Developing Cyber-Physical Experimental Capabilities for the Security Analysis of the Future Smart Grid

Authors: B. Genge, C. Siaterlis

Presenter: Joel D. Barrera

Submitted in Partial Fulfillment of the Course Requirements for
ECEN 689: Cyber Security of the Smart Grid
Instructor: Dr. Deepa Kundur

Outline

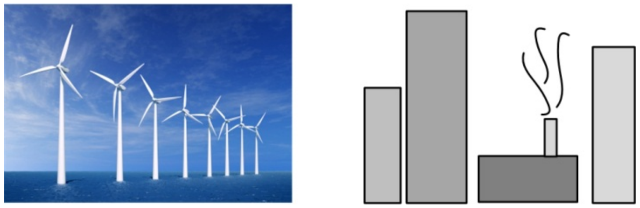
- Introduction
- Related Work
- Experimentation Framework Overview
- Framework Adaptation for Smart Grid Experimentation
- Study of Synchronized Cyber Attacks Against the Smart Grid
- Paper Assessment
- Conclusion
- References

Introduction

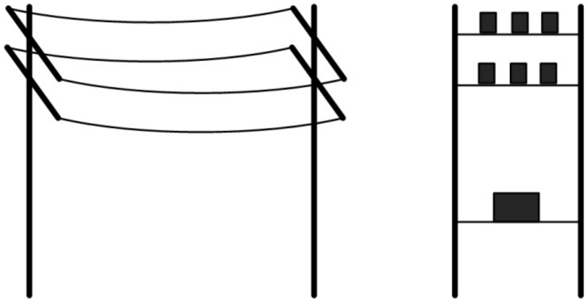
Motivation

- Smart Grid becoming more open
  - Adoption of Information and Communication Technologies (ICT) leads to greater efficiently, flexibility and interoperability between components → more components

Generation and Sub-stations



Transmission and Distribution



Home Area Networks

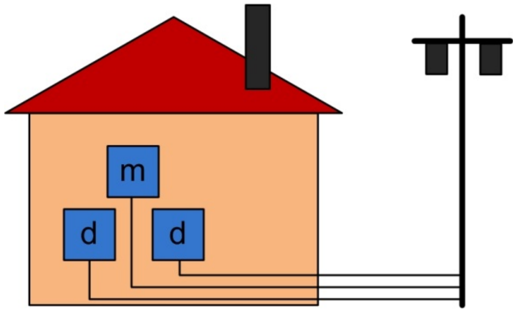


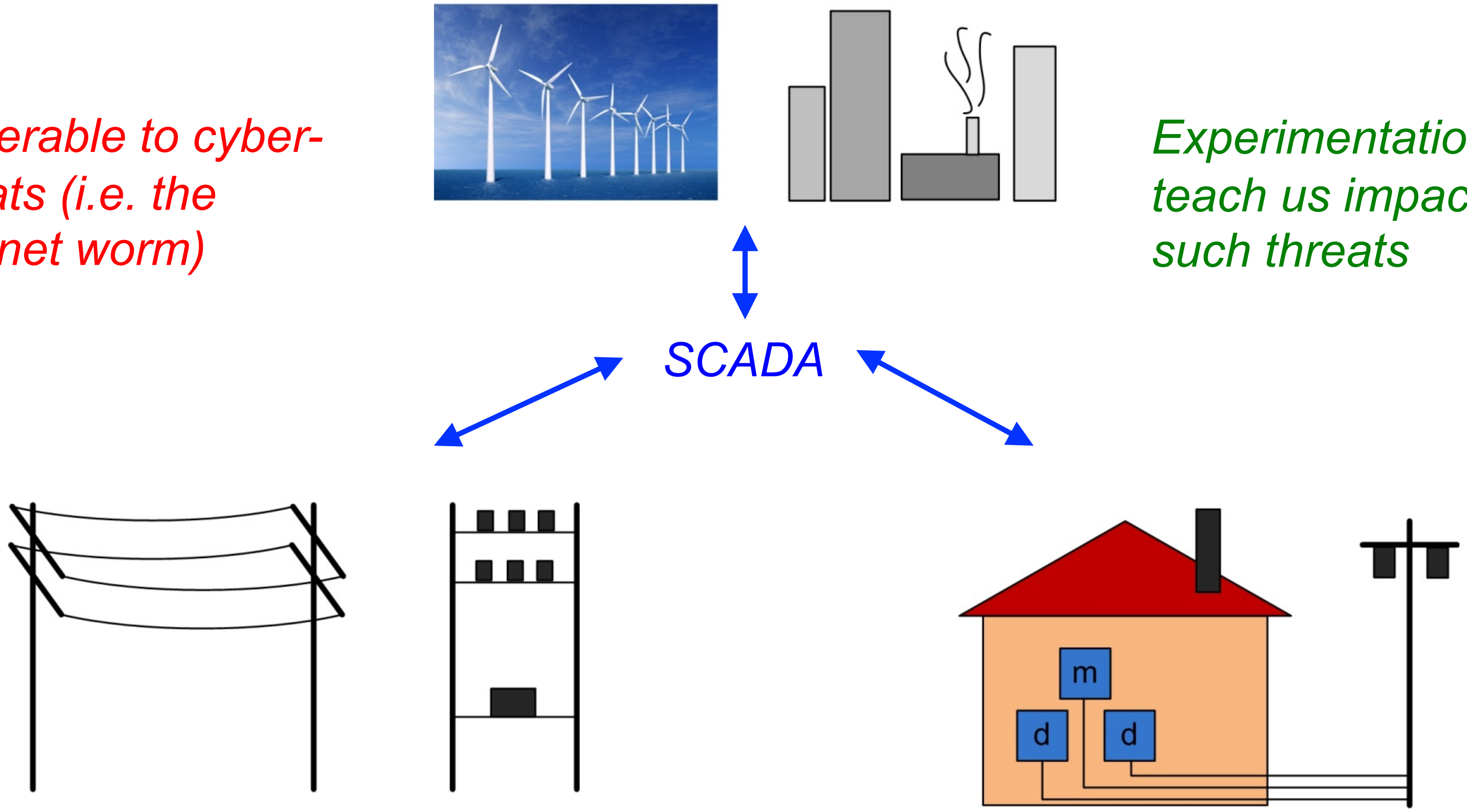
Photo: http://www.mywindpowersystem.com/2012/02/natural-gas-vs-wind-energy/

Introduction

Motivation

- Communications architecture
  - IPv6 and Supervisory Control And Data Acquisition (SCADA)

Vulnerable to cyber-threats (i.e. the Stuxnet worm)



