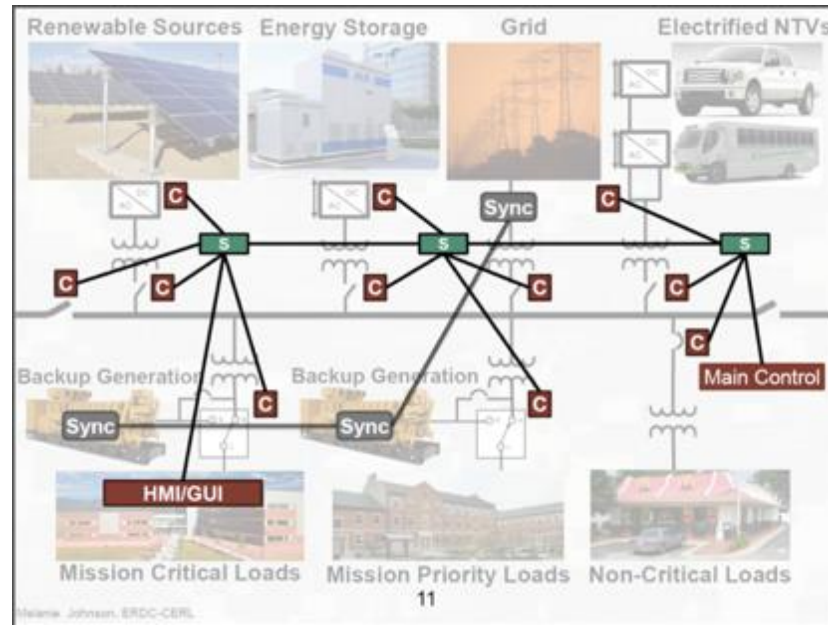
- Interface between the simulators (RTDS and CORE) is through a TCP/IP based interface implemented in Python

- Uses RTDS' feature - ListenOnPort
- Opens a socket by which RTDS can accept commands
- Data from RTDS sent – Breaker Statuses
- Data from CORE – New switch statuses (if necessary)
- Interface enables real-time cyber-physical closed-loop co-simulation of microgrid by combining simulators and controllers

