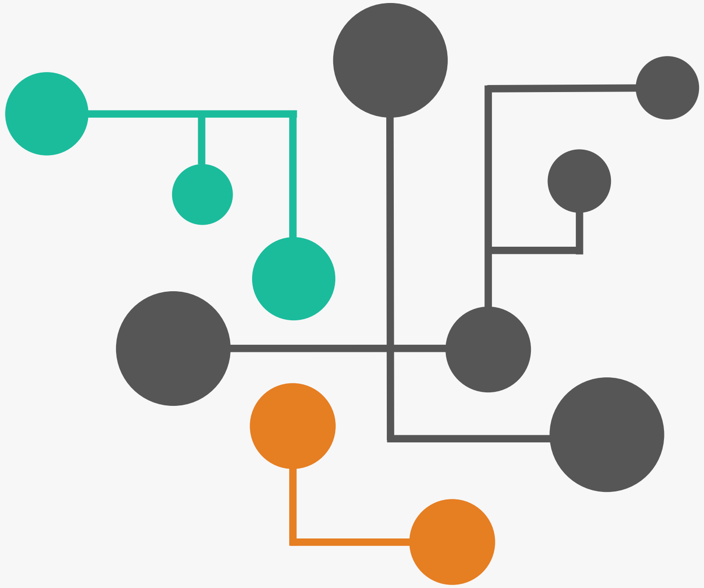
CREDC

CYBER RESILIENT ENERGY DELIVERY CONSORTIUM

Seminar Series



CEER

Cyber-Physical Experimentation Environment for RADICS

Advancing the state of art, CEER is a game changer.

A generational leap in capabilities for Cyber-Physical Experimentation in the Electric Power Grid

Increased usability, capability, and rigor.

Today's solutions

Why they don’t work

✗ Not True to Reality

✗ Can’t Scale

✗ Difficult to Use

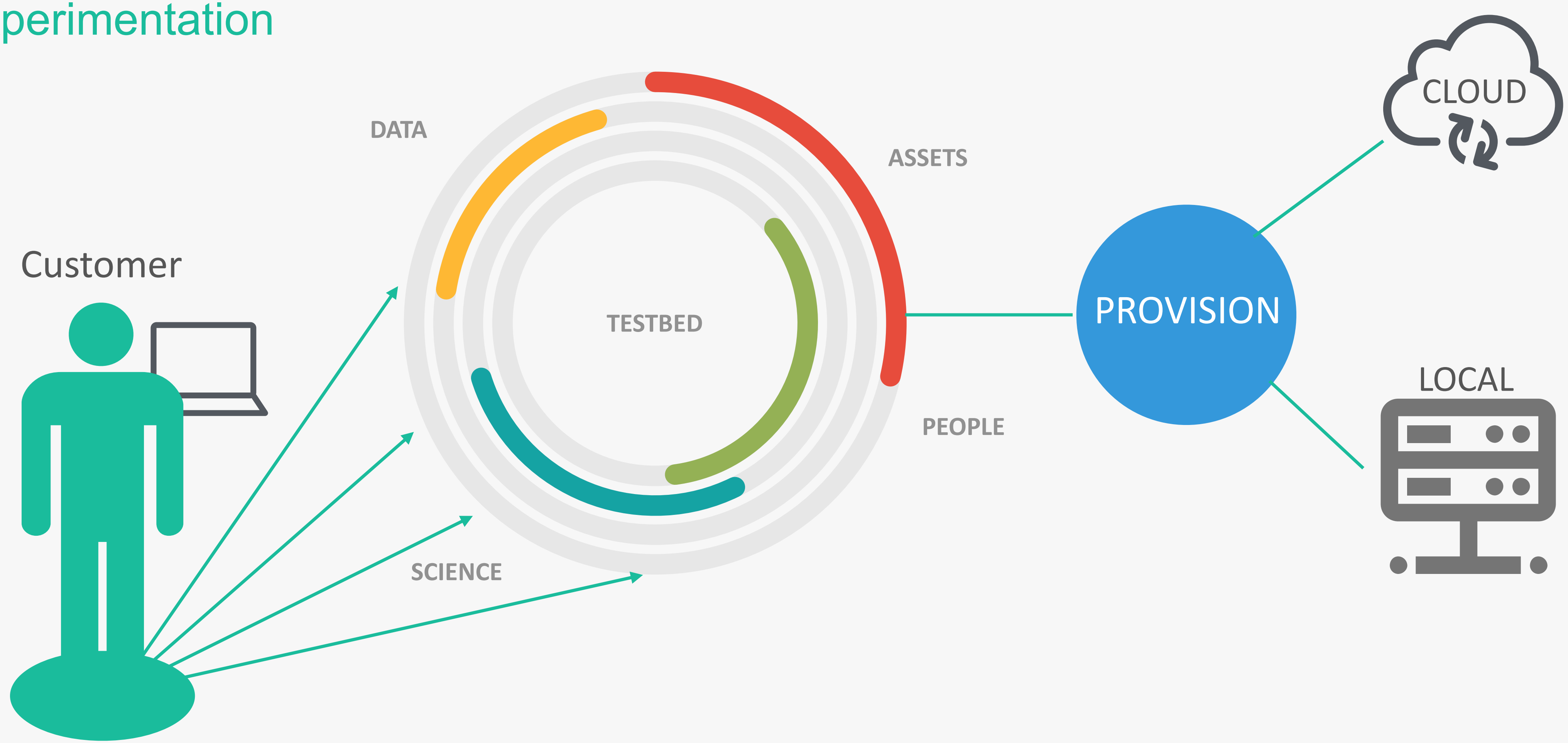
✗ Not Accessible

✗ Single Axis

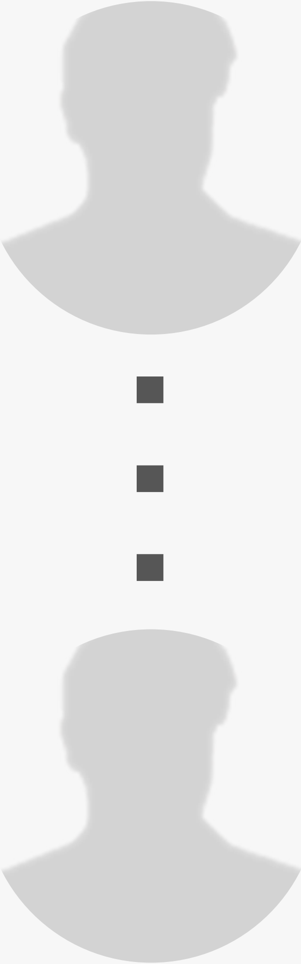
The solution

CEER: Cyber-Physical Experimentation

(testbed operation support)



