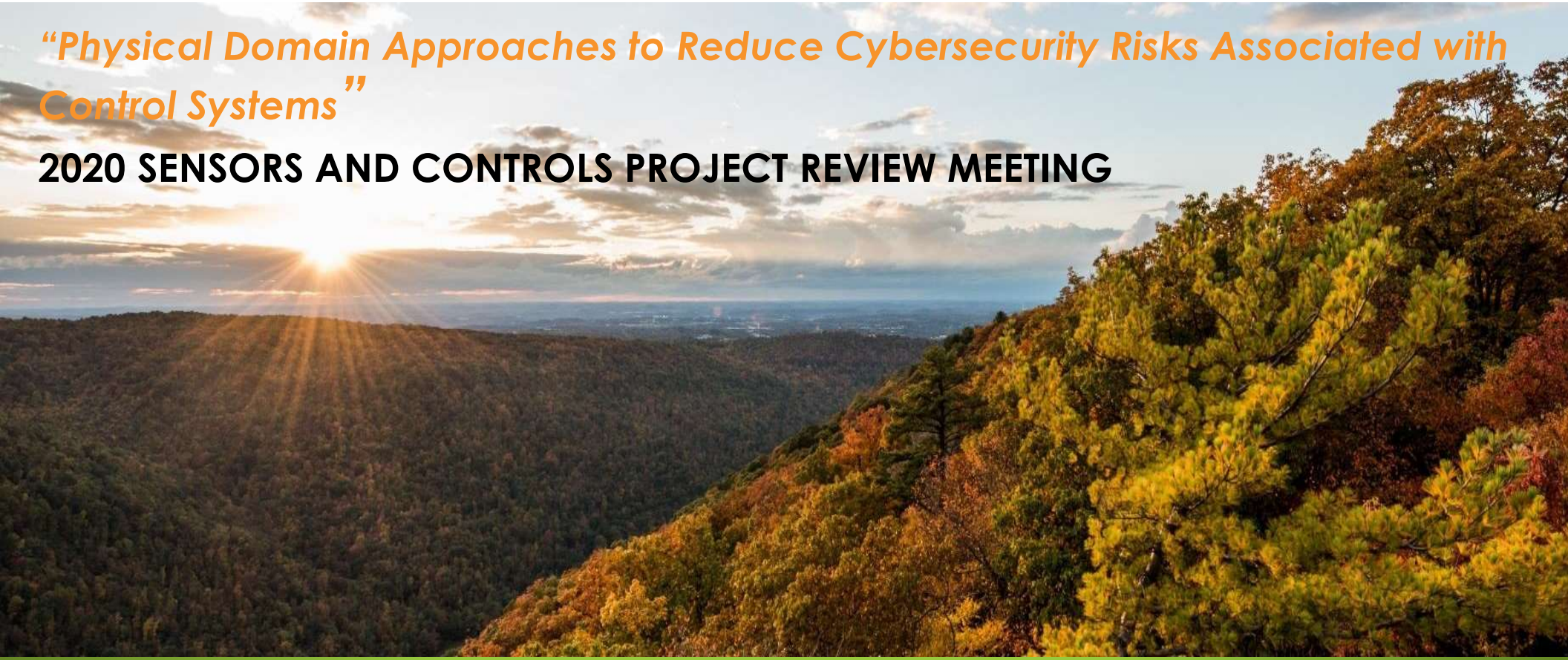
Award DE-FE0031641



"Physical Domain Approaches to Reduce Cybersecurity Risks Associated with Control Systems"

2020 SENSORS AND CONTROLS PROJECT REVIEW MEETING

Program Details

- PHYSICAL DOMAIN APPROACHES TO REDUCE CYBERSECURITY RISKS ASSOCIATED WITH CONTROL SYSTEMS
- Contract: DE-FE0031641
- PROJECT PERIOD: OCT 2018 THROUGH SEPT 2020
- NETL Program Manager: Chuck Miller
- GE Research PI: Daniel Holzhauer
- Key GE Research Team Members: Matt Nielsen , Michael Mylrea