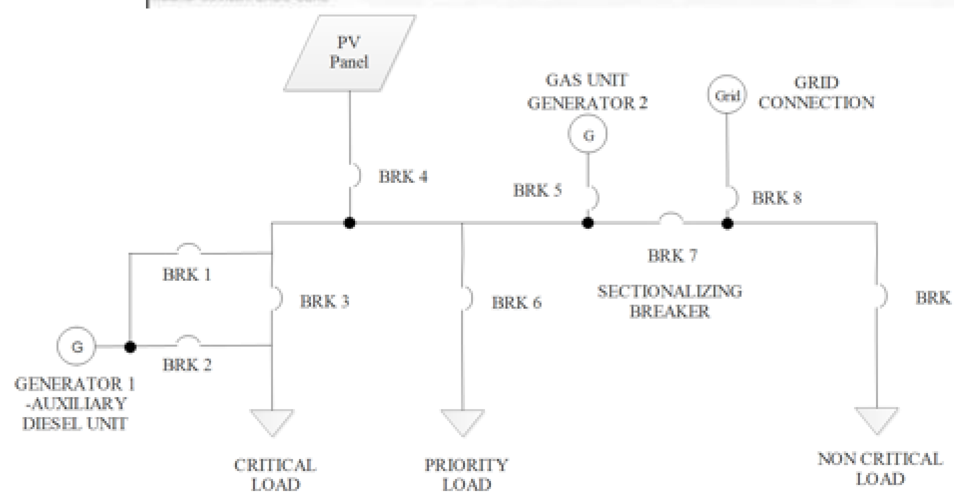


Test System – Physical System

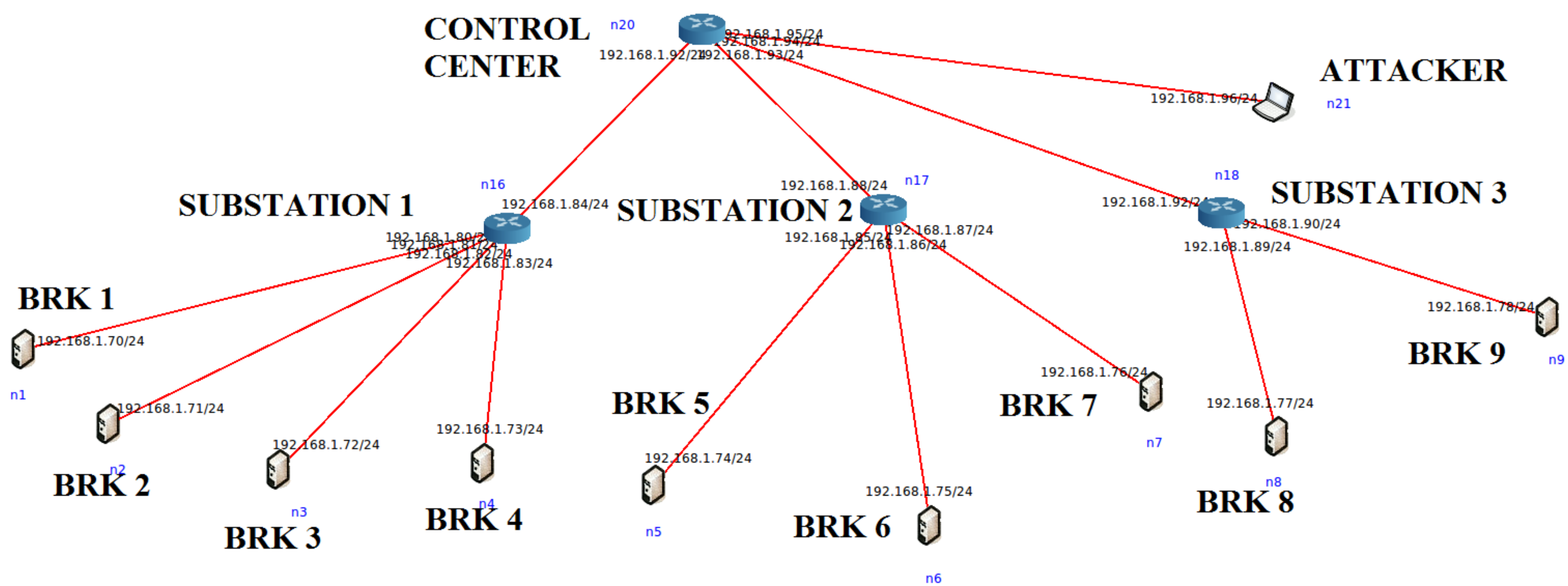
- Test system based on an US Army microgrid in Fort Carson, Colorado
- Some changes done for functionality in demonstrating reconfiguration
- Chosen for strong emphasis on cyber security
- Aux diesel unit usually not connected to system



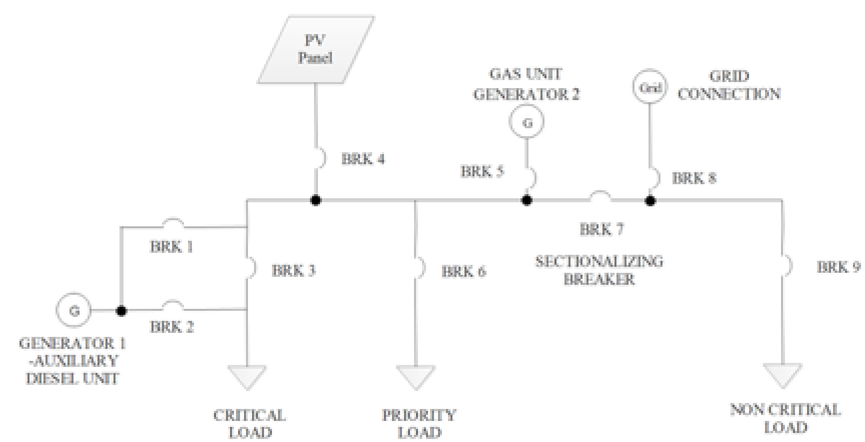
Loads	1.1 MW critical, 1 MW priority, 1.5 MW Non-critical load
Generation	2.25 MVA Gas Unit
Renewables	1 MW Solar Array
Breakers	9



Test System – Cyber System

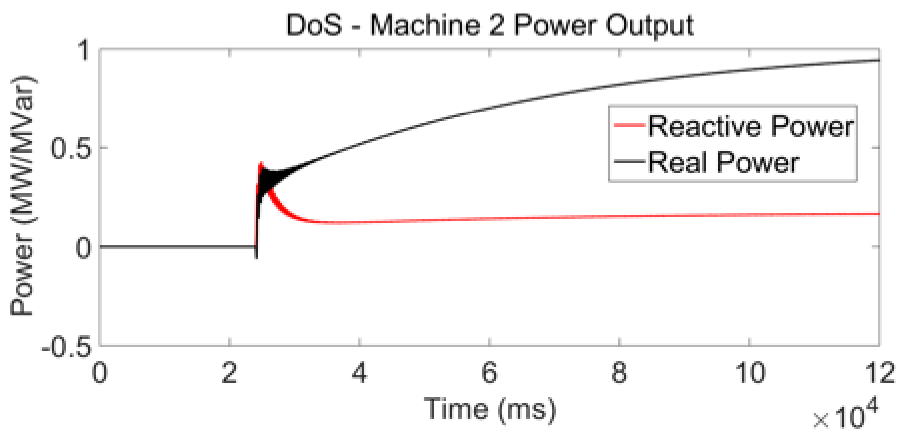


- Each breaker considered to be a host
- Connected to substation gateway/switch
- Switches connected to router and control center



