

Verification and Validation Assuring Reliability and Security (VARS)

PNNL

Seemita Pal and Jess Smith

Cybersecurity for Energy Delivery
Systems (CEDS)

Peer Review



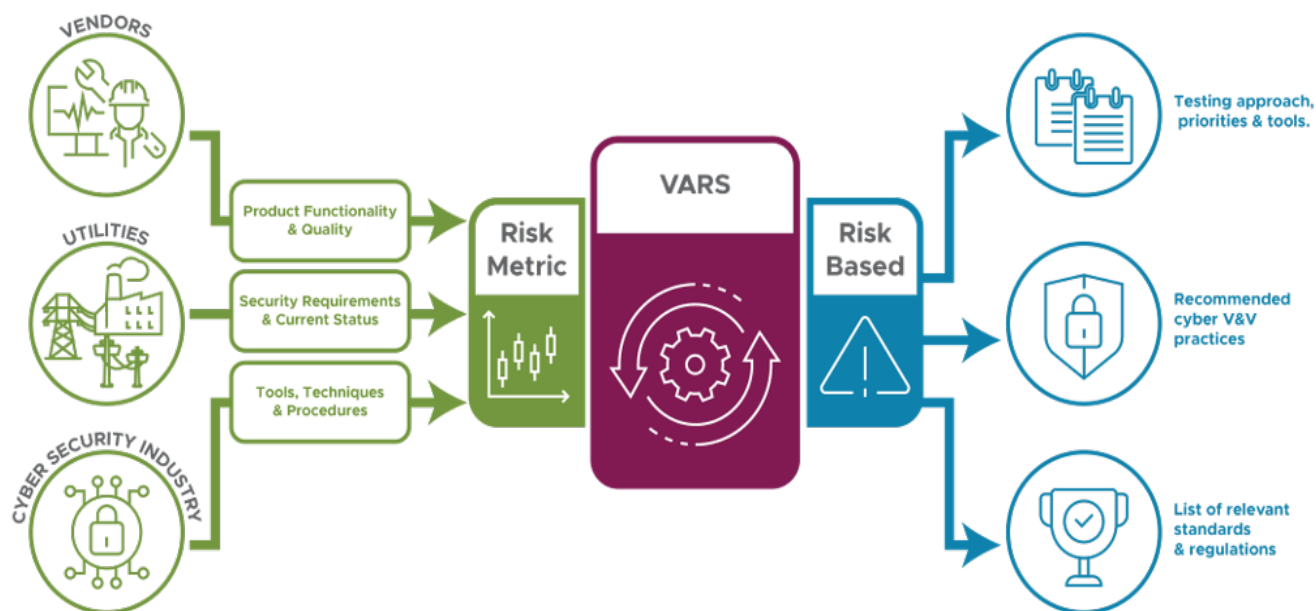
VARS Summary

Objective

Develop a *publicly available framework* and *web-based tool* that organizations can use to determine risk-informed Verification and Validation (V&V) approaches.

Schedule

- Oct. 2019 → Sept. 2022
- Landscape Assessment & Risk Metric
- Framework Development
- Web tool design, development & demonstration