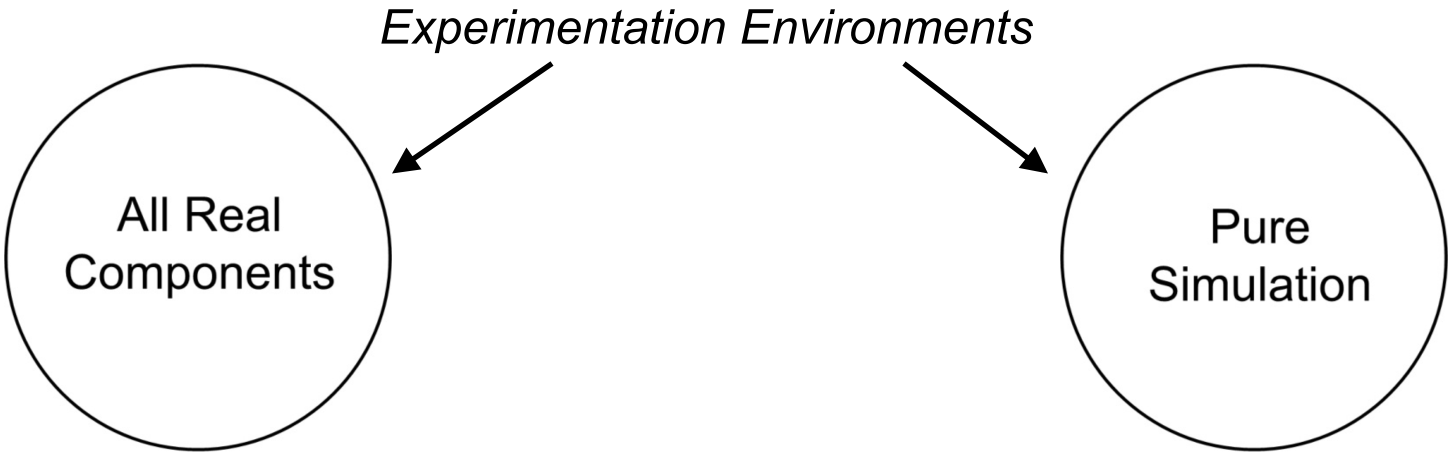
SCADA

Experimentation can teach us impacts of such threats

Photo: http://www.mywindpowersystem.com/2012/02/natural-gas-vs-wind-energy/

Introduction

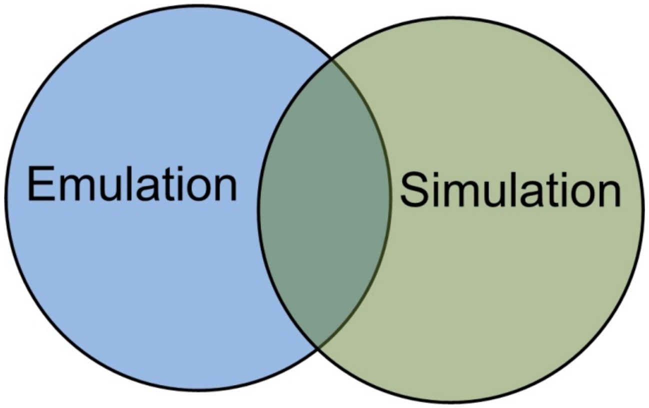
Current issues with cyber threat experimentation



- Impractical and Dangerous
  - Faults/disruptions/possible system shutdown
  - Difficult to create control environment
  - Expensive
- Difficult and Unfeasible
  - Due to diversity and complexity of Smart grid
  - Fail to capture functionality protocols and computer systems in general

Introduction

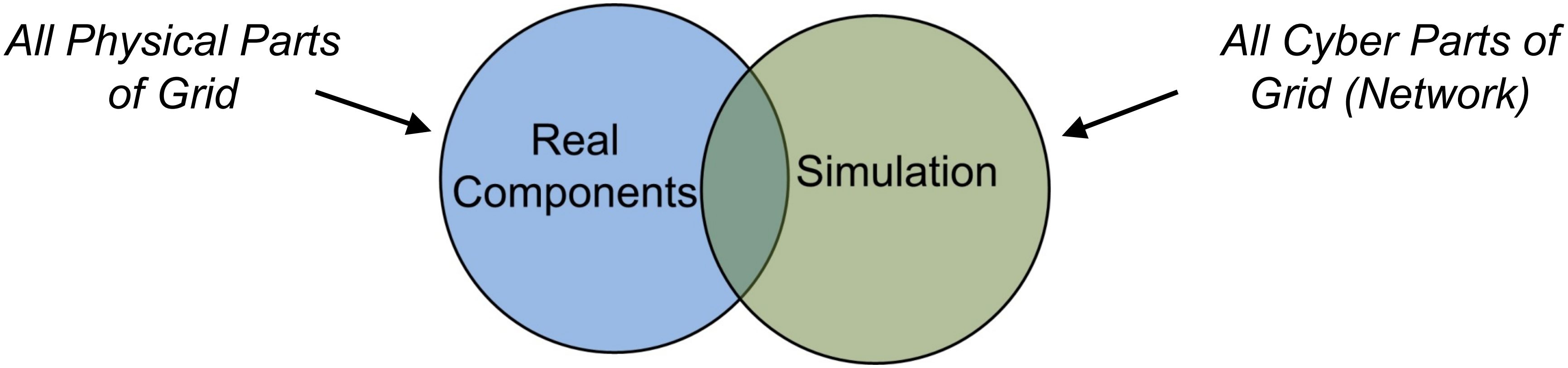
Hybrid approach to experimentation framework



Emulation – the ability of a computer program in an electronic device to emulate (imitate) another program or device

Related Work

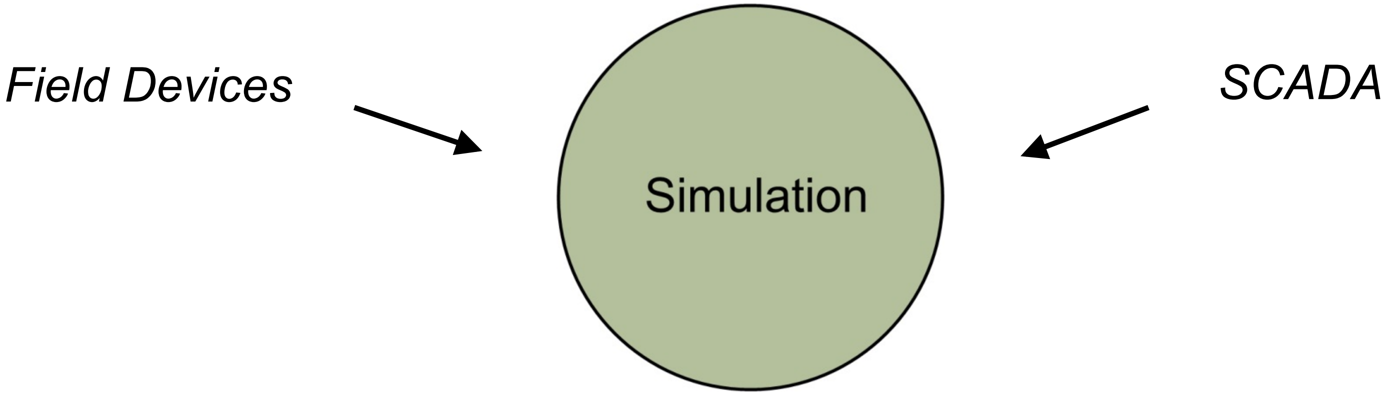
Real + Simulation by Chunlei, et. al. mentioned in [1]



- Advantages
  - Very reliable experimental data (mostly real components)
- Disadvantages
  - Difficult to support on large infrastructures
    - Distribution and transmission systems

