Smart Grid Testbed Overview

The Whirlwind Tour

Tim Yardley

Assistant Director, Testbed Services

Information Trust Institute

yardley@illinois.edu

University of Illinois Urbana-Champaign

Smart Grid Testbed Overview

- Testbed equipment and simulators span the grid system
  - Generation
    - Power system modeling, RTDS
  - Transmission & Distribution
    - Relays, Substation computers, PMUs, PDCs
    - EMS, Planning, Protocol test-harnesses
  - Advanced metering
    - Meter platforms, emulation testbed
  - Consumers
    - Energy monitoring, Home automation

What's the main purpose?

- Core Smart Grid Security Research (End-To-End)
  - Trustworthy, Resilient Critical Infrastructure
  - Systematic, not just single component view
- "Small-wire"
  - No high voltage, we work through our partners like Ameren for that.
- More than just a demonstration of technology
  - We heavily USE our equipment, software, etc.
- Not an engineering display of best practices
  - Although, we can do that too.

Composition

- Center Funding
  - Trustworthy Cyber Infrastructure for the Power Grid (TCIPG) – DHS, DOE
  - Illinois Center for a Smarter Electric Grid (ICSEG) – State of Illinois DCEO
  - Center for Assured Critical Application and Infrastructure Security (CACAIS) – Office of Naval Research
- Industry funding
- Donations

Testbed Donations Provided By

byres security inc
intrinsically secure

OSIsoft.

