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

VARS: Verification and Validation Assuring Reliability and Security

Pacific Northwest NATIONAL LABORATORY

A framework for guiding risk-informed verification and validation focusing on risk-based approaches of cybersecurity testing for the energy sector

As the complexity and connectivity of energy delivery systems (EDSs) increases, the associated cybersecurity requirements to ensure their safe and reliable operation also increases. It is critical to perform a thorough verification and validation (V&V) of the operational technology and associated information technology products that help monitor, operate, and control U.S. critical energy infrastructure. This project develops a publicly available framework for verification and validation assuring reliability and security (VARS) and a web-based tool for risk-informed V&V recommendations (RIVVR) that vendors, utilities, and academia can use to determine risk-informed approaches for V&V of EDS cybersecurity across the electric and oil and natural gas (ONG) subsectors. The development of this vendor and threat agnostic V&V tool provides quantitative risk metrics based on component vulnerability and potential impacts that can be caused by recognized cyber threats. The dependencies for business functions are also considered. The system identifies, scores, and analyzes risks in EDS, allowing utility owners and operators to take a more informed and systematic approach to mitigating critical vulnerabilities.

KEY TAKEAWAYS

- Formalizes a consistent, risk-informed approach for verifying and validating cybersecurity of energy delivery systems
- Ensures awareness of previously reported relevant vulnerabilities, computes cyber-risk score with consideration to business function dependencies, and recommends cybersecurity testing techniques prioritized based on risk scores
- Lists relevant standards, techniques, and tools for cybersecurity verification and validation testing

OUTCOME

This project delivers a publicly available V&V framework and web tool that organizations can use to drive secure design and development of EDS products and formalize cybersecurity testing as a part of the V&V process. This will enhance the cybersecurity and reliability of common or critical EDS products, which will lead to enhancement of the security and reliability of the overall electric grid.

PARTICIPANTS	ROLE
Pacific Northwest NATIONAL LABORATORY	Performs landscape assessment, gathers inputs from all partners and advisors, and leads the development of the VARS framework and the RIVVR tool.
HITACHI ABB	Provides vendor's perspective on cybersecurity requirements and V&V tests requested by utilities, share insights on vendors' testing procedures, and performs site demonstration.
NRECA America's Electric Cooperatives	Provides utilities' perspective on cybersecurity V&V testing, guides solution development to ensure that the VARS framework and RIVVR tool can be adopted by asset owners and operators, and helps organize a workshop with NRECA member utilities as participants.
Argonne NATIONAL LABORATORY	Provides subject matter expertise in cybersecurity of fossil-based power generation systems, and reaches out to stakeholders in the ONG subsector to gather their inputs for making the VARS framework broadly applicable to ONG.
Western Area Power Administration	Provides a utility's perspective as an advisor on the project.

CONTACT INFORMATION

Initial Leads:

Carol Hawk
Program Manager

Seemita Pal
Principal Investigator
Pacific Northwest National Laboratory
509-372-4106
seemita.pal@pnnl.gov

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

Period of Performance: October 2019 – September 2022

Total Award Value: $2,700,000
DOE Share: $2,700,000
Cost Share: $0

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