People (multidisciplinary)



Edmond

Ashwini

Yu

Prosper

Steve

Jeremy

David

Richard

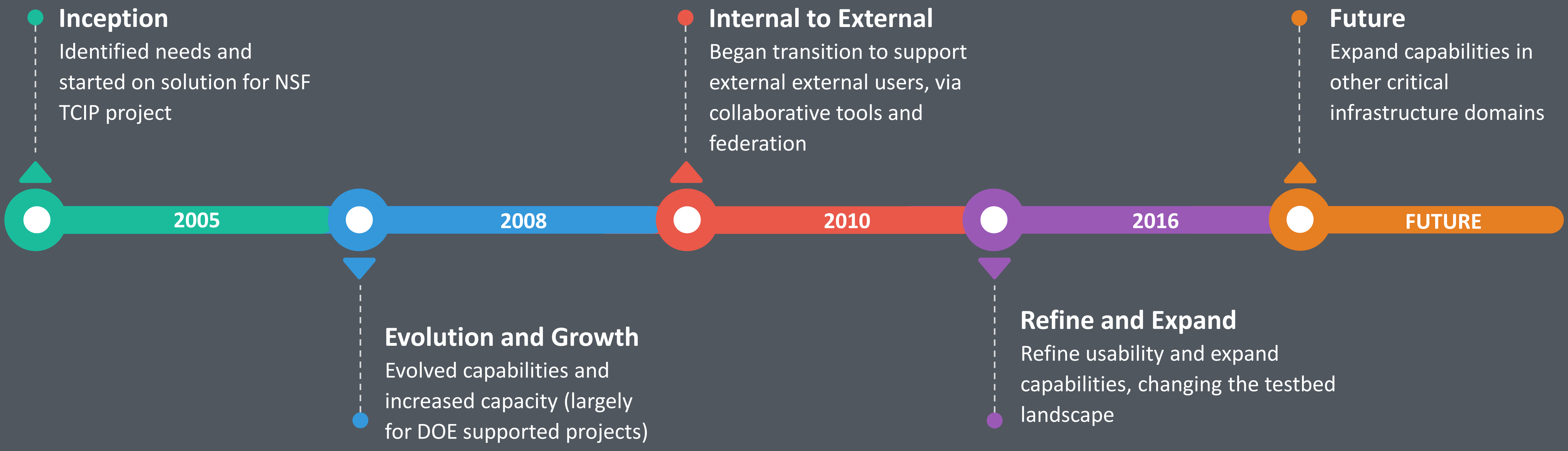
Shane

Tim

Ziping

CEER Lineage

An Evolution



Inception

Identified needs and started on solution for NSF TCIP project

Evolution and Growth

Evolved capabilities and increased capacity (largely for DOE supported projects)

Internal to External

Began transition to support external external users, via collaborative tools and federation

Refine and Expand

Refine usability and expand capabilities, changing the testbed landscape

Future

Expand capabilities in other critical infrastructure domains

The reason

Mission critical technology must be proven to be effective before we need it

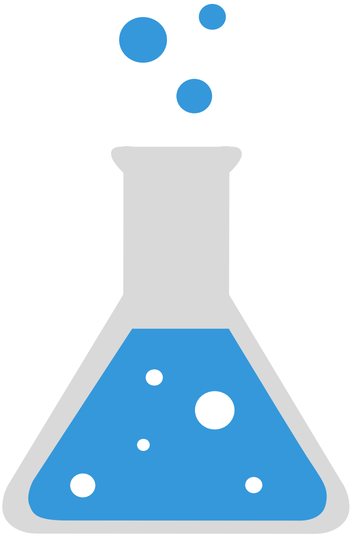
The capabilities to fully prove out this technology are not available today.

A realistic, recomposable, and well instrumented testbed is essential.

Our approach

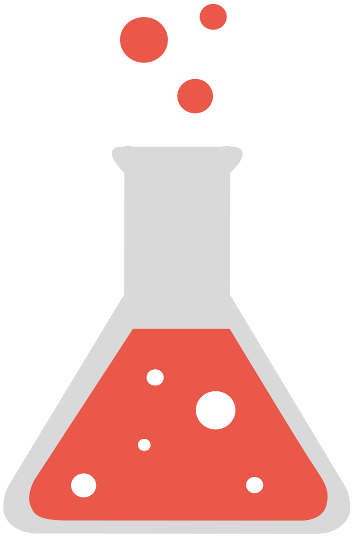
Driven Models

Scalable, accurate, and encompassing cyber and physical models that adapt to exercise needs based on performer input



Modularity

Adaptable composition, configuration, and deployment of testbed assets to accomplish exercise goals