endace

PowerWorld Corporation
The Visual Approach to Analyzing Power Systems

Trilliant

INSTEP

SEL SCHWEITZER ENGINEERING LABORATORIES

Mu Dynamics

OSI

Electric Power Group

SPACE-TIME INSIGHT

NATIONAL INSTRUMENTS

SISCO

U.S.NRC
United States Nuclear Regulatory Commission

Itron

GE

IBM

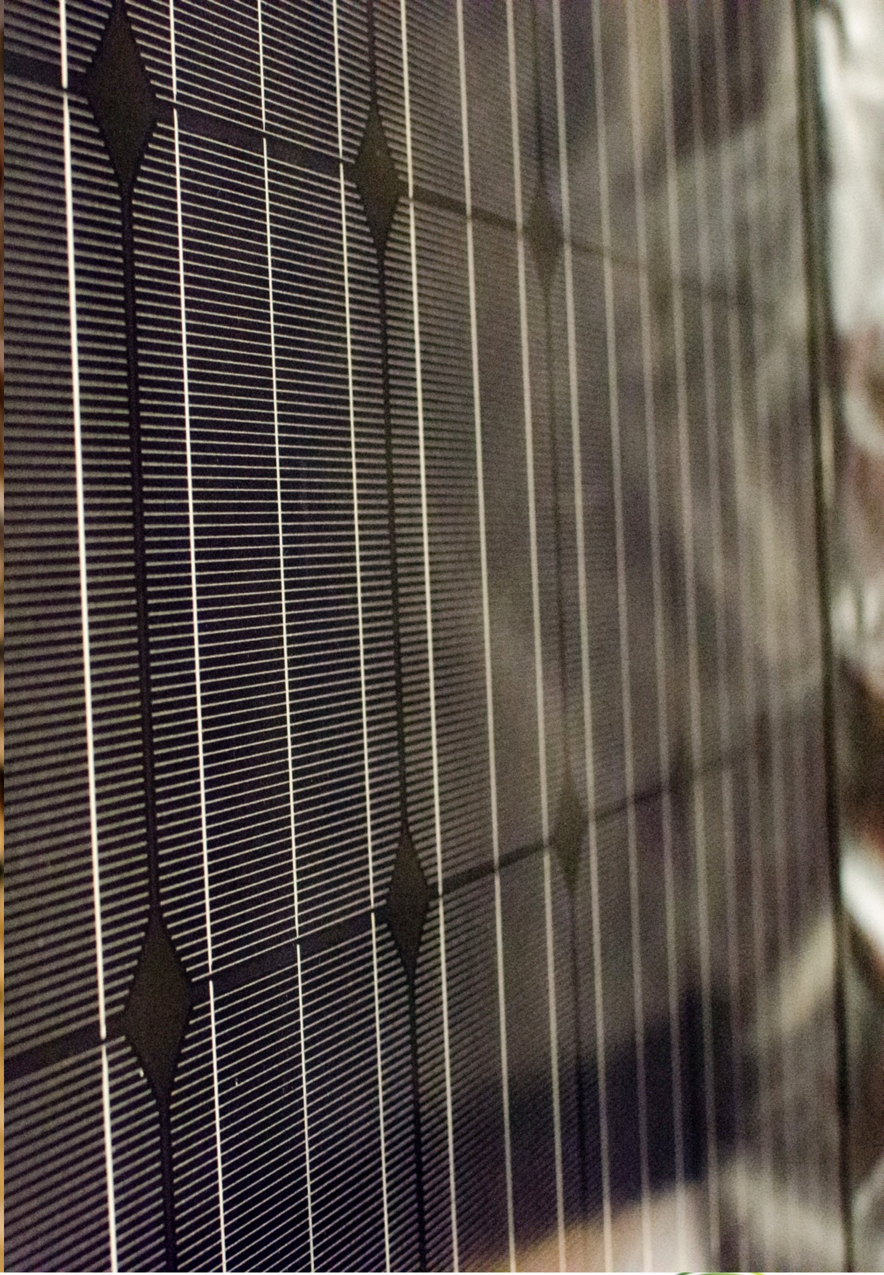
BAYSHORE NETWORKS

The Testbed Through Images

VISUAL TOUR

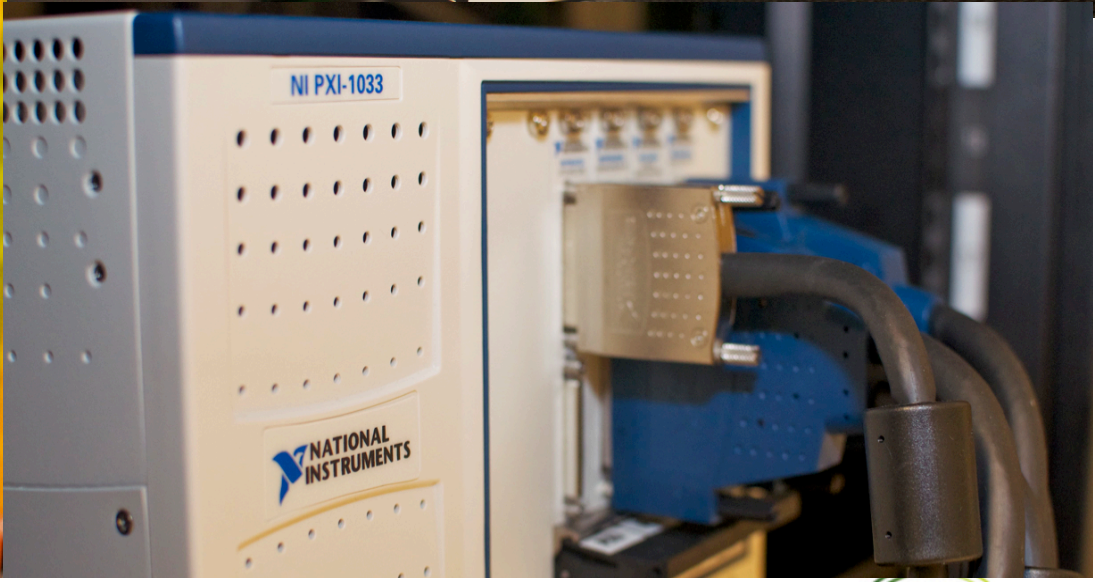
TCIPG Rack 1
TCIPG Rack 2
TCIPG Rack 3
TCIPG Rack 4
TCIPG Mu Dynamics
DELL
Donated by HP

SEL-421
SEL
RTDS ™
Real-Time Digital Simulator
RTDS
DIGITAL CHANNELS
DIGITAL IN
GROUND
DIGITAL OUT
PIN



120VAC/DC
PASS
FAIL
ALARM
TEMP
BAT LOW
POWER MODULE
MODEL 8310
120VAC/DC
PASS
FAIL
ALARM
TEMP
BAT LOW
POWER MODULE
NETWORK
SERIAL
3008
3008
3008

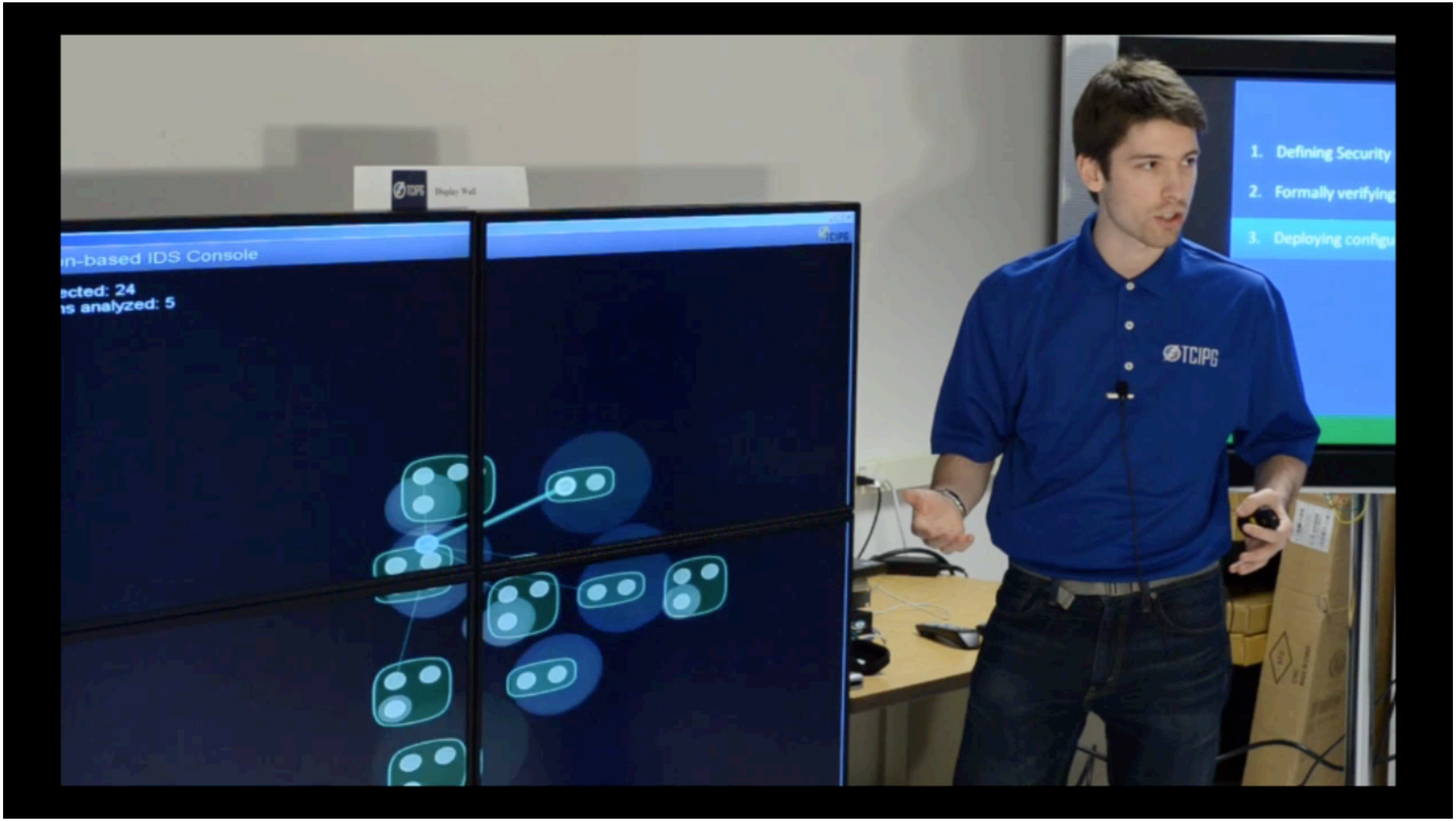
TRICONEX
BATTERY
A
B
C
TRICONEX
TRICON
FM
CONTACTS NOT FOR USE
HAZARDOUS LOCATIONS


