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

CREDC
Univ. of Illinois at Urbana-Champaign

Prof. David Nicol
University of Illinois at Urbana-Champaign

Cybersecurity for Energy Delivery Systems (CEDS) Peer Review

October 6-7, 2020

Project Overview

Objective

- Identify and perform cutting edge research and development whose results are actually used to increase cyber-resiliency of energy delivery systems.
- Supporting Objectives
  - Help management find rationale for EDS cyber-resiliency investment
  - Identify impediments and find highest impact adoptable solutions
  - Develop, validate, and verify high impact solutions, with industry
  - Make solutions available
  - Develop model of operation that is ultimately self-supporting

Schedule

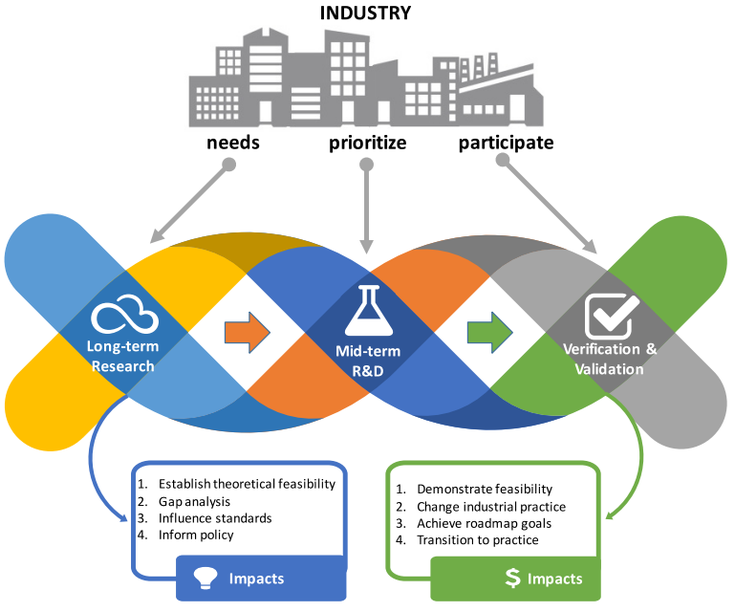
- Period of performance: Sep. 1, 2015 to Sep. 30, 2020
- No-cost time extension (NCTE) through May 31, 2022
- Project-level milestones and deliverables have been met.

Total Value of Award:	**$ 28M, $22.5 Federal**
Funds Expended to Date:	**81%**
Performer:	**University of Illinois at Urbana-Champaign**
Partners:	**See Below**

CYBER RESILIENT ENERGY DELIVERY CONSORTIUM

Consortium of universities, national labs, and industrial partners committed to:

- Identifying gaps in the existing cyber infrastructure for energy delivery with respect to enhancing EDS resiliency
- Identifying trends in emerging technologies that may impact resiliency
- Performing long-term and mid-term research to close gaps, with mid-term research leading to validated solution prototypes
- Developing software infrastructure for empirical evaluation on hardware testbeds
- Developing educational and out-research activities



For more information please visit http://cred-c.org/

Builds on the strong successes of TCIPG

5 Year, $28M project funded by DOE ($22.5M Federal plus cost-share)

CREDC Partner Institutions

CYBER RESILIENT ENERGY DELIVERY CONSORTIUM

- **University of Illinois (lead)**
- Arizona State U.
- Dartmouth
- MIT
- Oregon State U.
- Rutgers
- Tennessee State U.
- U. of Houston
- Washington State U.
- Old Dominion University
- University of South Florida
- ANL
- PNNL

For more information please visit http://cred-c.org/

Historical demonstration of value to Industry

Open Phasor Gateway

Entergy THE POWER OF PEOPLE

EPRI ELECTRIC POWER RESEARCH INSTITUTE

GRID PROTECTION ALLIANCE

ACS Intrusion Mitigation Agent

APPLIED COMMUNICATION SCIENCES

DTE Energy

EPRI ELECTRIC POWER RESEARCH INSTITUTE

Secure Information Exchange Gateway (SIEGate)

GRID PROTECTION ALLIANCE

Pacific Northwest NATIONAL LABORATORY

pjm

ALSTOM

SCADA Role Based Access Control

Honeywell

INL

Policy Based Configuration (PBCONF)

