U.S. DEPARTMENT OF ENERGY

OFFICE OF Cybersecurity, Energy Security, and Emergency Response

Cyber-Physical Protection for Natural Gas Compression

DE-OE0000903

GE Research

Matthew Nielsen

Cybersecurity for Energy Delivery Systems (CEDS) Peer Review

October 6-7, 2020

Project Overview

Objective

- ~1400 natural gas pipeline compression stations in US*.
- A new cyber-physical protection focused on prime mover, controls, & compressor.
- Deployed at the edge providing near real time asset protection and situational awareness.

Schedule

- Oct 1, 2018 – March 31, 2021.

Phase 1 Milestone/Deliverable	Status
Attack surface defined	complete
High fidelity digital twin simulator established	complete
Algorithms validated	complete
Secure I/O prototype produced	complete
Edge advancements completed	complete
CPP prototype delivered to INL	complete
Red team testing completed	complete

Total Value of Award: $3,890,126

Funds Expended to Date: 81%

Performer: GE Research

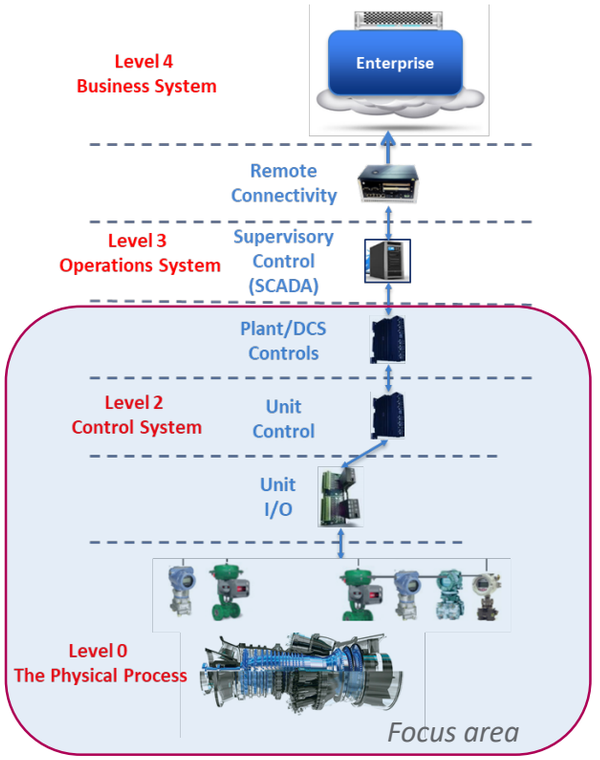
Partners: Baker Hughes
Idaho National Lab

*https://www.eia.gov/naturalgas/archive/analysis_publications/ngpipeline/index.html

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

Advancing the State of the Art (SOA)

- Describe current "state of the art".
  - OT Cybersecurity anomaly monitoring: network communications including packets/devices,
  - Machine learning: learning normal network traffic models.
- Describe the feasibility of your approach.
  - Assumes sophisticated adversary has obtained access and launches attacks to manipulate asset behavior.
  - Implements three core components:
    - ***Detection***: monitors for anomalous behavior.
    - ***Localization***: determines manipulated nodes.
    - ***Neutralization***: provides resiliency for potential of continued operation.
  - Combines Physics + ML + Controls.
  - Uses Digital Twin of asset to train algorithms.
  - Deploys solution at edge for near real-time operation.
- Describe how your approach is better than the SOA.
  - Adds cybersecurity to lower layers of Purdue ref model.
  - Provides fast detection & localization speeds: 10 msec.
  - Offers resiliency while attack is active.