NI PXI-1033
NATIONAL INSTRUMENTS

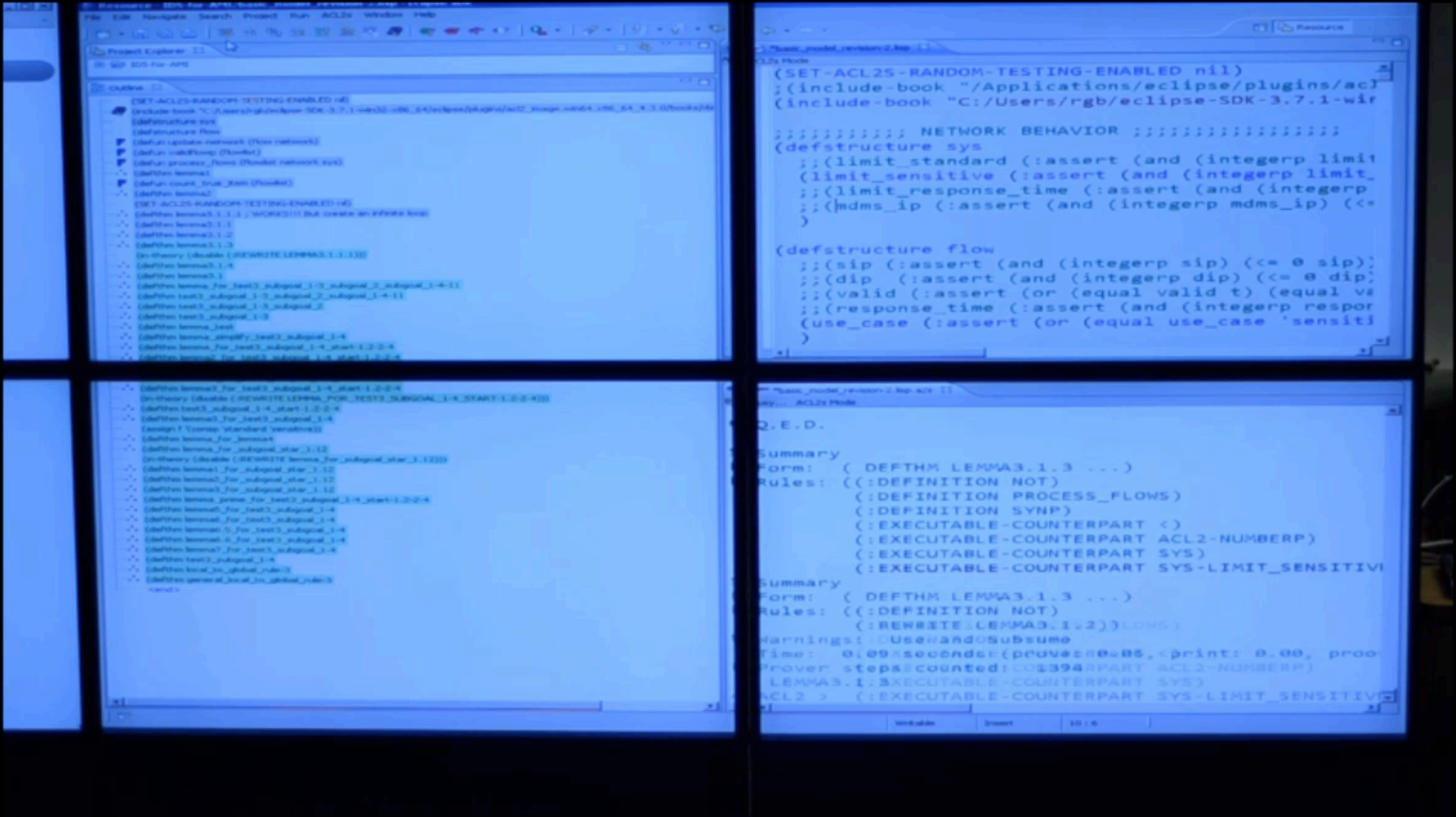
TCIPG
DETER
DETER MANAGEMENT

Visualization Wall

Interactive Visualization



Formal Verification

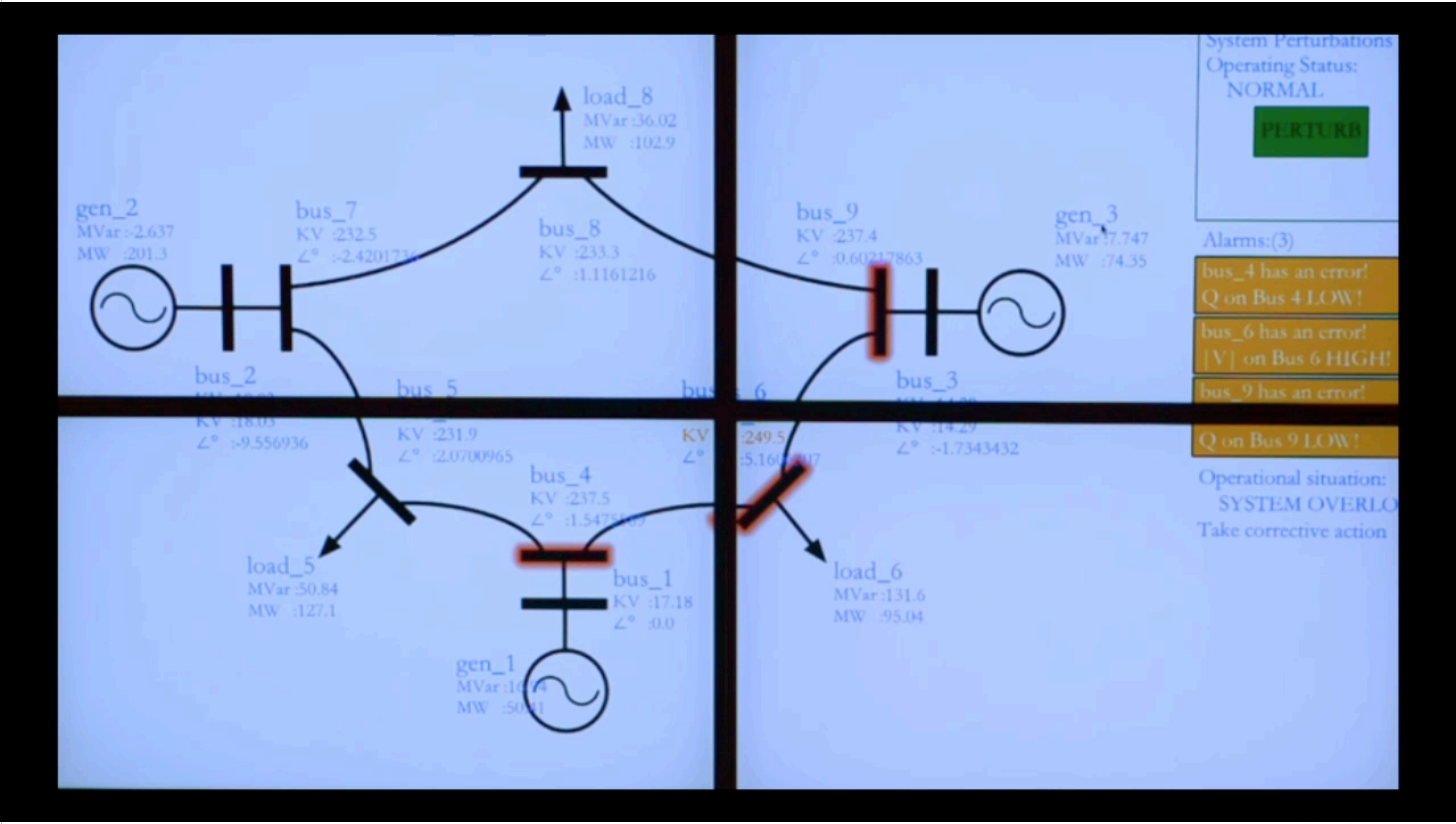


```
(SET-ACL2S-RANDOM-TESTING-ENABLED nil)
(include-book "C:/Users/rgb/eclipse-SDK-3.7.1-win32-x86_64/eclipse/plugins/acl2_image.win64.x86_64_4.3.0/books/de
(defstructure sys
(defstructure flow
(defun update-network (flow network)
(defun validflowp (flowlst)
(defun process_flows (flowlst network sys)
(defthm lemma1
(defun count_true_item (flowlst)
(defthm lemma2
(SET-ACL2S-RANDOM-TESTING-ENABLED nil)
(defthm lemma3.1.1.1 ; WORKS!!! But create an infinite loop
(defthm lemma3.1.1
(defthm lemma3.1.2
(defthm lemma3.1.3
(in-theory (disable (:REWRITE LEMMA3.1.1.1)))
(defthm lemma3.1.4
(defthm lemma3.1
(defthm lemma_for_test3_subgoal_1-3_subgoal_2_subgoal_1-4-11
(defthm test3_subgoal_1-3_subgoal_2_subgoal_1-4-11
(defthm test3_subgoal_1-3_subgoal_2
(defthm test3_subgoal_1-3
(defthm lemma_test
(defthm lemma_simplify_test3_subgoal_1-4
(defthm lemma_for_test3_subgoal_1-4_start-1.2-2-4
(defthm lemma2_for_test3_subgoal_1-4_start-1.2-2-4
(defthm lemma3_for_test3_subgoal_1-4_start-1.2-2-4
(in-theory (disable (:REWRITE LEMMA_FOR_TEST3_SUBGOAL_1-4_START-1.2-2-4)))
(defthm test3_subgoal_1-4_start-1.2-2-4
(defthm lemma3_for_test3_subgoal_1-4
(assign f '(cons 'standard 'sensitive))
(defthm lemma_for_lemma4
(defthm lemma_for_subgoal_star_1.12
(in-theory (disable (:REWRITE lemma_for_subgoal_star_1.12)))
(defthm lemma1_for_subgoal_star_1.12
(defthm lemma2_for_subgoal_star_1.12