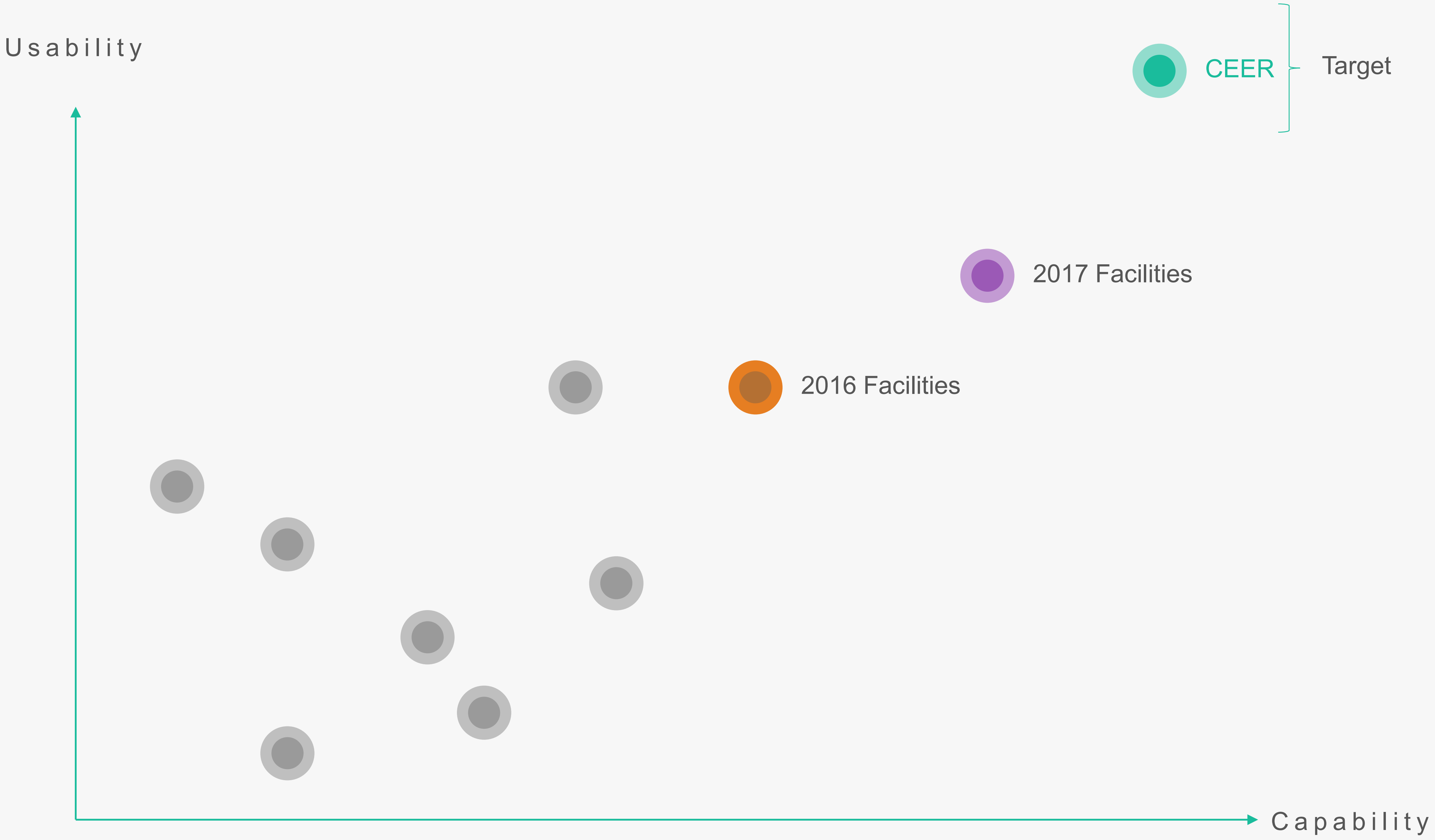


Instrumentation

Appropriate and accurate instrumentation to capture needed assessment knowledge without affecting results

Knowledge

Blend of academic, enterprise, manufacturing, and asset owner knowledge to ensure a multi-dimensional approach


Usability
CEER
Target
2017 Facilities
2016 Facilities
Capability

What’s available to those that need it TODAY?

10,000 Mile View

- Physical testbed access
- Dedicated (isolated) office space on site
- Dedicated remote access
- ICS software and equipment
- Computation and Storage support (within reason)
- Capacity to bring in special software and equipment

Network Overview

- 10GigE Uplinks and Fabric
- SDN-enabled
- Isolation and segregation
- Dedicated VPN access

Capabilities

- Full end-to-end Smart Grid capabilities
- Deployed Advanced Metering Infrastructure (AMI)
- Solar research platforms
- Real, emulated, and simulated hardware/software for scalability
- Real data from the grid, Industry partners, etc.
- Power simulation, modeling, and optimization of various forms
- Network simulation, modeling, and visualization of various forms
- Advanced hardware-in-the-loop cyber-physical simulation
- WAN/LAN/HAN integration and probes
- Security and protocol assessment tools (static/dynamic analysis, test harnesses, fuzzing)
- On-grid testing capabilities via Ameren TAC facility (with fiber optic interconnects to our primary testbed)

Hardware/Software Overview

- RTDS, PowerWorld, PSSE, PSCAD, PSLF, DSAtools, DynRed
- RINSE, tstBench, LabView, OSI PI, OSIi Monarch, SEL suites, PGDA
- Full range of open source power grid tools (openDNP3, openPDC, openPG, openXDA/openFLE, openHistorian, SIEGate)
- GPSs, substation computers, relays, PMUs, testing equipment, PLCs, security gateways, NI platforms
- Power analysis tools, PDCs, data analytics
- Full AMI deployment, TCIPG Smart Meter Research Platform
- RTUs, F-Nets, inverters, oscilloscopes, firewalls, embedded devices, sensors, spectrum analyzers, SIEMs, IDSs
- Home EMS, energy and environmental monitoring devices, zigbee, automation
- Display wall, visualization platforms (STI, RTDMS), training platforms
- Mu Dynamics, Fortify, security research tools, IBM Tivoli suite
- Cyber-physical extension via federation

Control Center

- OSIi Monarch EMS
- OSIsoft PI data historian
- Space Time Insight STAS system
- RTDMS and Phasor Grid Dynamics Analyzer
- Secure Information Exchange Gateway (SIEGate)
- Open Phasor Gateway (openPG)
- Open Phasor Data Concentrator (openPDC)
- Open Historian (openHistorian)

Generation

- Isolated Solar Test Lab
  - Single panel isolation for assessing behavior of solar in controlled conditions
- External Solar Array
  - 20kw array split into 5 separate strands
  - Varying technology of micro inversion, DC optimization, etc for each strand
  - Feeds into operational building for energy offset

Transmission and Distribution

- ABB
  - Relays (18 x REF 615)
  - Substation Gateway (2 x COM 600), plus virtualization
- Arbiter
  - PMU
- GE
  - D60 (Qty 2) – one upgraded to an N60 for 61850 support
  - F60
- Novatech
  - 8 x Orion LX
- Eaton/Cooper
  - 2 x SG4250 Substation Gateway