EPRI ELECTRIC POWER RESEARCH INSTITUTE

Ameren

Software Defined Networking

SEL

Ameren

Applied Resiliency for More Trustworthy Grid Operation (ARMORE)

GRID PROTECTION ALLIANCE

Pacific Northwest NATIONAL LABORATORY

Collaborative Defense for T&D Devices Against Attack

ABB

TVA

Cyber-Physical Modeling and Analysis for a Smart and Resilient Grid

PowerWorld CORPORATION

U.S. DEPARTMENT OF ENERGY

OFFICE OF Cybersecurity, Energy Security, and Emergency Response

Advancing the State of the Art (SOA)

- Security of EDS is an increasingly critical concern
  - Destructive cyberattacks against EDS have happened in Ukraine and the Middle East
  - Conventional IT security is adaptable, but only to a degree
  - Computational limitations, bandwidth constraints, time criticality, and emphasis on availability limit what security can be deployed
- CREDC research activities have examined a wide spectrum of EDS cyber resilience, but a common approach has been to "leverage the physics"
- CREDC has also examined interdependencies between, e.g., GPS spoofing and synchronization of wide-area PMU measurements, and developed mitigation
- More broadly, an academic consortium has freedom to look "over the horizon"
- The energy sector benefits by helping us identify important gaps and access to research results (interaction with PI's and students, access to knowledge, and access to reference implementations of key solution concepts)
- This approach benefits the sector by studying important problems and striking a balance of near-term and longer-term solutions

Progress to Date

Major Accomplishments

- Nearly 50 activities since project inception
  - Activities are typically headed by a faculty PI, with a few graduate research assistants, and ideally in close collaboration with an industry partner
- Every year, PI's submit activity proposals
  - Identify an EDS cyber resiliency gap
  - Describe a research plan, with schedule, milestones, and deliverables
  - Proposals are evaluated by the IAB
- As the main part of the project winds down, activity deliverables and milestones have largely been met.
- All top-level (CREDC as a whole) milestones and deliverables have been met
- 8 Activities initiated June 1, 2020 under a no-cost time extension (NCTE)

Challenges to Success in Self-Sufficient Model

Challenge 1: Find a business model that

- Takes advantage of unique contributions of universities
  - Education, access to students, knowledge of cutting edge of research directions
- Incentivizes participation by industry
  - Requires understanding our value proposition to industry
- Incentivizes participation by faculty and students
- Is unique in the space of various organizations industry supports

Challenge 2: Industry Engagement

- Expectations/needs of OEMs and utilities are different
  - Impact on utilities usually requires provisioning of software
  - Commercialization is **hard**
  - Impact on OEM …. IP issues abound

Collaboration/Sector Adoption

Reflection

Industry seems to value academia through

- Expanding knowledge horizon
- Hiring pipeline
- Demonstrating ideas that may (or may not) be worth pursuing
- Technology development and adoption for ideas that work and make business sense
- Training and workforce development

For most, the research we do is valued more as enabling knowledge development and hiring than developing operational technology

- Is industry willing to invest in this, and how?

Training and workforce development is out of scope for CREDC, but is a critical component for self-sufficiency

Collaboration/Sector Adoption

Examples of Collaboration With Major Stakeholders

- Data-driven approach to correct PMU data under GPS spoofing attacks (SEL)
- PMU Data Compression using Graph Signal Processing (OSISoft)
- Ontology-based modeling of EDS threats, coupled to impact assessment (ABB)
- Embedded code agent for IIOT end-device security (Schneider)
- LangSec research into secure language parsers for embedded systems (GE)
- Controller device resilience (Siemens)
- Reliability First is piloting a resiliency self-assessment tool

Collaboration/Sector Adoption

- 65 Attendees
  - Energy industry
  - CREDC researchers
  - Federal, state, local government
  - National labs

