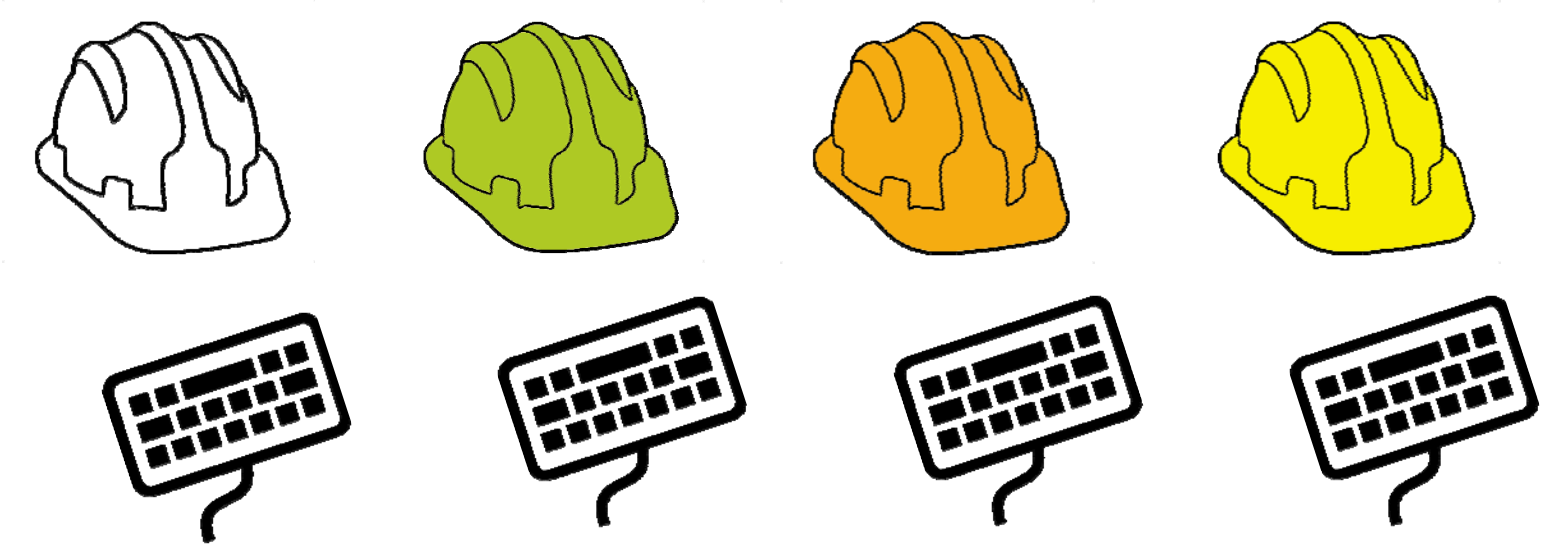
CYBER RESILIENT ENERGY
DELIVERY CONSORTIUM

- Consortium of universities, national labs, and industrial partners committed to:
  - Identifying gaps in the existing cyber infrastructure for energy delivery with respect to enhancing EDS resiliency (electric power and oil & gas)
  - Identifying trends in emerging technologies that may impact resiliency
  - Performing long-term and mid-term research to close gaps, with mid-term research leading to validated solution prototypes
  - Developing software infrastructure for empirical evaluation on hardware testbeds
  - Developing educational and out-research activities
- Build on the strong success of TCIPG
- 5 Year project funded by Department of Energy, Office of Electricity Delivery and Energy Reliability


CREDC
DARTMOUTH
VOX CLAMANTIS IN DESERTO
1769
ASU
WASHINGTON STATE UNIVERSITY
RUTGERS
THE STATE UNIVERSITY OF NEW JERSEY
OSU
Oregon State UNIVERSITY
UNIVERSITY OF HOUSTON
TENNESSEE STATE UNIVERSITY
Pacific Northwest NATIONAL LABORATORY
Argonne NATIONAL LABORATORY

CREDC in a nutshell

- identify and perform cutting edge research and development **whose results are actually used** to increase cyber-resiliency of energy delivery systems



