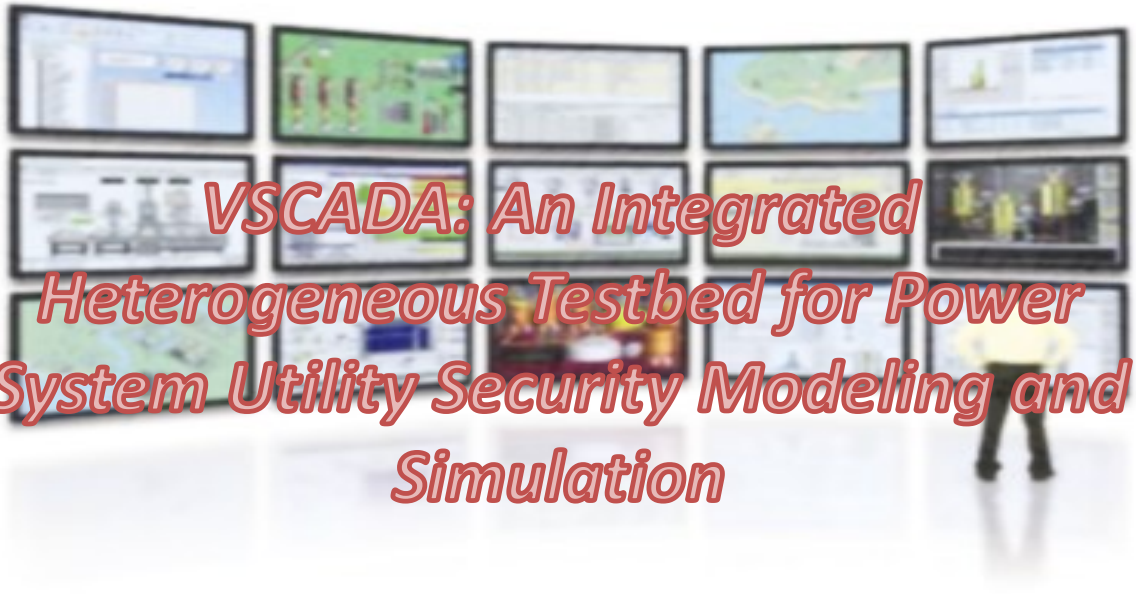


VSCADA: An Integrated Heterogeneous Testbed for Power System Utility Security Modeling and Simulation

Yi Deng, Avik Dayal, and Sandeep Shukla

April 1, 2015

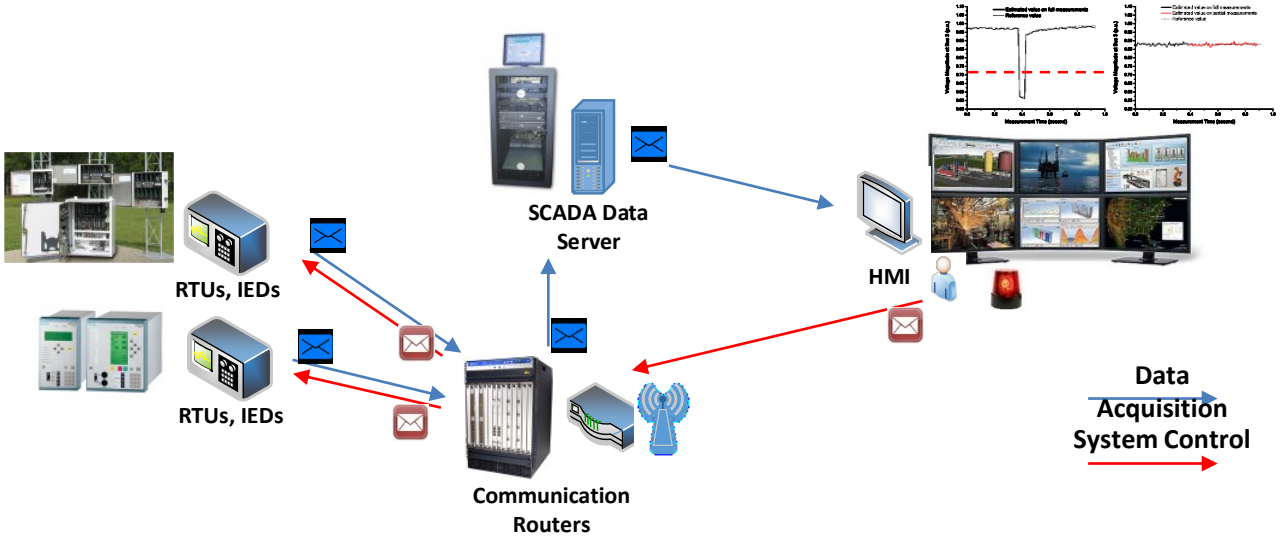
Bradley Department of Electrical & Computer Engineering

VirginiaTech

Introduction

- SCADA systems are critical to the control and monitoring of complex cyber-physical systems.
- Now with advanced computer and communications technologies, SCADA systems are connected to networks or the Internet, increasing threats facing SCADA system.
- To protect SCADA systems, important to simulate attacks launched on system, such as Man-in-the-Middle and Denial of Service(DOS) attacks.
- SCADA Testbed is a important tool to study the operations, the securities of SCADA systems.

SCADA System Overview

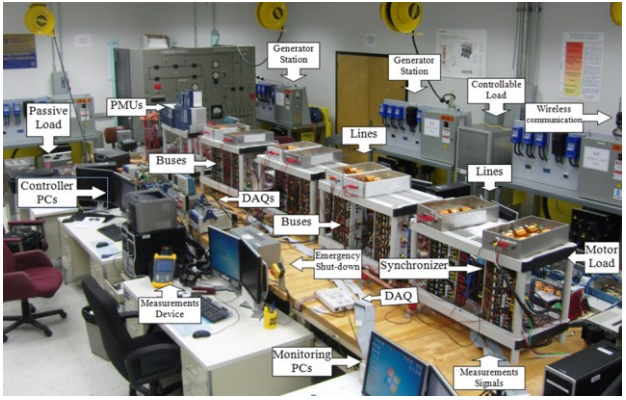


Existing SCADA Testbed Review

- Previous works use a few design criteria in creating SCADA test-beds
  - Choice of sensor backend configuration with real equipment, a virtual test bed with modular software or construct a hybrid of laboratory with hardware in the loop methods.
  - Choice of which SCADA communication protocols to use.
  - Choice application that it is serving, whether it be a power system, nuclear plant, or transportation system.
  - Other criteria includes multiple users accessing the test bed simultaneously and providing remote access.