Advancing the State of the Art (SOA)

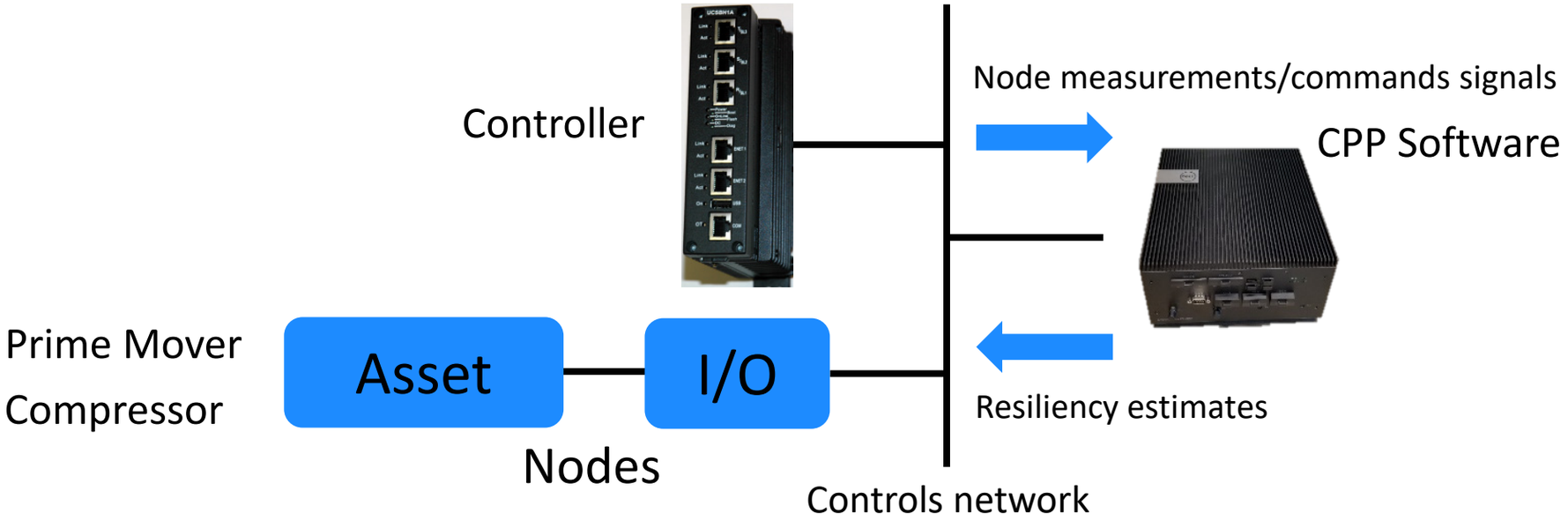
- Describe how the end user of your approach will benefit.
  - Increased situational awareness: cyber and faults [added return on investment].
  - Improved rapid detection, localization and resiliency (neutralization).
- Describe how your approach will advance the cybersecurity of energy delivery systems.
  - Adds new layer of security and situation awareness based upon asset behavior.
  - Provides model adaptation to accommodate natural machine performance degradation.
  - Enhances resiliency performance to cover > 50% of attacked nodes even during non-linear operation.
- Describe the potential for sector adoption.
  - Potential to be integrated with Baker Hughes cybersecurity solutions*.
  - Does not require “rip-n-replace” of current controls or OT systems.
  - Synergistic with existing OT cybersecurity systems.

*https://www.bakerhughesds.com/nexus-controls/industrial-cybersecurity/nexus-otarmor-cybersecurity-solution

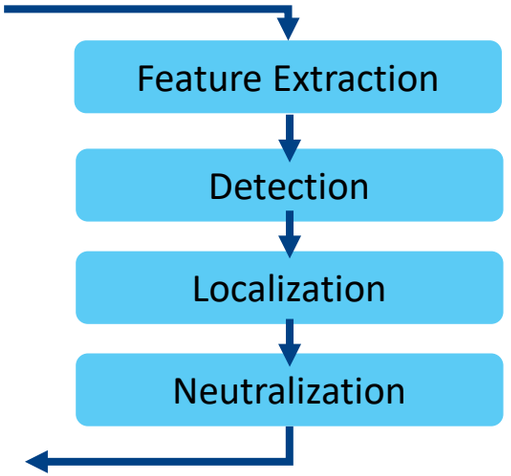
CPP Architecture

Protecting prime mover + compressor

How is it connected?