Related Work

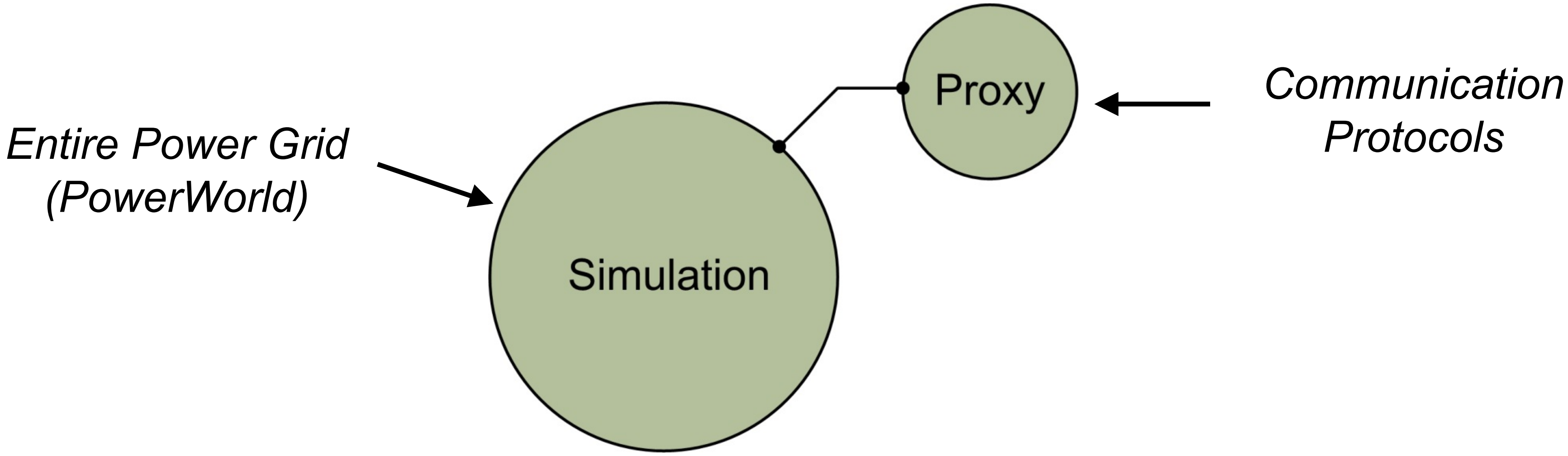
All simulation by Chabukswar, et. al. mentioned in [1]



- Command and Control WindTunnel (CSWindTunnel)
  - Multi-mode simulation environment enabling the interaction between various simulation engines
- Disadvantages
  - Analyzing cyber-physical effects of malware not trivial
    - Requires detailed description of ICT components and dynamics of malware

Related Work

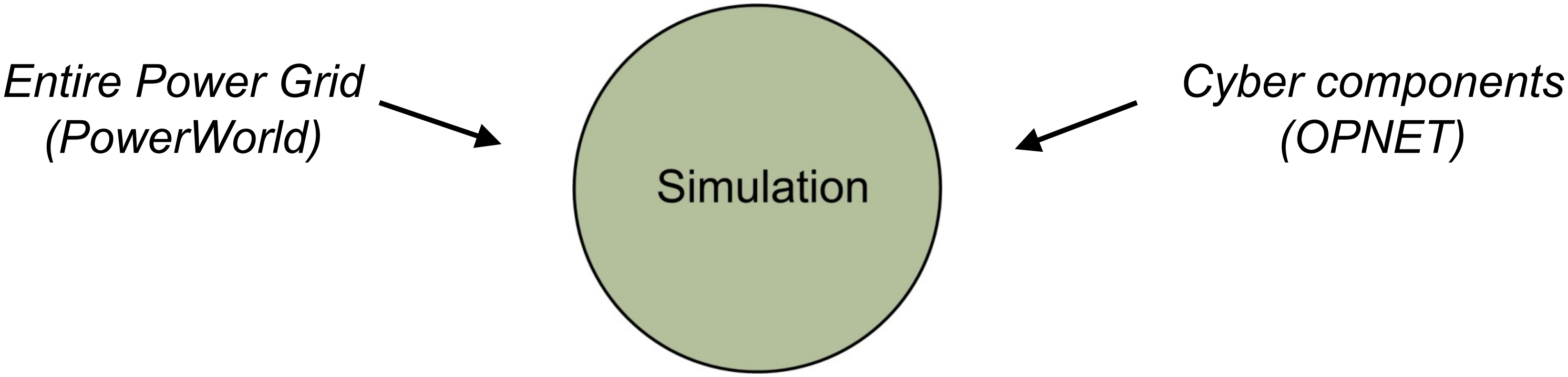
All simulation by Davis, et. al. mentioned in [1]



- PowerWorld
  - Simulation server for modeling power systems
- Disadvantages
  - Does not include key components in cyber-physical system
    - PLCs and SCADA Masters

Related Work

All simulation by McDonald, et. al. mentioned in [1]


Entire Power Grid (PowerWorld)

Simulation

Cyber components (OPNET)

- Disadvantages
  - Requires simulation of the interactions between malware and simulated networks
    - Not trivial

Experimentation Framework Overview

Process control architecture overview

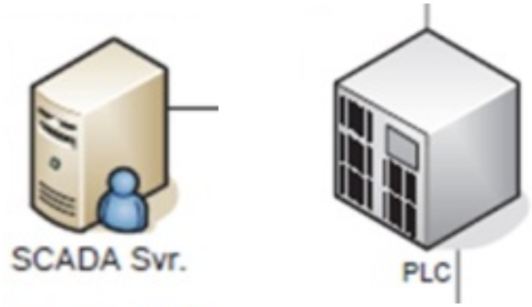
Cyber Layer

- All ICT devices
- Software (data acquisition, command delivery)
- SCADA protocols

+

Physical Layer

- Actuators
- Sensors
- Other hardware devices

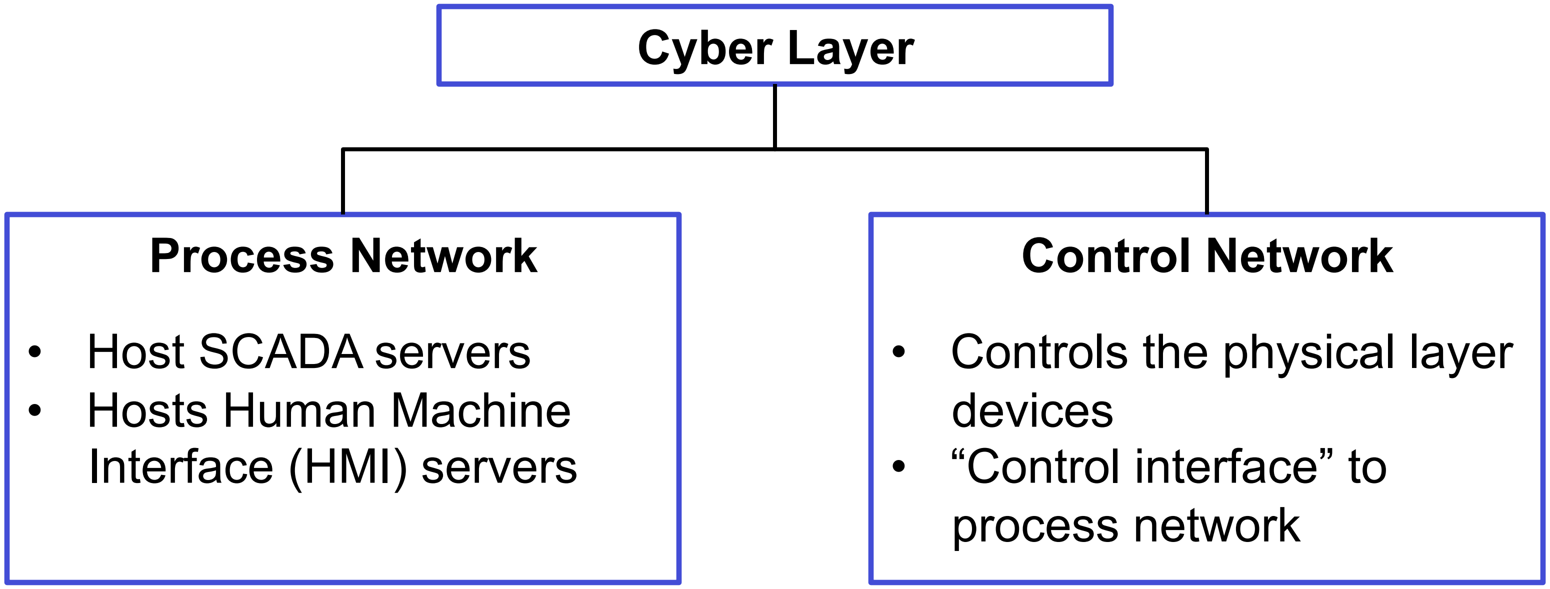


From [1]