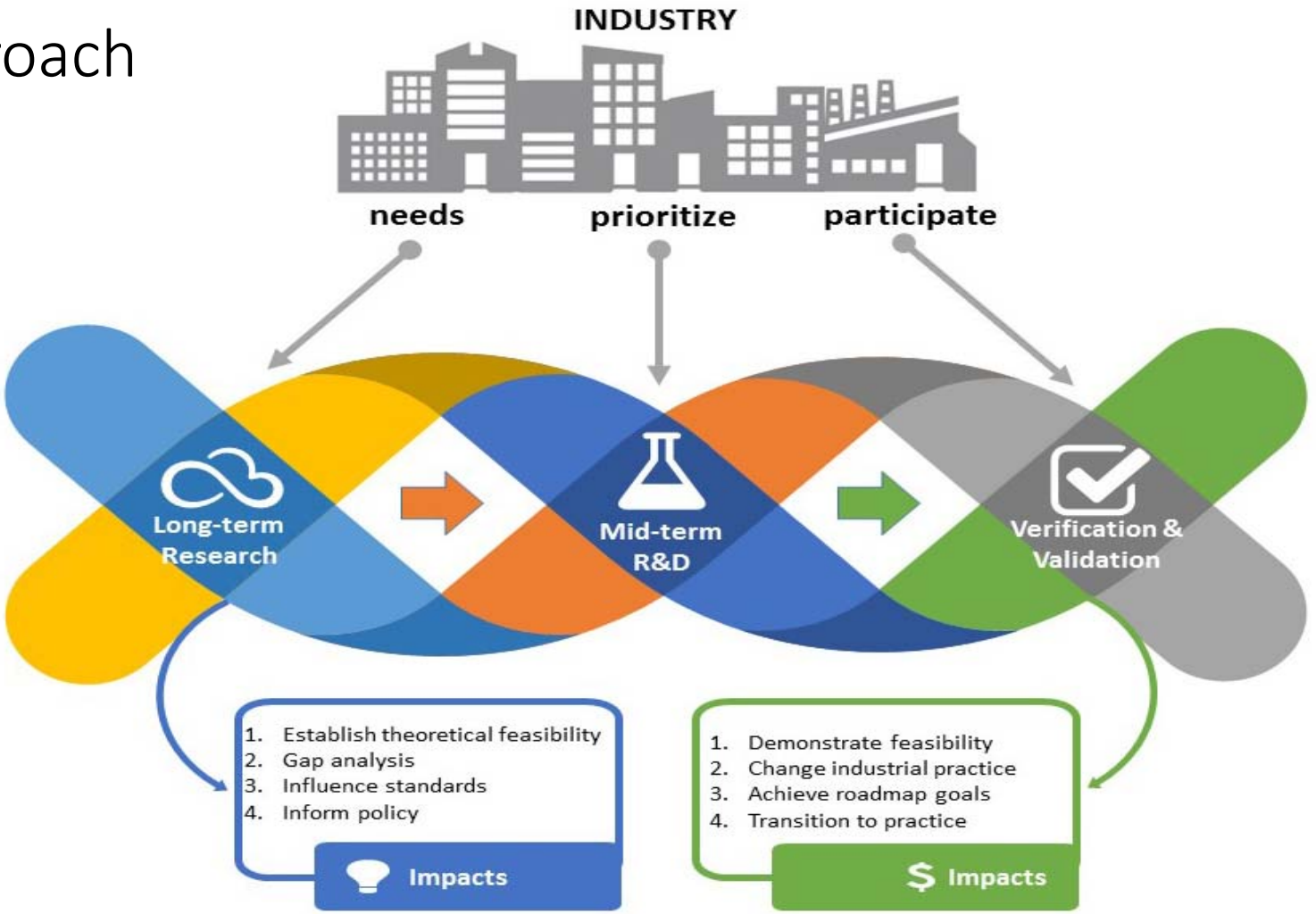
Supporting objectives

- Help management find rationale for EDS cyber-resiliency investment
- Identify impediments and find highest impact *adoptable* solutions
- Develop, validate, verify high impact solutions, with industry
- Make solutions available
- Develop model of operation that is ultimately self-supporting





Approach


INDUSTRY
needs
prioritize
participate
Long-term Research
Mid-term R&D
Verification & Validation
1. Establish theoretical feasibility
2. Gap analysis
3. Influence standards
4. Inform policy
Impacts
1. Demonstrate feasibility
2. Change industrial practice
3. Achieve roadmap goals
4. Transition to practice
Impacts

Verification and Validation

Ensure that CREDC technologies is designed to meet customer needs, is implemented correctly, and meets technical specifications

Remote Management

- Design, execute, analyze experiments without physical access

Test-bed Federation

- Develop technology for combining assets of distributed test-beds, and an understanding of the contexts where this is technically and scientifically feasible

Design and Execute V&V Evaluations

10,00 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

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)

Existing Testbed Donations Provided By

CREDC

Industrial Advisory Board

- **Mark Browning,** Exelon Utilities
- **Dennis Gammel**, Schweitzer Engineering Laboratories
- **Richard Jackson**, formerly with Chevron Corporation
- **Himanshu Khurana**, Honeywell Building Solutions
- **Blake Larsen**, Western Refining
- **Scott Mix**, North American Electric Reliability Corporation (NERC)
- **Paul Myrda**, Electric Power Research Institute (EPRI)
- **David Norton**, Federal Energy Regulatory Commission (FERC)
- **Kymie Tan**, Jet Propulsion Laboratory, Cyber Defense Engineering and Science Directorate
- **Zach Tudor**, Idahoe National Laboratory

A few examples of projects partnering with industry

- Network Perception --- industry participation helped pivot to NERC-CIP support
- Amilyzer --- Utility concerned about intrusions into AMI network
- IDS for DNP3 --- “how can we use Bro to do intrusion detection”
- On-site authentication to remote devices
- Lightweight bump-in-wire encryption for legacy pt-to-pt serial communications
- Hardened platform for data sensing and communication
- Evaluation of device configurations vis a vis security policy
- Role-based access control revisited for industrial control systems
- Validation of software defined network configurations with respect to security policies
- Secure information exchange and protection
- Ontology-based representation of grid components

Annual Industry Day

Break-out sessions in 2016

- Challenges to EDS cyber resiliency from an expanding attack surface
- Regulatory Compliance
- Cross-Sector Issues
- Data Analytics for EDS Security
- Evolving Adversary
- Human Factors and Usability
- Supply Chain Security
- Workforce Development, Training, and Education

Getting Engaged

- External Consortium Member
  - Annual paid dues associated with deeper access to CREDC research and other benefits
- Industry Advisory Board (IAB)
  - Small panel of industry leaders that help direct research efforts
- Industry Participation Board (IPB)
  - Larger group of entities that represent their companies engagements with or interest in CREDC research

Come talk to us!

Tim Yardley, yardley@illinois.edu

info@cred-c.org

http://cred-c.org

@credcresearch

facebook.com/credcresearch/