Agenda

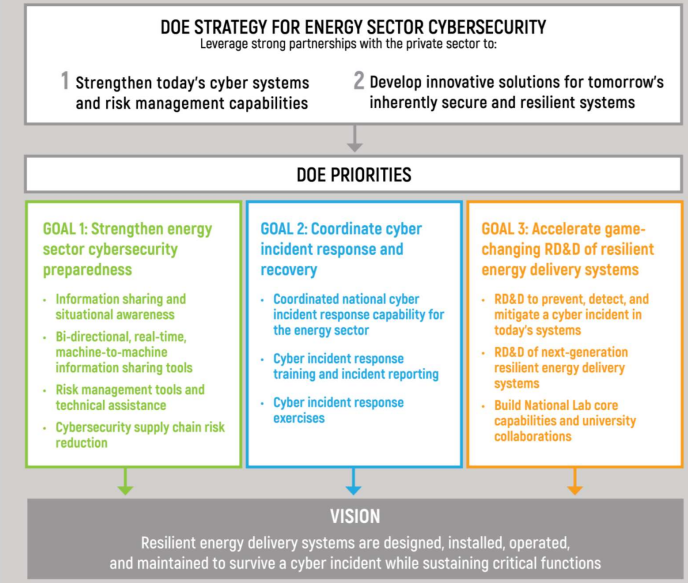
- Project description and objectives
- Program task status
- Work related to cyber resilience
- Cyber physical detection system
- Test demonstration
- Challenges
- Next steps
- Concluding remarks
- Questions

Project Description and Objectives

- **Study current physical domain approaches** potentially applicable to reducing cybersecurity risks associated with the deployment of advanced controls to fossil power generation assets
- Develop survey of **cyber security landscape** affecting control systems of fossil fuel power plants
- Perform list of high-risk threats and faults, identify vulnerabilities, risk factors, and their impacts
- Study **capabilities of existing fault detection and fault-tolerant** control systems
- Evaluate applicability of other DOE funded efforts to fossil power generation context
- Evaluate applicability of **secure communication technology** to cybersecure sensors and controls in combined power plants of the future
- **Identify gaps, develop requirements and recommendations** for advanced monitoring solutions

Project Description and Objectives

- Strategic alignment of project to Fossil Energy objectives
  - Cybersecurity
  - Machine Learning
  - Secure communication
- Project Status now
  - Functional attack detection , localization and neutralization system demonstrated on a real physical asset
    9HA.02 HD GT [CEDS Program DE-OE0000833]
  - Simulation platform of real-time neural network demonstrating fault-cyber classification



Reference: U.S. Department of Energy Office of Electricity Delivery & Energy Reliability. Multiyear Plan for Energy Sector Cybersecurity. March2018.
https://www.energy.gov/sites/prod/files/2018/05/f51/DOE%20Multiyear%20Plan%20for%20Energy%20Sector%20Cybersecurity%20_0.pdf