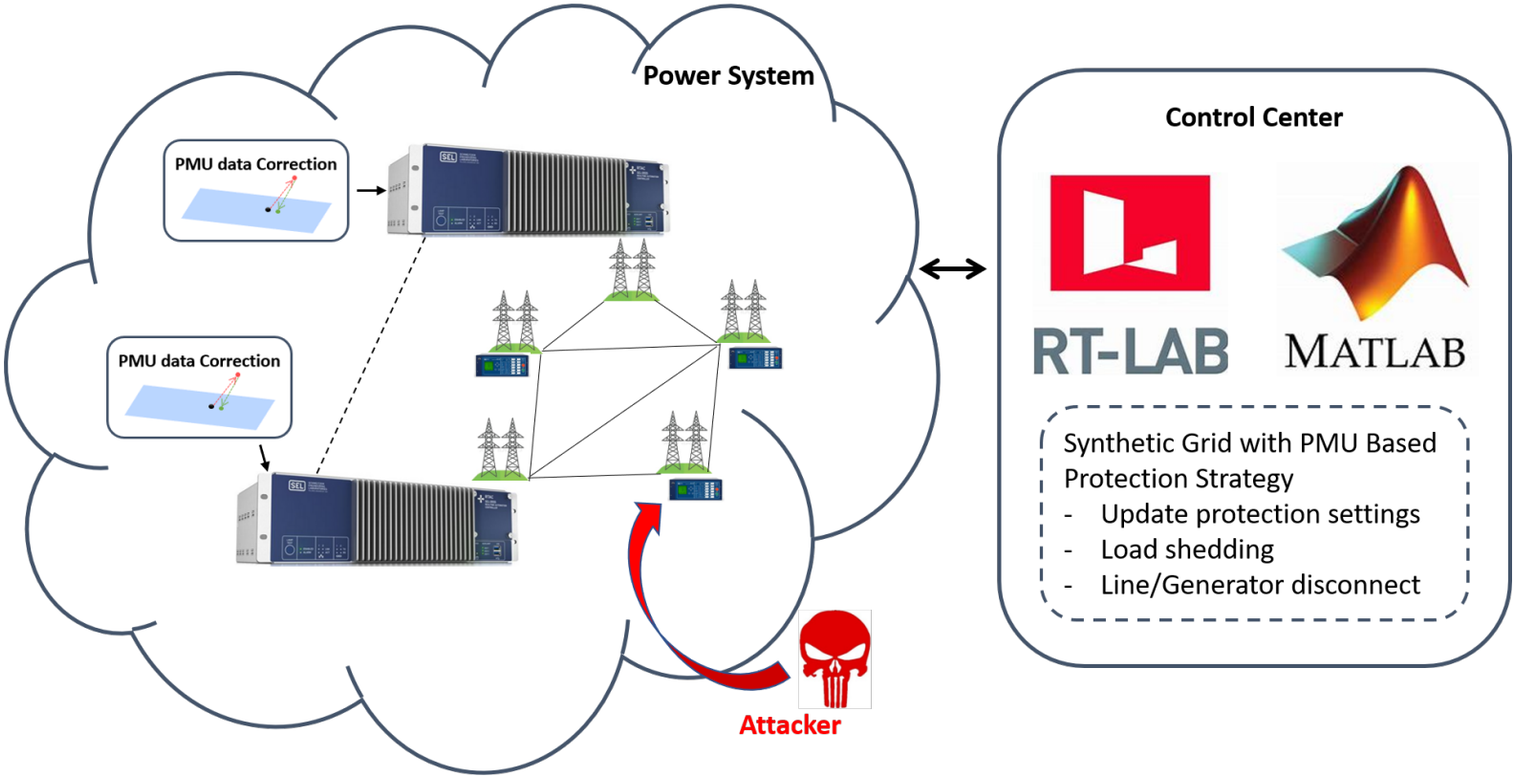
- Topics included:
  - IIOT security
  - Supply chain security
  - Legislative and regulatory cyber landscape
  - Accelerating tech to industry applications
  - What's next?

Next Steps for this Project

Approach for the next year or to the end of project

- CREDC has completed its initial period of performance
- Eight new activities were initiated in June 2020 as a no-cost time extension
- NCTE runs through May 31, 2022

Attack Resilient Data Analytics for Power Grid Operations (OSU)