(defthm lemma3_for_subgoal_star_1.12
(defthm lemma_prime_for_test3_subgoal_1-4_start-1.2-2-4
(defthm lemma5_for_test3_subgoal_1-4
(defthm lemma6_for_test3_subgoal_1-4
(defthm lemma6.5_for_test3_subgoal_1-4
(defthm lemma6.6_for_test3_subgoal_1-4
(defthm lemma7_for_test3_subgoal_1-4
(defthm test3_subgoal_1-4
(defthm local_to_global_rule3
(defthm general_local_to_global_rule3
<end>
```

```
(SET-ACL2S-RANDOM-TESTING-ENABLED nil)
;(include-book "/Applications/eclipse/plugins/acl
(include-book "C:/Users/rgb/eclipse-SDK-3.7.1-win

;;;;;;;;;;;; NETWORK BEHAVIOR ;;;;;;;;;;;;;;;;;;;
(defstructure sys
  ;;(limit_standard (:assert (and (integerp limit
  (limit_sensitive (:assert (and (integerp limit_
  ;;(limit_response_time (:assert (and (integerp
  ;;(mdms_ip (:assert (and (integerp mdms_ip) (<=
  )

(defstructure flow
  ;;(sip (:assert (and (integerp sip) (<= 0 sip);
  ;;(dip  (:assert (and (integerp dip) (<= 0 dip;
  ;;(valid (:assert (or (equal valid t) (equal va
  ;;(response_time (:assert (and (integerp respor
  (use_case (:assert (or (equal use_case 'sensiti
  )
```

```
Q.E.D.

Summary
Form:  ( DEFTHM LEMMA3.1.3 ...)
Rules: ((:DEFINITION NOT)
        (:DEFINITION PROCESS_FLOWS)
        (:DEFINITION SYNP)
        (:EXECUTABLE-COUNTERPART <)
        (:EXECUTABLE-COUNTERPART ACL2-NUMBERP)
        (:EXECUTABLE-COUNTERPART SYS)
        (:EXECUTABLE-COUNTERPART SYS-LIMIT_SENSITIVI
Summary
Form:  ( DEFTHM LEMMA3.1.3 ...)
Rules: ((:DEFINITION NOT)
        (:REWRITE LEMMA3.1.2))
Warnings:  Use and Subsume
Time:  0.09 seconds (prove: 0.06, print: 0.00, proo
Prover steps counted: 1394
 LEMMA3.1.3
ACL2 >
```