NETL Program Task Status

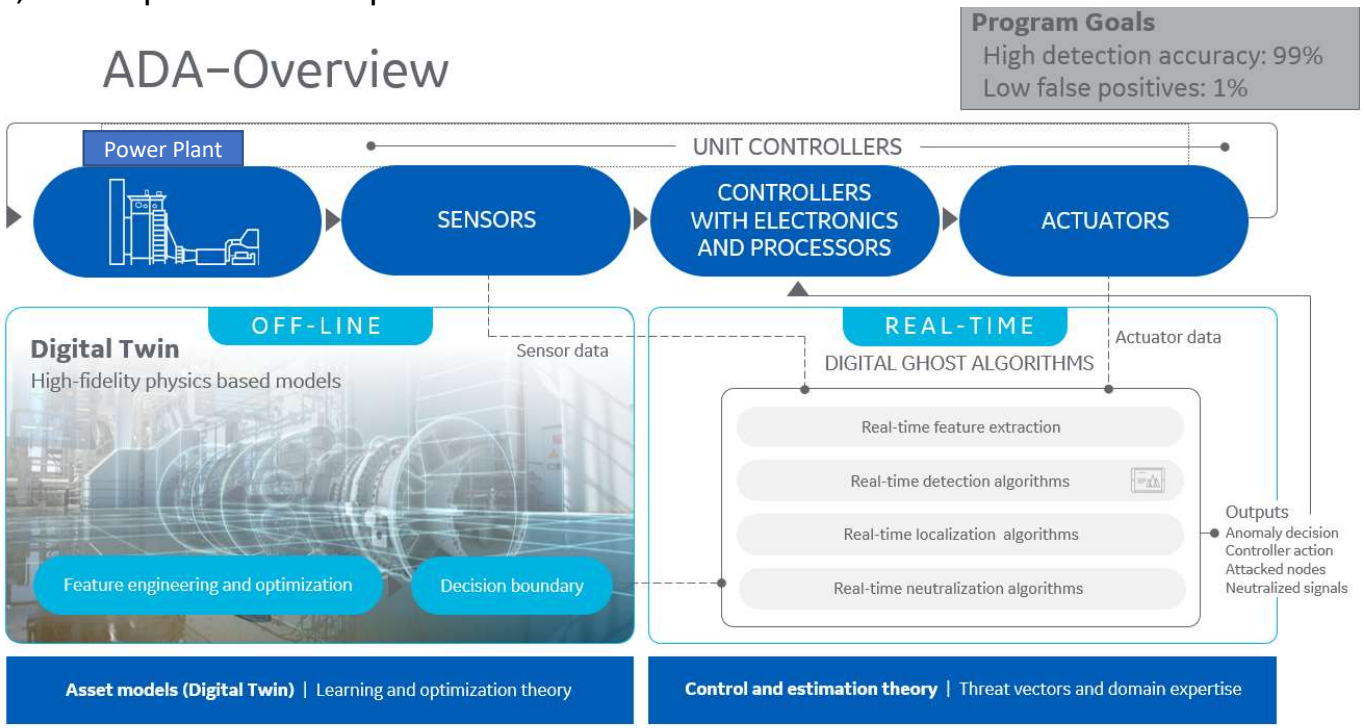
Study current state-of-the-art physical domain approaches

- Develop survey of **cybersecurity landscape** affecting critical cyber assets and control systems of fossil fuel power plants
- Perform list of **high-risk threats** and faults, identify vulnerabilities -list of threats that may affect gas turbines, steam turbines, coal-fired boilers, and clean coal systems, plus balance of plant systems
- Study **capabilities of existing fault detection** and fault-tolerant control systems
- Evaluate applicability of other **DOE funded efforts** to fossil power generation context
- Evaluate applicability of secure communication technology to **cybersecure sensors and controls** in combined power plants of the future
- **Identify gaps**, develop requirements and **recommendations** for advanced monitoring solutions