Transmission and Distribution

- Schweitzer Engineering
  - GPS Clocks (4 x SEL-2407, 2 x SEL-2488)
  - Substation Computers (SEL-1102, SEL-3351, 3 x SEL-3354, 1 x 3355)
  - Relays (3 x SEL-351S, 5 x SEL-421)
  - Adaptive Sources (5 x SEL-AMS)
  - Automation Controller (SEL-RTAC, SEL-3555)
  - Encrypting Devices (2 x SEL-3022, 4 x SEL-3025)
  - Network Switches (2 x SEL-2730M)

Advanced Metering

- Itron
  - 22 Openway Meters
  - 4 Cell relays
  - 1 MDMS Itron Enterprise
- Trilliant tstBench Meter Emulation
  - Allows for scaling meter assets
- TCIPG Smart Meter Research Platform
  - Custom research board built from the ground up to research AMI unencumbered
- Full protocol stacks (C12.22 and DLMS/COSEM)

Power System Protocols

- Protocols (binary/source)
  - C37.118
  - 61850 (and 61850-90-5)
  - DNP3
  - ICCP
  - Modbus
  - AMI (C12.22, DLMS/COSEM)
  - Zigbee/Zwave
  - Proprietary
- Test harnesses and more

Modeling

- Power
  - Opal-RT 5700 fully loaded
  - Real Time Digital Simulator (RTDS)
    - 2 chassis units, well optioned with various protocol packages
    - Allows for hardware in the loop, pure simulation, and emulation
    - Doble F6350e, 2 x F2100
    - Pacific Power 112AMX
  - PowerWorld, PSSE, PSLF, PSCAD, *SAT, DynRed
  - OpenDSS, GridLabD
- Cyber
  - RINSE/SSF, NS{2,3}, Emulab/DETER, etc

Security Specific

- ICS Security Vendor Commercial Products
- Secure Software Analysis Tools (Commercial and Open)
- Mu Dynamics MU-8000 + Mu Studio
  - Security scale testing and fuzzing
- Tofino SCADA Firewall (old and current gen)
- Bayshore SCADA Firewall
- Sonicwall, Cisco, and Firewall1 Firewalls
- Custom Linux VPN and Cisco ASA 5510
  - VPN/Firewall for lab facilities
- IDS and SIEM systems
- IBM Tivoli product suite
- Openflow switching and Layer 3+ switches
  - IP routing and segregation for lab facilities
  - 10GE uplinks on core switches

Computation

- 60+ High-end servers
  - Provide computational support, experimentation set up and teardown, etc.
  - Currently hosting hundreds of VMs supporting research
- Latest Virtualization and Container Capabilities
- Federation of assets and internal provisioning of both cyber and physical assets
  - Professional enterprise-class range provisioning and management platforms being integrated

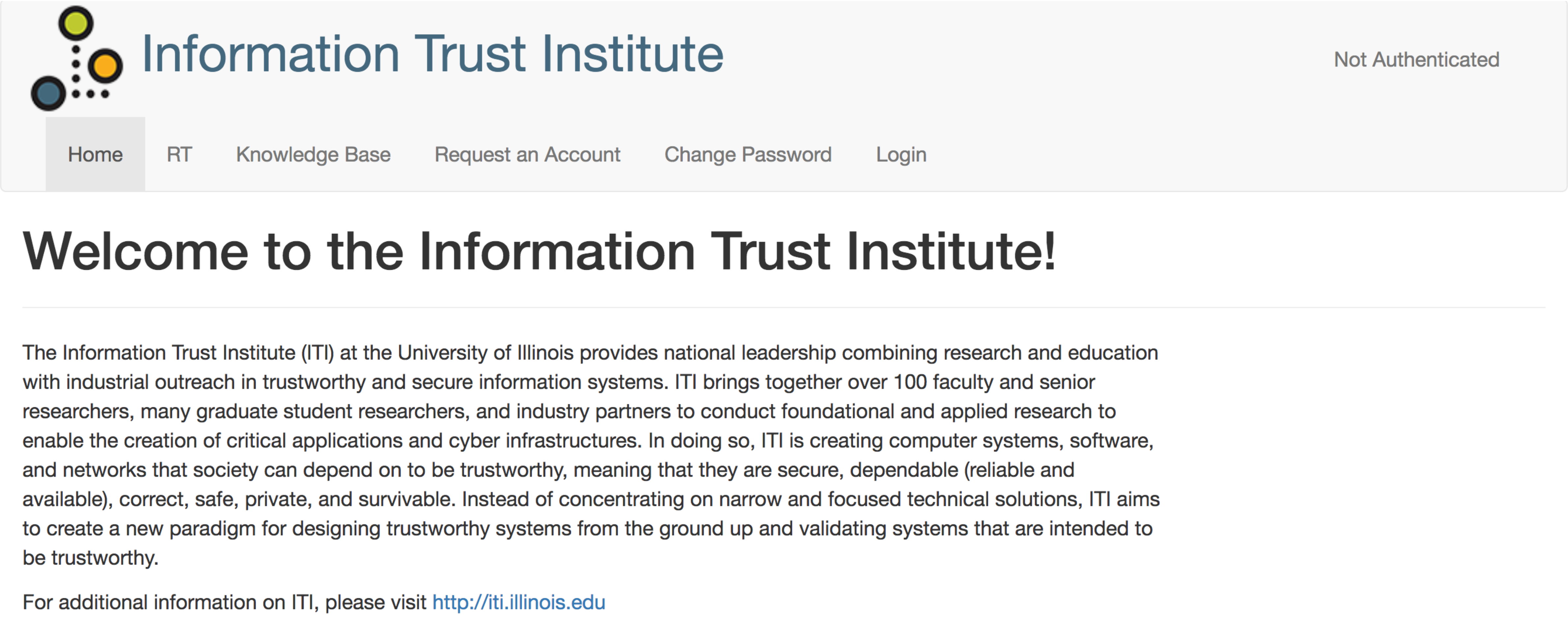
Miscellaneous

- F-Net (Qty. 11)
  - Wall outlet “PMU”s
- Osiris RTU
  - Connects server with legacy devices
- Semikron Inverters (Qty 4)
  - DC inverters for voltage stability framework
- National Instruments DAQ and PXI chassis
  - Analog/Digital Taps
  - National Instruments LabView
    - Programmable logic for A/D taps
- Arduino, Beagleboards, Raspberry PI, etc
- Misc. Software to utilize the hardware
- Advanced display wall for visualization and research

Unique Integration

- Special builds of various software
- Custom tools to integrate cyber-physical systems
- Custom tools to automate experimentation
- Programmatic control of a variety of the assets
- Software Defined Radio capabilities
- Full lab packet capture

Testbed Portal



Welcome to the Information Trust Institute!