http://en.wikipedia.org/wiki/Smart_meter

Experimentation Framework Overview

Process control architecture overview



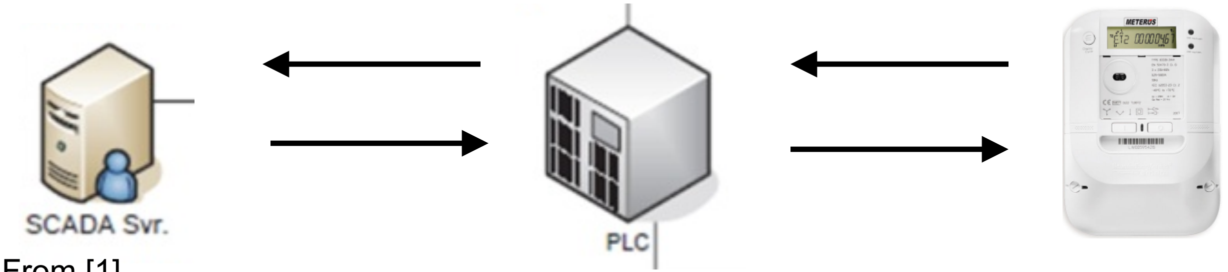
Cyber Layer

Process Network

- Host SCADA servers
- Hosts Human Machine Interface (HMI) servers

Control Network

- Controls the physical layer devices
- “Control interface” to process network



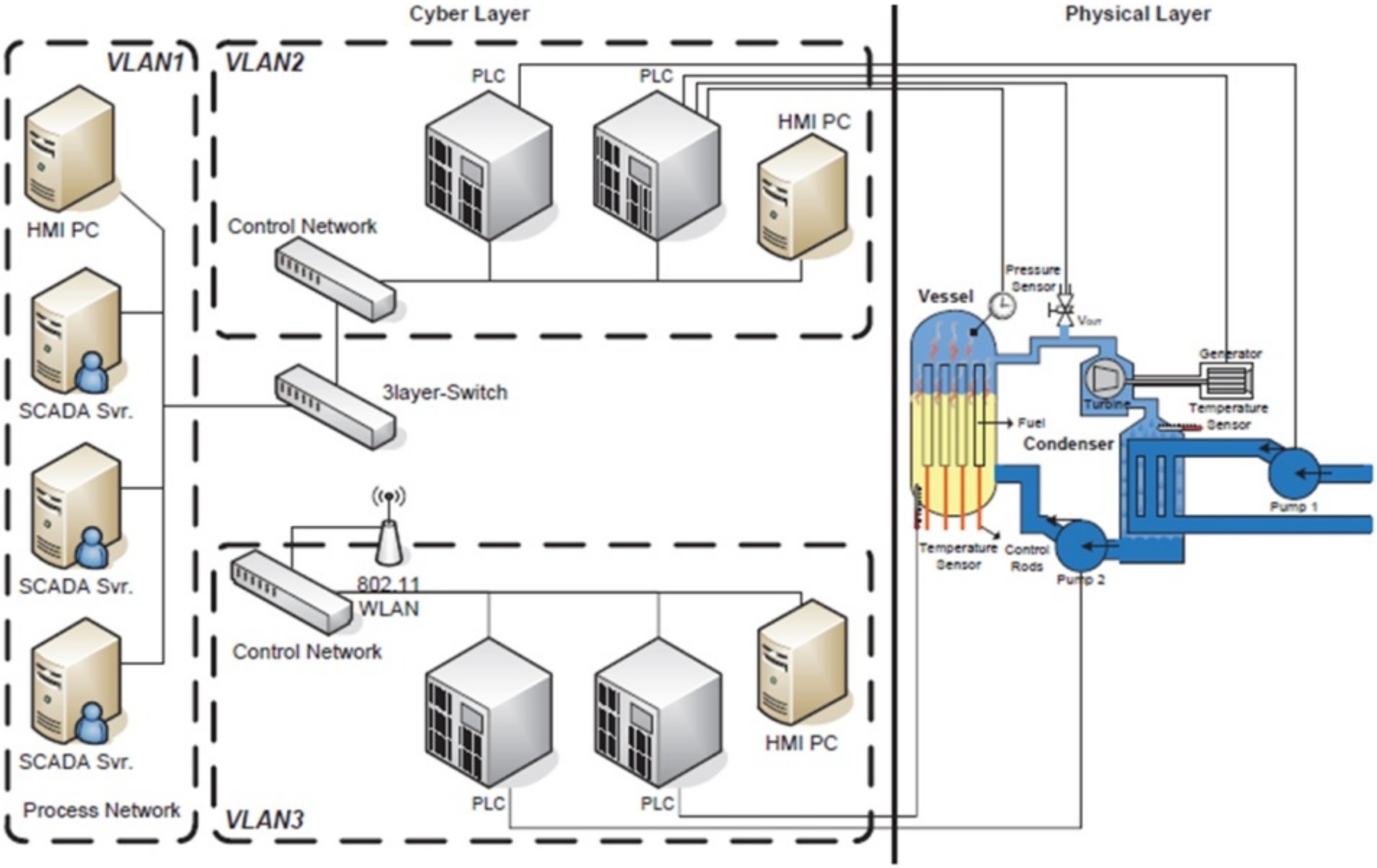
From [1]

From [1]