SCADA System Testbed

- Mitigate and identify and existing vulnerabilities
- Identify and promote best cyber security methodologies
- Increase the awareness of control systems security within the energy sector
- Develop advanced control system architectures and technologies that are more secure and robust



From: http://www.energy.fiu.edu/research/projects/smart-grid-research/researchprojectssmart-grid-researchreal-time-monitoring/
Florida International University

SCADA Testbed Category

Real SCADA Testbed: laboratory-scale industrial control system with real equipment (a few commercial or custom devices)

- Pros
  - The data reflect realistic measurement, variations that would be present in an actual process control system.
  - The communication patterns and latencies will be entirely accurate and not vulnerable to inaccuracies in simulated variables (OS scheduling load, etc.)
  - Devices are vulnerable to many attacks that may not be present in the design specification of virtual testbed. (protocol implementation vulnerabilities/bugs, teardrop attacks, LAND attacks, web application attacks, buffer overflows, etc.)
  - Other security issues such as poorly protected passwords will only appears in real scada testbed.
  - Combinational attacks testing with normal background traffic.
- Cons
  - Expensive to develop and maintain
  - Industrial control system software could be brittle and not user-friendly
  - Adding or changing features in a real SCADA testbed could be difficult
  - Scalability issues: the size of the real SCADA testbed is limited
  - The testbed is usually smaller and less featured than real systems

Virtual SCADA Testbed: consists of simulated devices and may include a simulated process

- Pros
  - Simpler to develop and maintenance, low costs
  - Easy to enlarge the size of systems (spend more development time, no further purchase needed)
  - Easy to add or change features of the existing systems, easy to design/replace/extend new components
  - Industrial control system protocols and communication interfaces can be changed easily
  - Virtual SCADA testbed can be distributed widely to many researchers (replace their own IPS systems by other research groups)
  - Easy to learn and user friendly to students who wish to learn SCADA system and security
- Cons
  - Certain attacks, especially attacks that rely on device implementation errors may not work against virtual testbeds
  - Virtual testbed may not perfectly exhibit the same behavior as a real ICS.

Hybrid laboratory-scale and simulated system: combination of real SCADA devices and simulated process such as communication process

National SCADA TestBed Program

- Start from 2003, a national resource to address the cybersecurity challenges of energy delivery systems
- The NSTB combines the national lab's testing facilities with research, development, analysis, training, and discover security vulnerabilities
- The NSTB offers testing and research facilities, advanced visualization and modeling tools
  - ***Los Alamos National Laboratory***: Quantum Key Distribution, algorithms to encrypt energy sector information, etc.
  - ***Idaho National Laboratory***: analyzing technical, cybersecurity threat, and understand how these threats affect their overall risk posture.
  - ***Sandia National Laboratory***: investigating moving target defenses to better secure the energy sector against attack.
  - ***Lawrence Berkeley National Laboratory***: considering the physical limitations of devices to develop specifications and enhanced monitoring techniques.
  - ***Argonne National Laboratory***: developing and deploying control system standards, including the IEC 61850 substation automation standard and trustworthy wireless standards

UIUC Trustworthy Cyber Infrastructure for the Power Grid (TCIPG) Testbed

- Span transmission, distribution & metering, distributed generation, and home automation and control, providing true end-to-end capabilities
- Analyze research across varying fidelities and scales
- Full end-to-end smart grid capabilities
- Real, emulated, and simulated hardware/software for scalability
- Power simulation, modeling, and optimization of various forms
- Network simulation, modeling, and visualization of various forms
- Advanced hardware-in-the-loop cyber-physical simulation
- Security and protocol assessment tools (static/dynamic analysis, test harnesses, fuzzing)

From "TCIPG Testbed Overview" by Tim Yardley, Jeremy Jones, et al. TCIPG

State-of-the-art Co-simulation Techniques

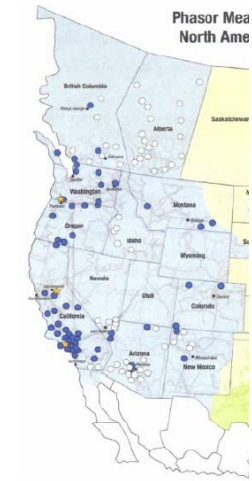
Table I: Overview of State-of-the-Art Co-Simulation Approaches

	Recent Focus	Power System Simulator	Network Simulator	Simulation Frameworks	Time Strategy	Scalability	Execution Mode
GECO [12][13]	PMU-based WAMPAC, high voltage grid	PSLF	NS-2	Ad-hoc (TCL linking)	Global event-driven	Large systems	NA
INSPIRE [14][15]	WAMPAC, high voltage grid	DIgSILENT PowerFactory	OPNET Modeler	IEEE 1516-2010 (HLA evolved)	Dynamic time stepped	Large systems	NA
EPOCHS [16]	Multi-agent protection and control systems	PSCAD/ EMTDC, PSLF	NS-2	IEEE 1516-2000 (HLA)	Fixed time stepped	Large systems	NA
ADEVS [17]	WAMPAC	ADEVS	NS-2	Ad-hoc (integrated in NS-2)	DEVS	Large systems	NA
VPNET [18]	WAMPAC	VTB	OPNET Modeler	Ad-hoc (Sockets)	Time stepped	Small systems	NA
GridSim [19]	WAMPAC	Powertech TSAT	GridStat	Ad-hoc	Fixed time stepped	Components can be distributed	Real-time + HIL
PowerNet [20]	Controlling power devices	Modelica	NS-2	Ad-hoc (Unix named pipes)	Time stepped	Small systems	NA
Bergmann et al. [21]	Evaluation of DERs and VPPs	NETOMAC	NS-2	Ad-hoc (JNI)	Time stepped	Small systems	Close to real-time
Babazadaeh et. al. [22][23]	WAMC, HVDC, low voltage/mid voltage Grid	OPAL-RT	OPNET SITL	Ad-hoc, emulated, sockets	Real-time	Small (HIL), medium (emulated)	Real-time
Greenbench [24]	Cyber security, low voltage grid	PSCAD	OMNeT ++	Ad-hoc (IPC)	Global event-driven	Tested for small systems	NA

