SMART GRID TESTBEDS
AN EVOLUTION

MARCH 31, 2015

TIM YARDLEY
ASSOCIATE DIRECTOR OF TECHNOLOGY
UNIVERSITY OF ILLINOIS, INFORMATION TRUST INSTITUTE

YARDLEY@ILLINOIS.EDU

FUNDING SUPPORT PROVIDED BY DOE-OE AND DHS S&T

UIUC'S INFORMATION TRUST INSTITUTE

Providing World-Wide Excellence in Information Trust and Security

Institute Vision:

Trust in Complex Systems

Institute Personnel:

Core faculty from CS and ECE
90+ faculty, 28 departments, 11 colleges

Primary Research Themes

- Power Grid
- Evaluation
- Data Science
- Systems and Networking

Background

- Since 2004 startup ITI has won $85M+ in research funding
- Solutions for societal and industrial problems
- Major corporate partnerships
- Led by the University of Illinois College of Engineering

SMART GRID SECURITY EFFORTS @ ILLINOIS

Centers

TCIPG — Trustworthy Cyber Infrastructure for the Power Grid
~$26.3M effort across 10 years

- Drive the design of a more secure, resilient, and safe electric power infrastructure
- $7.5M NSF center (2005 – 2010), $18.8M DOE-OE (CEDS) & DHS center (2010 – 2015)
- University of Illinois, Washington State, Dartmouth, Arizona State

ADSC — Smart Grid Subprogram (~$15M effort across 5 years)

Cybersecurity, Microgrids, DERs, and HANs

Illinois Center for a Smarter Electric Grid (~$5M effort across 5 years)

- Validation of IT and control aspects of the Smart Grid
- Operates facilities equipped with HW/SW to aide in the validation of emerging smart grid systems
- Focus on both power and cyber related issues

Assured Cloud Computing (~$6M effort across 6 years)

- Leveraging trustworthy cloud computing for critical infrastructure

Science of Security Systems (~$8.5M effort across 4 years)

- Resiliency, security, and trust in complex engineered systems

Highlighted Projects

Policy Based Configuration (PBCONF)
EPRI Electric Power Research Institute, Ameren

Software Defined Networking
SEL, Ameren

Applied Resiliency for More Trustworthy Grid Operation (ARMORE)
Grid Protection Alliance, Pacific Northwest National Laboratory

Collaborative Defense for T&D Devices Against Attack (CODEF)
ABB

Cyber-Physical Modeling and Analysis for a Smart and Resilient Grid
PowerWorld Corporation

… and many more

TCIPG AS CATALYST FOR INDUSTRY TECHNOLOGY

- TCIPG capabilities and technologies are being **transitioned into the field**:
  - NetAPT / NP-View
  - Amilyzer
  - LZ Fuzz
  - CONES
  - Autoscopy Jr.
  - Api-do contributions to KillerBee
  - Vulnerability assessment
- TCIPG develops expertise that enables **deeper engagement** with the sector under DOE Industry-led projects:
  - SIEGate (GPA)
  - Applied Communications Sciences
  - Honeywell
  - Entergy SGIG
- **Synergistic Industry funding** on related projects:
  - EPRI
  - Fujitsu
  - GE
  - Lockheed Martin
  - Northrup Grumman
  - SEL
- TCIPG opens door to **opportunities:**
  - Emerging microgrid collaborations
  - Microgrid as on-grid/near-grid testbed for TCIPG and possibly other DOE portfolio performers
  - Building integration and other driving infrastructure

GRADUATED SMART GRID SECURITY EFFORTS @ ILLINOIS

Open Phasor Gateway

Entergy — THE POWER OF PEOPLE
EPRI ELECTRIC POWER RESEARCH INSTITUTE
GRID PROTECTION ALLIANCE

ACS Intrusion Mitigation Agent

APPLIED COMMUNICATION SCIENCES
DTE Energy
EPRI ELECTRIC POWER RESEARCH INSTITUTE

Secure Information Exchange Gateway (SIEGate)

GRID PROTECTION ALLIANCE
Pacific Northwest NATIONAL LABORATORY
pjm
ALSTOM

SCADA Role Based Access Control

Honeywell
INL

Korean DOS Mitigation in Metering

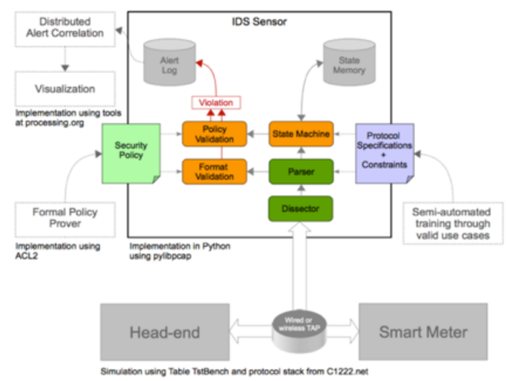
ETRI

CACAIS Testbed

Available Technology

np-view

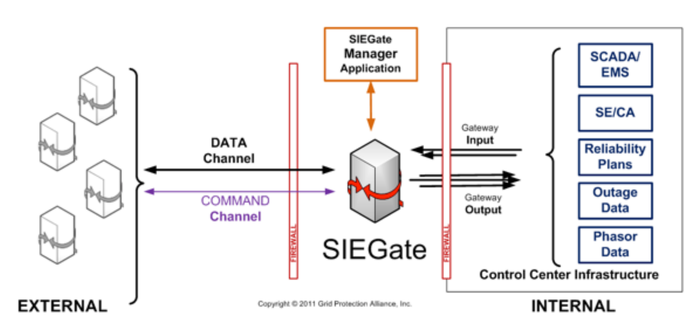
NP-view: Automated and comprehensive network path analysis of firewall and router configurations against a global policy



AMIlyzer: Specification based intrusion detection system for Advanced Metering Infrastructure (AMI)

Möbius

Mobius: Model based environment for validation of system reliability, availability, security, and performance



SIEGate: Secure Information Exchange with publish-subscribe to improve Utility cyber security posture and reduce operational costs

... and more coming.

