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

Distributed and Automated Security Analysis of Critical Energy Delivery Controller Software

CREDC
CYBER RESILIENT ENERGY DELIVERY CONSORTIUM

A plugin security solution to analyze and protect large-scale cyber-physical power grid infrastructures

The secure operation of next-generation cyber-physical energy delivery systems (EDS) requires effective, scalable, and formal state verification and predictive situational awareness capabilities. Existing methods of static, offline system analysis are unable to scale up to address the state of large cyber-physical infrastructures, and dynamic monitoring and situational awareness solutions act in real-time, leaving little to no buffer for effective manual or automated response and recovery. This research develops a distributed, scalable, vendor-agnostic EDS security analysis solution called the Trusted Controller Verifier (TCV) that uses a hybrid static/dynamic approach to stay ahead of the actual EDS system state during security verifications. TCV validates programmable logic controller (PLC) implementations to assess current estimated system states in order to model and analyze the security of potential future system states. This gives EDS operators sufficient time to react in the event of an unsafe state realization and proactively prepare against adversarial activities. TCV is also capable of learning selected tolerance strategies so that it reacts automatically upon early realization of previously seen similar unsafe states.

KEY TAKEAWAYS

- Enables power grid operators to proactively assess current and future system states and prepare for potential cyberattack scenarios
- Overcomes the barrier to effectively securing programmable logic controllers across large-scale cyber-physical infrastructures
- Delivers an architecture-agnostic plugin solution for complex system analysis and predictive modeling

OUTCOME

TCV offers an accessible, pluggable, and validated software-based solution to secure PLC against malicious program execution, allowing operators to quickly and easily verify the security of complex EDS infrastructures. The research team's collaboration with Siemens provides a critical testbed for ensuring widespread industry adoption of the TCV software by the end of the project.

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.
RUTGERS	Leads research, development, and testing
SIEMENS	Enables the technology's transition to practice on real PLC devices

CONTACT INFORMATION

Initial Leads:

Saman Zonouz
Rutgers Site Lead, Assistant Professor
Rutgers University
848-445-8508
saman.zonouz@rutgers.edu

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