http://en.wikipedia.org/wiki/Smart_meter

Experimentation Framework Overview

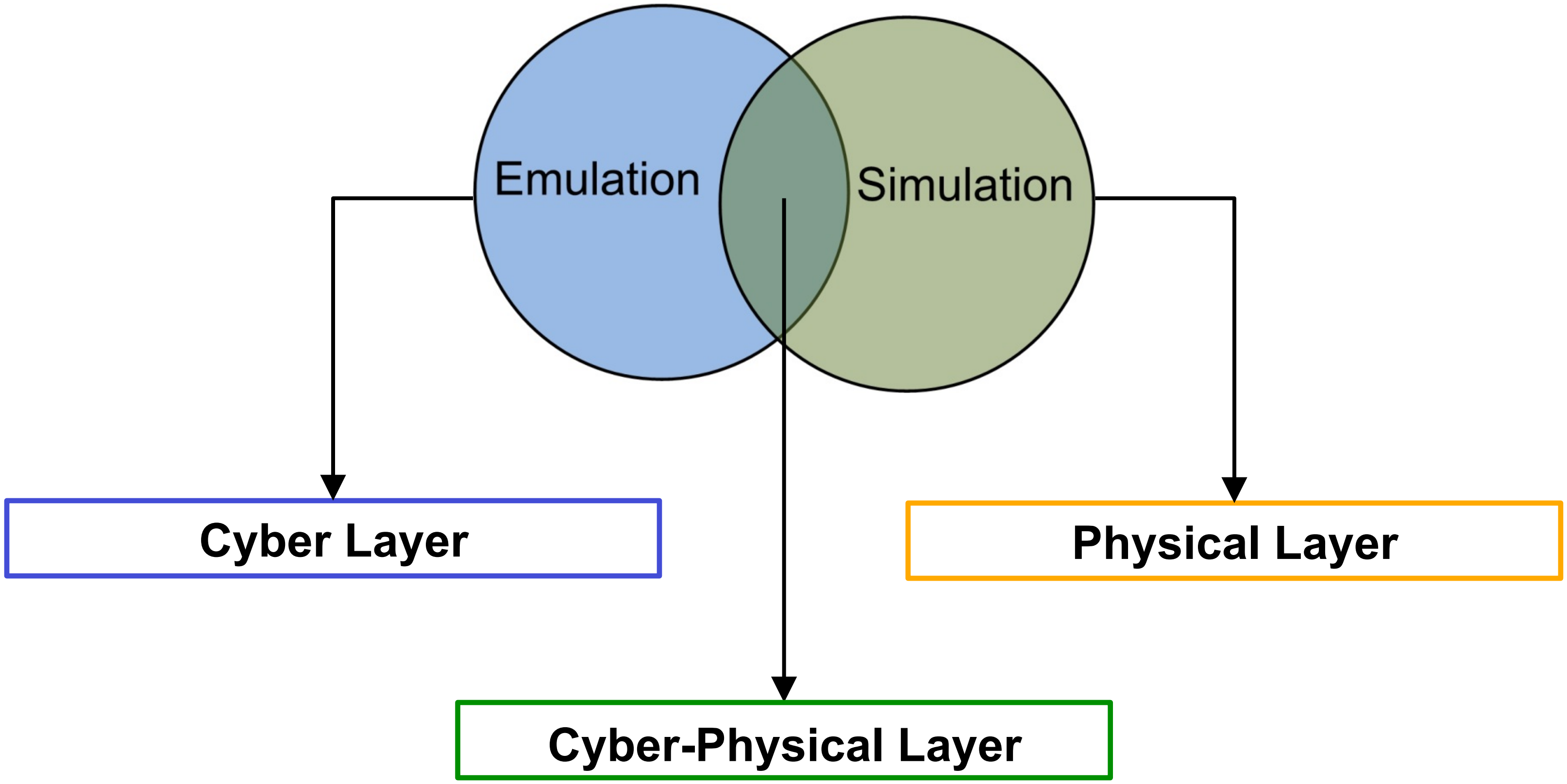
Process control architecture overview



From [1]

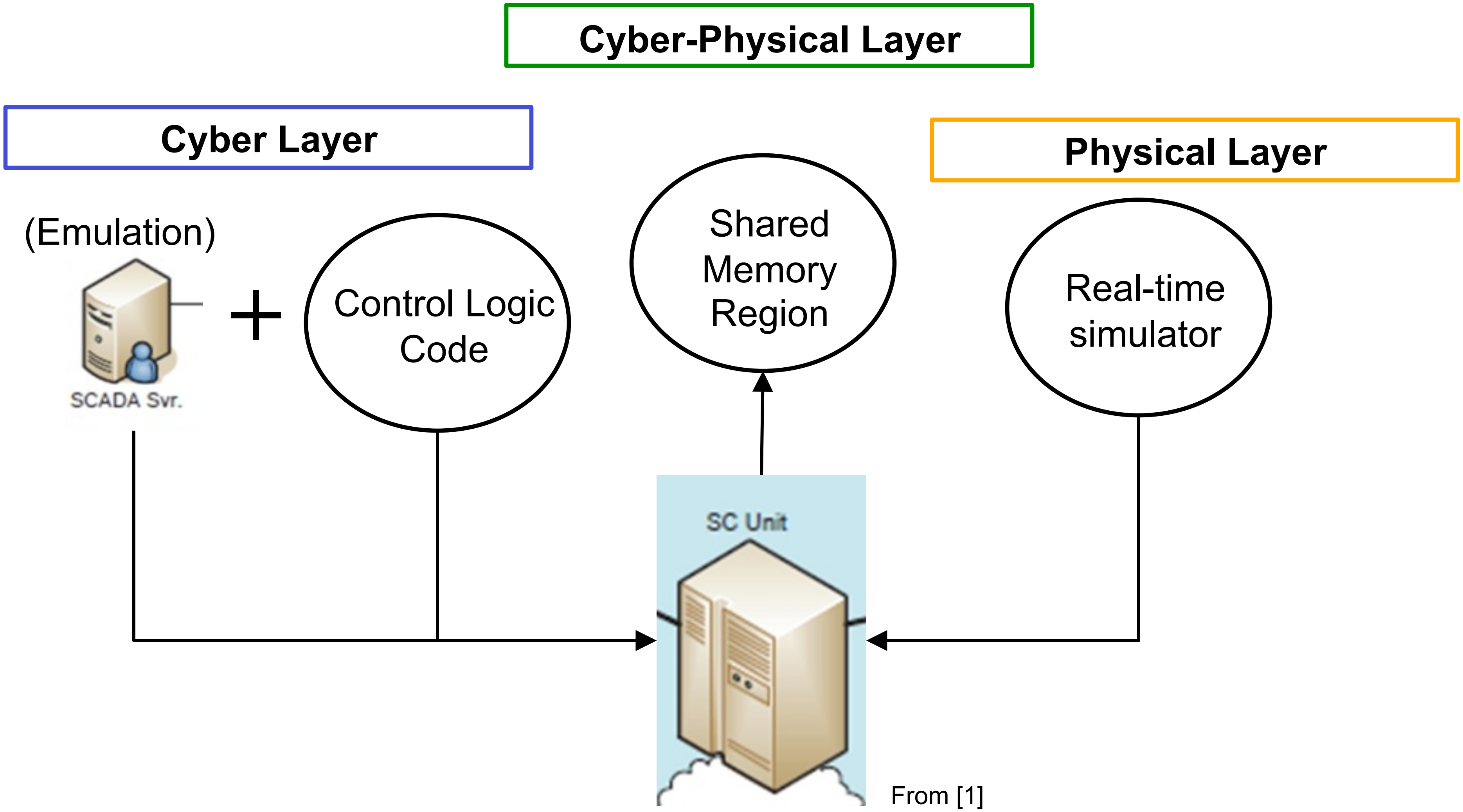
Experimentation Framework Overview

Experimentation framework architecture based on hybrid approach



Experimentation Framework Overview

Experimentation framework architecture based on hybrid approach



Cyber-Physical Layer

Cyber Layer

Physical Layer

(Emulation)