Custom Power System Visualization



System Perturbations
Operating Status:
NORMAL

Alarms:(3)

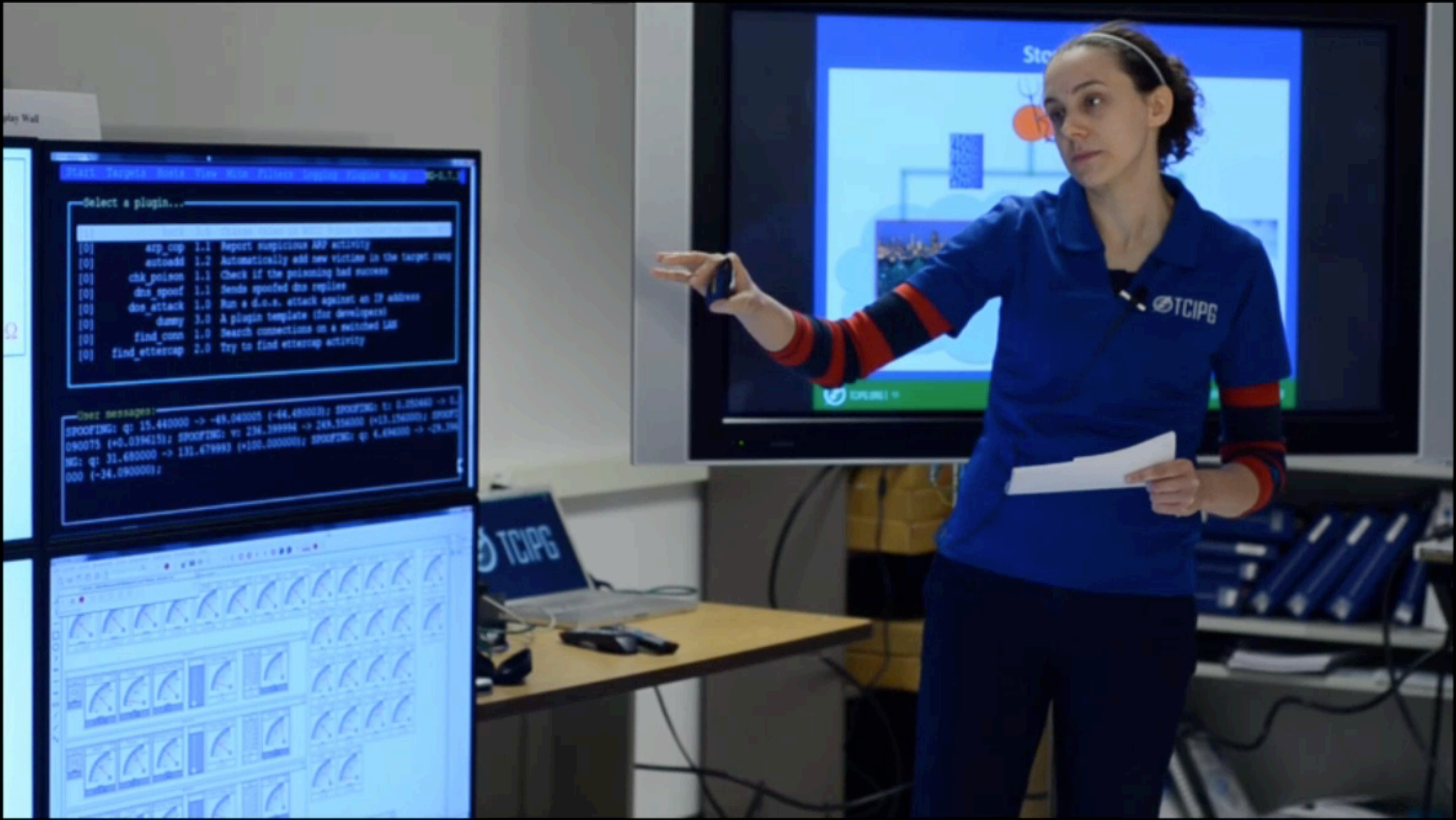
bus_4 has an error!
Q on Bus 4 LOW!