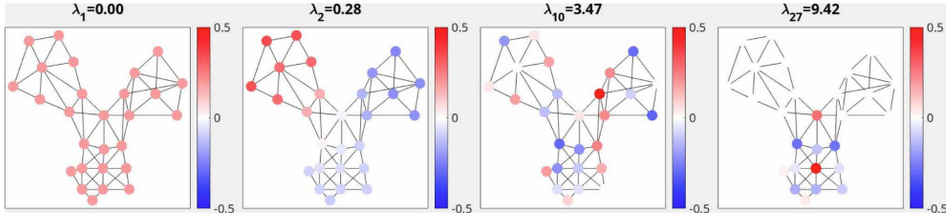


- Objective: Defend PMU-based protection and control schemes against PMU data falsification attacks such as GPS spoofing attacks.
- Achievements: Distributed scalable data correction algorithm that can be implemented at local PMU data aggregators for real time data correction
- Technology transition: In collaboration with SEL, we will implement RTAC codes and disseminate them for public use.
- Industrial advocate: SEL

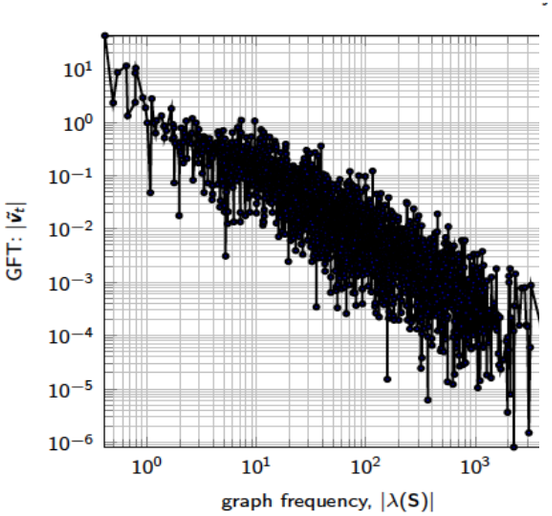
Grid Graph Signal Processing (ASU)

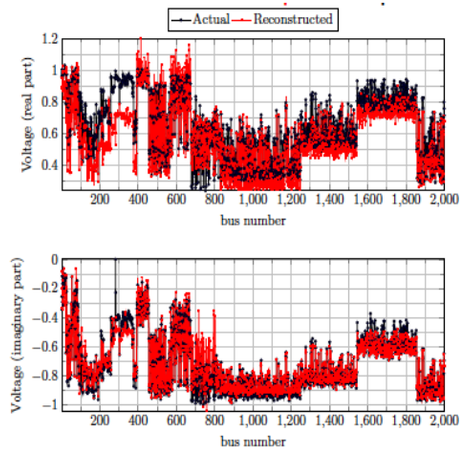
- Machine learning for time series and images rely on **filters and Fourier analysis** heavily **to extract informative features from data.**
- Graph Signal Processing (GSP) extends the notion of **filter** and **Fourier analysis** to signals that have support on a graph.
- Project applied GSP to voltage phasors
- The model shows that voltage phasors are a low-pass graph signal, which explains properties of the signal.
- Extends ability to perform data analytics
- The example in the figures shows results pertaining
  - The reconstruction of missing measurements
  - The inference of the underlying network
  - The detection of anomalies that can be indications of false data injection attacks

- **Industry interactions:**
- OSIsoft, Siemens, Cordova Electric (a co-op)

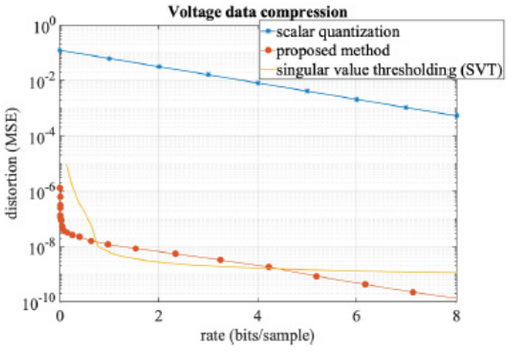


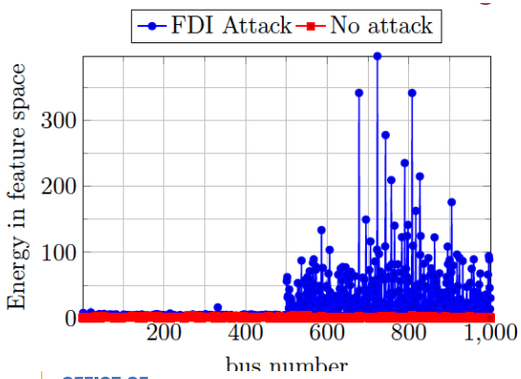
Graph frequency components (**λ** is the frequency)





Voltage reconstruction with 5% measurements, $K = 100$.

