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

A Cyber-Physical Security Assurance Framework Based on a Semi-Supervised Vetting (CYVET)

PI: Juan Lopez Jr., PhD

Co-PI: Kalyan Perumalla, PhD

Oak Ridge National Laboratory

Cybersecurity for Energy Delivery Systems (CEDS) Peer Review

October 6-7, 2020

Project Overview

Objective

- To develop verification and validation capabilities to test deployed systems against cybersecurity requirements, using a new specification framework in which elements in standards presented in human-readable language are transformed into machine-executable and verifiable formats and verified on hardware test-beds.

Schedule

Item	Duration	Period
Tally-Vet	9 months	Sep’19-Jun’20
Test-Vet	9 months	Jul’20-Mar’21
Prototype	6 months	Apr’21-Sep’21
Demonstration	12 months	Oct’21-Sep’22

Total Value of Award:	**$454,515 cost share + $2,986,801 federal = $3,441,316**
Funds Expended to Date:	**% 32**
Performer:	**Oak Ridge National Laboratory**
Partners:	**University of Nebraska-Lincoln Omaha Public Power District Nebraska Public Power District South Sioux City National Strategic Research Institute Lincoln Electric Systems**

Advancing the State of the Art (SOA)

- **State of the art**: Gap exists for cybersecurity feature compliance certification.
- **Feasibility of our approach**: Apply proven compliance certification approaches (like UL, Energy Star rating) to energy sector component cybersecurity features.
- **Advancement over SOA**: Our semi-automated methodology provides a new, systematic path and initial framework to enable certification.
- **Advancement of the cybersecurity of energy delivery systems**:

1. Equally usable by vendors and asset owners.
    - Unbiased solution that is a win-win for both vendors and users.
    - Vendors benefit from quality differentiation.
    - Users benefit from consistent and assured performance.
2. Comprised of readily manageable advanced tools, technologies and techniques that do not impede critical energy delivery functions.

Advancing the State of the Art (continued)

- **End user benefits**: Our system will improve:
  1. Interoperability.
  2. Scalability (large grids, microgrids, renewal energy).
  3. Backward compatibility regarding OT asset generational evolution across critical infrastructure domains.
  4. Compatibility with current security assessment methods:
     - DOE C2M2, NIST CSF, NERC CIP
  5. Vendor-agnostic design.
  6. Semi-automated capability of testing process.
- **Potential for sector adoption**:
  1. Cost of entry for vendors is reduced due to adoption of DOE R&D.
  2. Our customer needs-focused solution is received favorably by stakeholders and commercialization partner involvement.

Challenges to Success

Challenge 1

- Obtaining sufficient involvement of relevant stakeholders
- Solution: Secured commitment from 3 out of 5 categories
  - The rest were out of scope or postponed for involvement

Manufacturers*
(NRECA)

*Anticipated future collaboration

Regulatory Agencies*
(NERC, FERC)

Asset Owners
(OPPD, NPPD)