TCIPG SMART GRID TESTBEDS

TESTBEDS

- Illinois
  - Primary TCIPG Testbed
  - Illinois Center for a Smarter Electric Grid
- Washington State University
  - Energy Systems Innovation Center
  - Smart Grid Demonstration and Investigation Lab
- Dartmouth
  - Zigbee and other misc. equipment
- UC-Davis
  - Misc. equipment

TCIPG TESTBED @ ILLINOIS

- A lab-contained but true-to-reality implementation of critical infrastructure
- Leverages over $6.5 million worth of hardware and software (much of which is donated)
- Brings together power system equipment, emulation, and simulation
  - Supports cutting-edge research on grid topics from generation to consumption
- Automated for efficient and effective provisioning of power and cyber assets per experiment
- Used for internal TCIPG research, collaboration with national labs, and projects with industry
- Focus on the Grid…

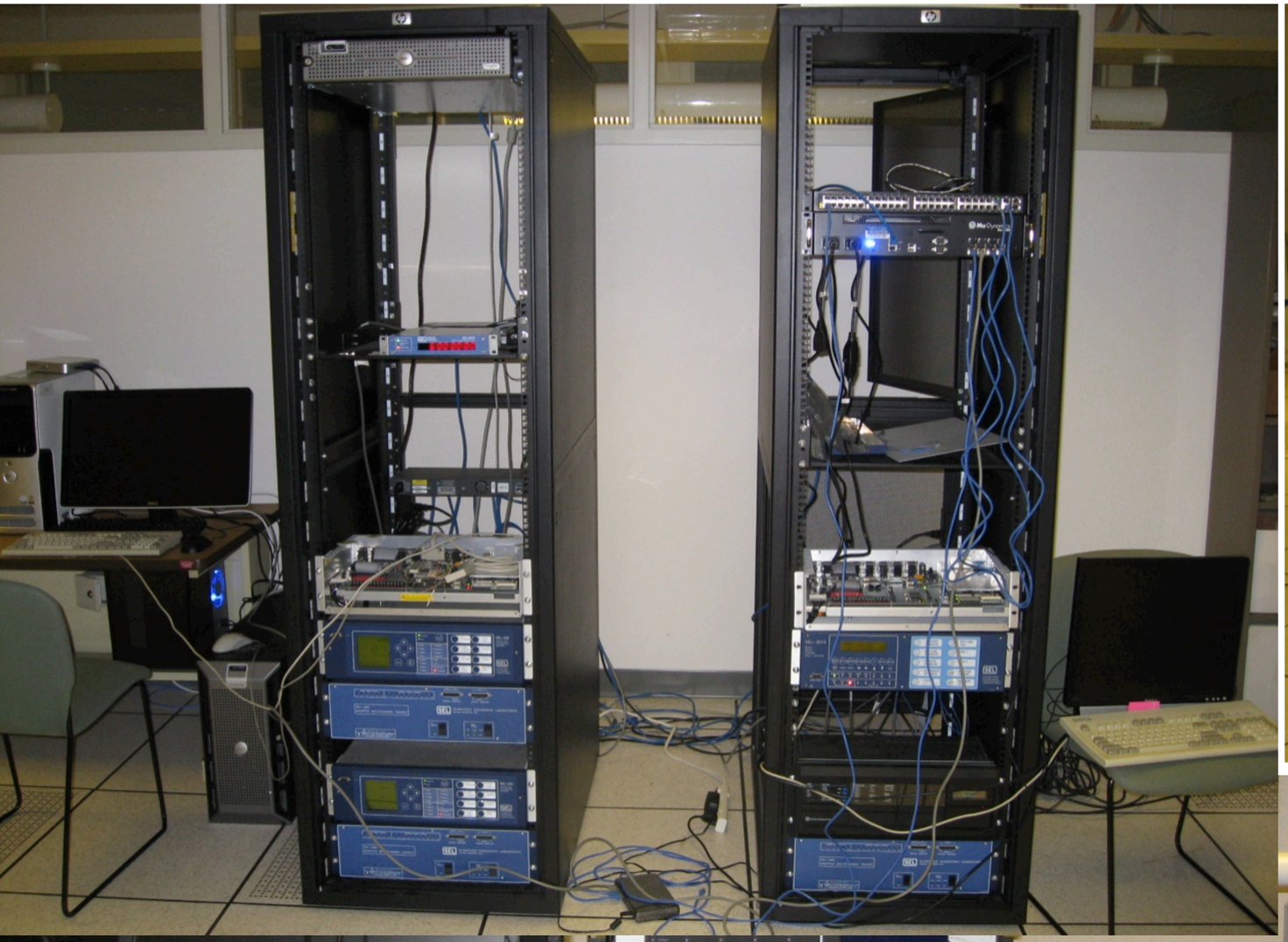
BACK STORY

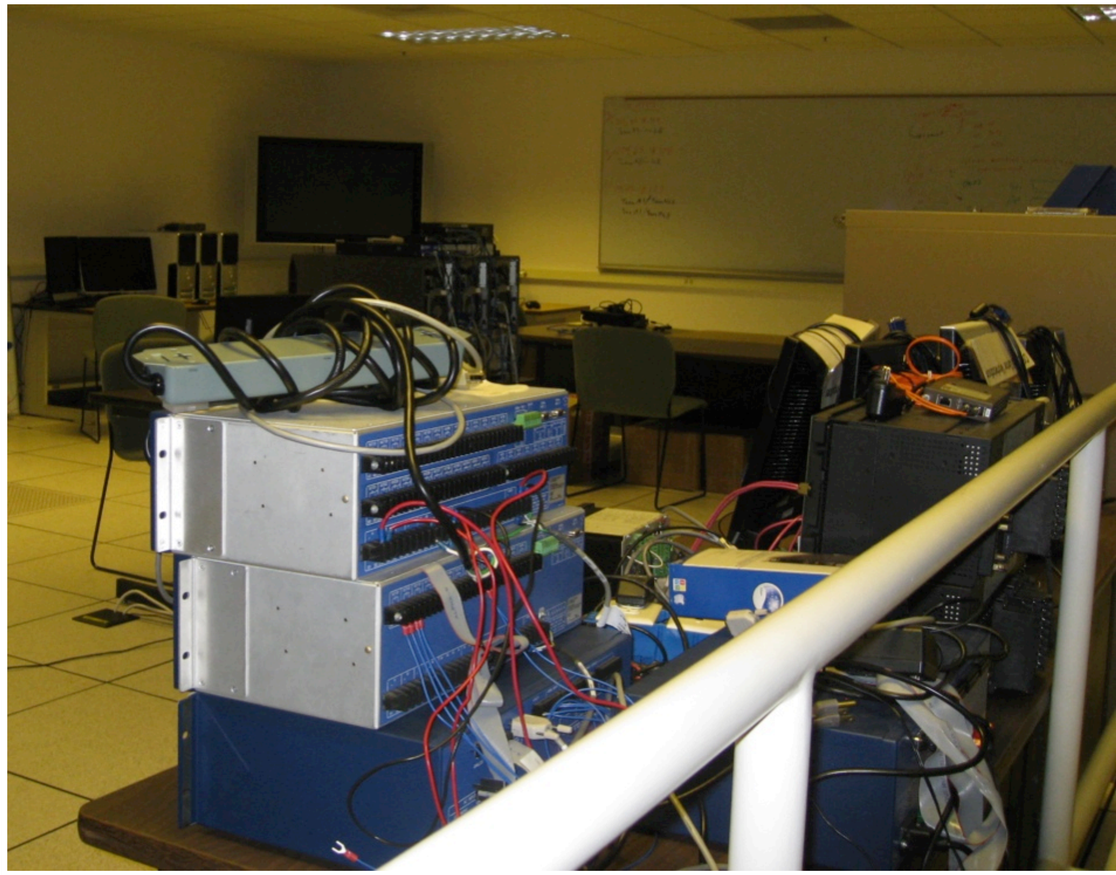
- Testbed was designed to support cyber security research for the grid
  - But also enable exploration of the possible grid of the future
- Nothing like this really existed circa 2005
  - But it didn't happen overnight