The Information Trust Institute (ITI) at the University of Illinois provides national leadership combining research and education with industrial outreach in trustworthy and secure information systems. ITI brings together over 100 faculty and senior researchers, many graduate student researchers, and industry partners to conduct foundational and applied research to enable the creation of critical applications and cyber infrastructures. In doing so, ITI is creating computer systems, software, and networks that society can depend on to be trustworthy, meaning that they are secure, dependable (reliable and available), correct, safe, private, and survivable. Instead of concentrating on narrow and focused technical solutions, ITI aims to create a new paradigm for designing trustworthy systems from the ground up and validating systems that are intended to be trustworthy.

For additional information on ITI, please visit http://iti.illinois.edu

Power System Modeling

Power System Modeling

- To support the advancement of research, verification, and validation of smart grid cyber tools
- Capability to **generate realistic power grid scenarios** derived from real data but without conveying sensitive information
- Capability to **support communications traffic** that models the real systems
- Capability to **interface and drive hardware devices** in the loop

Power System Modeling Tools

- In general power system modeling tools are categorized into two parts:
  - Electromechanical transient tools (millisecond time scale)
    - PowerWorld
    - Siemens PSS/E
    - GE PSLF

    Transmission level
    3 phase balanced

    - OpenDSS
    - GridLab-D

    Distribution level
    Phase unbalance

  - Electromagnetic transient tools (microsecond time scale)
    - Real Time Digital Simulator (RTDS)
    - Opal-RT
      - Hypersim
      - RT-Lab (interface with Matlab Simulink)
      - eFPGAsim (detailed power electronic converters, nano-second scale)
  - Opal-RT ePhasorsim (millisecond time scale)

  Real-Time fidelity
  3 phase balanced
  Phase unbalance

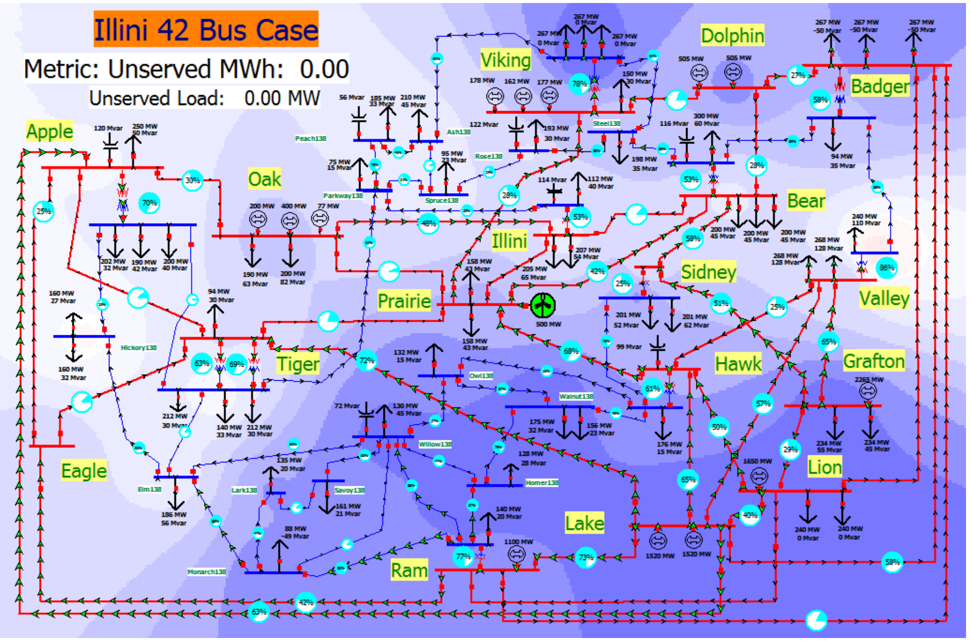
Communication Tools

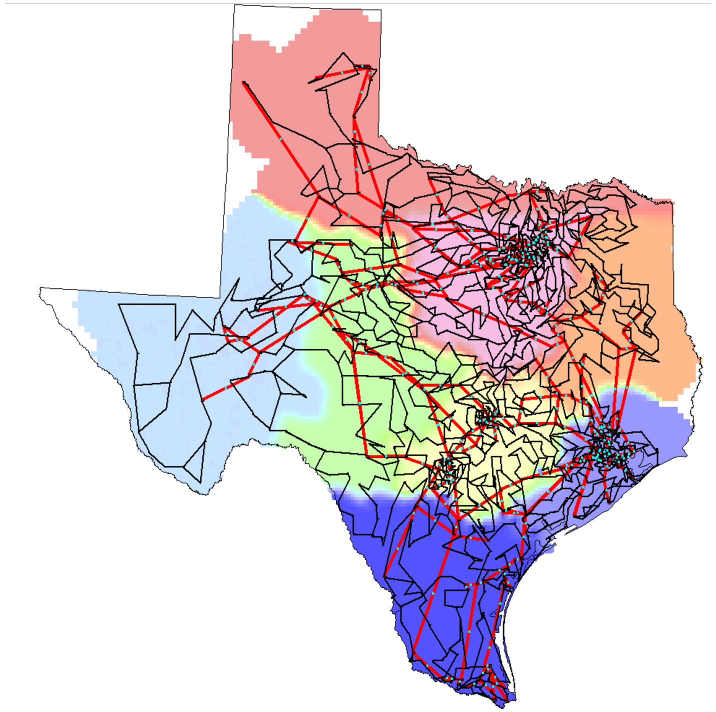
- Communication tools are needed to communicate realistic telemetry and control signals from and to the power grid simulation scenarios
  - RTDS GTNET Interface
  - Opal-RT Communication Cards
  - Protection relays (SEL and ABB)
  - Substation Automation (ABB, Novatech, SEL)
  - SCADA/EMS (OSI Monarch)
- Capability to speak number of different protocols generally used in the field
  - DNP3
  - IEC61850
  - Modbus etc.