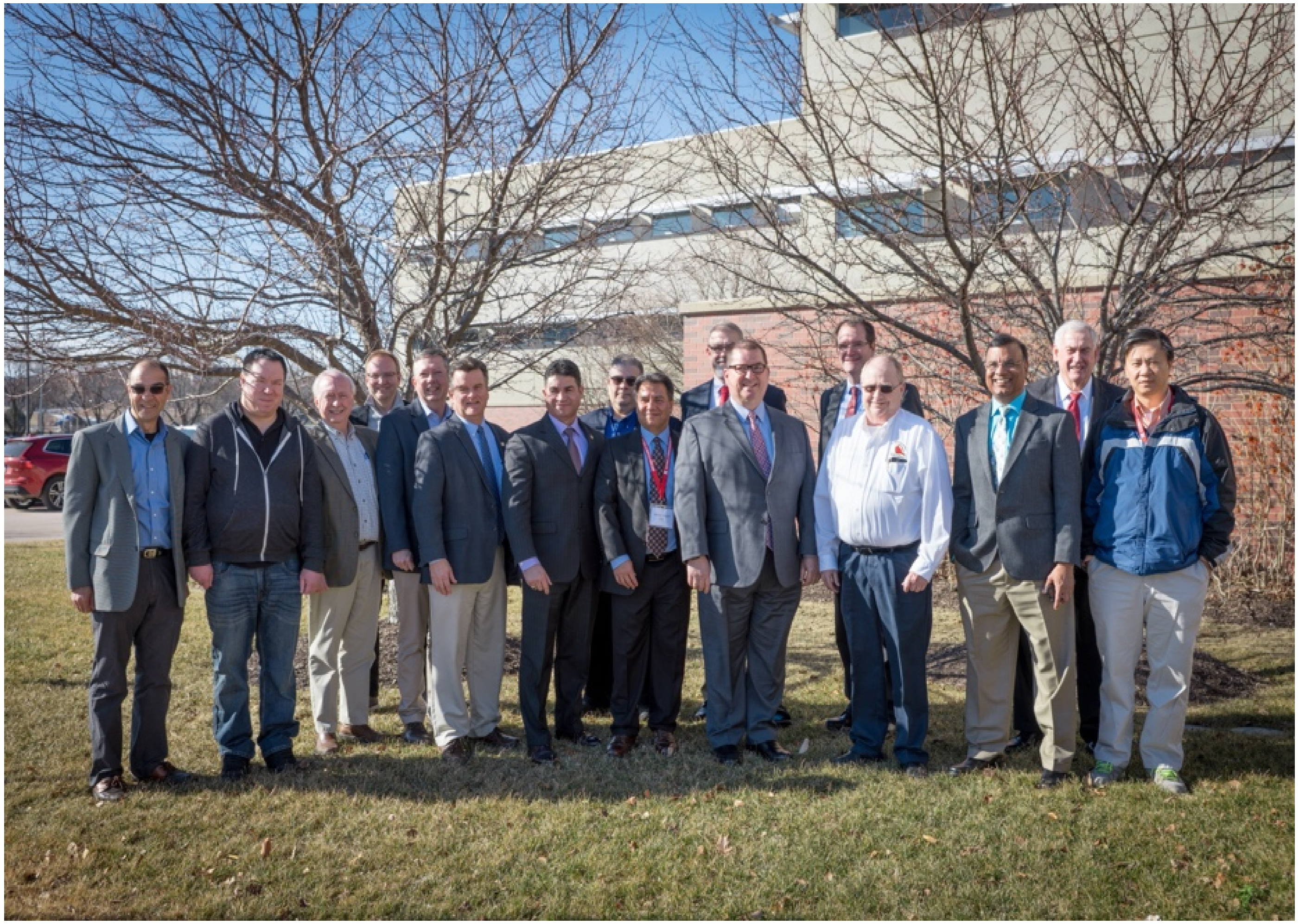
Entrepreneurs
(NSRI, NuTech Ventures)

Users
(South Sioux City, Lincoln Electric System)

Stakeholder Board

- Held workshop meeting in Nebraska (Feb 2020)
- Power utility partner institutions: OPPD, NPPD, LES, SSC, NSRI

- Director Security & Information Protection, OPPD
- VP Customer & Corporate Services, NPPD
- VP Technology Services, Chief Technology Officer, LES
- City Administrator, SSC
- Executive Director, NSRI
- Director, STRATCOM Mission Systems, NSRI
- Vice Chancellor for Research & Economic Development, UNL
- Associate Dean of Research, Engineering, UNL