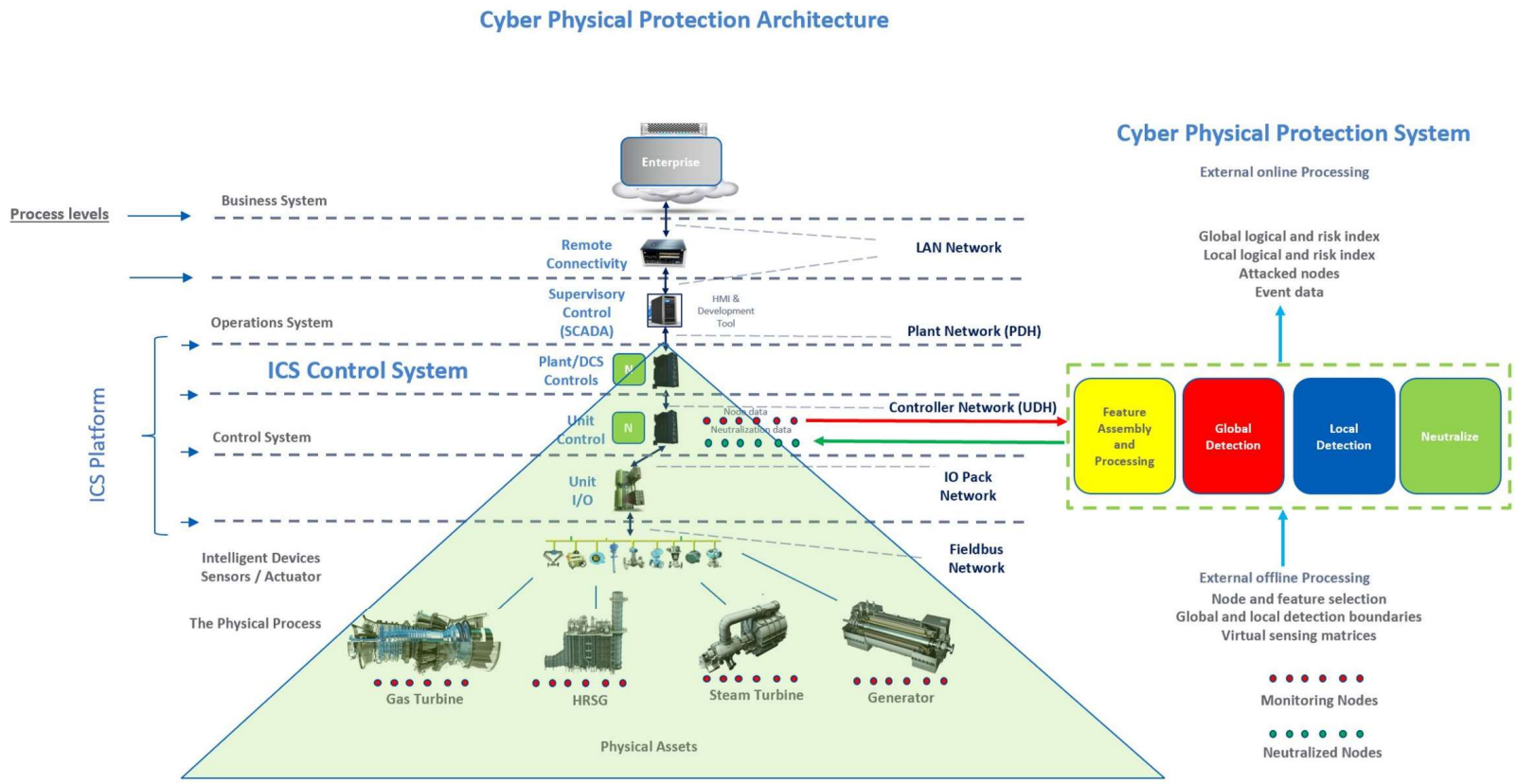
- Complete

GE Work Related to Cyber Resilience

Cyber Resilience is part of GE's Culture and DNA - With over a third of the world's power and a large percentage of operational technology in critical energy infrastructure, GE has distilled these unique data sets, into transformative cyber intelligence supporting next gen advanced threat detection, mitigation and recovery research, development and implementation