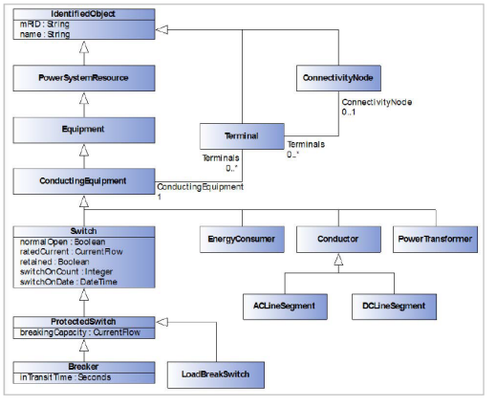


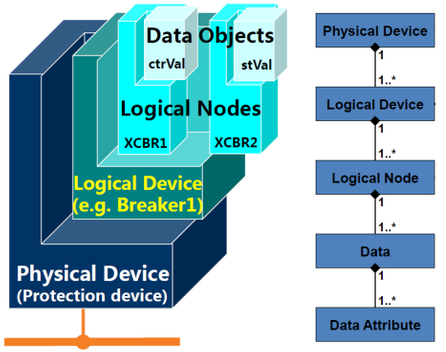


Reliability and Cyber-Physical Threat Model Generation from a Standards Influenced Ontology (UIUC)

Objectives

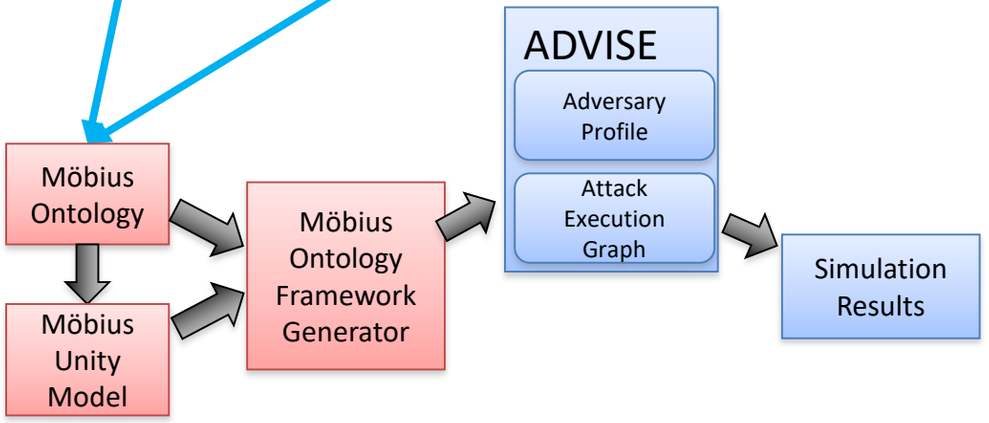
- Develop discrete-event stochastic model generation ontologies to study
  - Traditional Reliability
  - Cyber-Physical Threats
  - Interplay Between The Two
- Integrate machine-in-the-loop simulation (e.g., OPAL-RT) with Discrete-Event Simulation models
- Transition model generation tool and ontologies to industry partners
- A variant of ontology-based threat modeling has transitioned to a UIUC-ABB collaboration
- Industrial interest by ABB