THE BEGINNING

- The testbed formed out of a necessity to enable and validate research
- Started as just a few substation devices and computing infrastructure (2007)
- Increased in scale, complexity, and capability since

2010





SEL-351S
SEL-351S
SEL-734
SEL-AMS
ADAPTIVE MULTICHANNEL SOURCE

2011

TCIPG Testbed
Byres Security
Endace
GE
InStep Software LLC
Mu Dynamics
Open Systems International
OSIsoft
PowerWorld
Schweitzer Engineering Lab.
Siemens AG
Space Time Insight
Trilliant Inc.
RTDS

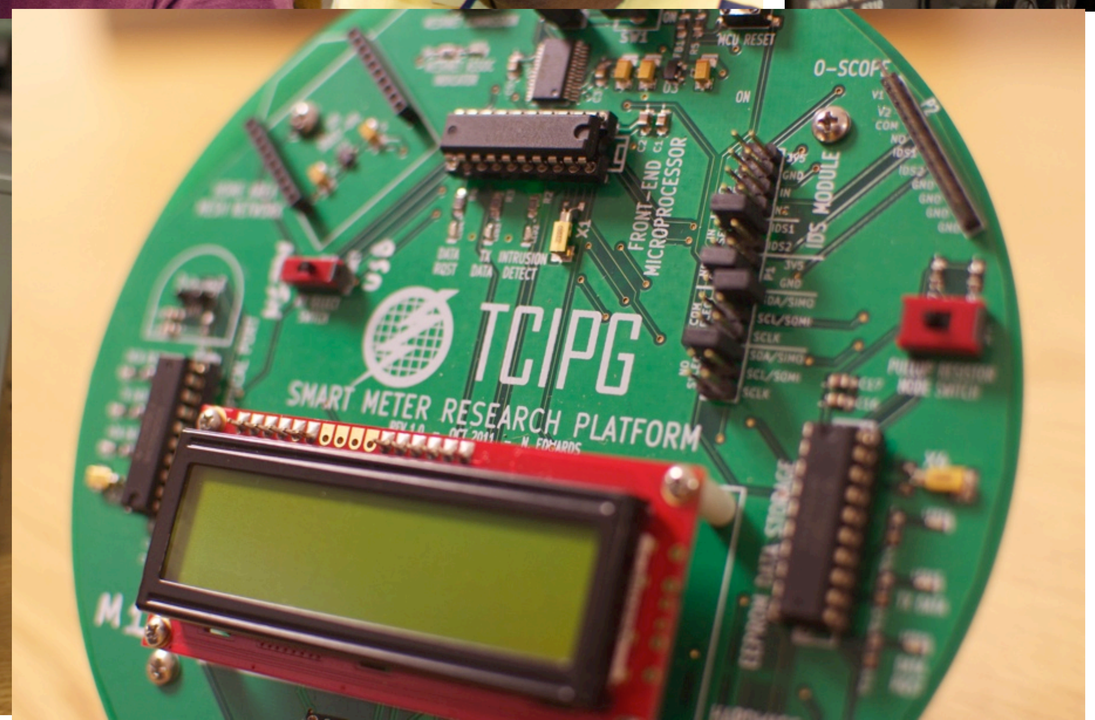
TCIPG
TCIPG
TCIPG
TCIPG
TCIPG
TCIPG

2012

RTDS
Real-Time Digital Simulator

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

DANGER / PELIGRO


TCIPG
SMART METER RESEARCH PLATFORM
FRONT-END MICROPROCESSOR

2013

Training Lab

2015

GROWING

- Bigger, better, faster, stronger
- New facility
- New capabilities
- New interconnections

EXPANSION

- Individual circuit level monitoring
  - 64 Circuits dedicated to rack equipment
    - Power was an issue before
- HVAC, noise, proximity sensors, etc.
  - Monitoring & Data Collection
- Network Upgrades
  - 10Gb uplinks (upgradeable to 40Gb)
  - Research network connected (<1ms infrastructure latency)
  - Full Software Defined Networking (SDN) control

SOME HIGHLIGHTS

- Research network allows full open internet research
  - Honeypots, IDS/IPS intelligence, Dark IP, etc.
- Pulled dark fiber to the testbed
  - Allows for fiber specific research including time-slices communication and true-WAN comms
- Increased collaboration, visibility, and professional appeal
- Researcher office space located in close proximity