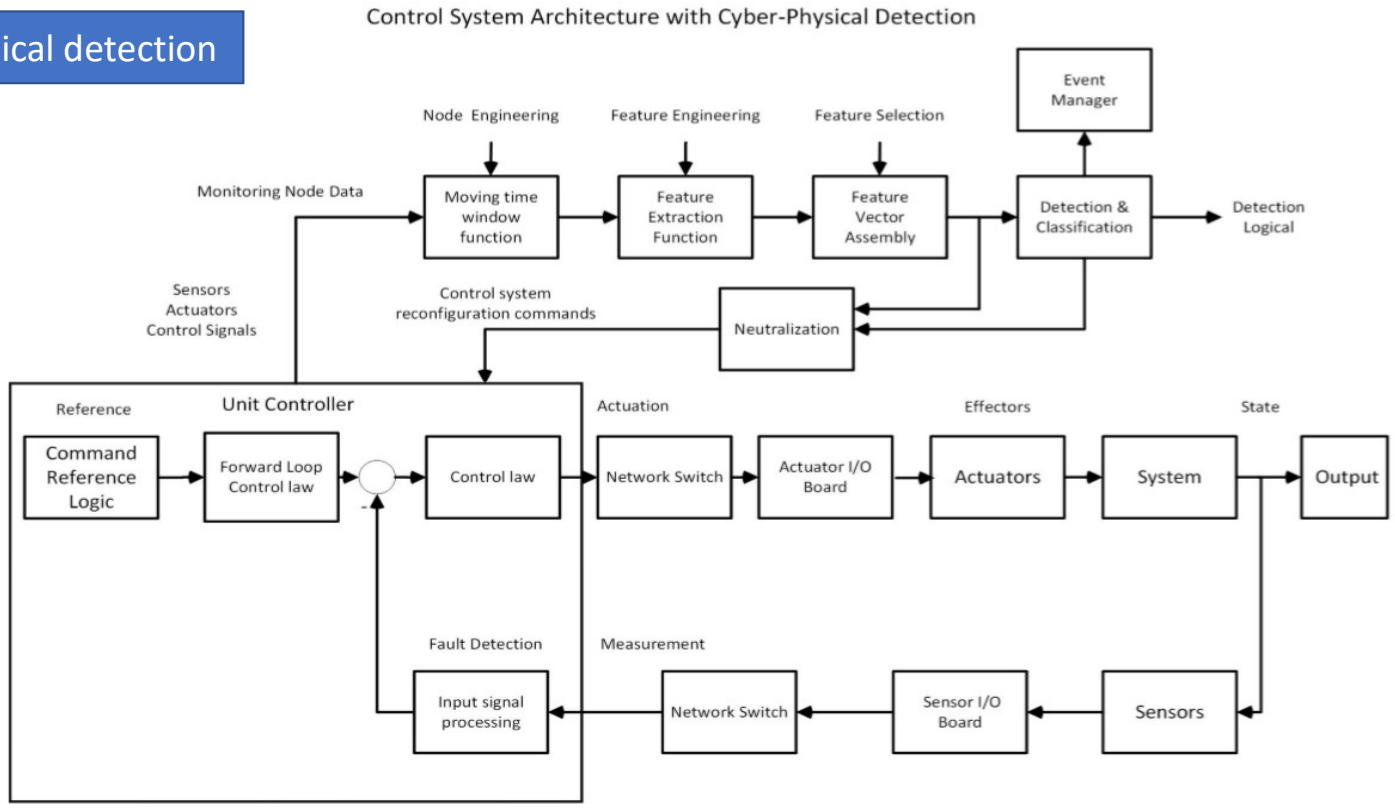
Cyber Physical Architecture



Cyber Physical Detection System

Cyber physical attack detection, localization and neutralization

Cyber physical detection



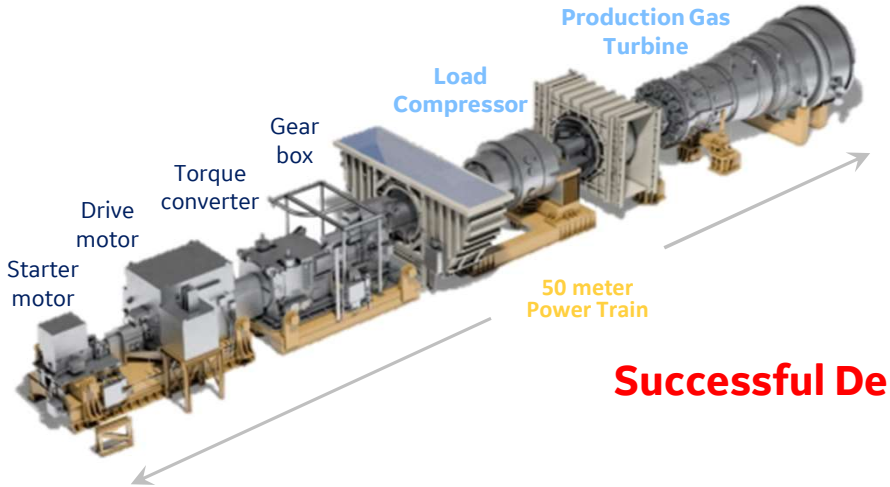
Cyber-Physical Protection

Control System & Plant

Test Stand 7 – 9HA.02 FSFL Validation

