U.S. DEPARTMENT OF ENERGY | Office of Cybersecurity, Energy Security, and Emergency Response

# PreventOTPhysDamage: Anticipating and Preventing Catastrophic Operational Technology Physical Damage Through System Thinking Analysis

CREDC
CYBER RESILIENT ENERGY DELIVERY CONSORTIUM

*Protecting physical energy operational technology infrastructure against targeted cyberattacks that may cause physical damage to difficult-to-replace devices*

Most energy delivery system (EDS) cybersecurity programs are designed to prevent unauthorized system access because, to date, most EDS attacks have targeted software-led processes that may be restored by restarting the affected components. In the case of operational technology (OT), once system access is obtained, sophisticated cyberattacks have the additional potential to cause physical damage or destruction to the devices themselves. The team is conducting research within the MIT co-generation plant to identify and anticipate physical risks to OT as a result of coordinated cyberattacks. The team will develop an analysis tool that OT operators can use to identify vulnerable EDS physical targets and failure scenarios, and create enhancements that minimize physical damage. The resulting web-based tool, with advanced graphics and an easy-to-use interface helps OT operators identify critical cybersecurity vulnerabilities, determine the specific control hierarchy, evaluate the effectiveness of control mechanisms and potential failure modes, and provide mitigation recommendations.

## KEY TAKEAWAYS

- Simplifies energy delivery system analysis to identify and anticipate critical cyber-physical risks
- Eliminates or restricts hazard conditions that can lead to a dramatic loss through physical destruction of operational technology
- Implements effective, data-driven countermeasures during design and operation for operational technology

## OUTCOME

This research will eliminate or restrict hazard conditions that can lead to loss of EDS operations and implements effective countermeasures during design and operation for OT operators. The team will develop an accessible system analysis tool to maximize the implementation of cyber-physical security programs.

| PARTICIPANTS | ROLE |
|---|---|
| CREDC CYBER RESILIENT ENERGY DELIVERY CONSORTIUM | The CREDC performs multidisciplinary research and development that focuses on the cybersecurity of energy delivery systems. The central project goal is to create an ecosystem where research results lead directly to the development of applications and methodologies, which are then validated in realistic contexts. |
| Massachusetts Institute of Technology | Lead institution; validates tool at the MIT cogeneration facility |
| ENGIE | Engages stakeholders |
| ExxonMobil | Delivers presentations to stakeholders and leads other stakeholder engagement efforts |
| Schneider Electric | Received and reviewed report |
| HITACHI Inspire the Next | Explores application within a manufacturing facility |

## CONTACT INFORMATION


**Initial Leads:**

**Carol Hawk**
Program Manager

**Stuart Madnick**
Site Lead, Professor
Massachusetts Institute of Technology
617-253-6671
smadnick@mit.edu

**Current Contact as of February 2020:**

**Akhlesh Kaushiva**
Senior Technical Systems and Cybersecurity Advisor
Department of Energy (DOE)
Office of Cybersecurity, Energy Security, and Emergency Response (CESER)
202-287-6062
Akhlesh.Kaushiva@hq.doe.gov



This is a subproject sponsored by the CREDC academic consortium, led by the University of Illinois.

**CREDC Period of Performance:** October 2015 – May 2022

**CREDC Total Award Value: $28,099,258**
DOE Share: $22,476,290
Cost Share: $5,622,968

**CYBERSECURITY FOR ENERGY DELIVERY SYSTEMS (CEDS)**

CEDS projects are funded through DOE CESER, which aims to enhance the reliability and resilience of the nation's energy infrastructure by reducing the risk of energy disruptions due to cyberattacks.

Website: https://www.energy.gov/ceser

Date Written: June 2021