What is it doing?

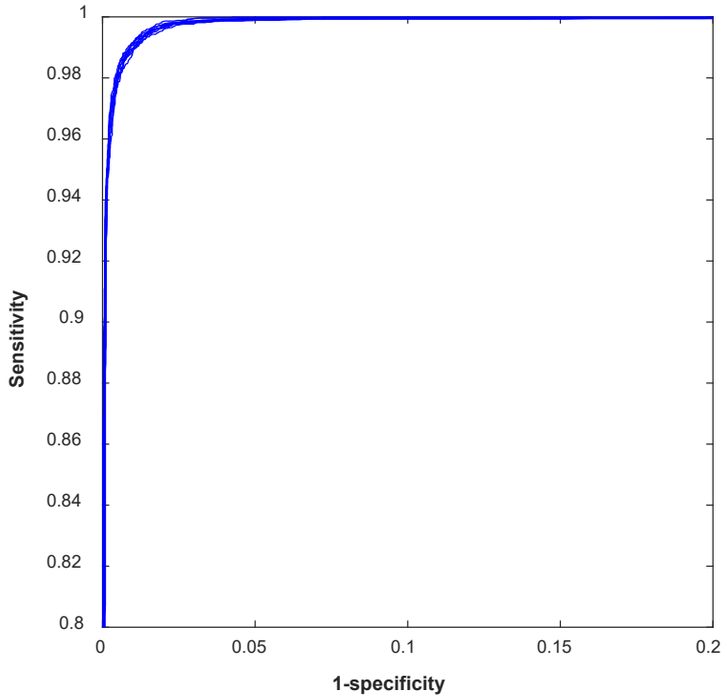


Detection Results

Attack detection development strategy

- Transform monitoring nodes measurements (multivariate time-series) to features via feature extraction and transformation.
- Perform feature-based attack detection using ensemble-based anomaly detection.
- Validate attack detection on dataset from independent simulation runs.

Attack detection performance summary*



Confusion matrix of 10-fold cross-validation on training dataset

		Predicted	
		Normal	Attack
True	Normal	**99.00%**	1.00%
	Attack	1.95%	**98.05%**

TPR = 98.05%
FPR = 1.00%

Confusion matrix on validation set

		Predicted	
		Normal	Attack
True	Normal	**99.37%**	0.63%
	Attack	7.20%	**92.80%**

TPR = 92.80%
FPR = 0.63%

Achieving High 98% Detection TPR at 1% FPR

Results based upon simulated normal and attack conditions on gas turbine and compressor

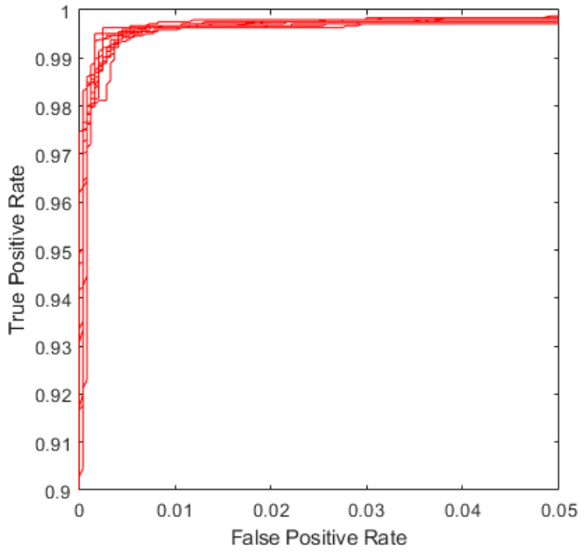
Localization Results

Attack localization development strategy

- Leverages features from detection module.
- Each node assigned to a subsystem.
- Performs anomaly monitoring at subsystem level -> determines which subsystem is being manipulated.