STUDENT RESEARCHERS

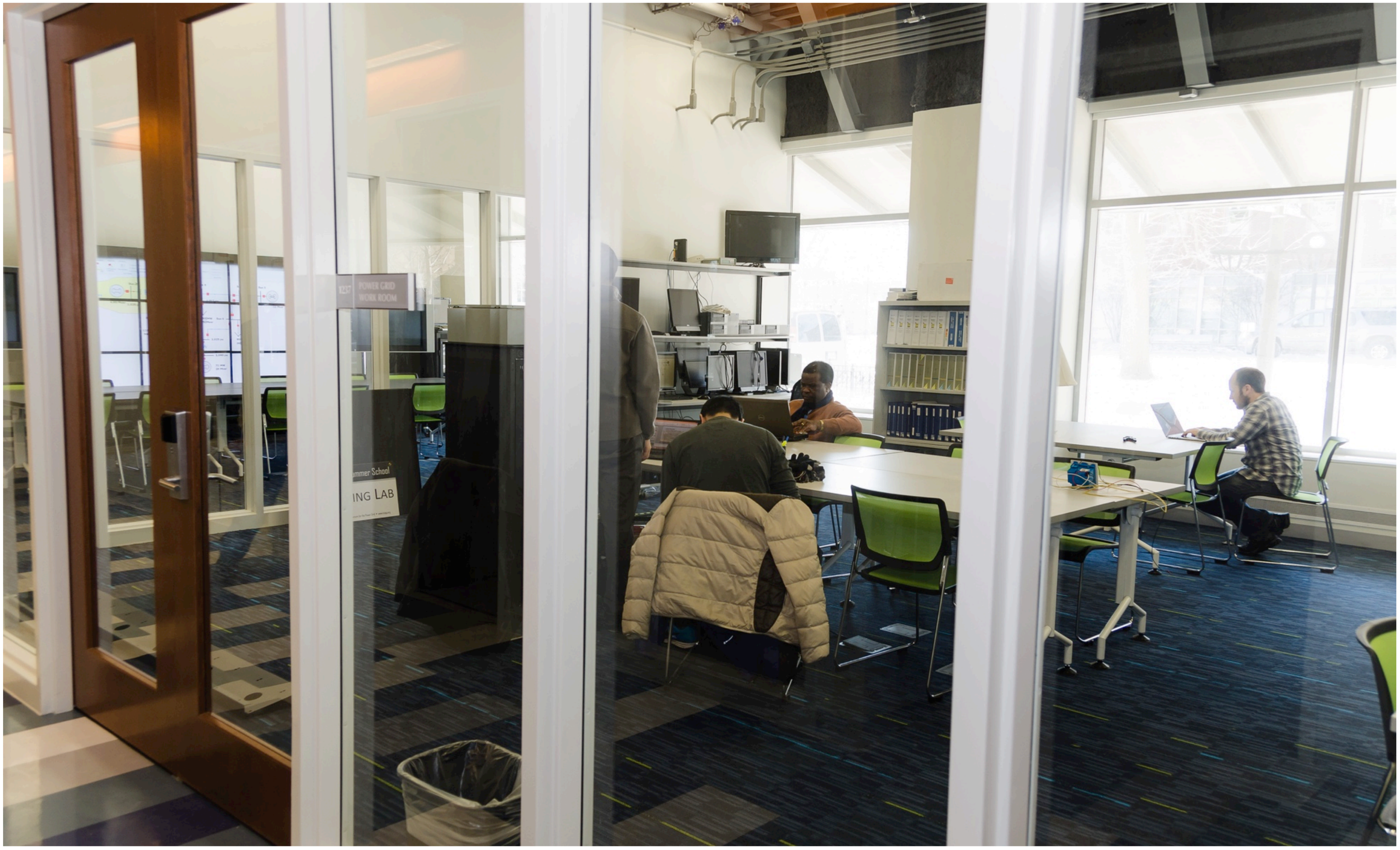
POWER ENGINEERS

RESEARCH PROGRAMMERS

DISPLAY ROOM

MULTI-ROOM CONFIGURATION

WORK ROOM



SERVER ROOM

ADJACENT TRAINING CLASSROOM

REALIZING TECHNOLOGY DOMAINS

Renewable Energy

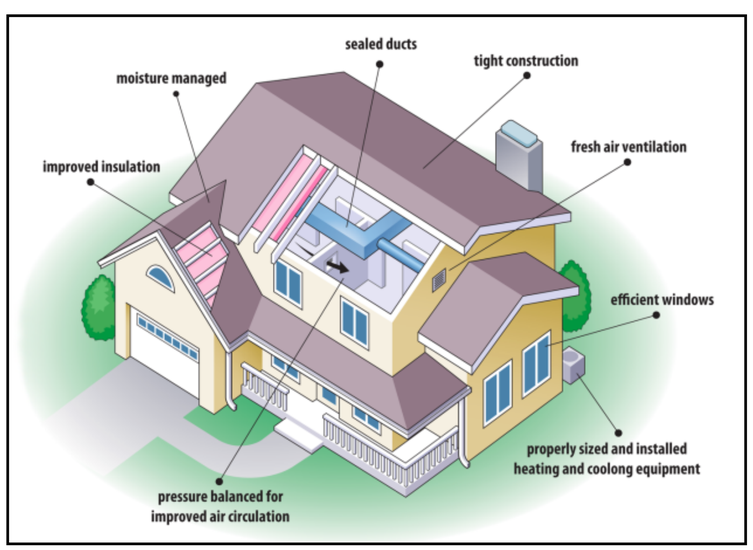
- Biomass
- Fuel Cells
- Energy Storage
- Geothermal
- Solar
- Turbines
- Wind

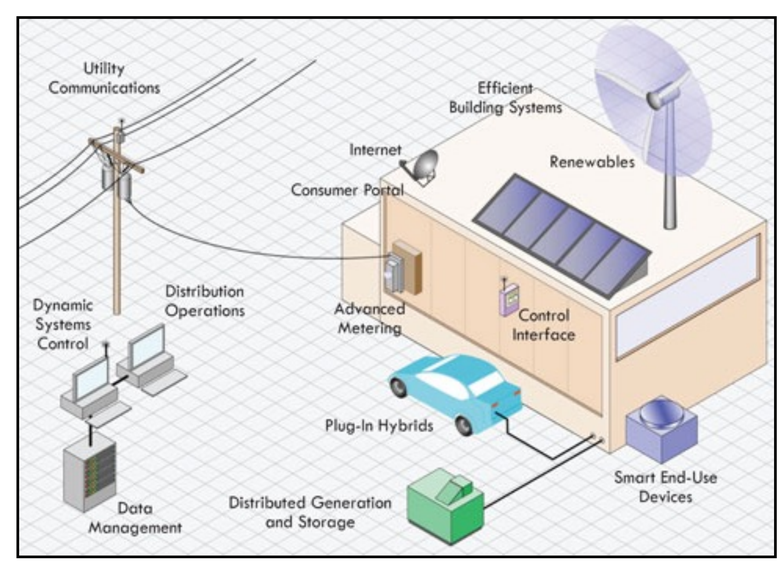
Energy Cost Reduction

- Air sealing and insulation
- Bldg. Automation Systems (BAS)
- Combined Heat & Power (CHP)
- Control/feedback systems
- HVAC systems
- Lighting Systems & Sensors
- Sub-metering
- Variable Frequency Drives (VFDs)