Total Value of Award: \$2,912,500

Funds Expended to Date: 33%

Performer: PNNL

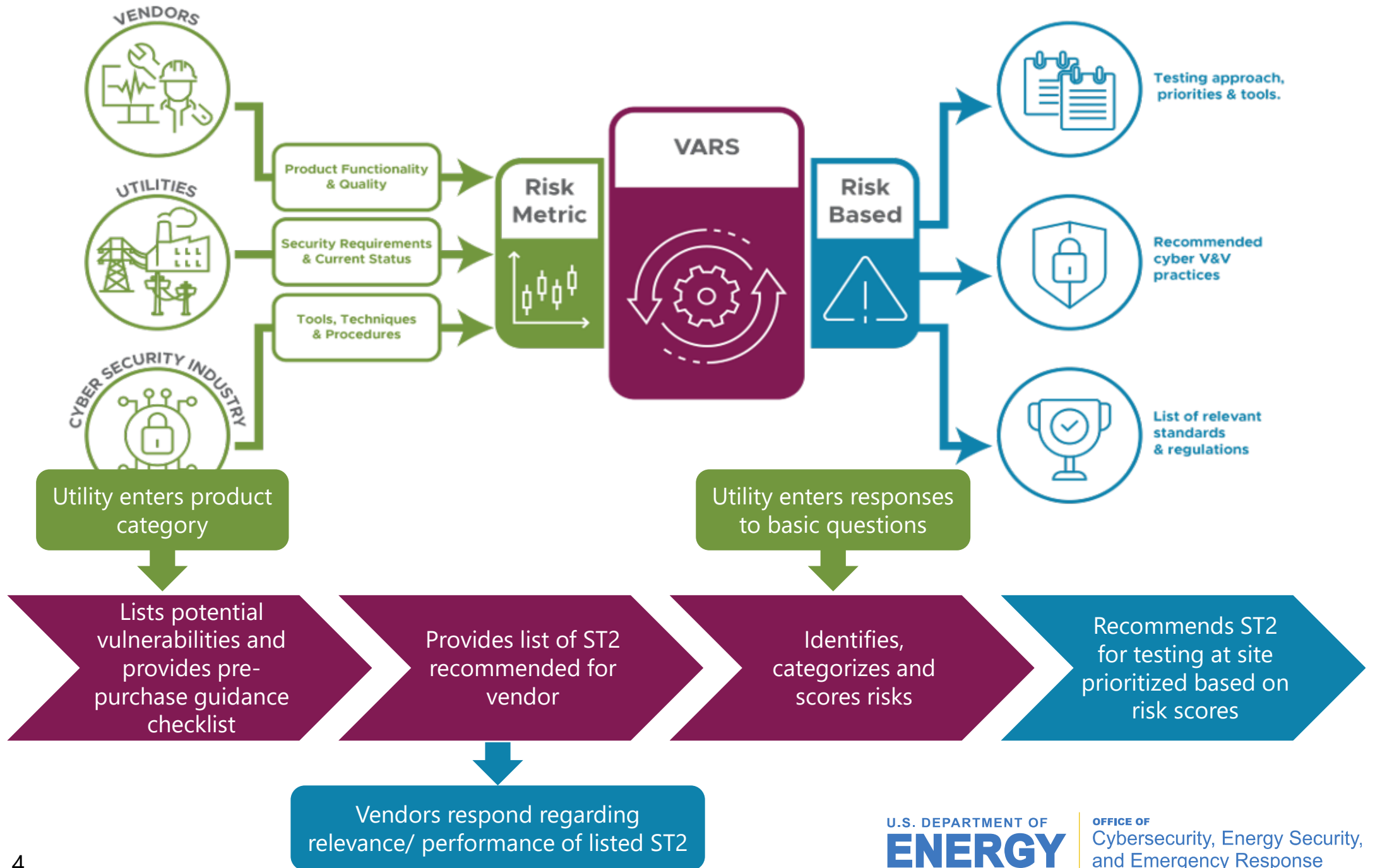
**Partners: Hitachi ABB Power
Grids, ANL, NRECA**

Advancing the State of the Art (SOA)