Attack localization performance summary*

Subsystem 1.0 ROC curves 10-fold cross-validation



Subsystem Localization Results

Subsystem	Number of Nodes	Number of Attack Factors	Localization True Positive Rate at 1% False Positive Rate
1.0	7	3	99.7%
2.0	4	1	100%
3.0	16	6	99.8%
3.1	7	3	100%
3.2	9	3	99.3%
4.0	4	1	100%

Achieving High 90's% Localization Accuracy for Subsystems at 1% FPR

Results based upon simulated normal and attack conditions on gas turbine and compressor

Challenges to Success

Project Specific

Challenge 1

- Demonstration approval delayed due to Covid related issues → continue engaging with compressor station owner; explore other options, such as historical data experiments.

Challenge 2

- Complex transient behavior of prime mover could cause lower TPR at desired 2% FPR → obtain historical site data to find actual operating modes and ranges of operation.

General Learnings

Challenge 3

- On-line learning leveraged by attacker → ***Invariant learning***: continuous on-line learning, constrained by the physics of the system and robust against learning attack behavior.

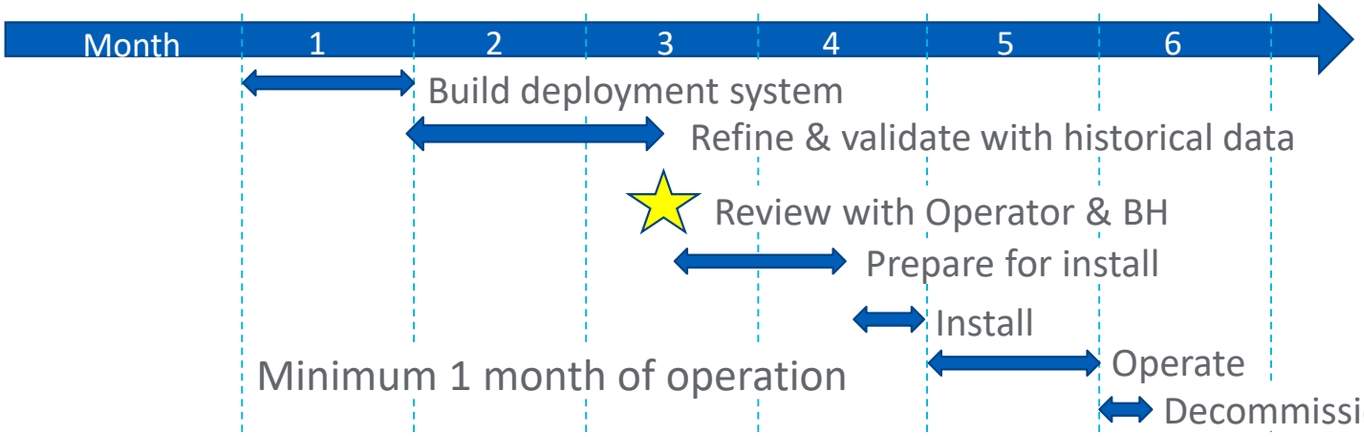
Challenge 4

- Operators don't trust "AI" system → ***Explainable AI***: for adoption, customers need to understand causality (trust the AI).

Collaboration/Sector Adoption

Plans to transfer technology/knowledge to end user

- What category is the targeted end user for the technology or knowledge?
  - Solution provided to the Asset Owner.
  - In discussion with Baker Hughes to incorporate into their cybersecurity solutions.
- What are your plans to gain industry acceptance?
  - Deploy CPP algorithms into near-real time software executable.
  - Install CPP software on Predix Edge OS compute platform.
  - Connect compute platform to controls network of compressor station.
  - Demonstrate at actual compressor station.



Next Steps for this Project

Approach for the next year or to the end of project

- Key Milestones to accomplish
  - Finalize demonstration details with compressor station operator.
  - Submit NEPA forms and obtain DOE approval for Phase 2.
  - Complete demonstration.
    - Preparation and final tuning of algorithms per site specifications.
    - Installation.
    - Data analysis + report.
- Upcoming significant events
  - Key outcomes or measurement criteria expected:
    1. Robustness of software system.
    2. Actual operational data versus simulated data.
       - New operating modes.
       - Unexpected environmental or boundary conditions.
    3. Operator interactions.