bus_6 has an error!
|V| on Bus 6 HIGH!

bus_9 has an error!
Q on Bus 9 LOW!

Operational situation:
SYSTEM OVERLO
Take corrective action

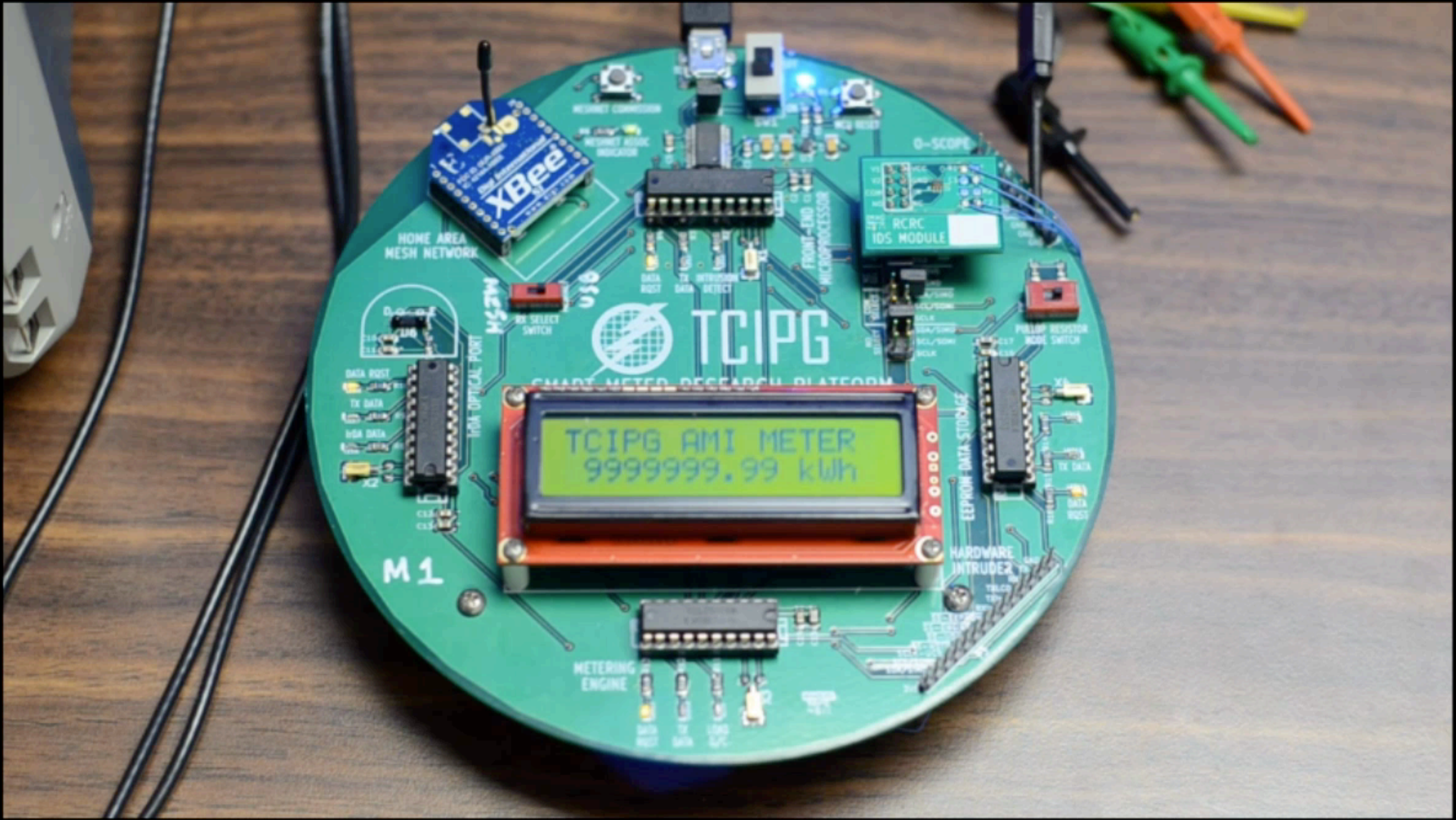
Multi-System Integrated Demonstration



```
Select a plugin...
[0]        arp_cop  1.1  Report suspicious ARP activity
[0]        autoadd  1.2  Automatically add new victims in the target rang
[0]     chk_poison  1.1  Check if the poisoning had success
[0]      dns_spoof  1.1  Sends spoofed dns replies
[0]     dos_attack  1.0  Run a d.o.s. attack against an IP address
[0]          dummy  3.0  A plugin template (for developers)
[0]      find_conn  1.0  Search connections on a switched LAN
[0]  find_ettercap  2.0  Try to find ettercap activity

User messages:
SPOOFING: q: 15.440000 -> -49.040005 (-64.480003); SPOOFING: t: 1.050460 -> 5.
090075 (+0.039615); SPOOFING: v: 236.399994 -> 249.556000 (+13.156000); SPOOF
NG: q: 31.680000 -> 131.679993 (+100.000000); SPOOFING: q: 4.694000 -> -29.396
000 (-34.090000);
```