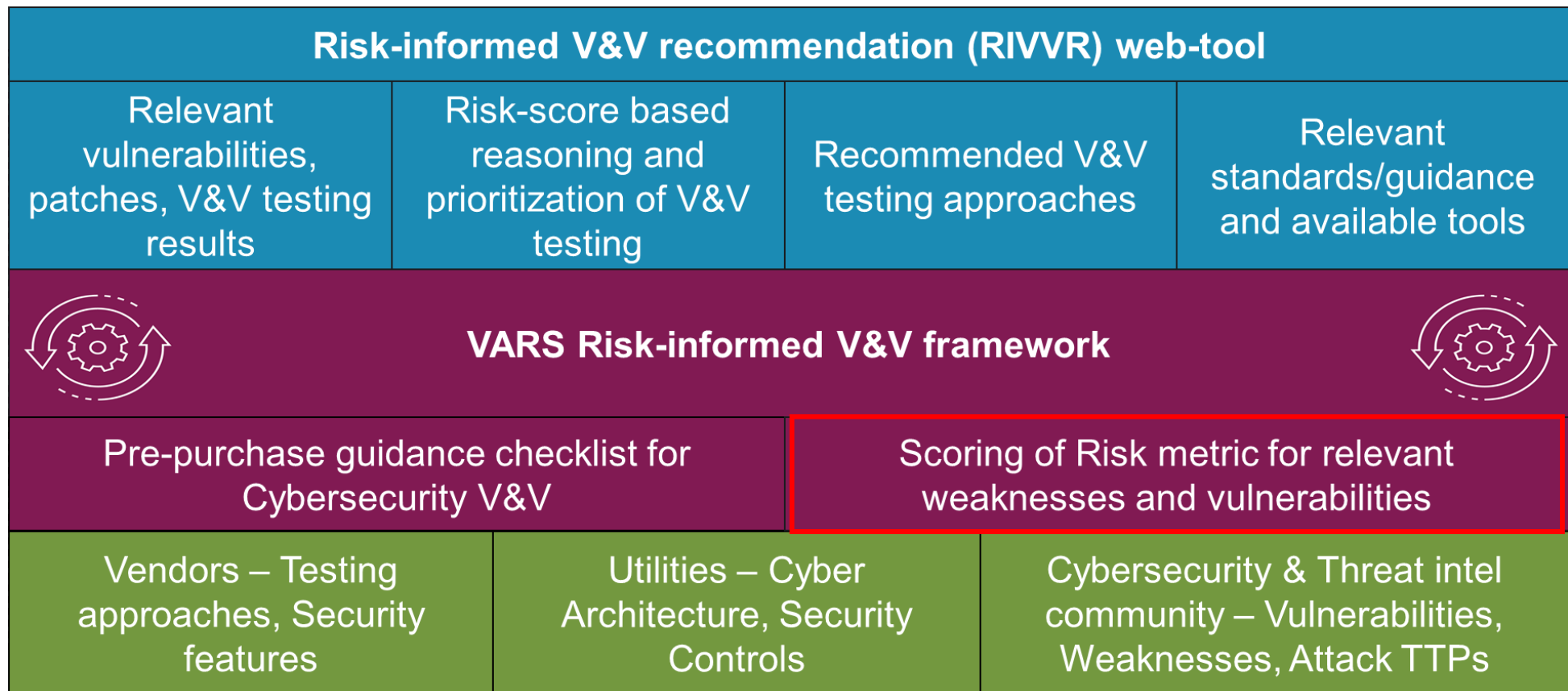
- Currently, there is lack of a thoroughly researched, widely accepted, risk-informed V&V approach for cybersecurity in EDS products.
- VARS (publicly available framework) and RIVVR (web-based tool) will guide risk-informed V&V tailored to the specific lifecycle and domain.
 - Increases much-needed awareness of potential vulnerabilities.
 - Standardizes cybersecurity V&V testing based on domain and lifecycle.
 - Efficiently minimizes risk exposure through prioritized testing.
 - Lists relevant standards, techniques and tools (ST2).