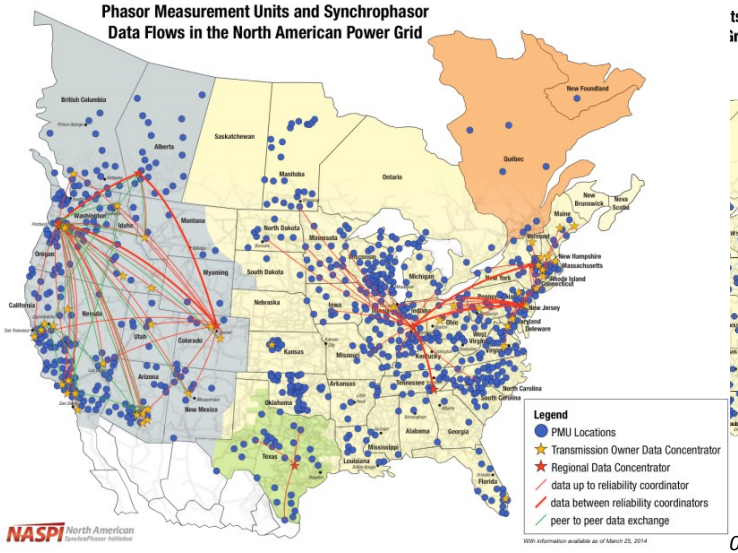
Virtual SCADA Testbed Objective

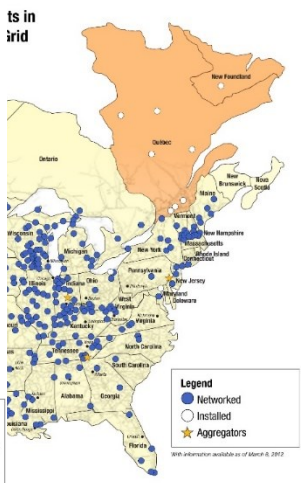
- Build a virtual SCADA testbed system with configurable software emulated sensors, actuators, and PLC, network emulators for communication, and SCADA system with data analytics, cyber security assessment, and vulnerability investigation.
- Designed to model and simulate different SCADA systems. The Virtual SCADA testbed is capable to integrate all the SCADA industries.
- With virtual testbed, can verify the control systems, vulnerability assessments, and risk analysis to improve cyber security.
- For the educational purpose, we will provide a user friendly GUI and let the testbed easy to understand and use.
- An open architecture, researchers or students can contribute to this testbed.