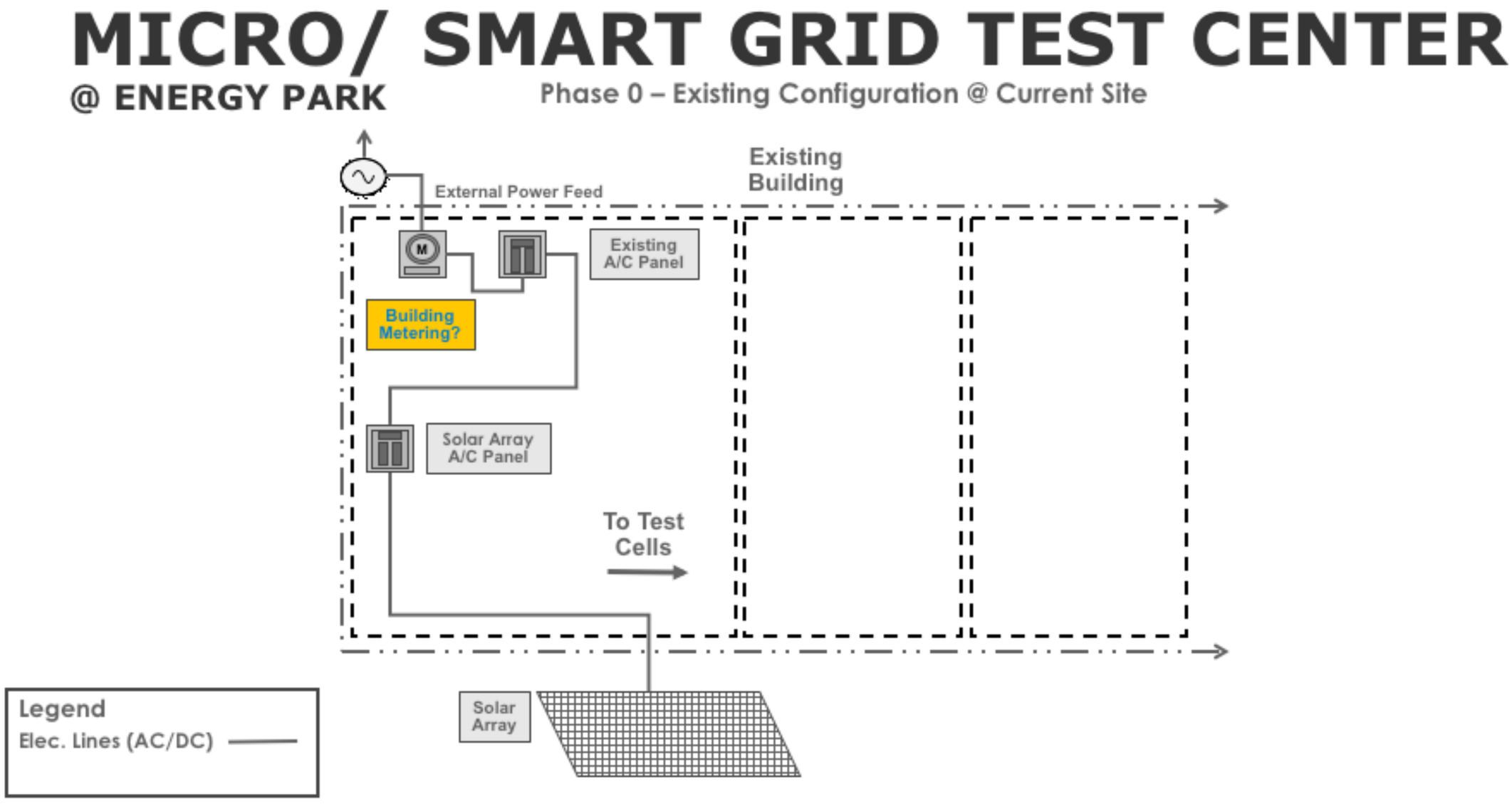
Smart Micro-Grid

- Cybersecurity
- Demand-Response
- Grid-Tie & Islanding
- SCADA
- Smart Metering
- Wireless