+

Control Logic Code

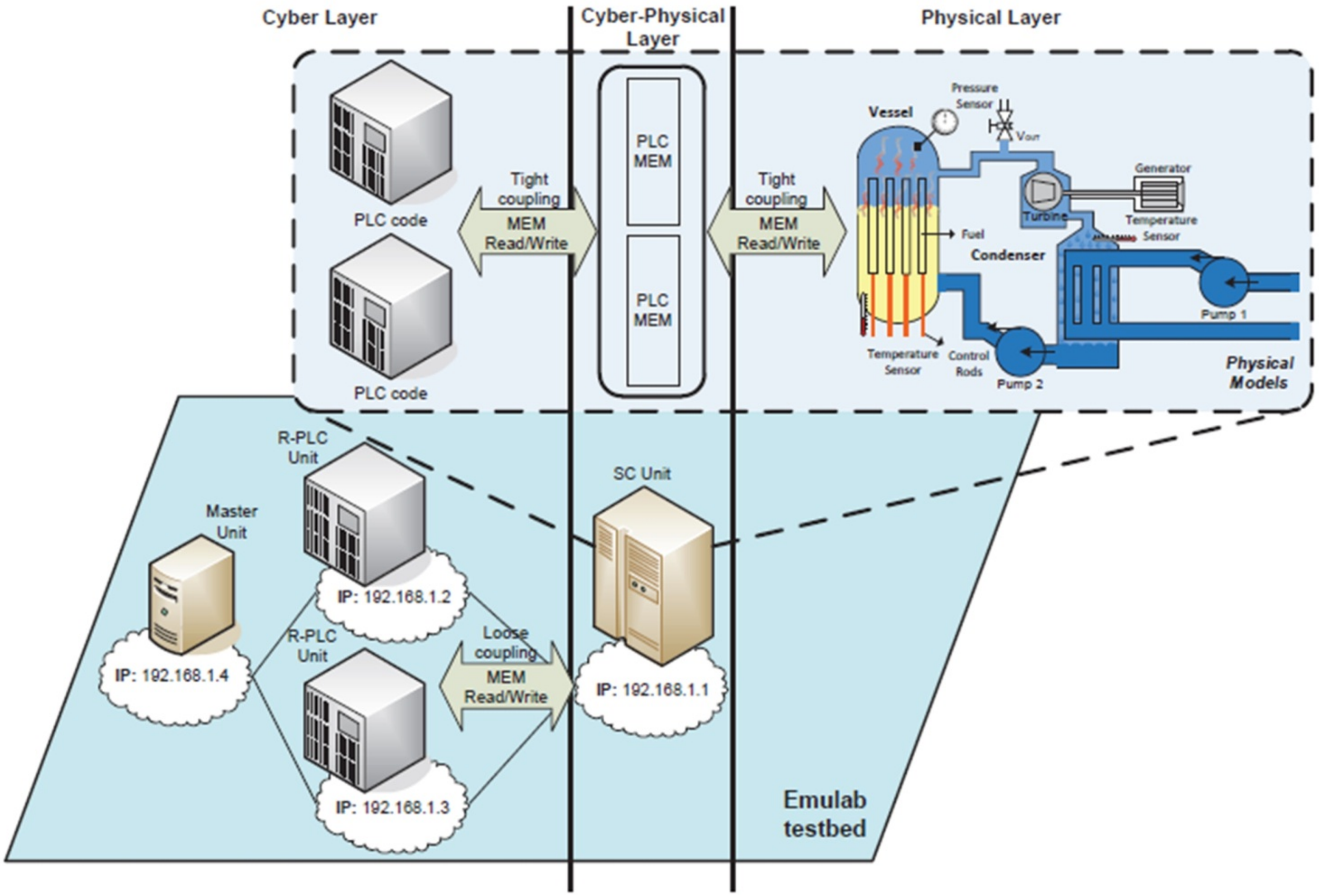
Shared Memory Region

Real-time simulator

From [1]

Experimentation Framework Overview

Experimentation framework architecture



From [1]

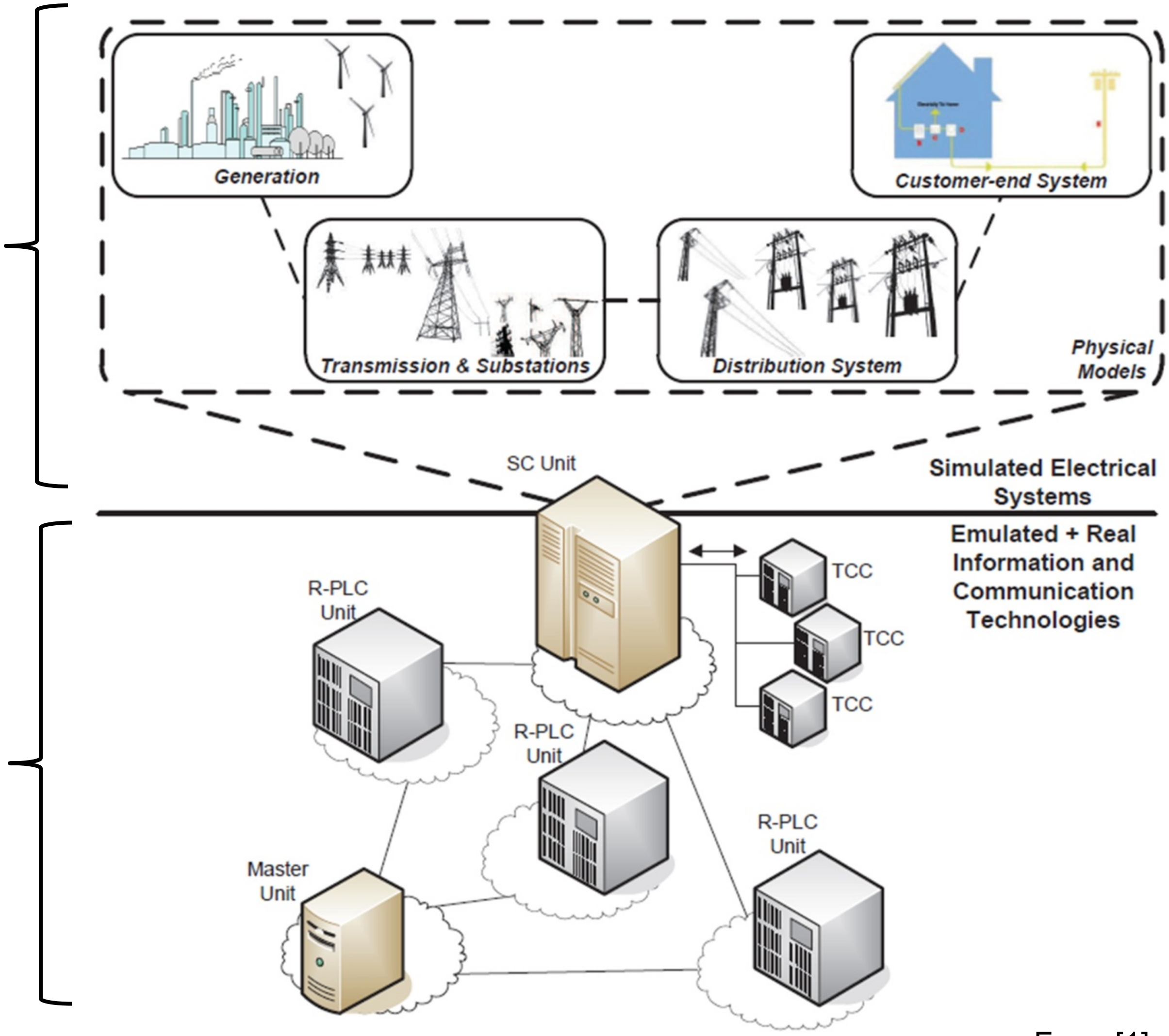
Framework Adaptation for Smart Grid Experimentation

Physical Layer

- Additional smart gird components
- Not exhaustive
- Flexible

Cyber Layer

- Additional SCADA/ ICT components
- Flexible

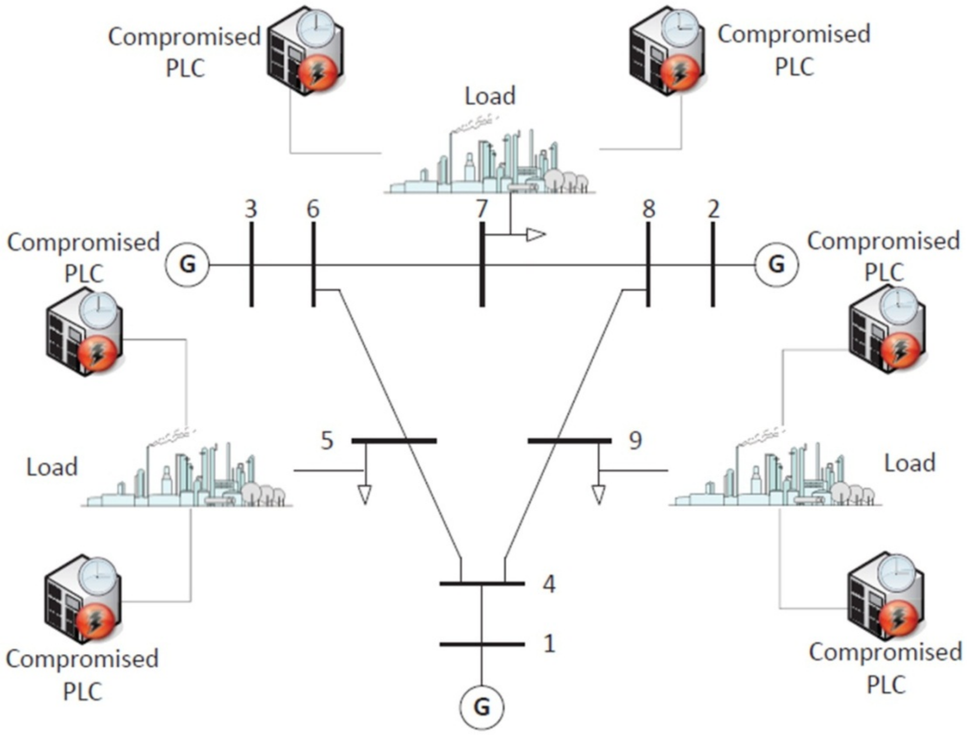


From [1]