PMU based Wide Area Measurement Systems



Phasor Measurement Units (PM
2009



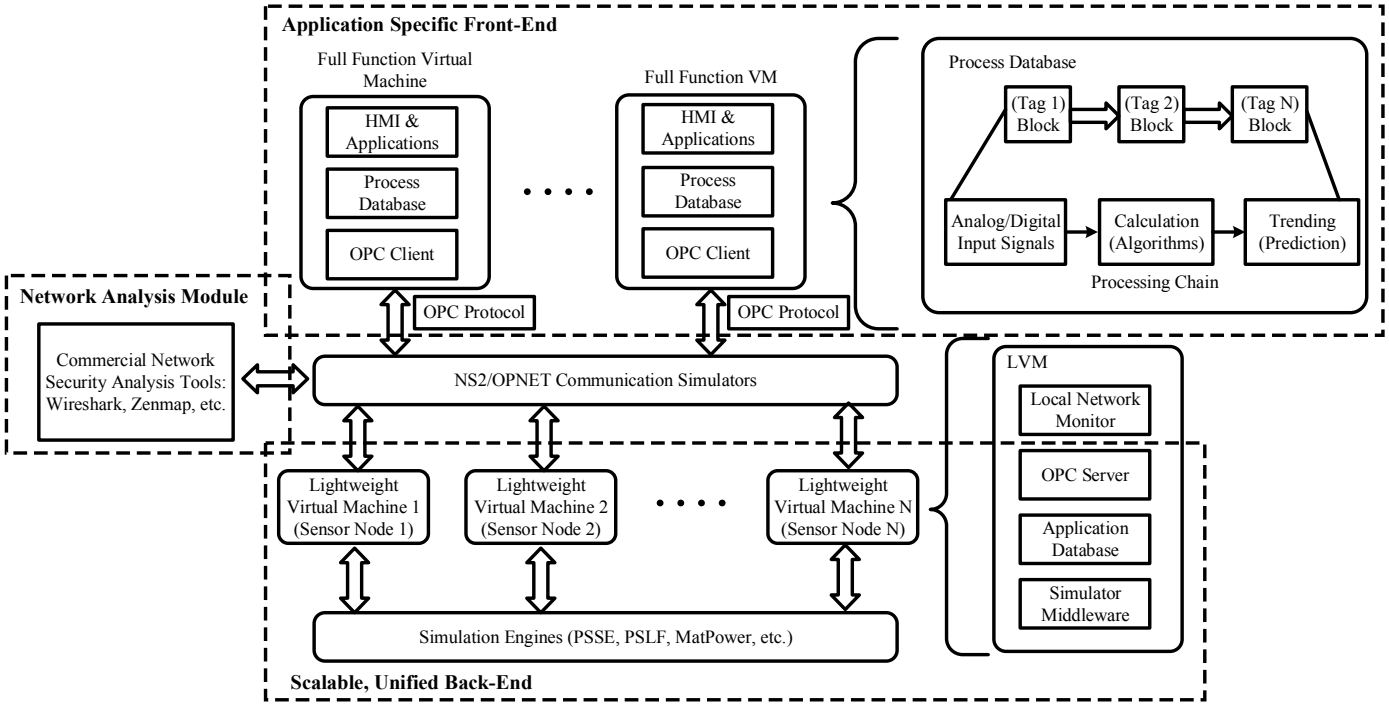


00 PMUs Installed.

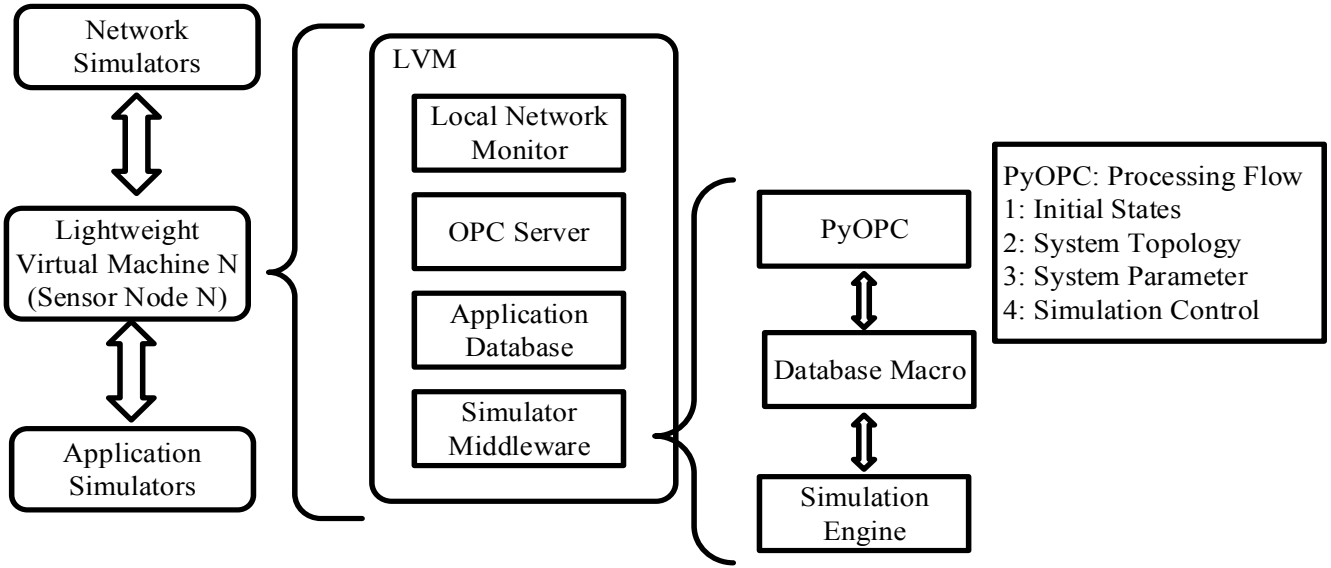
March 2014: Over 1000 PMUs installed.

Source: North American SynchroPhasor Initiative

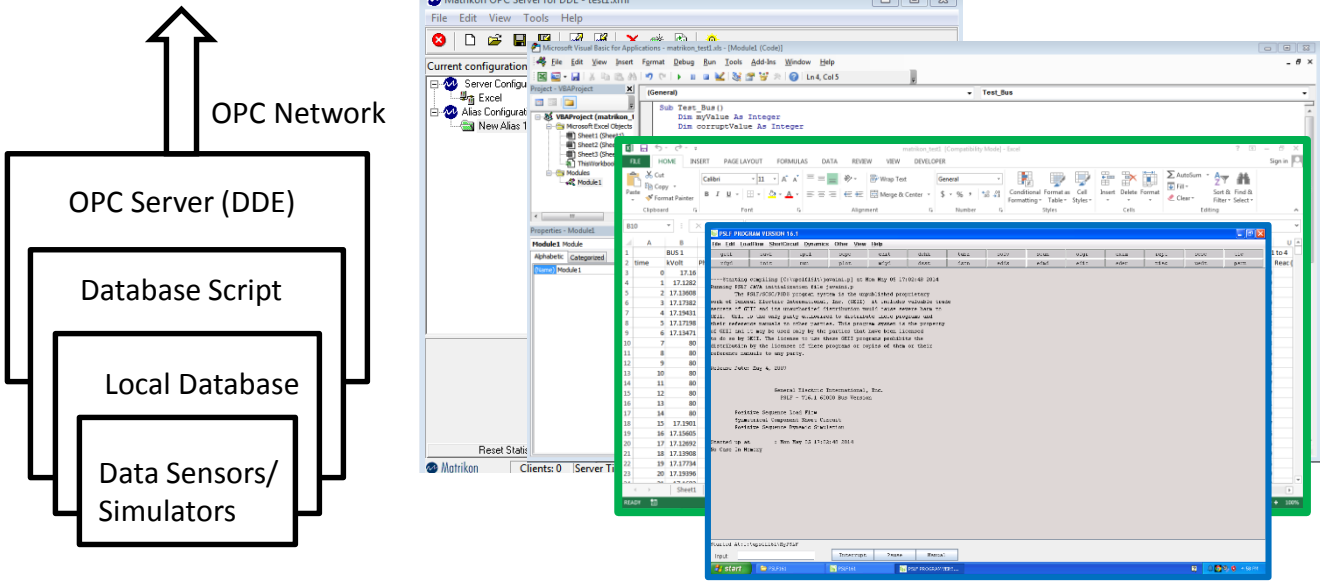
Hierarchical Software Architecture of VSCADA



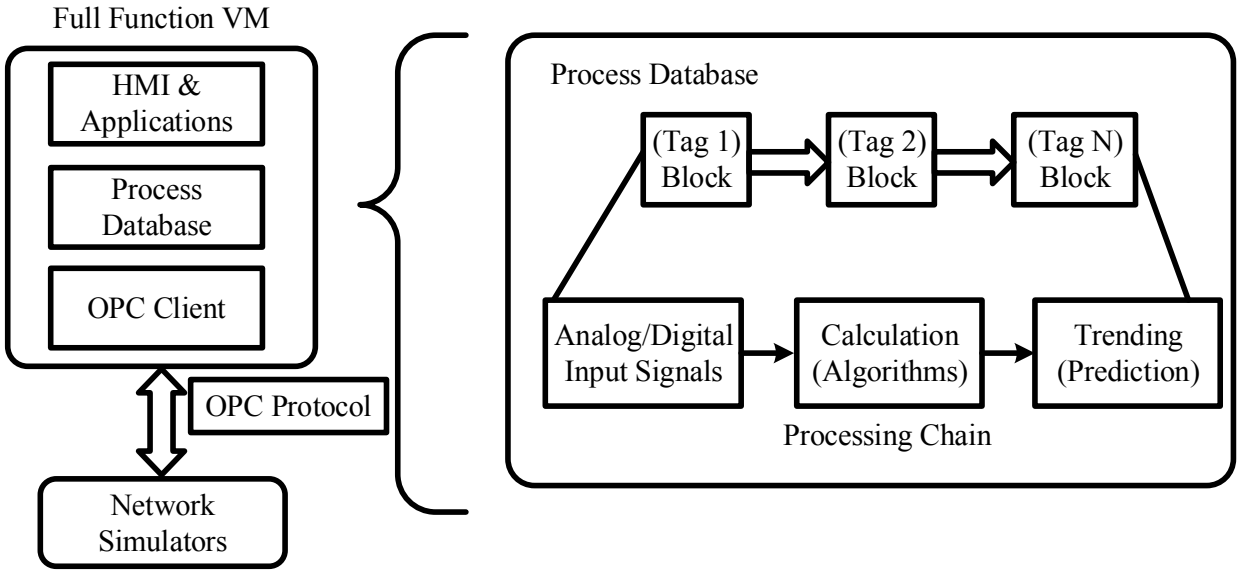
Back-End Infrastructure Function Block Diagram