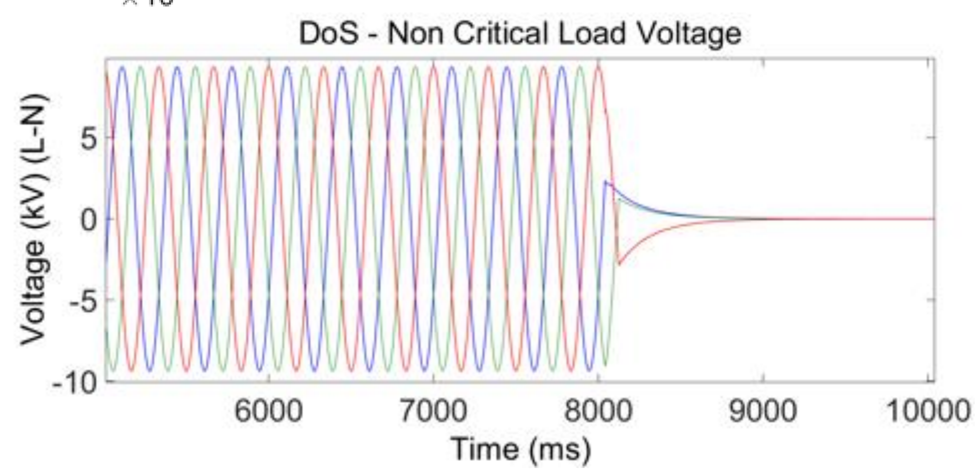
Simulation Results – DoS Attack

- Denial of Service attack – Cyber + Physical attack
- Attack on grid tie breaker