Study of Synchronized Cyber Attacks Against the Smart Grid

Attack scenario

- Power grid
  - IEEE 9-bus test system
- Attack details
  - Logic bomb inserted into compromised PLC
  - Attack initiated upon reaching time conditions
- CIA
  - Mainly availability

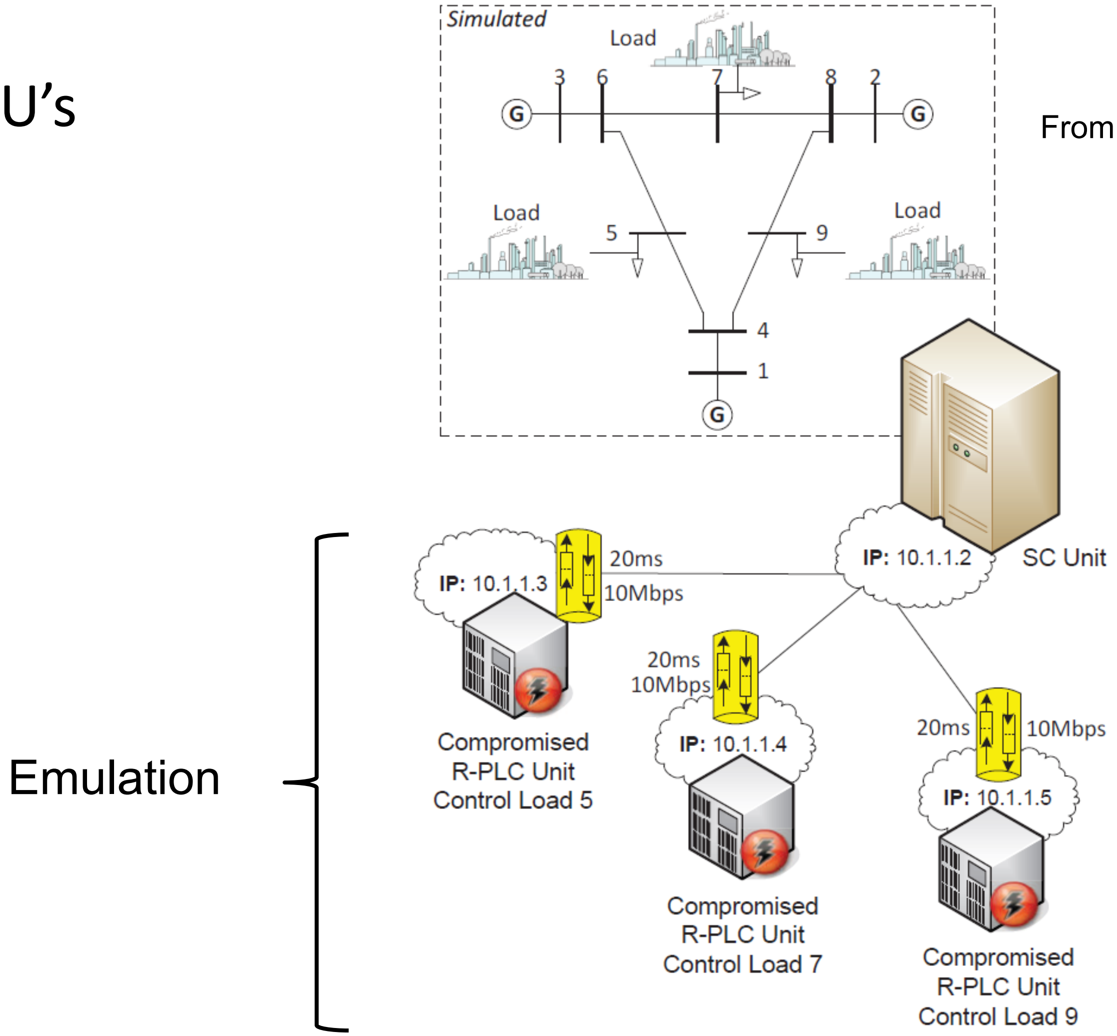


From [1]

Study of Synchronized Cyber Attacks Against the Smart Grid

Attack scenario implementation on exp. framework

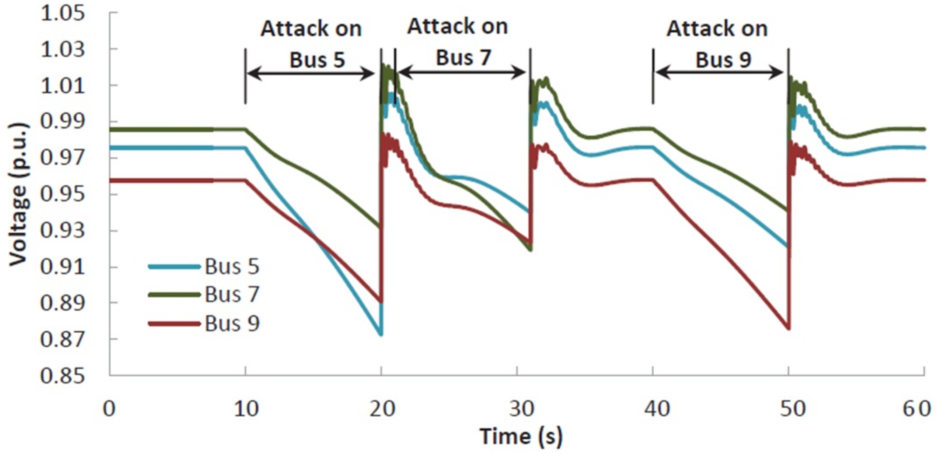
- Compromised R-PLU’s
  - Buses 5,7, and 9
- Observations
  - Variation on load

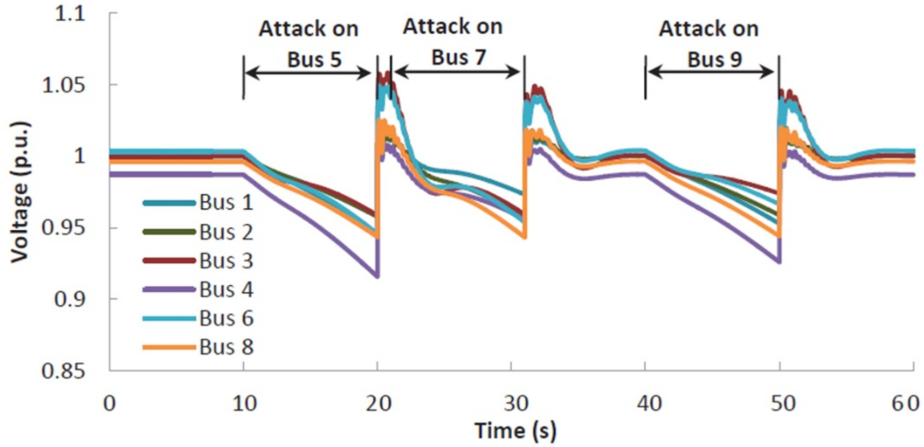


From [1]