Common Information Model Primer, EPRI 2015 Technical Report

seclab.illinois.edu/wp-content/uploads/2011/03/iec61850-intro.pdf



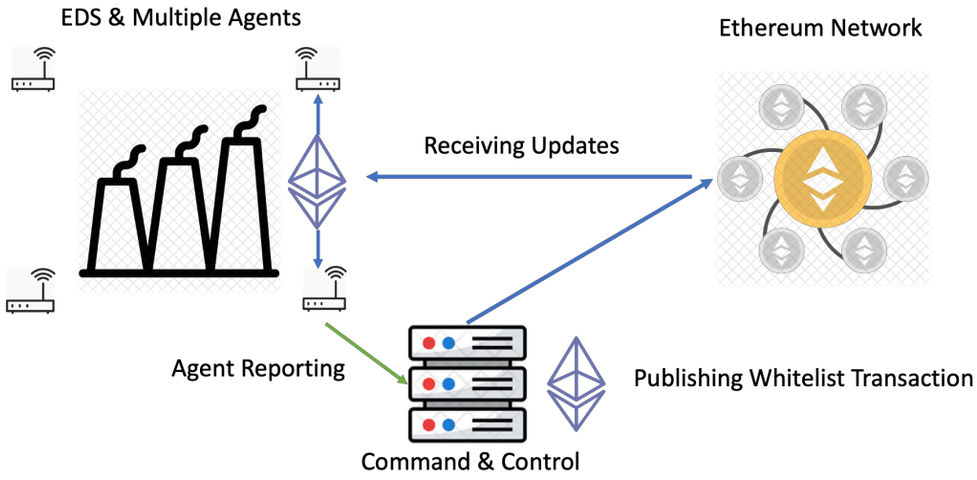
U.S. DEPARTMENT OF ENERGY | OFFICE OF Cybersecurity, Energy Security, and Emergency Response

Defeating IIoT Device Hackers (MIT)

Software tools to secure distributed Energy Delivery Systems

- Developed a *light-client* for the blockchain protocol, designed to be run on IoT/IIoT (memory/compute constrained) devices
- *Light-client* is a secure communication protocol for distributing device updates
- Built several prototypes (~1mb in size on Github) on several different chip architectures and operating systems
  - Security Agent for locking down devices using whitelists
  - Secure update agents for device **firmware / patching**
  - Utilize light-client for receiving updates and C & C
- Established baseline application to cloud-virtualized environment

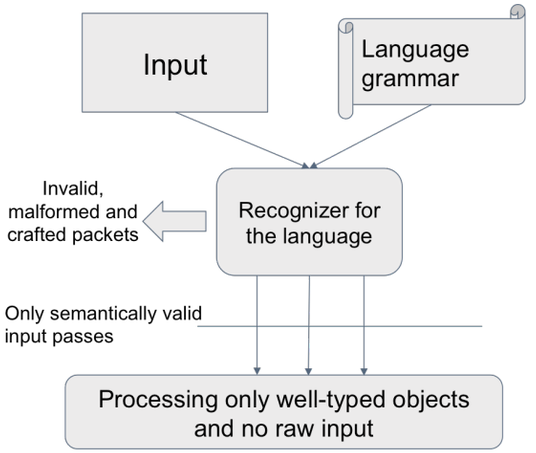
Solution Diagram



Industrial Collaboration: Schneider Electric, Exxon Mobil, Engie, Cisco

Language-Based Security (LangSec)-Dartmouth

- *Problem: Endemic 0-days via Crafted Input*
- *Solution: LangSec*
  1. Define a grammar that represents a "secure subset" of the protocol.
     - No more than context-free!
     - ...or maybe PEG
  2. Build a parser that accepts *only* this grammar.
     - Via invocations to parser combinators
     - Invocations match the grammar!
- *And we're standardizing toolkits to make this easy for any ICS developer!*



Current LangSec parsers include:	● DNP3 ● C37.118	● IEC 61850 ● GOOSE	● MMS ● HTTP HMI

Dartmouth LangSec research portfolio:

DOE CREDC (sub to UIUC)	***software*** interfaces for ICS in energy (with GE, and others)
DARPA RADICS (sub to SRI)	***software*** detection of malicious packets in power grid networks
ONR Secure Popcorn Linux (sub to VaTech)	***software*** function calls, message passing in dist sys
DARPA SAFEDOCS (sub to SRI)	***software*** parsing of PDF
DARPA GAPS (sub to GE)	***hardware and software*** on connections between security domains