- Gas unit switched ON

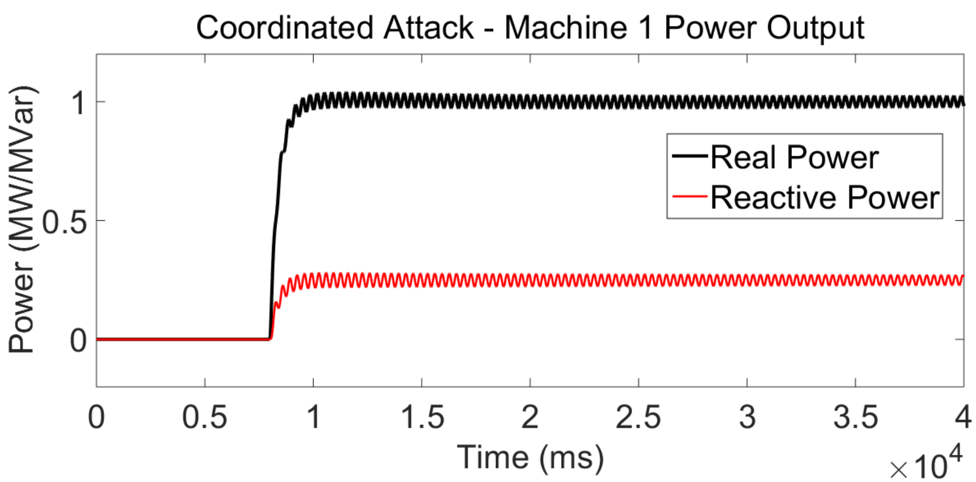
- Non-critical load shed



V. Venkataramanan et. al, “Real-time co-simulation testbed for microgrid cyber-physical analysis,” (MSCPES), April 2016.

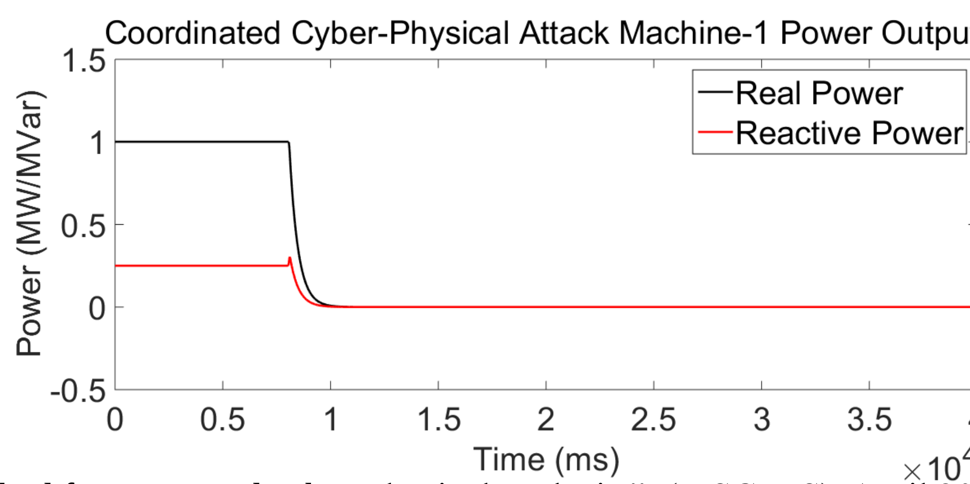
Simulation Results – Coordinated Attack

- Attacker assumed to have complete system information
- Uses multiple time coordinated agents



- Auxiliary diesel unit switched ON
- Attacker cannot access this breaker as it is not on the network, need physical attack