CEDS, DOE Contract: Cyber-Attack Detection and Accommodation for the Energy Delivery System Contract: DE-OE0000833

Test Stand Design

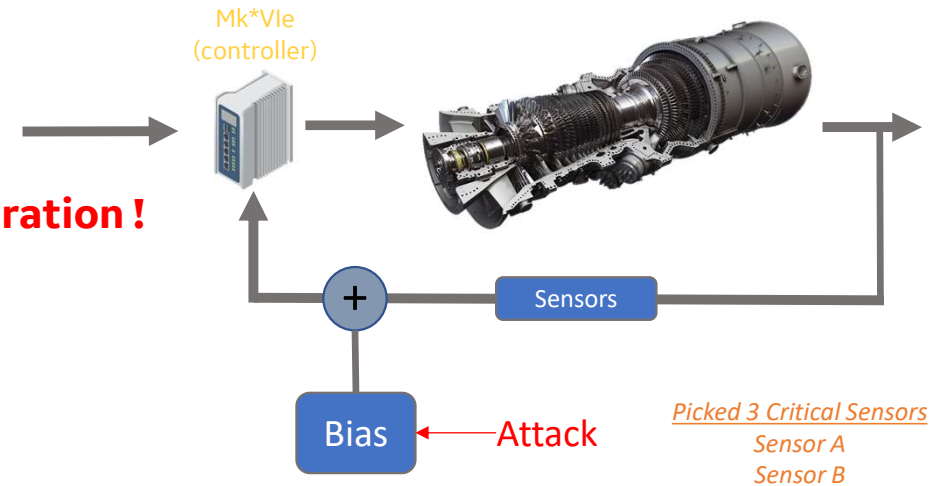


Greenville Test Stand
- >$300MM GE Investment
- >4k Instruments

9HA.02
- >63% combined cycle efficiency
- >500MW output in simple cycle

Digital Ghost Implementation

Cyber Attacks → Sensor Spoofing
Addition of bias to sensor signals



Successful Demonstration !