Modeling Cases

- ITI has made available various power system models (reference and synthetic):

https://github.com/ITI/models





MUCH more to come

ICS Data Generation

Open Source Soon

DNP3 Protocol Generator

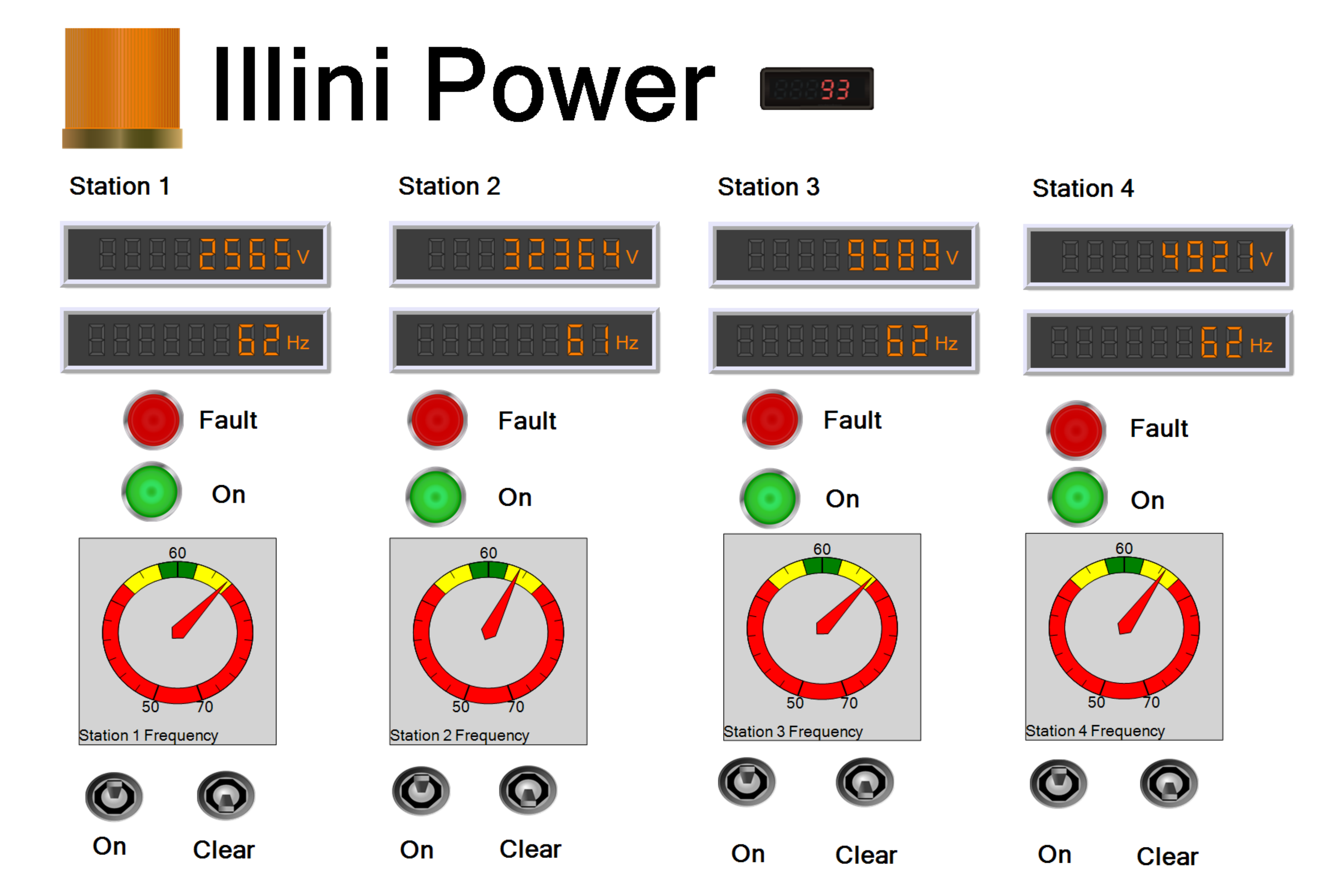
- Based on OpenDNP3 open source under Apache license
- Can simulate masters, outstations or both
- Can be deployed on virtual machines, Docker containers or Raspberry Pi
- Flexible data generation rules
- Embedded lua scripting engine
- Replay real power telemetry

Modbus Protocol Generator

- Based on Pymodbus open source under BSD license
- Similar in capabilities to DNP3 Generator
- Cannot replay telemetry yet

Distributed Test Manager (Triangle Microworks, Inc)

- Commercial license
- Windows based software
- Has GUI, simpler to set up
- Visual representation of your system
- DNP3, Modbus, IEC 61850, IEC 60870-5 protocols (ICCP in beta)
- Data generation and visuals are scriptable via Javascript