- All other loads shed

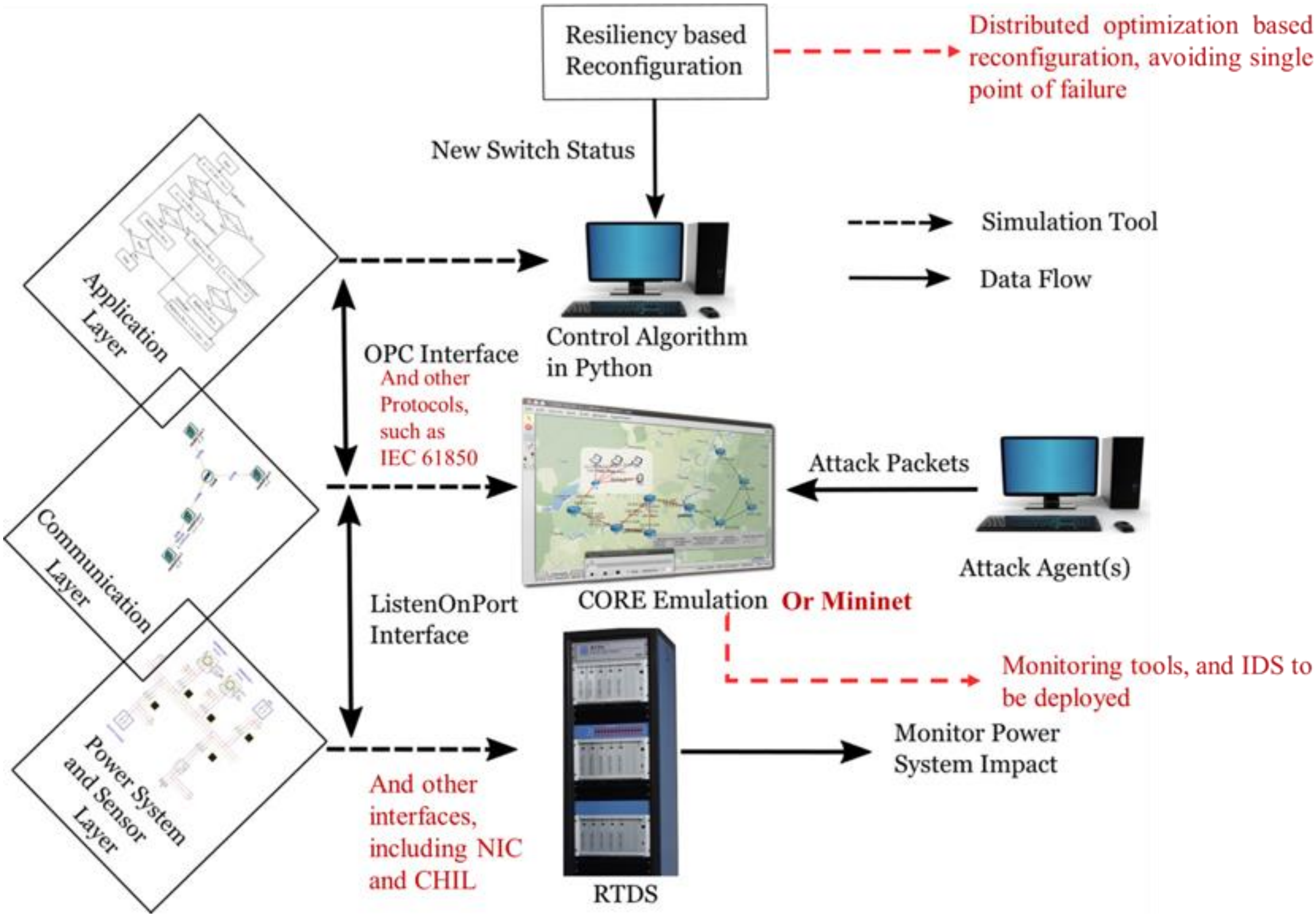


V. Venkataramanan et. al, "Real-time co-simulation testbed for microgrid cyber-physical analysis," (MSCPES), April 2016.

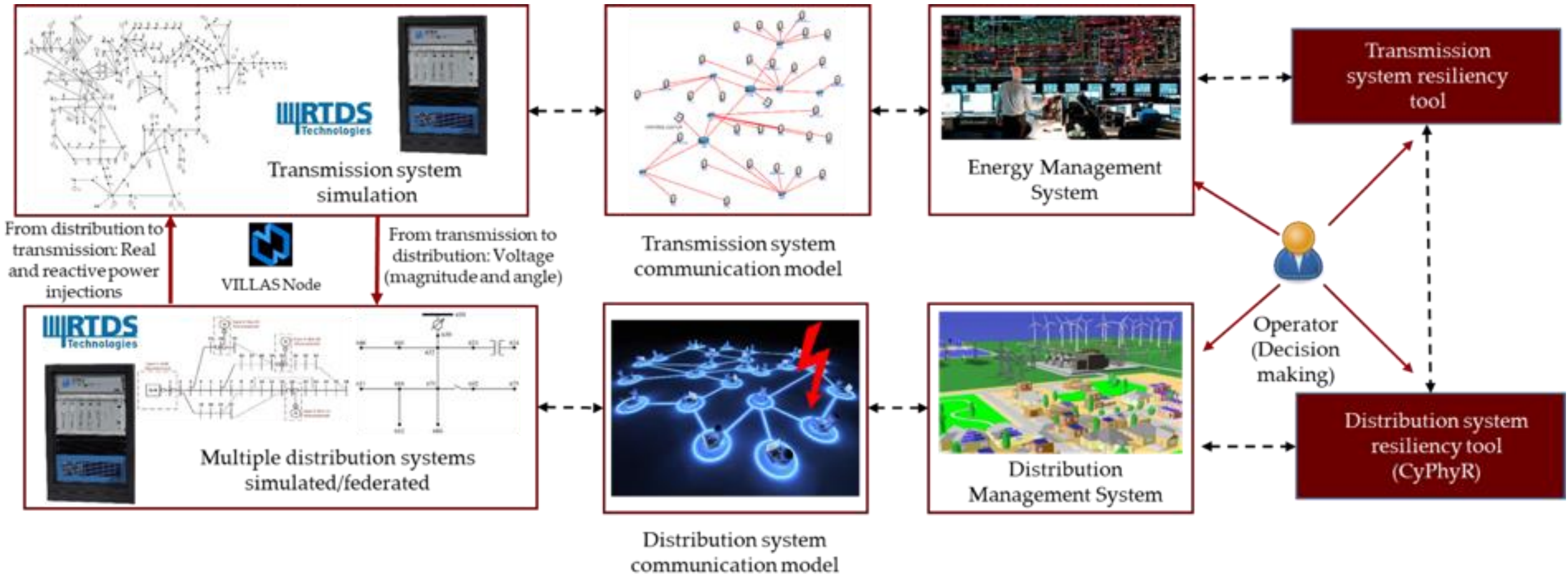
Lessons learned

Security Experiment	Requirements	Use-case	Possible Implementation
Man in the middle attack	Emulation of communication network	Microgrid reconfiguration	Emulation with network card based communication and TCP/IP sockets with third party libraries
Latency effects	Simulation of communication network	Transmission system algorithms (such as RAS) testing	Offline simulation with network simulation tools such as NS-3
Real time cyber attack implementation	Emulation and use of real devices	Transmission system closed loop testing	Transmission system needs to be smaller, and vulnerabilities need to be exploited to study the effects on the power system
Implementing defense mechanisms	Emulation testbed with use of security tools	Evaluating defense mechanisms	Emulated networks with granular models of network devices, and hardware based testbeds

What are we doing now?



Future work



Acknowledgement

This work is partially supported by the US Department of Energy under Award Number DE-OE0000780. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

We would like to Acknowledge Dr. Manimaran Govindarasu from Iowa State University for supporting some of the presented work. We would also like to acknowledge ARPA-E, Siemens and RTDS for all the support.

Questions?