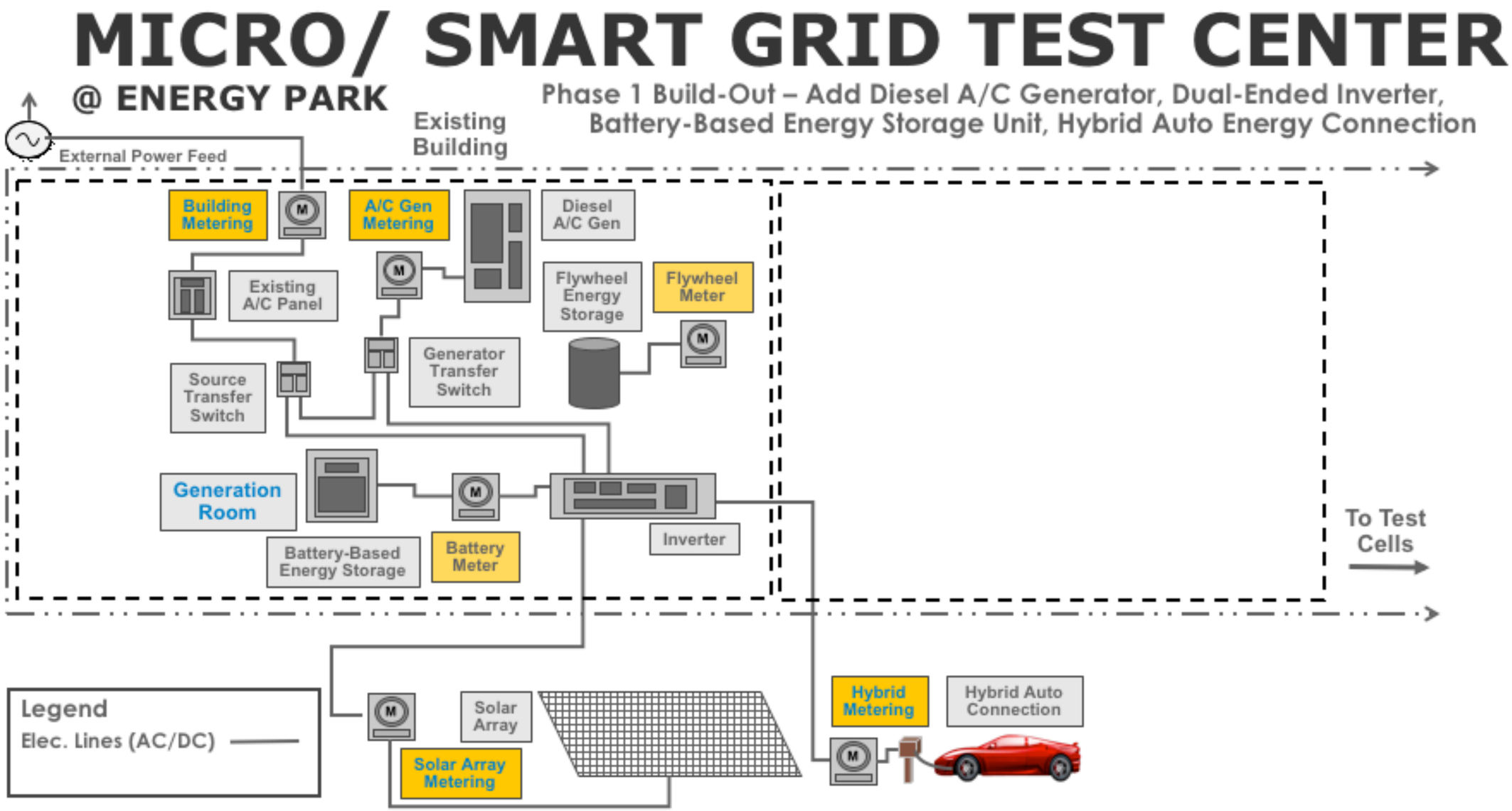




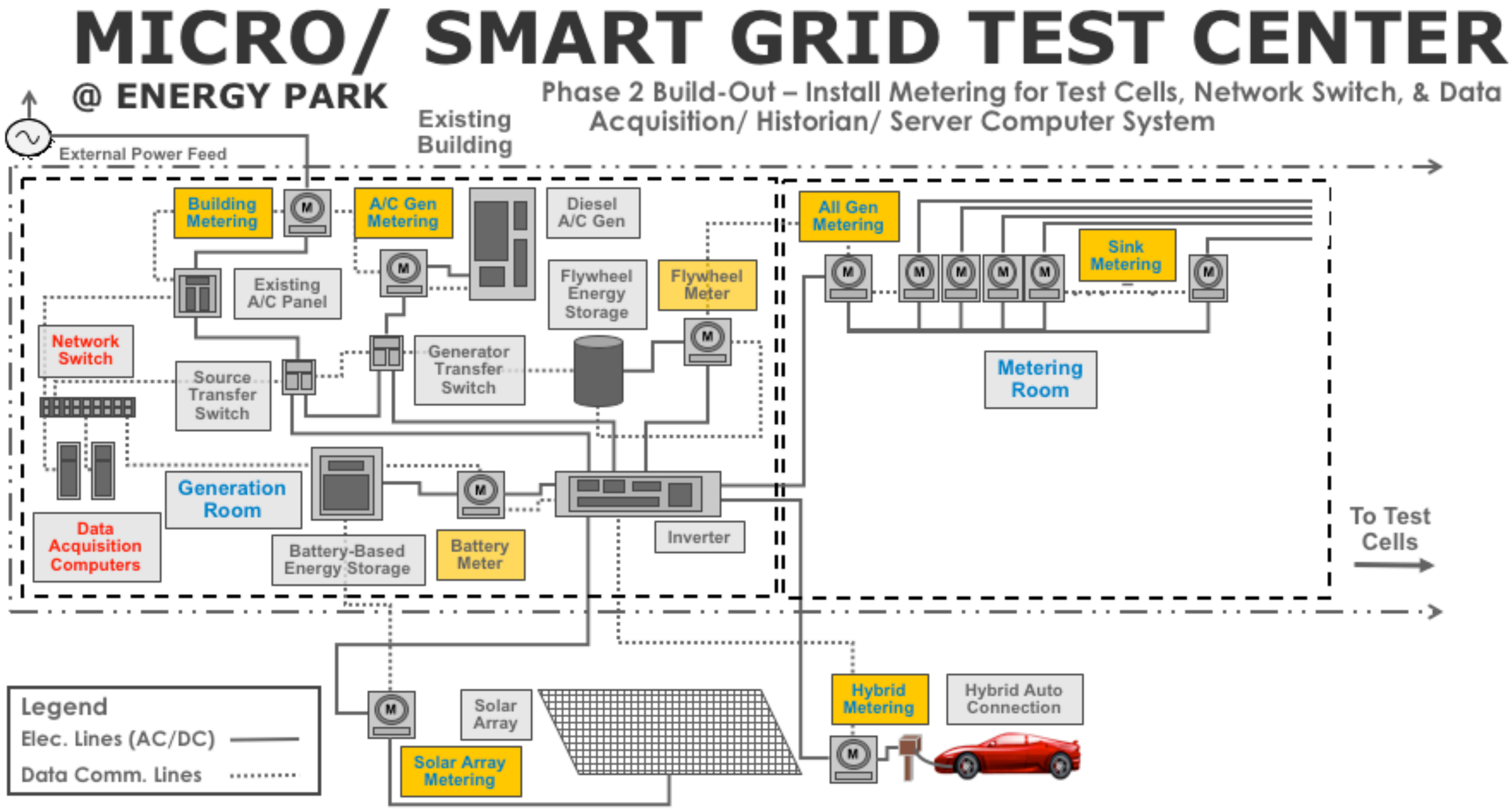
ENERGY PARK TODAY



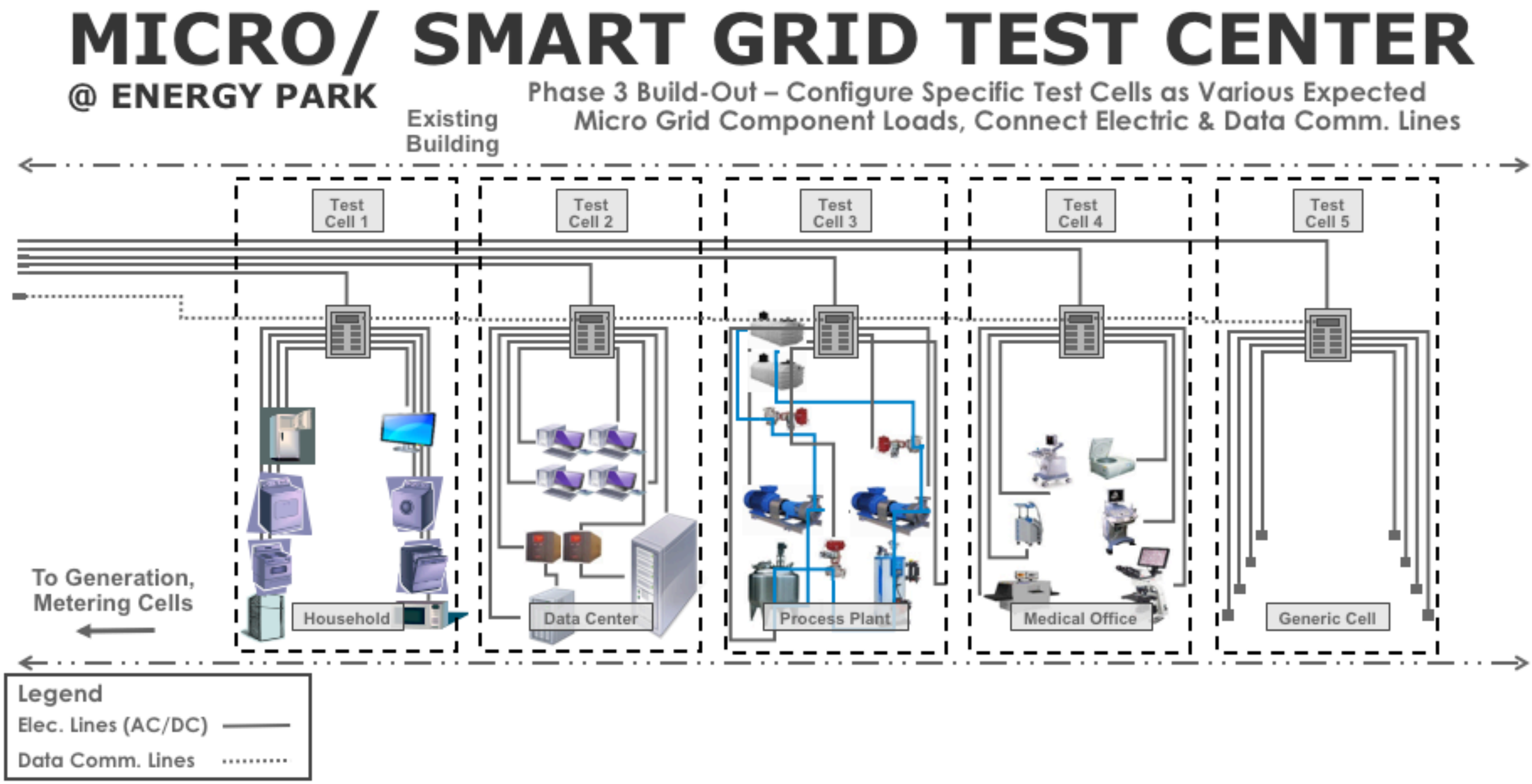
ENERGY PARK PHASE 1 EXPANSION



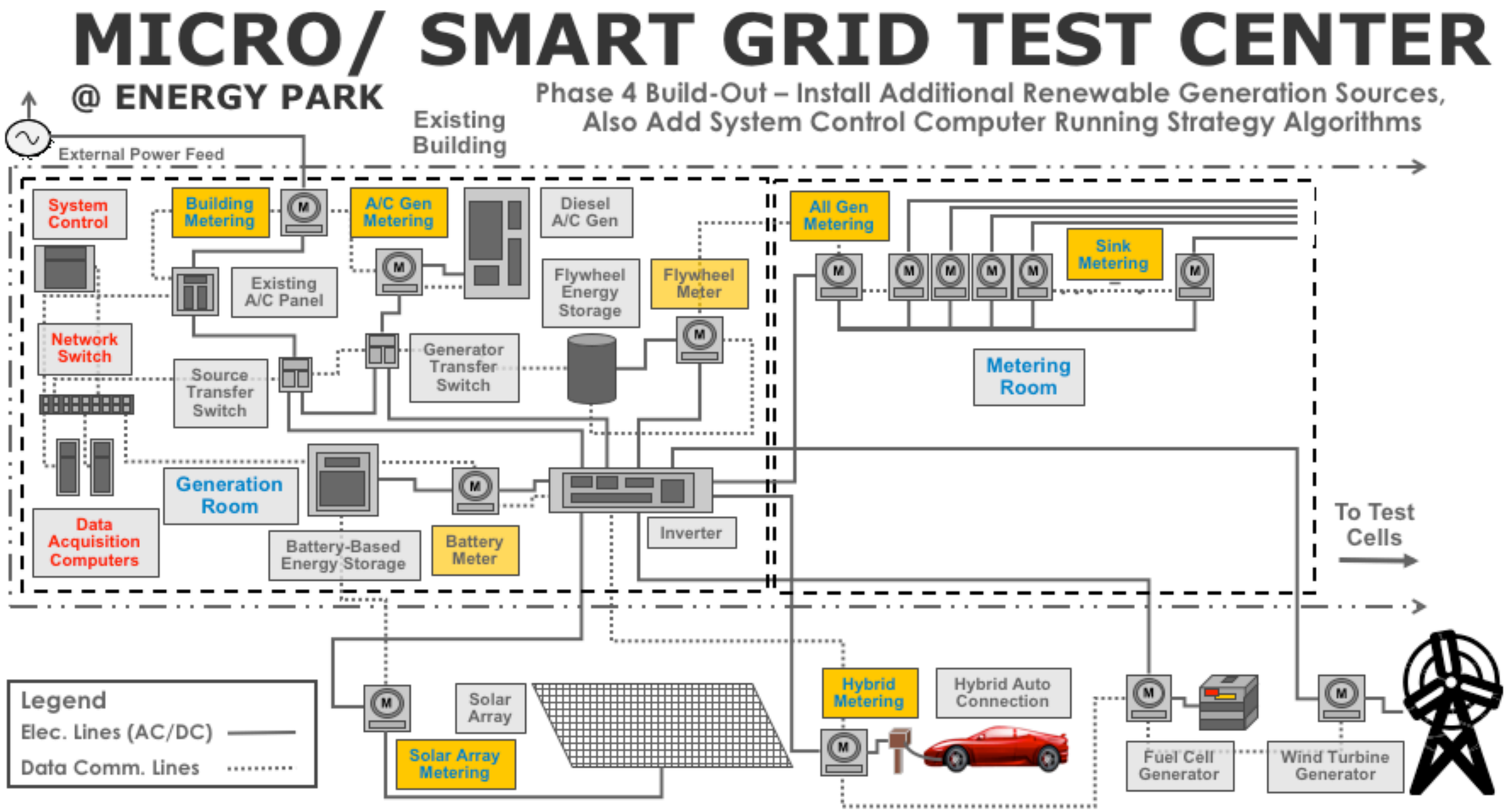
ENERGY PARK PHASE 2 EXPANSION



ENERGY PARK PHASE 3 EXPANSION



ENERGY PARK PHASE 4 EXPANSION



ASSETS

- Testbeds – platforms for experimentation
  - Power System Testbed (cyber security focus)
  - Solar Research Testbed (microgrid research)
  - Cloud Computing Testbed (application of cloud to critical infrastructure)
  - Software Defined Networking Testbed (application of controllable network definition)