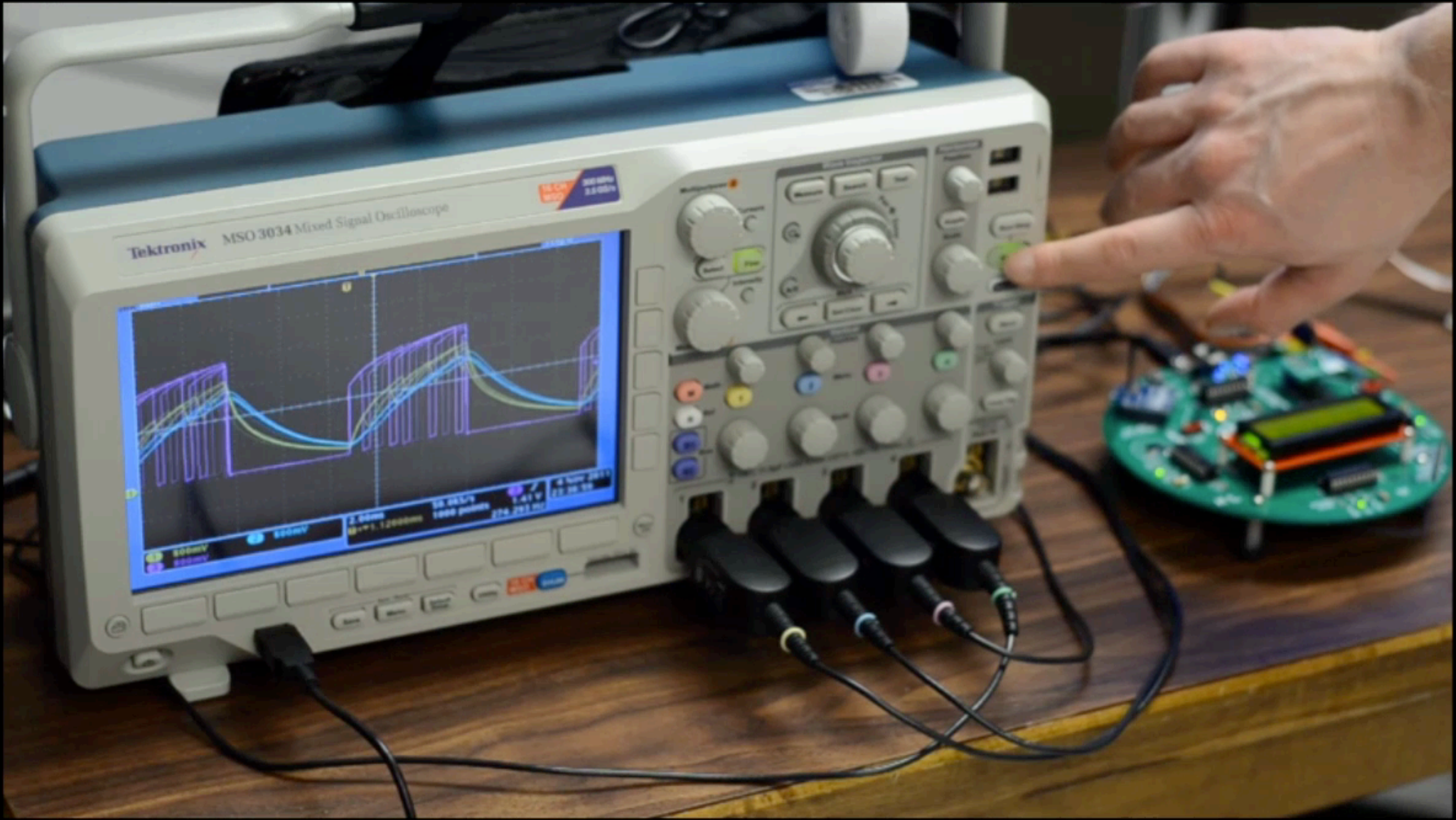
PMU Interaction

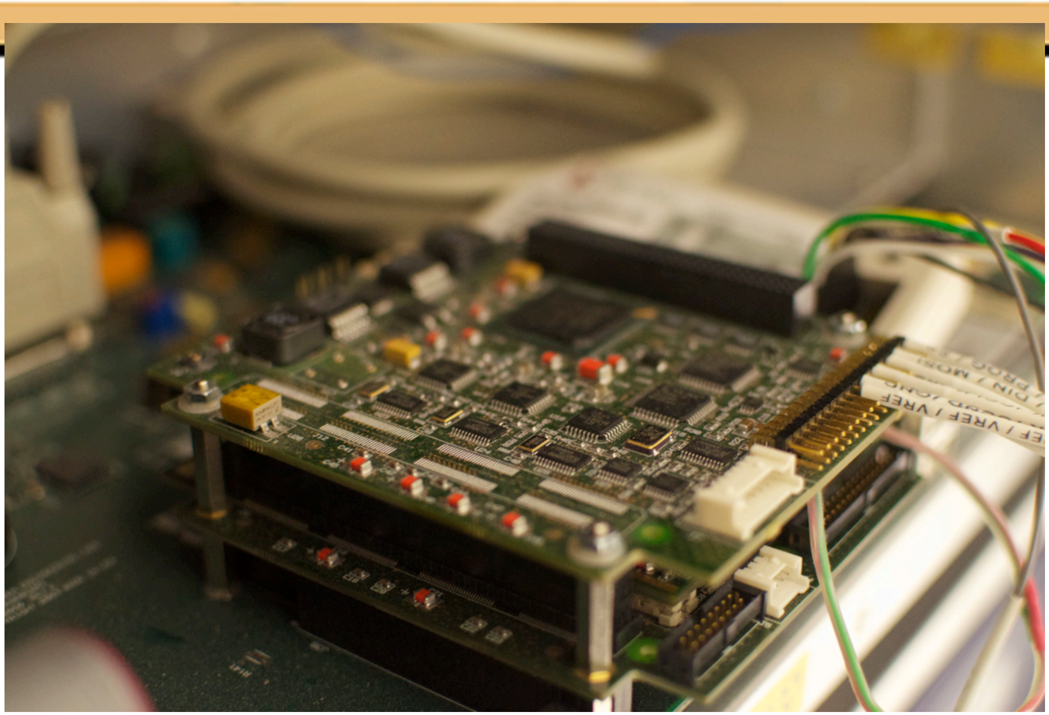
TCIPG Smart Meter Research Platform



DANGER / PELIGRO
HAZARD OF ELECTRICAL SHOCK OR BURN
SERVICE BY UTILITY AUTHORIZED PERSONNEL ONLY
DO NOT PAINT OVER OR REMOVE THIS LABEL
PELIGRO DE DESCARGA ELECTRICA O QUEMADURA
SOLAMENTE PERSONAS AUTORIZADAS DE LA COMPANIA
ELECTRICA PUEDEN MANTENARLO
NO PINTE ENCIMA NI REMUEVA ESTA ETIQUETA
CENTRON
07 21130548
CL200 240V 3W TYPE C2SOD 30TA 1.0Kh
MARKETING SAMPLE
306 382 289
OpenWay
Itron
USA
CL200 240V 3W TYPE C2SOD 30TA 1.0Kh
MARKETING SAMPLE
306 382 306
OpenWay

Hardware Tracing





SEL
SCHWEITZER ENGINEERING LABORATORIES
137:14:42:47

RTAC
SEL-3530
REAL-TIME AUTOMATION CONTROLLER
AUX 7
AUX 8
AUX 9
ETH F
USB A
USB B
Mu Dynamics
Mu-8000

University of Illinois Urbana-Champaign

TCIPG Testbed
made possible through the generous donations of:
Byres Security
Endace
GE
InStep Software LLC
Mu Dynamics
Open Systems International
OSIsoft
PowerWorld
Schweitzer Engi
Siemens AG
Space Time
Trilli
SAMSUNG
SAMSUNG

THE PIECES

Capabilities

- Full end-to-end “Smart Grid” capabilities
- Advanced Metering Infrastructure (AMI)
- Real, Emulated, and Simulated Hardware/Software
- Real data from the grid, Industry partners, etc.
- Power Simulation, Modeling, and Optimization
- Network Simulation and Modeling, Visualization
- Hardware-in-the-loop cyber-physical simulation
- WAN/LAN/HAN integration and probes
- Security and Protocol assessment tools (static/dynamic analysis, test harnesses, fuzzing)

Hardware/Software

- RTDS, PowerWorld, PSSE, PSCAD, PSLF, DSAtools, DynRed
- RINSE, testBench, LabView, OSI PI, OSIi Monarch, SEL Suites
- GPSs, Sub. Comps, Relays, PMUs, Testing Equipment, PLCs, Security Gateways, NI platforms
- Power Analysis Tools, PDCs, Data Analytics
- Full AMI deployment (meters, relays, MDMS), TCIPG Smart Meter Research Platform
- RTUs, F-Net, Inverters, Oscilloscopes, Firewalls, Embedded devices, Sensors, Spectrum analyzers, SIEMs, IDSs