Illini Power

93

Station 1

2565 V

62 Hz

Station 2

32364 V

61 Hz

Station 3

9589 V

62 Hz

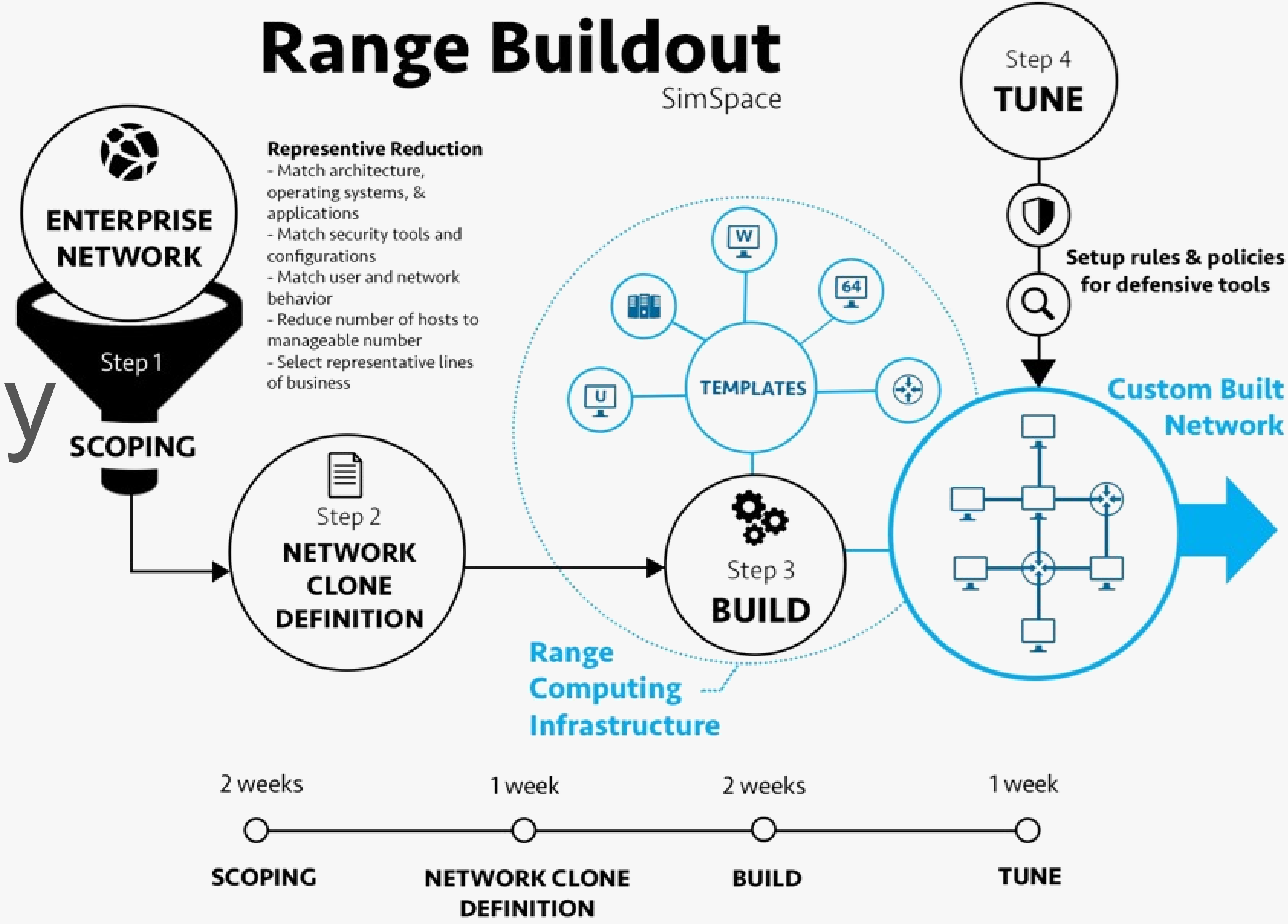
Station 4

4921 V

62 Hz

What’s coming in the near FUTURE?

Powered by SimSpace

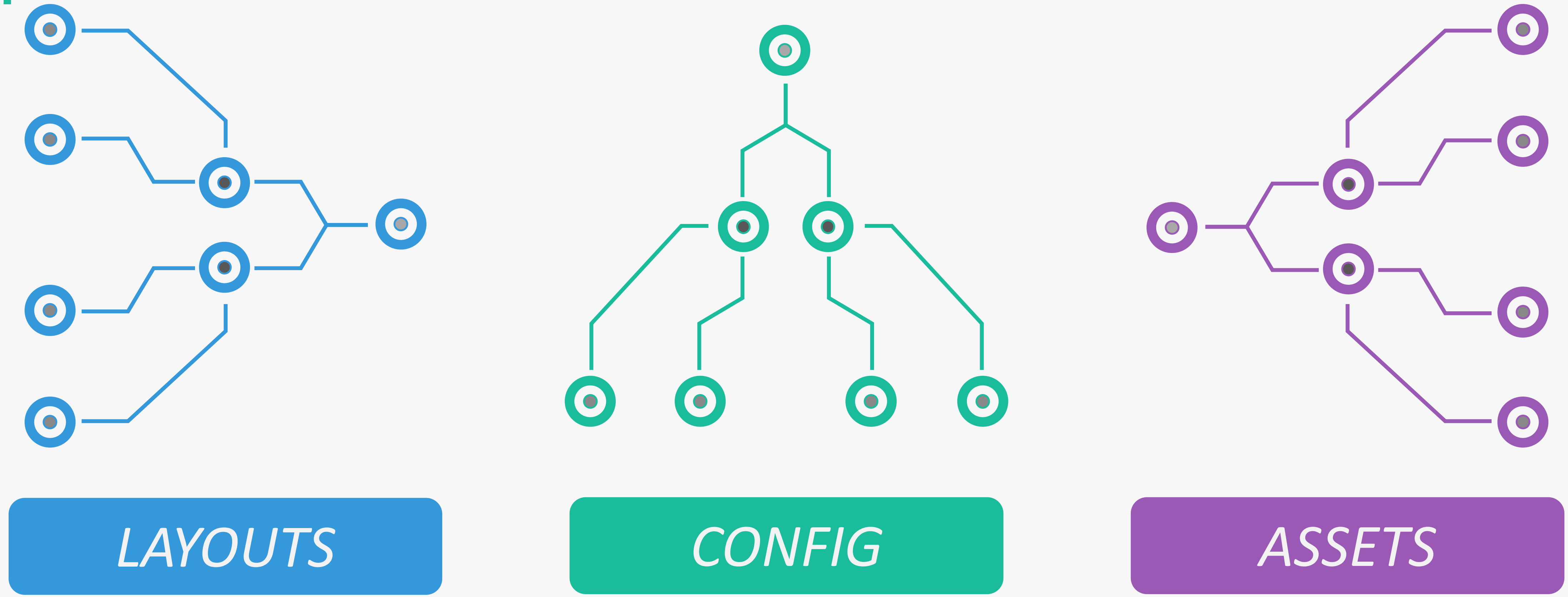


Range Buildout

SimSpace

Representive Reduction
- Match architecture, operating systems, & applications
- Match security tools and configurations
- Match user and network behavior
- Reduce number of hosts to manageable number
- Select representative lines of business