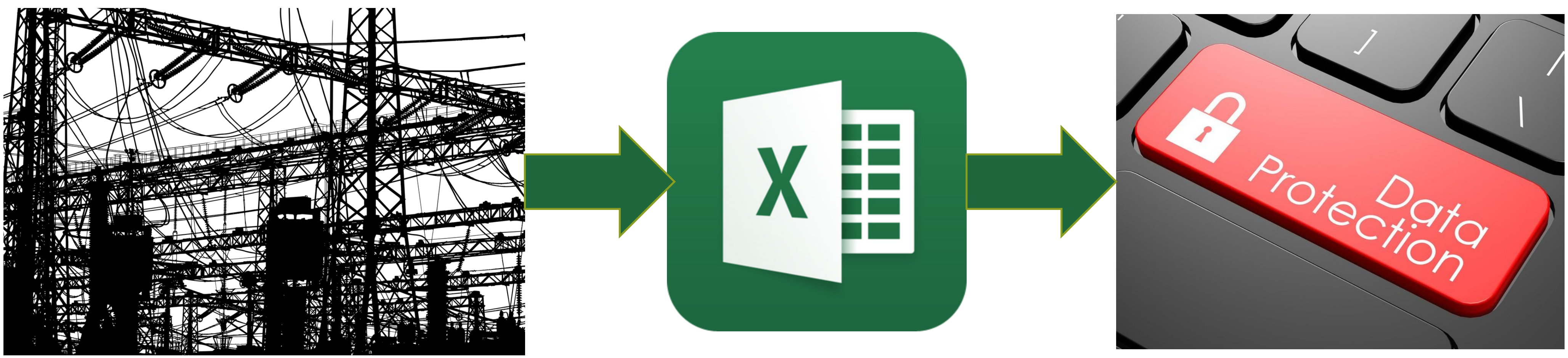


U.S. DEPARTMENT OF ENERGY | OFFICE OF Cybersecurity, Energy Security, and Emergency Response

Challenges to Success (continued)

Challenge 2

- Obtaining cooperation from stakeholders to identify relevant asset types and configurations.
  - Typically regarded as competition-sensitive information.
- Solution:
  - Obtained asset inventory.
  - Built on previously established trusted partner relationships.
  - Articulated mutual benefit from partnerships.
  - Implemented OUO safeguards (transmission, storage, access, processing).

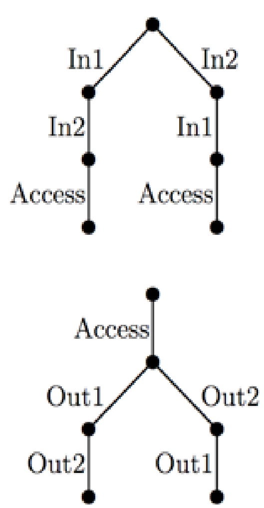


Challenges to Success (continued)

Challenge 3

- Integration of technical specifications to executable runtime on hardware components.
  - How can the information ingested from NLP-based extraction be (semi-)automatically converted into executable and testable script?
- Solution:
  - Generate machine readable statements.
  - Explore formal specification frameworks.
  - Candidates include Estelle, LOTOS and SDL that have been successfully applied to telecommunication protocol specifications previously.

```
  (
    In1; Access; stop
  |[Access]|
    In2; Access; stop
  )
|[Access]|
  (
    Access; Out1; stop
  |[Access]|
    Access; Out2; stop
  )
```



Challenges to Success (continued)

Challenge 4

- Operation under COVID restrictions:
  - How to adapt research and development for distributed, work-from-home, asynchronous operation?
- Solution:
  - Periodic video calls.
  - Partial hardware testbeds replicated at homes.
  - Transitioning partial testbeds to the lab with social distancing.
    - Only parts of team co-located in lab at any given time.
  - Virtual conferences to publish and present findings to the community:
    - IEEE KPEC KSU 2020
    - ACI ICCWS 2021

Collaboration/Sector Adoption

Plans to transfer technology/knowledge to end user.

- Targeted end-users:
  1. Vendors of operational technology equipment.
  2. Asset owners such as grid utility companies.
- What are your plans to gain industry acceptance?
  1. Socialize through the commercialization partners on our team.
  2. Closely maintain relevance to utility grid stakeholders and partners.
- Planned testing and demonstrations:
  1. Field site testing at a to-be-determined location of utility companies:
     - Field site prep – early year 3
     - Field testing – mid year 3
     - Field refinement – end of year 3
  2. Final demonstration to be videotaped for commercialization and adoption purposes.