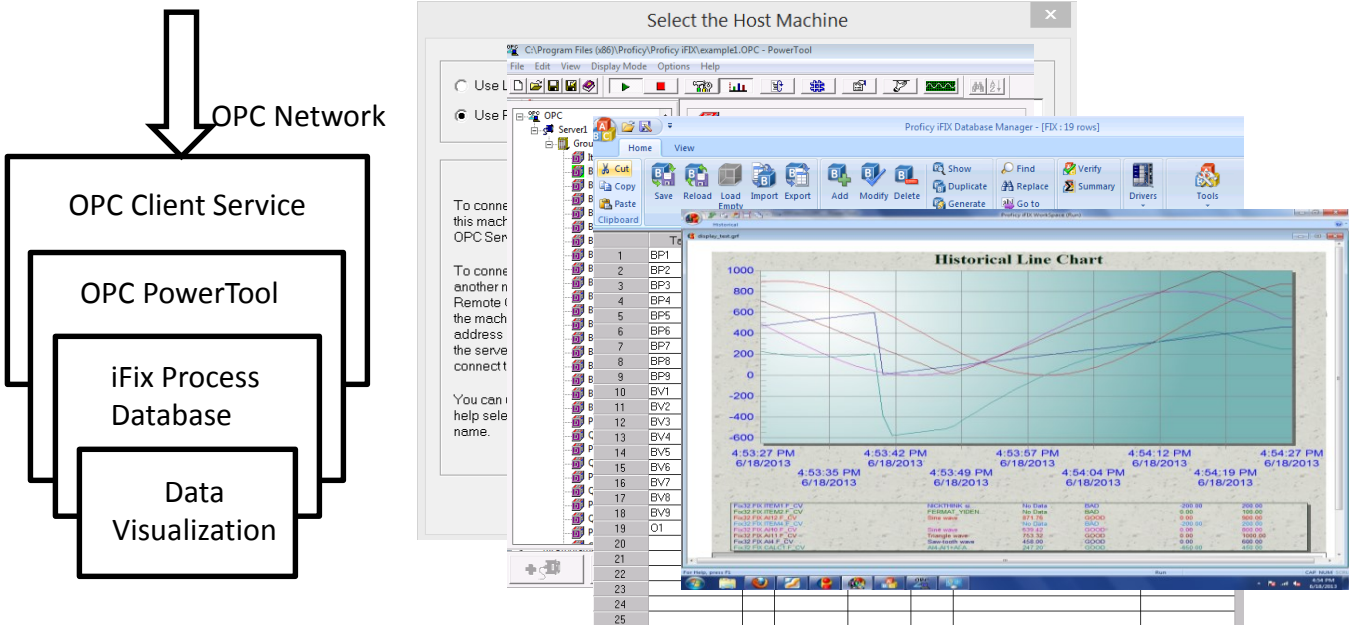
Hierarchical Implementation of Back End Construction



Front-End Infrastructure Function Block Diagram

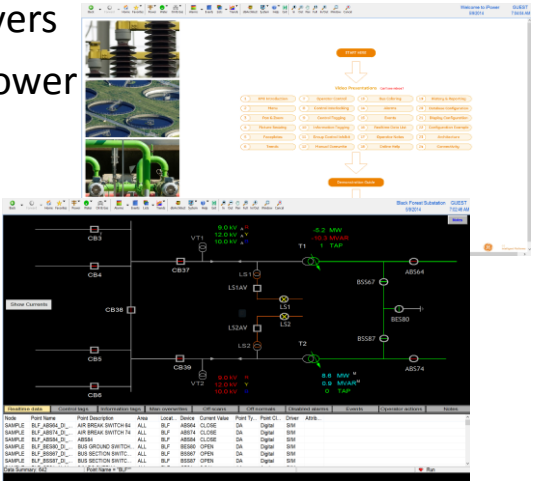


Hierarchical Implementation of Front End Construction



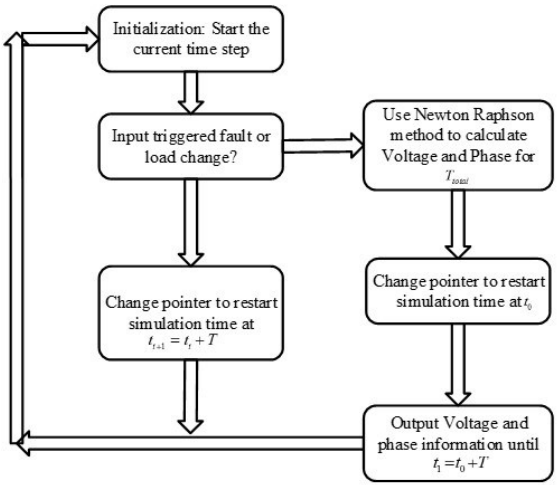
Implementing Software (GE iFix and iPower)

- GE Intelligent Platforms automation software
- Powerful software used around the world
- Extensive documentation and support existing
- Uses Visual Basic for Applications (VBA), ActiveX, and OLE for Process Control (OPC)
- Software discovers and configures I/O drivers
- Designed for electrical application with iPower
- Scalable from substation automation systems to complex computer networks in larger utility control rooms