One stop shop for guidance on
cybersecurity V&V testing of EDS products

Overview of VARS Tool



VARS Framework



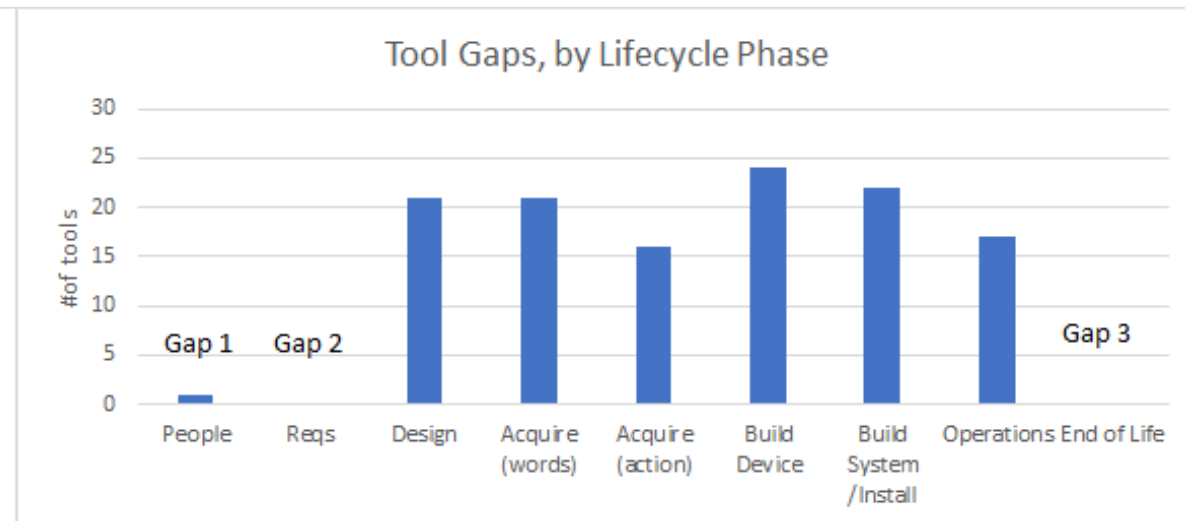
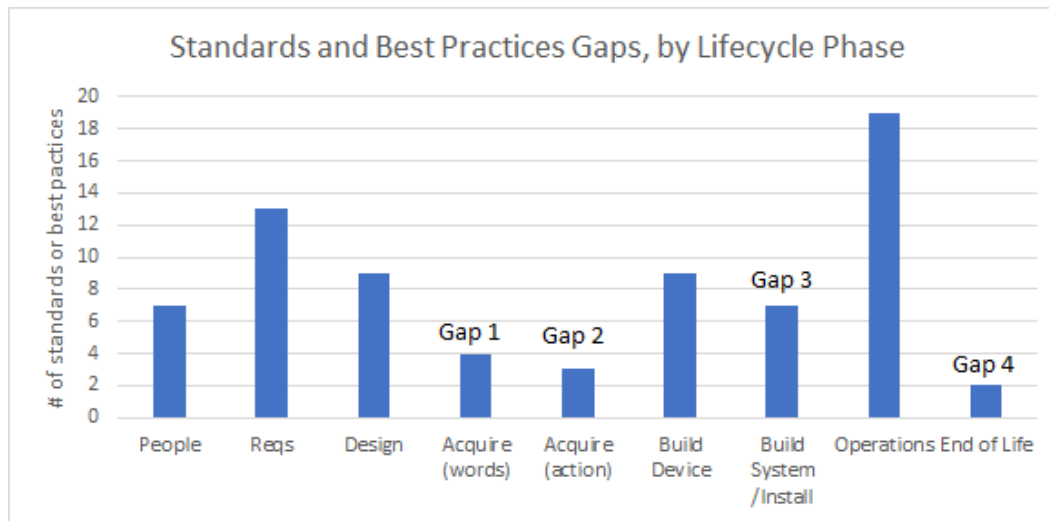
Landscape Assessment Findings

Objectives

- Identification of EDS vendors and product offerings
- Identification of V&V standards and best practices
- Identification of V&V tools

Gaps

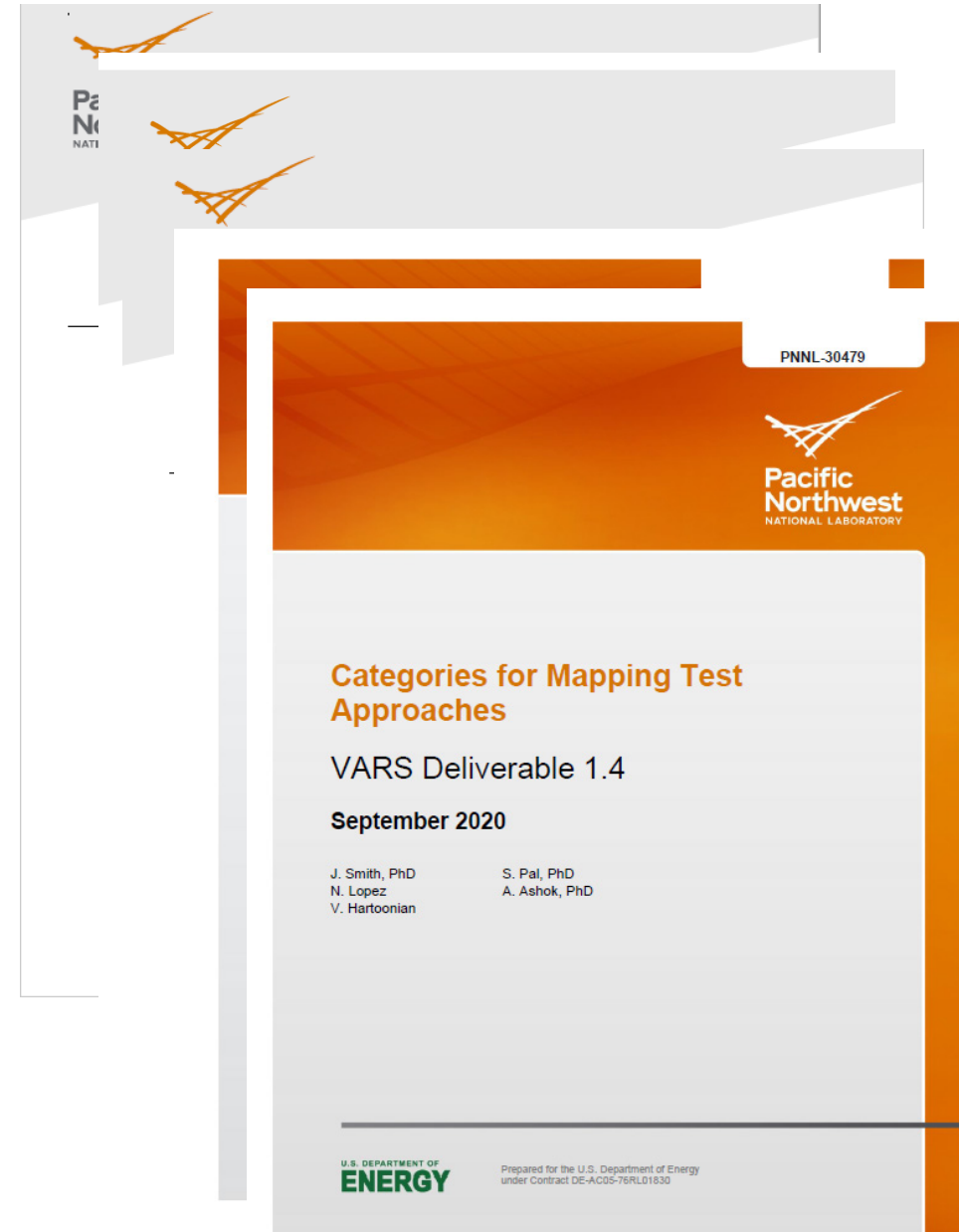
- All Standards Gaps Areas highlight problems in the gaps of acquiring or abandonment of equipment.
 - Design and build V&V are done at the manufacturer
 - Installation and operation V&V are done at the end user
- Tools Gaps Areas highlight problems with ensuring the human side of the lifecycle.