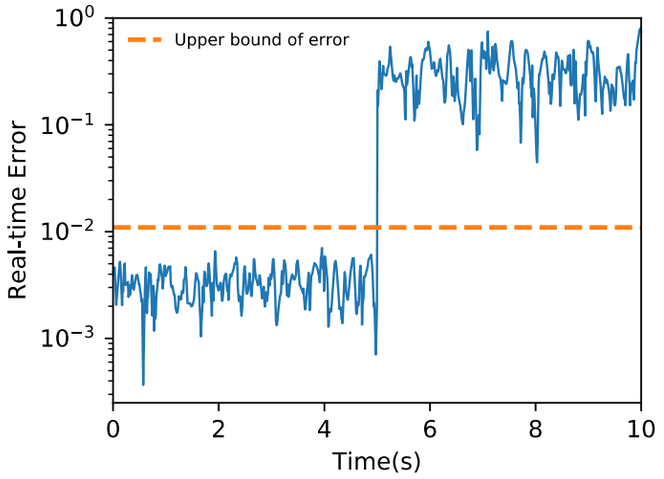
Industrial collaborator: GE

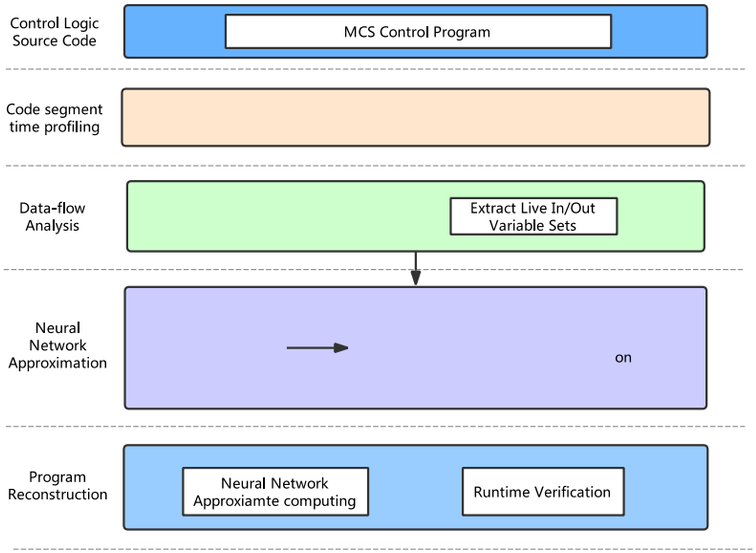
Controller Device Resilience Metrics (Rutgers)

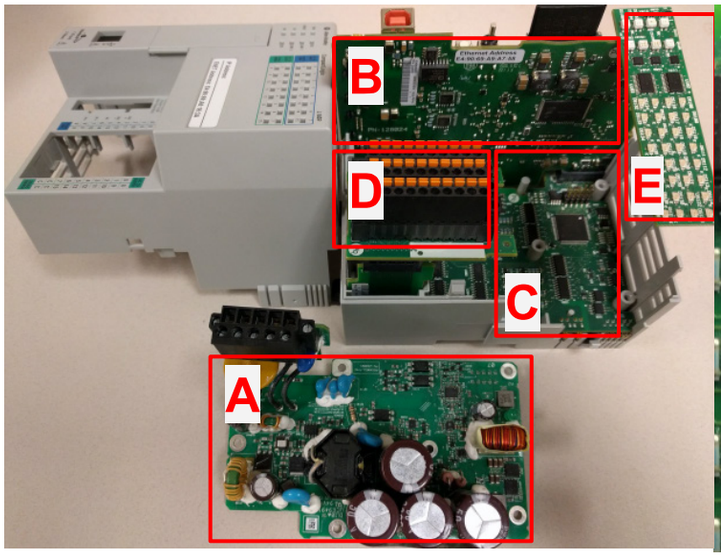
PLC code analysis

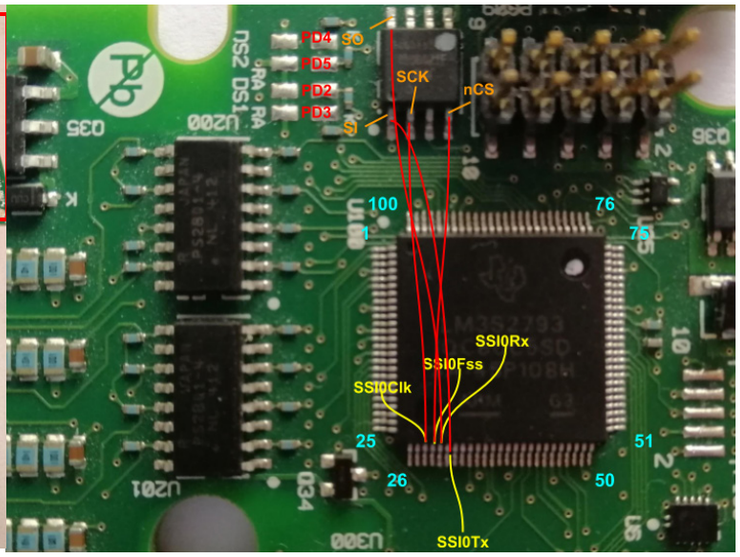
- Hierarchical decomposition extracting control flow, timing profile, and liveness.
- Neural network training on correct behavior
- Embedded NN based checking into PLC code for run-time verification