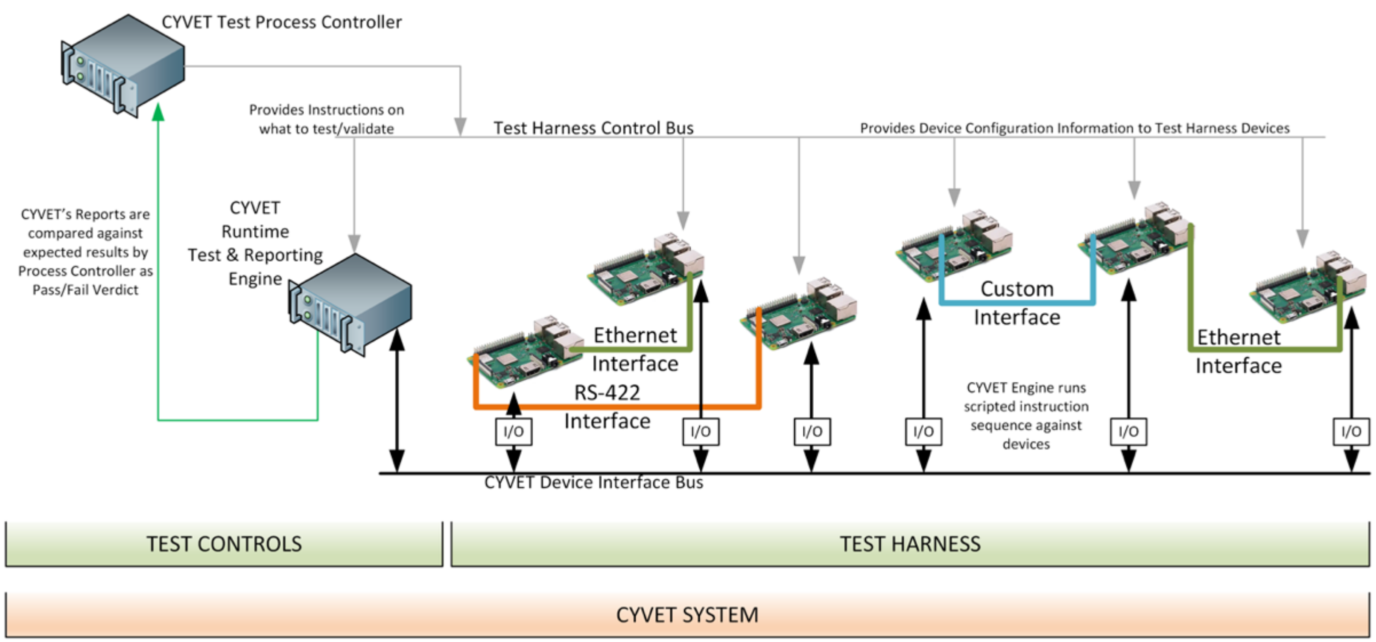
NSRI
NATIONAL STRATEGIC RESEARCH INSTITUTE at the University of Nebraska