Progress to Date

Major Accomplishments:

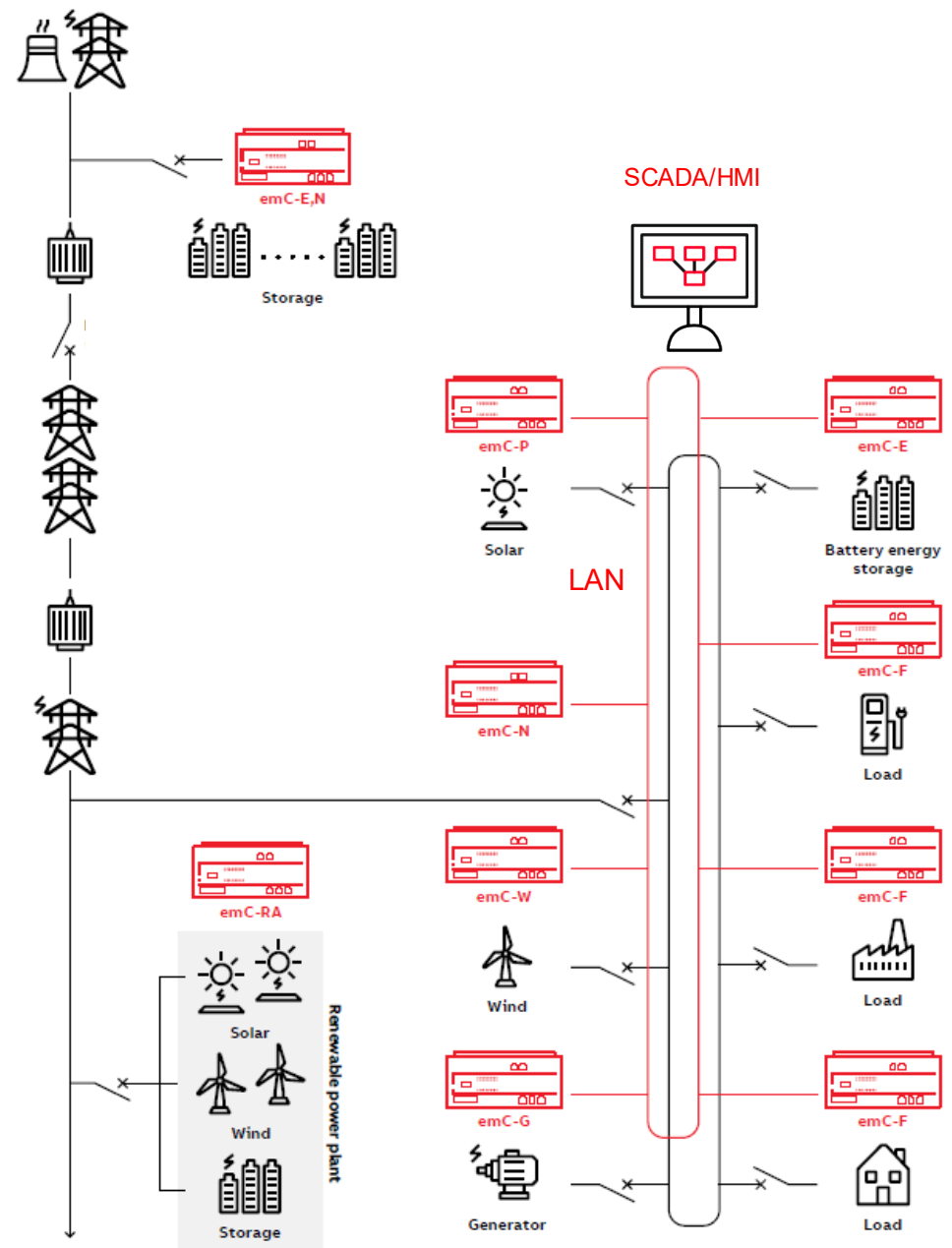
- D 1.1 => Initial Landscape Survey
- D 1.2.1 => Identification of Common & Critical Devices and Key Vendors
- D 1.2.2 => Practical Cyber-Risk Metric for Guiding Verification and Validation
- D 1.3 => Best Practices for Practical Implementation of Verification and Validation of Energy Delivery System Components
- D1.4 => Categories for Mapping Test Approaches



