



Cyber Resilient Energy Delivery Consortium (CREDC)

Academic consortium working closely with utilities, asset owners, and equipment manufacturers in energy delivery systems (EDS) to identify and perform cutting edge research and development to increase the security and resiliency of cyber-systems in EDS.

Background

Cyber technology is permeating energy delivery systems (EDS) such as Supervisory Control and Data Acquisition (SCADA) systems in the electric sector as well as in oil and gas pipelines. This trend is accelerating and has the potential to make EDS safer, more efficient, and better able to address societal objectives in sustainable energy technologies and innovative energy markets. However, the “cyber plane” in EDS presents potential opportunities for adversaries seeking to disrupt, destabilize, or damage EDS through cyber or blended cyber-physical attack. Also, as cyber becomes more prevalent in EDS, issues of secure communications and operations across heterogeneous systems (including inter-dependency of EDS infrastructure) become critical.

Barriers

Some major challenges to EDS cyber resiliency include:

- New attack surfaces continuously created by technology: Internet of Things, cloud, distributed generation, electric vehicle (EV) infrastructure
- Continuous evolution of adversaries’ targets, methods, tools, and objectives
- Increased integration of renewable energy, including from third-party providers
- Issues of emerging markets such as aggregation and home energy management
- Business case for adoption of innovative technology in support of EDS cyber resiliency, in particular during economic constraints (collapse in oil prices)

Project Description

CREDC performs multidisciplinary R&D in support of the Energy Sector Control Systems Working Group’s Roadmap of resilient Energy Delivery Systems (EDS) that focuses on resiliency and security of the *cyber components of EDS*. CREDC addresses the cyber-resiliency of power grids and oil & gas refinery and pipeline operations, which has been the subject of legislation, standards, and executive actions. There is growing awareness that the industry must move beyond *cyber-security* to include *cyber and physical resiliency* to ensure that EDS sustain critical functions in the presence of disruptive events arising from attacks, accidents, or errors, and to rapidly recover from disruptions to full functionality.

CREDC develops projects with significant and measurable sector impact, involving industry partners (asset owners, equipment vendors, and technology providers) *early and often*, with activities that range from helping us to identify critical sector needs, to performing pilot deployment and technology adoption. The central project goal is to create a research and development ecosystem where research results lead directly to development of applications and methodologies which are then validated in realistic contexts, as illustrated in Figure 1 (reverse side). We will demonstrate the unique utility of this approach to industry as the foundation of a longer-term approach to CREDC self-sufficiency. As an academic consortium, we will also address goals of research excellence, education, and workforce development. This project is co-funded by the Department of Homeland Security (DHS) Science & Technology Directorate.

Benefits

- World-leading R&D in many aspects of EDS cyber resiliency
- Develop professional workforce competent in cyber and energy disciplines
- Transition impactful solutions to EDS sectors addressing critical sector needs

Partners

- University of Illinois at Urbana-Champaign (lead)
- Argonne National Laboratories
- Arizona State University
- Dartmouth College
- Massachusetts Institute of Technology
- Oregon State University
- Pacific Northwest National Laboratories
- Rutgers University
- University of Houston
- Tennessee State University
- Washington State University

Website

- <http://cred-c.org>

Program Objectives

- Develop rationale for support of EDS cyber resiliency in terms understandable to EDS investment decision-makers
- Identify impediments and find the highest-impact *adoptable* solutions
- Develop, verify, and validate high-impact solutions with industry and national lab partners
- Make solutions available
- Develop self-sustaining model of operation

Long-Term Research

- Anticipate and address long-term issues impacting EDS cyber resiliency
- Multi-year horizon
- “Prime the pump” for mid-term R&D

Mid-Term Research & Development

- Issues addressing critical industry need, in partnership with industry
- Typically, 2-year horizon from research to prototype

Verification and Validation

- Develop testbed capabilities
- Support evaluation of developed solution prototypes
- Curate evaluation data, make openly available

Stakeholder Outreach

- Industry Advisory Board
- Industry Participation Board
- Annual Industry Workshop
- Workforce Development
- “Summer School” Training
- K-12 and Public Outreach

End Results

Project results will include:

- EDS that are able to operate through cyber attack or accidental failure
- Solutions that enhance resiliency even as EDS systems encompass evolving cyber-technologies, EDS technologies, and changing EDS markets
- Business case to build a culture of security in EDS sectors
- A self-sustaining consortium to maintain and advance improvements in EDS resiliency

January 2016

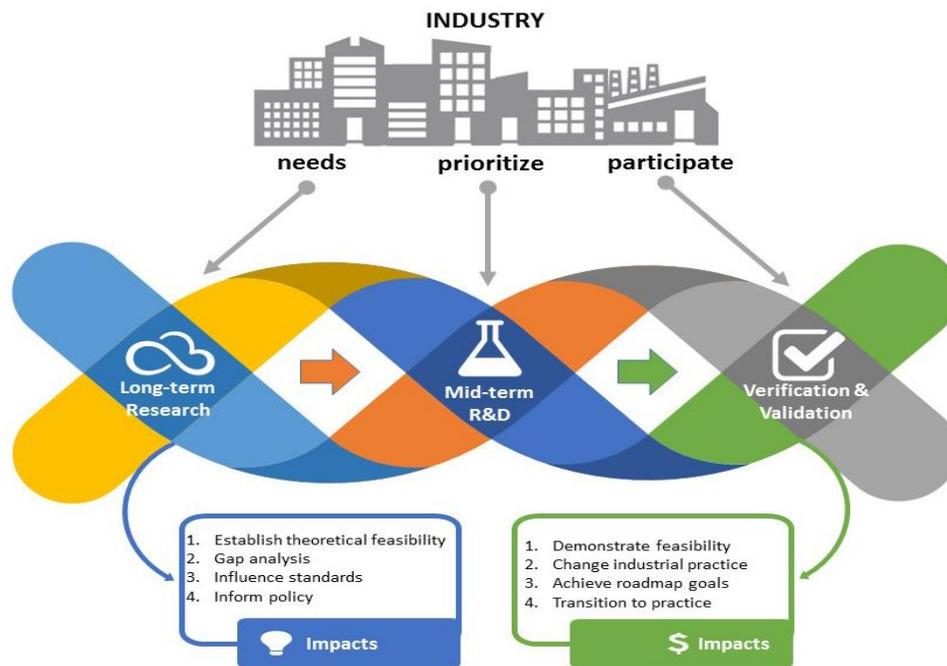


Figure 1. CREDC Research Ecosystem for Impact on Energy Delivery Systems

Cybersecurity for Energy Delivery Systems (CEDS)

CEDS projects are funded through the Department of Energy's (DOE) Office of Electricity Delivery and Energy Reliability (OE) research and development (R&D) program, which aims to enhance the reliability and resilience of the nation's energy infrastructure by reducing the risk of energy disruptions due to cyber attacks.

For More Information:

Carol Hawk
Program Manager
DOE OE R&D
202-586-3247
carol.hawk@hq.doe.gov

David Nicol
Principal Investigator
University of Illinois
217-244-1925
dnicol@illinois.edu

For More Information:

- <http://energy.gov/oe/technology-development/energy-delivery-systems-cybersecurity>
- www.controlsroadmap.net
- <http://cred-c.org>