Deployment profiles



LAYOUTS

CONFIG

ASSETS

A little on vision…

A Sneak Peak

Overall, we seek to…

- Advance the state of art for cyber experimentation
- Increase usability through tailored tools and seamless integration
- Focus on development and integration of modular re-usable pieces
- Drive models and their conditions from real telemetry
- Incorporate and extend the work done by other researchers
- Document and package experiments

- Drive research with reproducible, releasable, and recreate-able experiments
- Develop environments that aid learning, research understanding, and translate to operational advancement

Future Capabilities

- Multi-axis converged modeling
- Historical data extrapolation for modeled data
- Seamless coherency between cyber and physical
- Detailed sandbox environment
- More true-to-reality utility architectures
- Enhanced data generation, injection, and correlation tools
- Experiment data analysis collection and processing tools

Future Directions

- Event/Impact libraries
- Multi-axis converged modeling
- Historical data extrapolation for modeled data
- Seamless coherency between cyber and physical
- Detailed sandbox environment
- More true-to-reality utility architectures
- Enhanced data generation, injection, and correlation tools
- Experiment data analysis collection and processing tools

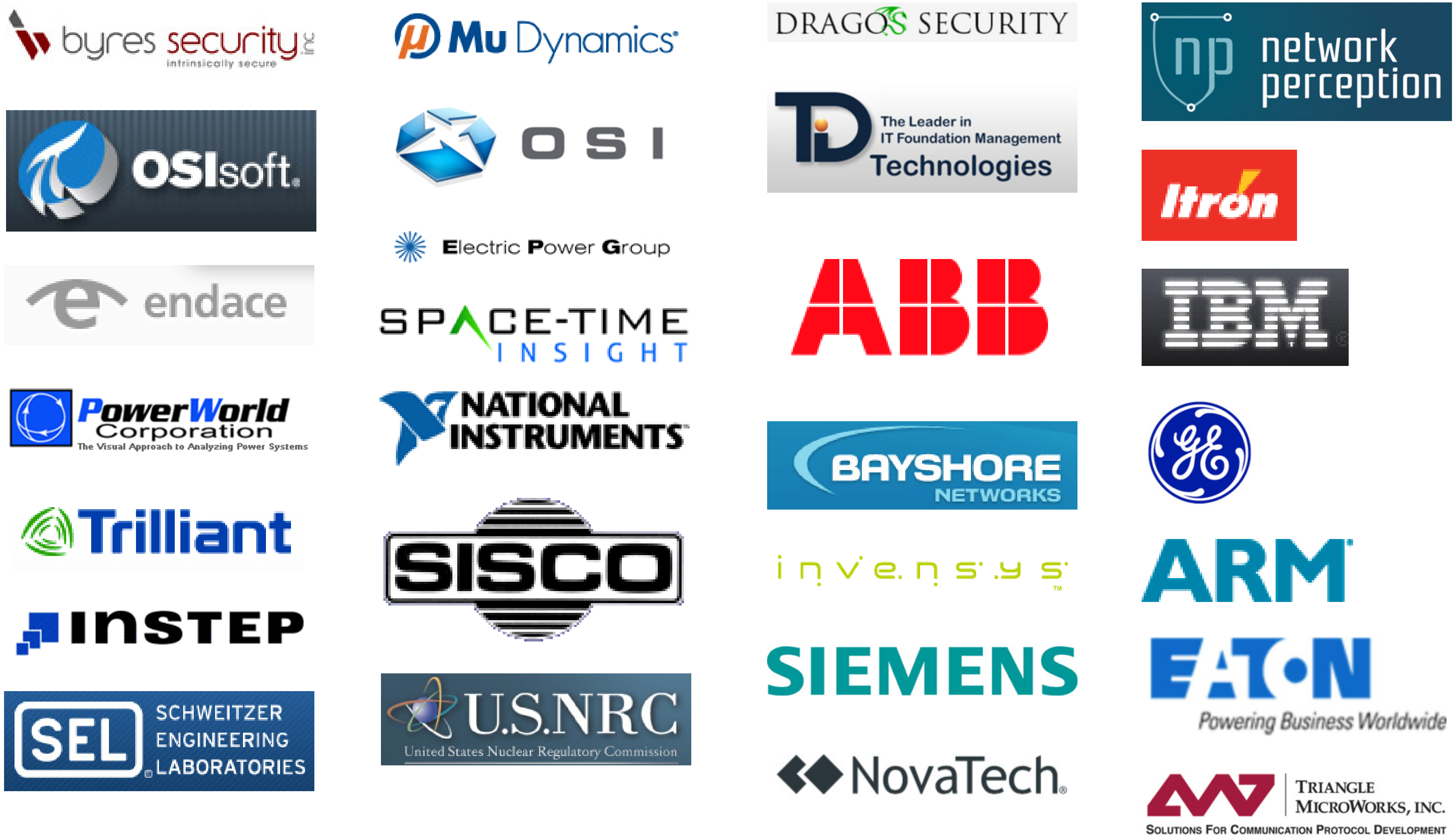
Stretch Goals

- Power
  - Automated model ingestion
  - Reversible generation (you give me real data and I reconstruct the physical system)
  - Coherent weather pattern inclusions
  - Synthesized outage information
  - Incorporation of market data
  - Squirrels
- Cyber
  - Automated model ingestion
  - Reversible generation (you give me real data and I reconstruct the cyber system)
  - Humans

(Some) Current Research Projects

- Sandboxing
  - Emulation of devices by executing pieces of actual firmware on same architecture
  - LLVM-based lifters to convert native code to IR representation for execution on different architectures
- Reverse Engineering
  - Automated reverse engineering of constructed multi-stage payloads to determine impact and safety of execution
- Instrumentation
  - Low-level augmentation of embedded systems for traceability and increased internal visibility
- Analysis
  - Network correlation and timelining to determine course of event propagation
- Co-simulation
  - Evaluation of different co-simulation approaches applied to this domain to determine bounding constraints of effective operation (e.g., HLA, FMI, VPNET)
- Configuration and provisioning
  - “return to sane” methodologies for devices that may be tainted by malware
  - Automated methods for configuring and sanitizing devices and their configuration

Testbed Donations Provided By



THANK YOU

The Whole Testbed Team at Illinois

yardley@Illinois.edu