MODELS

- Models and interoperability - Models are representations; there are different types of models (e.g., model of an experiment vs. model of the grid).
  - Power System Cases
    - http://publish.illinois.edu/smartergrid/power-cases/
    - 9 Standard IEEE Models in various forms (PowerWorld, PSLF, PSSE, RTDS – updates pending)
  - Cyber Models
    - Mobius/Advise models (various, some releasable)
    - Not yet fully categorized
  - Tools
    - Testbed Automation
      - RSCADstreamer
      - SEL provisioning
    - Smart Grid specific research tools
      - Modeling and reasoning
      - IDS
    - Generic security tools
      - Modeling
      - Fuzzing

DATA & EXPERTISE

- Data – a collection of data
  - Ability to generate (and have various archives of) various representative data sets for various ICS protocols
  - Large archives of utility specific data (under NDA)
- Expertise – subject matter expertise, brain power + connections
  - World-renowned faculty in
    - Power Systems Engineering
    - Computer Security, Resiliency, Trust, and Critical Infrastructure
    - Foundational experimentation and formal methods
    - Various other interdisciplinary topic areas
  - Full time staff with domain expertise
    - Power Engineers
    - Research Programmers
    - Research Scientists

APPROACH

- Process / methodologies – how to build scientifically valid, methods to execute models and produce data
  - Formal courses and professional staff
  - Tools (Mobius, Testbed automation)
- Policies – information and data sharing access policies
  - Data protection archive systems
  - Mechanisms for addressing NDA requirements
- Education and training – teaching how to do scientifically correct experiments
  - Formal courses and professional staff
  - Lay-of-the-land “bootcamp” in smart grid systems
  - Short courses in power systems and computer security
  - Hands on training in SCADA system assessment
  - Professional staff and internal documentation (specific to Illinois resources) and tools to assist researchers

USE CASES

- Use cases
  - Various publications
  - Deployable experiments (specific to Illinois resources)
  - Tools and documentation for similar research

RESEARCH INTERACTIONS

- Idaho National Lab
  - IFMAP interfacing between applications (Sophia/NetAPT)
- Los Alamos National Lab
  - Quantum cryptography validated as applied to power grid communications
- PNNL
  - VM images of SIEGate for rapid security testing
- Purdue
  - AMI research/validation
- UMASS
  - Power fingerprinting research support via energy device composition
- USC-ISI/DETER
  - Multi VM Image selection; PMU provisioning; Offsite DETER standup; Various bugfixes

APPLIED INTERACTIONS

- ABB
  - 61850 modeled environment
- Applied Communication Sciences
  - ICS protocol interfacing and vulnerability analysis
  - Model proving and validation
- Electric Power Research Institute
  - Energy sector device configuration; data sharing; testbed architecture
- Entergy
  - Scale testing; Security assessment; data sharing
- Grid Protection Alliance
  - Scale testing; Security assessment
- Honeywell
  - PoC testbed implementation; Scale testing
- Schweitzer Engineering Laboratories
  - Protection; Software Defined Networking

OTHER INTERACTIONS

- Various utilities, coops, municipalities
  - Data sharing; Analytics
- Education and Training
  - Curriculum, Short courses, and hands-on training development regarding cyber security in the smart grid
  - Courses taught to external entities, planned open release in near future

RELEASED TOOLS

- Display Wall Control
  - Display wall dynamic interaction
  - https://github.com/ITI/displayweb
  - https://github.com/ITI/wallctl
  - https://github.com/ITI/libnti
  - https://github.com/ITI/libwall
- IFMAP client
  - IFMAP interface for mapping information from one location to another
  - https://github.com/ITI/ifmap-python-client

OTHER TOOLS

- RSCADStreamer
  - https://github.com/ITI/rscadstreamer
  - Tool to automate control and simulation interaction with the RTDS
- Device Interfacing (pending release)
  - Connect to and configure SEL devices via various mediums (IP and serial)
- ArchiveReader (pending release)
  - Tool to extract data archives from the GPA openHistorian data format
- Power simulation analysis
  - Tool to analyze the output of various power simulation software and prepare reports
- Traffic Generator
  - Tool to simulate traffic patterns with defined periodicity rather than average bandwidth or rate
- LZFuzz
  - Black box protocol fuzzer, leveraged for analyzing security of proprietary protocols
- SCADA hands-on training lab
  - Automation of the virtualized training environment including setup and provisioning
  - Not deployable in DETER today (portable environment)

GRADUATED TOOLS

- NetAPT/NP-View (pending commercialization)
  - Network accessibility tool to compare global policy against actual device configuration to determine violations
- Mobius (pending commercialization)
  - Formal modeling tool for interaction and validation
- Amilizer
  - Specification based intrusion detection system for AMI
- Response and Recovery Engine (RRE)
  - Active intrusion response based on reasoning around adversarial models (both static and dynamic)
- Bro protocol parsers (ICS)
  - DNP3 protocol parser, consultation on modbus parser, with more to ocme

CURRENT TESTBED DONATIONS PROVIDED BY

- byres security inc — intrinsically secure
- Mu Dynamics
- Itron
- OSIsoft
- OSI
- GE
- endace
- Electric Power Group
- IBM
- PowerWorld Corporation — The Visual Approach to Analyzing Power Systems
- SPACE-TIME INSIGHT
- BAYSHORE NETWORKS
- Trilliant
- NATIONAL INSTRUMENTS
- invensys
- INSTEP
- SISCO
- SEL SCHWEITZER ENGINEERING LABORATORIES
- U.S.NRC — United States Nuclear Regulatory Commission

MORE INFORMATION

- Tim Yardley – yardley@illinois.edu

- TCIPG Testbed Tour
  - http://tinyurl.com/tcipgtestbed

- TCIPG Summer School 2015
  - https://tcipg.org/2015-summer-school