your energy partner®
OPPD
Omaha Public Power District

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

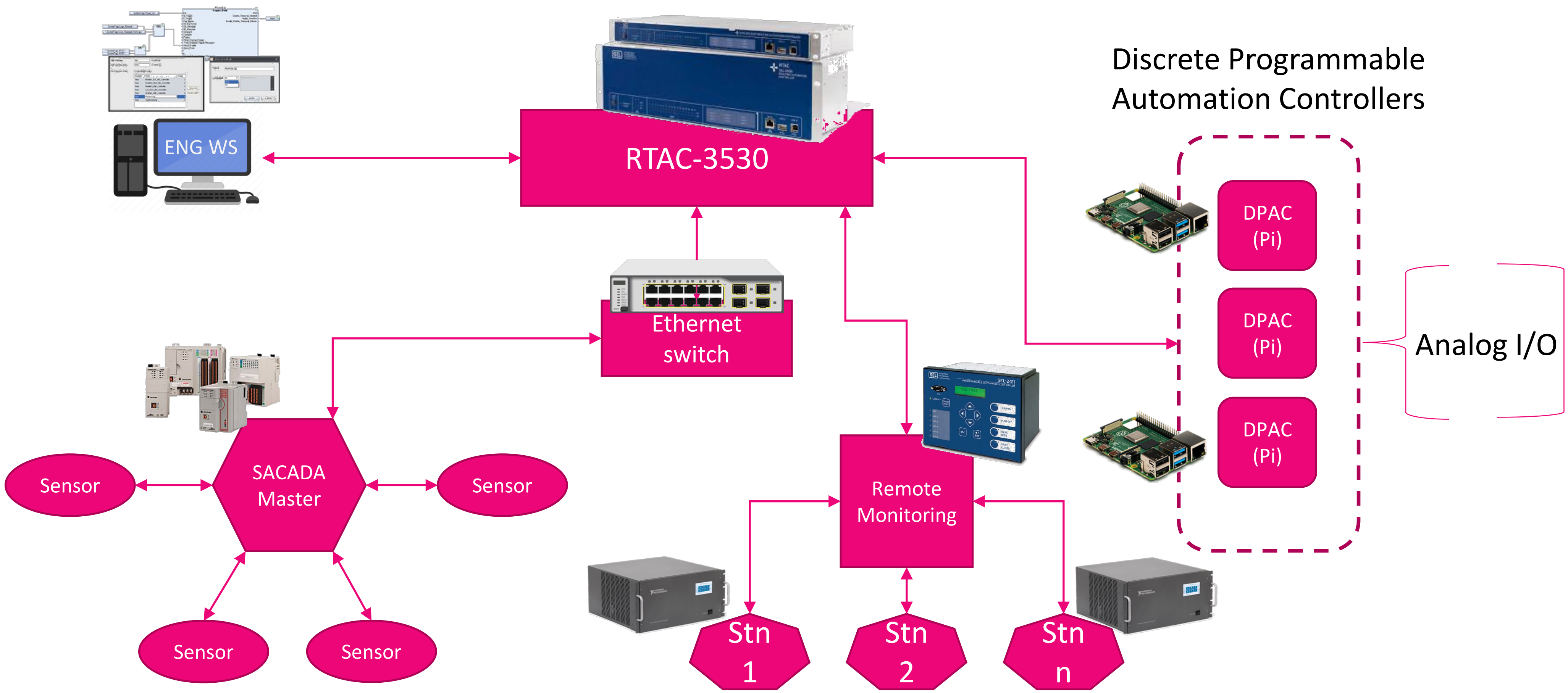
Next Steps for this Project

Research & Development			Demonstration			
Tally-Vet ✓	Test-Vet ✓	Prototype	Field Site Prep.	Field Testing	Field Refinement	Deploy- Strategy Design



Next Steps for this Project (continued)

Hardware Testbed Architecture



Progress to Date

Major Accomplishments

- Double-blind reviewed publication published in the IEEE Kansas Power and Energy Conference 20: K. Perumalla, J. Lopez, M. Alam, O. Kotevska, M. Hempel, and H. Sharif, "CYVET: A Novel Vetting Approach to Cybersecurity Verification in Energy Grid Systems".
- Submitted publication to the ACI International Conference on Cyber Warfare and Security'21: K. Ameri, M. Hempel, H. Sharif, J. Lopez, K. Perumalla, "Smart Semi-Supervised Accumulation of Large Repositories for Industrial Control Systems Device Information".
- Submitted publication to the ACI International Conference on Cyber Warfare and Security'21: S. Sintowski, J. Asiamah, J. Lopez, R. Borges-Hink, "Resilience Analysis of Real-time Automation Controllers (RTAC) under Cyber Stress".
- DOE SULI intern in this project selected as semi-finalist among all ORNL interns for summer 2020, for the poster "Analysis of Cybersecurity Embedded Features in Energy Control System Components".
- Obtained initial cyber-physical asset inventory of power industry partners.
- Down-selected devices from the asset inventory to two specific devices of interest for proof-of-concept research and development (Rio and SEL).
- Initial hardware test-bed established with 3 RTACs, 4 Raspberry Pis, network switches, sensor emulators, packet capture device.
- Repository initialized of cyber-physical device user manuals, installation guides; scripts for incremental web scraping and classification of vendor supplied feature documents.