Industrial collaborator: Siemans



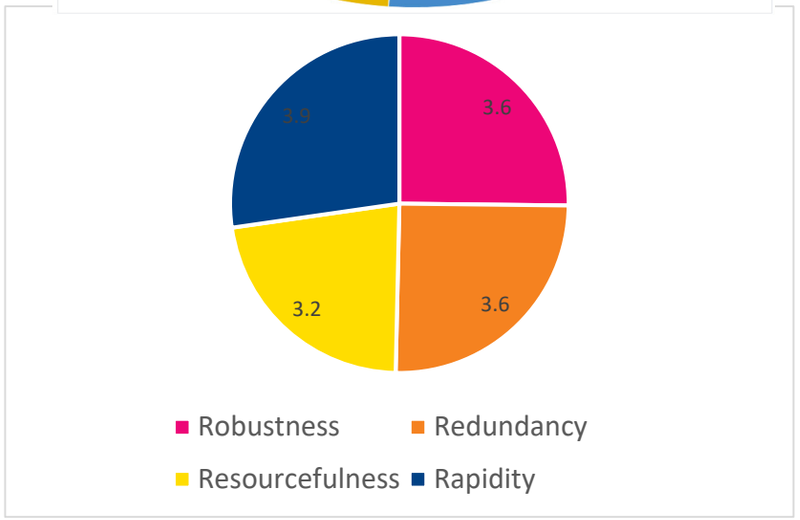


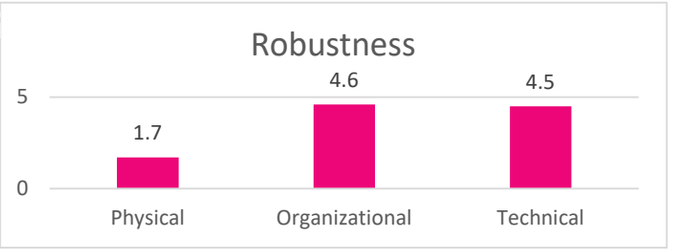


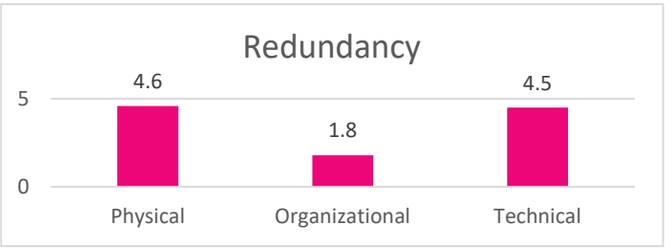


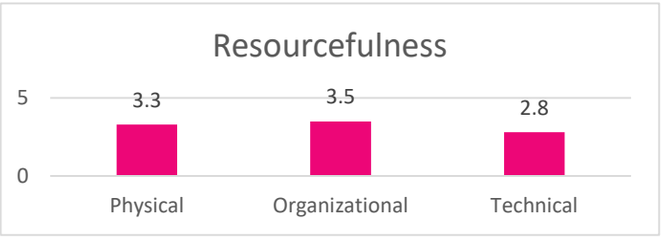
Resiliency Self—Assessment Tool (ODU)

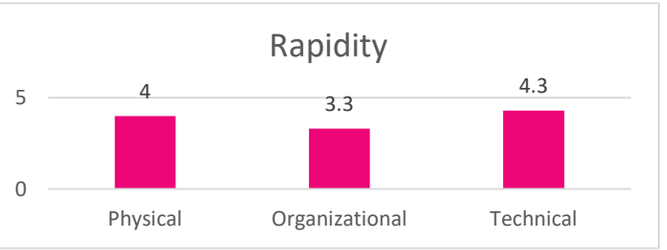
- **In use as a pilot by Reliability First**
- **Utilities self-evaluate on dimensions of Robustnes Redundancy, Resourcefulness, and Rapidity**











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