- Home EMS, Energy Monitoring devices, Zigbee, Automation
- Display Wall, Visualization Platforms (STI, RTDMS), Training
- Mu Dynamics, Fortify, Security Research tools
- DETER integration and cyber-physical extension

EXAMPLE RESEARCH

Example Research

- Data Quality Investigation
  - Sensor vs Infrastructure error investigation and quantification
  - Methods for active detection of sensor tampering
  - Combined measurement validation
- Protocol Assessment
  - AMI specification-based IDS
  - Protocol security extension analysis
  - Specification assessments/analysis for flaws
- Architecture Assessments
  - AMI deployments
  - Firewall connectivity and security policy analysis

Example Research

- Next Generation Architectures
  - OpenFlow combined with vPro to control intrusions/infections
- Time synchronization
  - Intelligent GPS spoofing
  - System-wide effect, power system impact
- Application of/to emerging solutions
  - AMI operations/visualization tools
  - PMU gateways
  - SIEMs, SCADA-specific IDS sensors
  - Protocol Security (Encryption, Authentication, Authorization)
  - IEEE 1588 Time Synchronization

Example Research

- Solar PV Labs (all w/ research capabilities)
  - Building our own in-building lab
  - Putting up small scale solar on rooftops
  - Campus is launching 10-20MW scale solar as well
- Abbott Power Plant and UIUC Distribution Grid
- What we are studying
  - Microinverters (AC systems)
  - Microgrids
  - Controlled Loads
  - Safety
  - Installation
  - Permitting
  - Home EMS

Example Related Work

- Honeywell RBAC
  - Research, develop and commercialize a role-based access control (RBAC) driven, least privilege architecture for control systems
- Telcordia Protocol Analysis
  - Research energy-sector communication protocol vulnerabilities, and develop mitigations that harden these protocols against cyber-attack and that enforce proper communications within energy delivery systems
- SIEGate
  - Secure Information Exchange Gateway for the Electric Sector

… AND MUCH MORE!