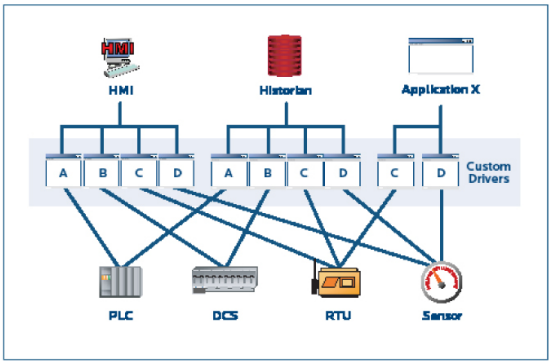
Implementing Simulation(PSS/E)

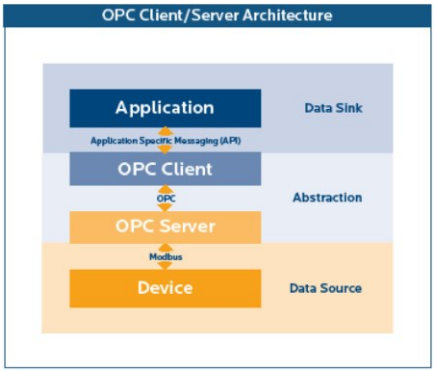
- Power system simulated by Power System Simulator for Engineering (PSS/E)
- PSS/E is a power system software package designed by GE which provides both steady-state and dynamic power system simulations
- PSS/E gives a library of electromechanical dynamic models and can simulate a system with up to 60000 buses. The software suite is written in Java and provides application-programming interfaces (APIs)
- Does dynamic simulation of faults



OPC Protocol

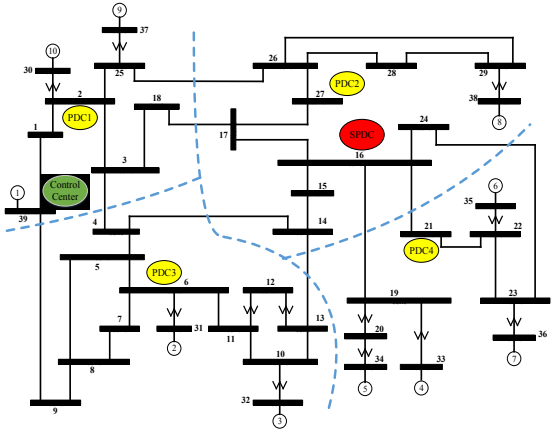
- OPC: OLE for process control, is a software interface standard that is widely used to allow Windows program to communicate with industrial hardware devices.
  - OPC aggregation: Connect an OPC client to several OPC servers.
  - OPC tunneling: Connect an OPC client to an OPC server over a network.
  - OPC bridging: Connect an OPC server to another OPC server to share data.
- OPC DataHub is a combination OPC server and OPC client that supports multiple connections. It can connect to several OPC servers.





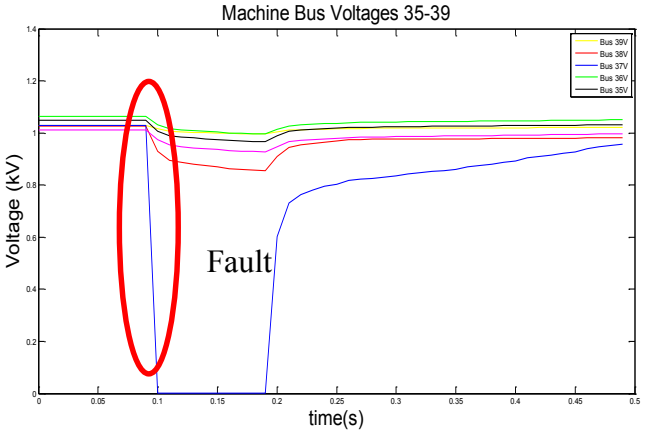
39-Bus Case Study

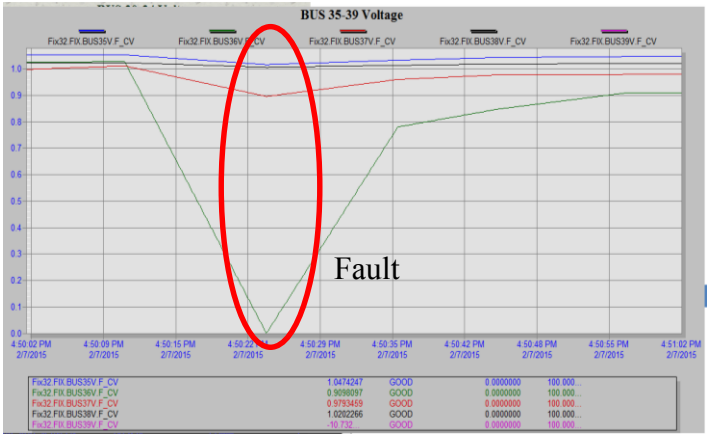
- Created 39-bus system shown to right, with a allowed at all generator buses.
- User is be able to detect when a fault occurs and then be able to trip the fault
- PSS/E is used to create a time stamped simulation of this scenario using load values from the IEEE 39 Bus system as a reference.



- Values are created for a 5-minute interval of time.
- Initially values are created for the 39-bus system in steady state and for when a fault is triggered in the 39-Bus system.
- 39 buses with 10 generators with faults and load change capabilities at each generator