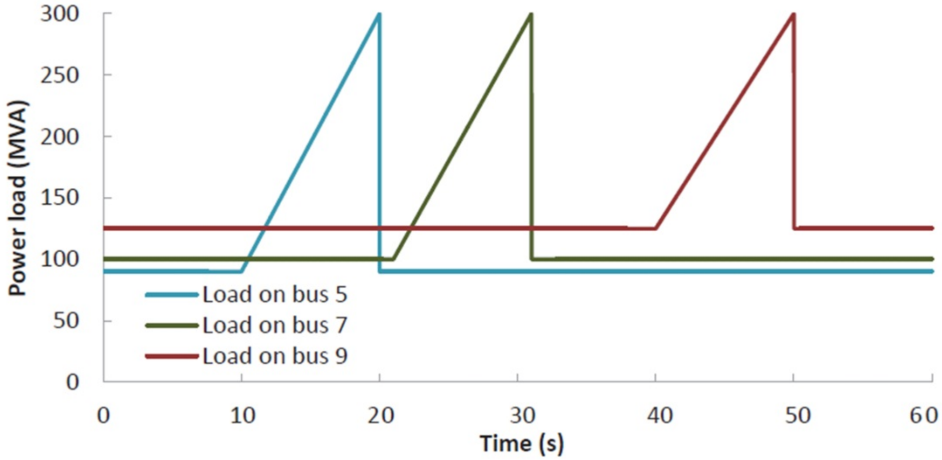
Study of Synchronized Cyber Attacks Against the Smart Grid

Non-synchronized attack





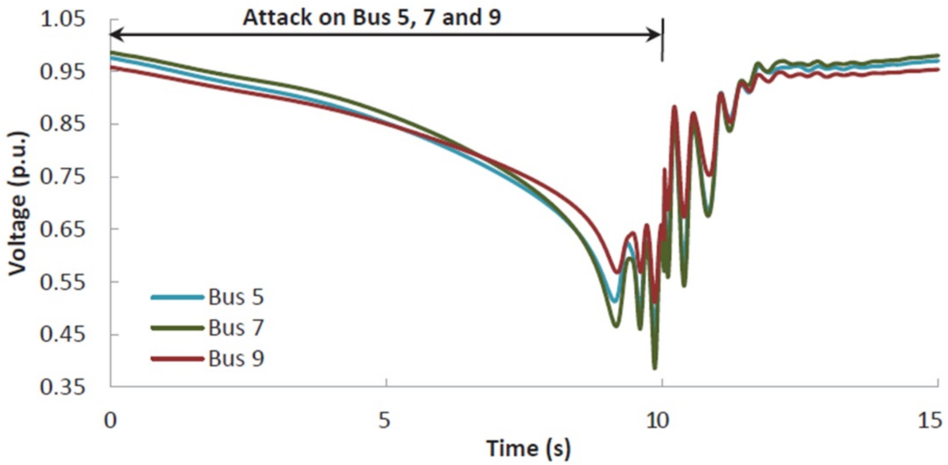
- 10s attacks from multiple locations at different times
- Overall oscillations stabilized after each attack

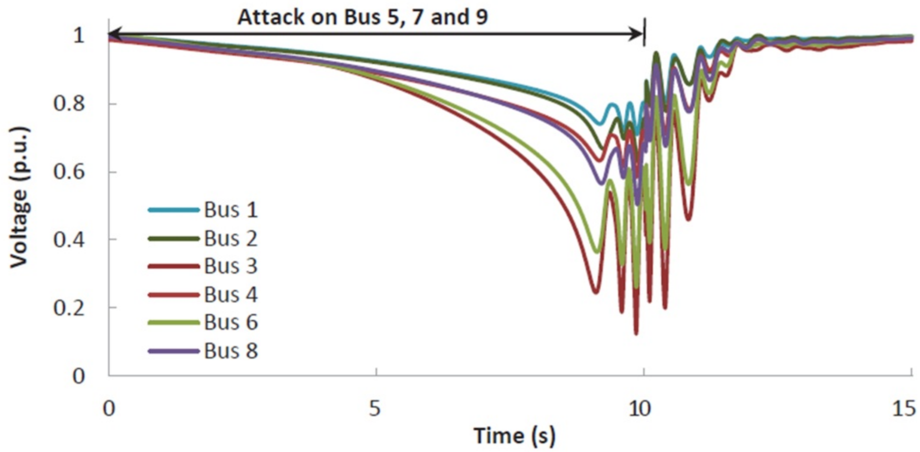


Plots from [1]

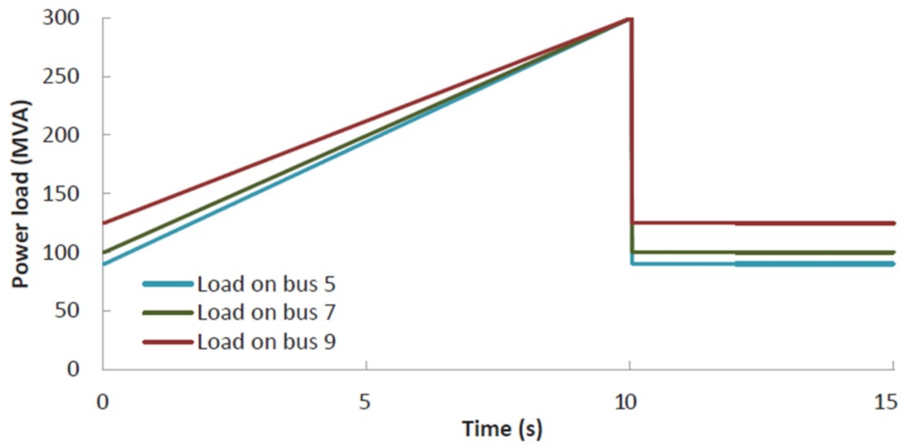
Study of Synchronized Cyber Attacks Against the Smart Grid

Synchronized attack





- 10s attacks all at once
- Major oscillations on all buses
- Voltage drops shows power grid approaching voltage collapse



Plots from [1]

Paper Assessment

Positive aspects

- A look at simulation and experimentation
  - Importance (cost, efficiency, safety)
  - Personal research
- Real data shown as proof-of-concept
- Good formulation of problem
  - Why do we need experimentation?
- Overall
  - Well written and structured paper

Paper Assessment

Possible improvements

- Unclear definitions
  - Powerworld, OPNET
  - Personal background limited
- Discussion of results
  - More in-depth
    - Why 10s attacks?
    - Shown the average of a series of attacks
- Limitations of hybrid approach
  - No discussion

Conclusions

- An experimental framework for analysis cyber attack on Smart Grid developed
  - Hybrid approach (emulation + simulation)
- A proof-of-concept experimentation shown
  - A synchronized attack from multiple locations causes can cause the power grid to approach voltage collapse.
  - Security studies can be conducted on the Smart Grid
- Flexibility of experimental framework
  - As Smart Grid becomes more and more complex, additional components (physical and ICT) to framework introduced

References

[1] B. Genge, C. Siaterlis, "Developing cyber-physical experimental capabilities for the security analysis of the future Smart Grid," *Innovative Smart Grid Technologies (ISGT Europe), 2011 2nd IEEE PES International Conference and Exhibition on*, pp.1-7, 5-7 Dec. 2011

Questions?