Picked 3 Critical Sensors
Sensor A
Sensor B
Sensor C

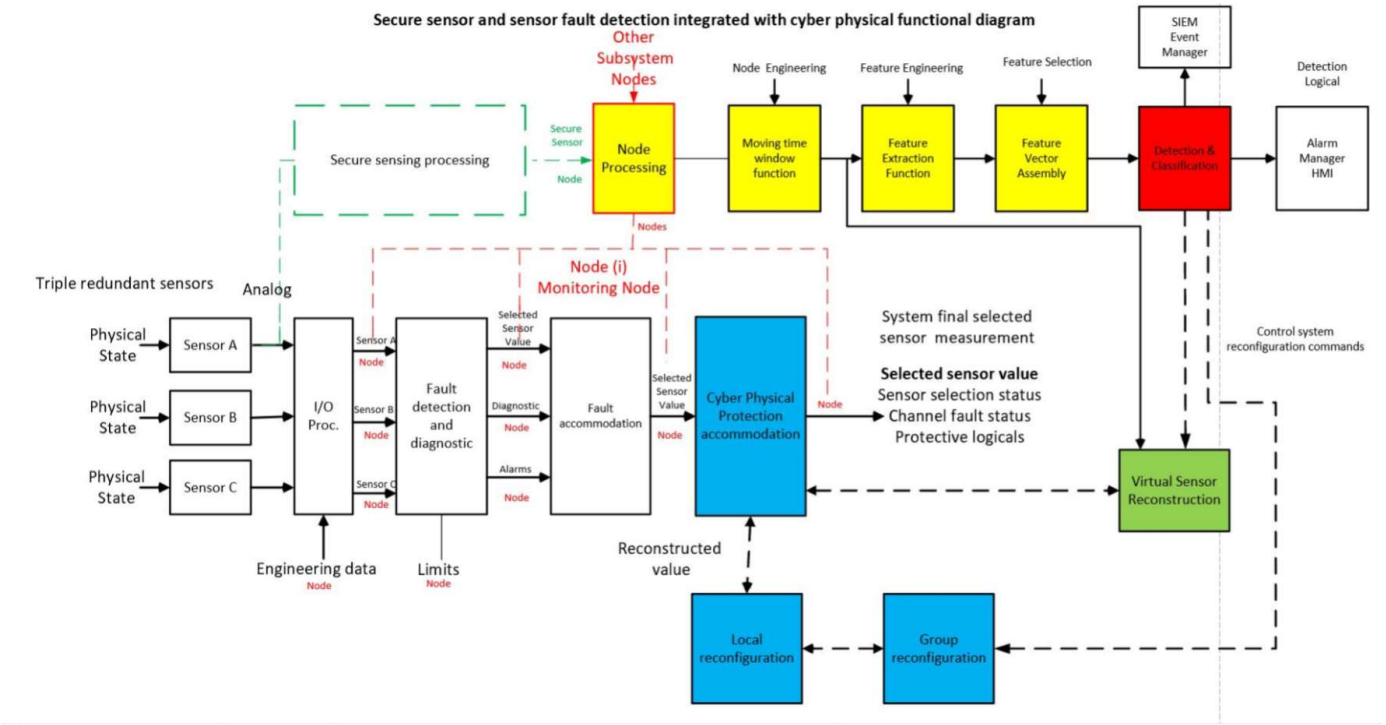
Cyber Resilience Game Changer: Validated And Verified Neutralization Capability On Largest Full Speed, Full Load Test Facility In The World !

Challenges To Cyber-Physical System Integration

NATIONAL ENERGY TECHNOLOGY LABORATORY

- Data communications for monitoring nodes
- System attack node definition
- System impact assessment
- System mode transients
- System nominal noise assessment
- Attack detection timing impact metric
- Reconfiguration timing impact metric
- Secure sensor monitoring nodes
- Time synchronization of monitoring nodes

Fault Tolerant Architecture



Next Steps

- Continue to build on the success of GE's ongoing DOE programs
- Research Machine Learning algorithms used in operating regions not originally included in training data
- Develop solutions to address node observability challenges that lead to poor resiliency performance
- Research methods to quantify assured, stable operations with resiliency functions

Next Steps

- Create methods for secure cross-domain communications and control
- Advance threat mitigation with improved cyber-attack detection and localization

Concluding Remarks

- Successfully demonstrated a cyber physical protection system on a physical test turbine

- Next step involves demonstration of technology on a fielded physical asset
  - Results will provide lessons learned and apply directly to strategic goals.
  - Productization of concept in process

- Cyber physical protection architecture applies to fossil fuel plants, natural gas pipeline distribution, wind turbines and a variety of industrial assets

- Clear need to continue to expand capability of and applications for cyber physical protection technologies