Bus Fault Example in iFix



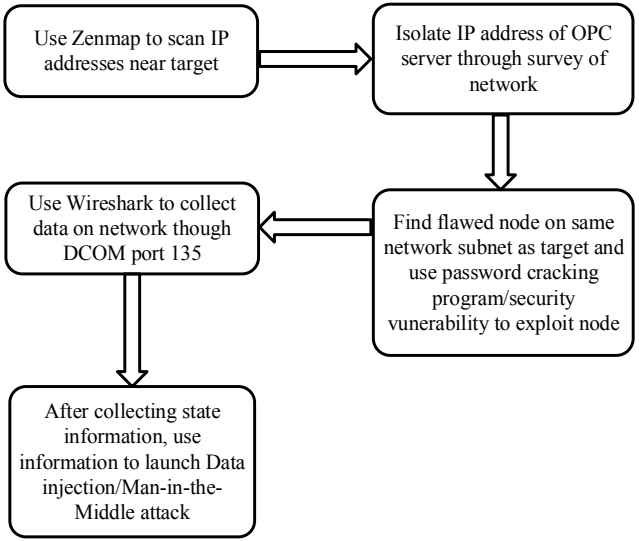


1. Demonstrated fault for 39 Bus system in simulation

Screenshot of Demonstrated fault in iFIX HMI

Network Security Case Study

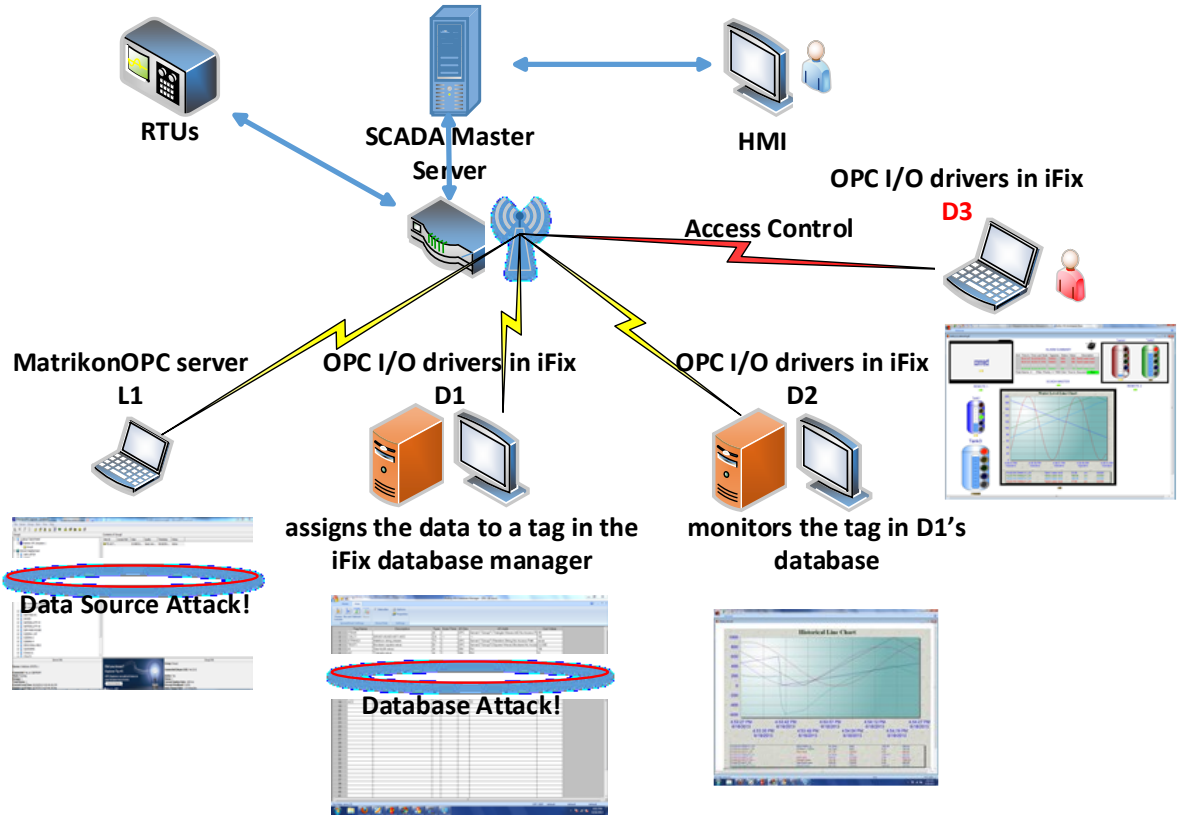
- Simulate scenario where we use network access to the SCADA server to learn information on network infrastructure.
- Use that information to launch data injection attack that can cause bus fault.
- Using System infrastructure information, can exploit HMI information to cause two bus faults that leads to cascading failure.



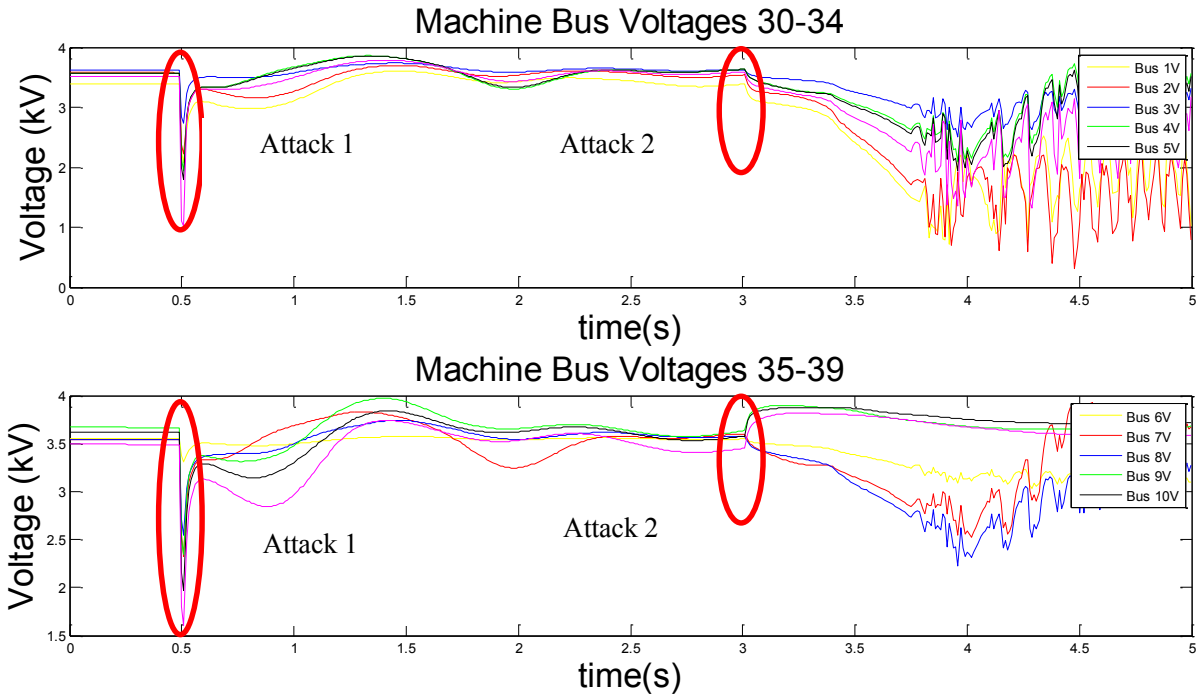
Cascading System Example

- Creating a three-phase fault on the line between buses 16 and 17 at time 1 second after running the system under steady-steady operating condition.
- The fault lasts 100m seconds before the relays act and trip off the line to clear the fault. After three seconds, thermal limit relays will act and trip the line between buses 15 and 16.
- Causes huge increase in the rotor angle difference between generators. All these events will be concluded by a complete shutdown of the power system.