Progress to Date

Major Accomplishments:

- *Selection of Hitachi ABB Power Grids' Product for Site Demonstration in 2022.*
 - e-mesh microgrid control system.
- *Guided development of VARS solution (landscape assessment and framework).*
 - *Inputs on industry's needs from vendor's perspective – Standards-based requirements for robustness testing, hardening, end-user documentation, vulnerability handling and patch management.*
 - *Inputs on vendors' approach to cybersecurity testing – secure design and secure code development, device and system-level security assessment, product and system-level testing guidelines.*



Progress to Date

Major Accomplishments:

- *Positive feedback and great insights from EDS Stakeholders at TechAdvantage.*
- Finalization of Outputs based on Stakeholder Needs:
 - *Pre-purchase guidance checklist* for product category.
 - *Relevant vulnerabilities* previously reported based on ICS-CERT, NVD etc. (e.g. CVE-2019-xxxx).
 - *List of recommended ST2* for utilities and vendors (e.g. static code analysis technique, Ghidra tool, IEEE 1686 standard).
 - *Risk metric* supporting and prioritizing recommendations.

ST2 includes lists of recommended

- V&V techniques
- Tools and their URLs
- Relevant standards/best practices

Challenges to Success

- **Possibility of restricting to virtual participation during the demonstration of selected ABB product at their site.**

Plan to ensure larger team can interact with and test the tool during site demonstration irrespective of mode of participation.

- **Cancellation of conferences this year and anticipated constraints in industry outreach in the near future.**

Present VARS at multiple venues to reach out to targeted users. Effective virtual demonstrations will be key for spreading the word among energy sector stakeholders and ensure maximum impact.



Collaboration/Technology Transfer

Plans to transfer technology/knowledge to end user:

- Targeted end user for the technology or knowledge:
 - Primary: Asset owners – Energy utilities
 - Secondary: Vendor & OEM – EDS hardware/software vendors
- Plans to gain industry acceptance:
 - Working with NRECA and their member utilities to do pilot testing and refine the tool to gain more industry acceptance.
- Testing and demonstrations planned & timeline:
 - Testing and demo at Hitachi ABB Power Grids – 6/30/2022
 - Workshop to present VARS and RIVVR to EDS Stakeholders – 9/15/2022
- Sector adoption – Ongoing work on tech to market plan

Next Steps for this Project

Approach for the next year or to the end of project:

- Mapping of approaches of cybersecurity V&V testing to different categories – March 2021
- Functional requirements for VARS web tool – September 2021
- Completion of first version of the web tool – December 2021

Thank you!

VARs will provide a publicly available framework and web-based tool that organizations can use to determine appropriate risk-informed V&V approaches.