Cyber Vulnerability Assessment



Cascading Failure Example



Demonstrated attacks for 39 Bus system in simulation

VSCADA Platform

VirginiaTech

Electrical & Computer Engineering

Virtual SCADA Lab

FERMAT *Lab*

Introduction: *Virtual Supervisory Control and Data Acquisition (SCADA) Lab developed by FERMAT (Formal Engineering Research with Models, Abstraction, and Transformations) Lab, Electrical and Computer Engineering Department, Virginia Tech is an educational and research platform with configurable software emulated sensors, actuators and/or Programmable Logic Controllers (PLCs), network emulators for communication simulation, and SCADA system with data analytics, cyber security assessment, and vulnerability investigation.*

VirginiaTech

Electrical & Computer Engineering

Virtual SCADA Lab

FERMAT *Lab*

Power Systems

Oil & Gas Transportation

Water Supply Distribution

Transportation

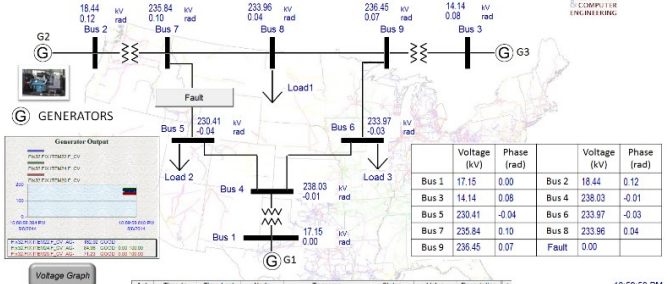
Manufacturing

Other Critical Industries

Power System Demo

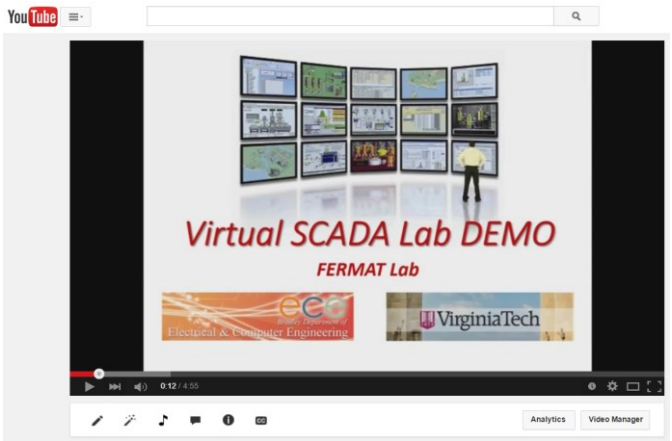
VirginiaTech

ece ELECTRICAL & COMPUTER ENGINEERING



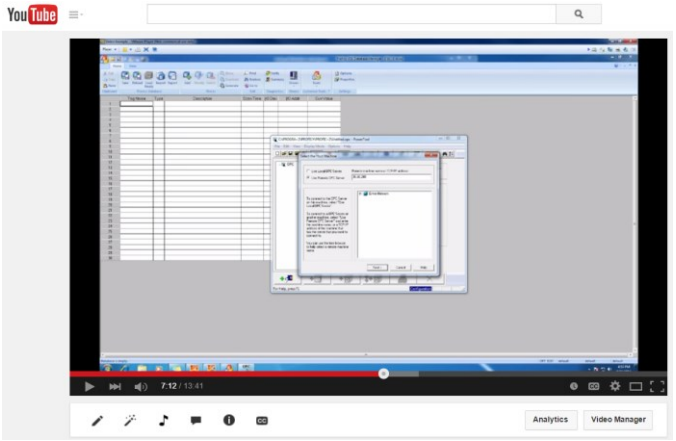
	Voltage (kV)	Phase (rad)		Voltage (kV)	Phase (rad)
Bus 1	17.15	0.00	Bus 2	18.44	0.12
Bus 3	14.14	0.08	Bus 4	238.03	-0.01
Bus 5	230.41	-0.04	Bus 6	233.97	-0.03
Bus 7	235.84	0.10	Bus 8	233.96	0.04
Bus 9	236.45	0.07	Fault	0.00	

Introduction Video about our Virtual SCADA Lab



Short Video Address:
https://www.youtube.com/watch?v=IrZ_1Butwb8

Long Video Address:
https://www.youtube.com/watch?v=XMFAm25uzZs



iFIX Tutorial Part 1: Software Preparation
https://www.youtube.com/watch?v=39eTO6UVjXs

iFIX Tutorial Part 2: Create Tags and OPC server
https://www.youtube.com/watch?v=39eTO6UVjXs

Conclusion

- Distributed Virtual Supervisory Control and Data Acquisition (VSCADA) Lab developed by FERMAT (Formal Engineering Research with Models, Abstraction, and Transformations) Lab at Virginia Tech, is an educational and research platform with configurable software emulated sensors, actuators and/or Programmable Logic Controllers (PLCs), network emulators for communication simulation, and SCADA system with data analytics, cyber security assessment, and vulnerability investigation.
- The Virtual SCADA Lab can support multi-user remote access, and simultaneous running applications, etc.
- Since it is purely defined by software, it provides the capability to reconfigure the virtual systems into different scenarios.
- The unified architecture can seamlessly integrate various kinds of simulators (real-time/non real-time) according to the applications.

References

1. Avik Dayal, Yi Deng, Ahmad Tbaileh, Sandeep Shukla, "VSCADA: A Reconfigurable Virtual SCADA Test-bed for Simulating Power Utility Control Center Operations", Power and Energy Society General Meeting (PES), 2015 IEEE, Denver, CO, July 26-30 2015.
2. Avik Dayal, Ahmad Tbaileh, Yi Deng, Sandeep Shukla, “Distributed VSCADA: An Integrated Heterogeneous Framework for Power System Utility Security Modeling and Simulation”, 2015 IEEE Workshop on Modeling and Simulation of Cyber-Physical Energy Systems, 13 April 2015, Seattle, WA, USA.