Authenticated Sensor Interface Device for Securing Sensors and Data Transmission
Cyber Threats & High Reliability Operations

- Cyber threats challenge the safety, security, and operation of all industries, including nuclear facilities and the protection of nuclear materials.
- What requires high reliability operations?
  - Critical Infrastructure and Key Resources
  - Dependent on the consequence of failure
    - Risk to the public
    - Risk to the workers
    - Risk to the environment
    - Loss of production
    - Financial cost
    - Reputation/Trust
Innovating Cyber Techniques and Tools

- **New techniques and tools are required**
  - Data security
  - Authentication
  - Protection
  - Detection
  - Mitigation

- **More than just policies, plans and procedures**
  - Bolster resiliency through diversity and defense-in-depth
  - Explore non-traditional methods
  - Next-Generation cyber
Safeguards, Security, & Process Sensor Applications

- **Drivers**
  - *Increasing number and capacity of nuclear facilities* and the amount of nuclear material in the world
  - *Increase in cyber attacks* on security, data, and industrial process control systems
  - *Increased cyber capability* of all adversaries
  - *Remote attacks* on processes can now be carried out
  - *Cyber-hardened sensors and control systems have not provided* by industrial vendors

- **ASID provides an “After-Market” Solution to secure vital sensors and aid in securing networks**
Authenticated Sensor Interface Device (ASID)

- **Secure**
  - Protect Each Party from attack or intrusion from all other parties
  - Protect the Sensor from manipulation from any party

- **Authenticate**
  - Authenticate Data transmitted to each party

- **Share Data**
  - Among a number of parties (if necessary)
ASID Functional Features

- **Sensor Interface**
  - Diverse input capabilities including digital protocols, voltages, mA, thermocouple, etc.
  - Bidirectional communications to sensor

- **Microcomputer Core**
  - Provides capability for adaptation to diverse applications

- **Predictable Data Source**
  - Available for authentication and/or encryption services

- **Data Diode Function**
  - Physically isolates each party and the sensor from attack

- **Non-volatile Memory & Battery Backup**

- **Modular Design**
  - Expandable number of inputs and outputs

- **Tamper Indicating Enclosure**
  - Protects ASID electronics from attack

"Secure, Authenticate, Share"
ASID Security Features

• **Data Diode**
  – Malicious or fraudulent data cannot be sent back into the device from a receiving party or external attacker

• **Sensor Integrity**
  – Even with two-way communications to the sensor, sensor integrity is maintained due to data diode protection

• **Segregation**
  – One party cannot attack or manipulate data being received by another party, or their systems

• **Authentication**
  – External attacker could not “spoof” data being sent to a party

• **Confidentiality**
  – Data is encrypted, preventing external attackers from reading the original sensor data stream

• **Anti-reply**
  – An external attacker cannot replay encrypted packets

“Secure, Authenticate, Share”
**Additional Features**

- **On-board Memory**
  - Stores raw sensor data
  - Stores each party’s data to permit retrieval in case of loss of communications

- **Bypass Switch**
  - In the event of a failure of the ASID, the operator could enter bypass mode to bypass the ASID to ensure operations are not impacted

"Secure, Authenticate, Share"
Field Testing of ASID

- **ASID tested with the Wohwa Accountancy Scale**
  - SRNL conducted a joint use demonstration using a 20,000 kg Wohwa Accountancy Scale
  - Prototype ASID designed with custom software to autonomously retrieve data from the Wohwa scale controller
  - The Wohwa controller required a bi-directional digital communications
    - ASID controller/sensor module requested data from the Wohwa controller
    - ASID controller module transmitted the data to each output module
    - Each output module transmitted the data to its respective data collection computer
  - Note that authentication and encryption was not tested or implemented prior to this testing.
Summary

Drivers

- Increasing number and capacity of nuclear facilities and the amount of nuclear material in the world
- Increase in cyber attacks on security, data, and industrial process control systems
- Increased cyber capability of all adversaries
- Remote attacks on processes can now be carried out
- Cyber-hardened sensors and control systems have not provided by industrial vendors
Summary

• Cyber threats challenge all aspects of industry, including the ability to secure nuclear materials and nuclear facilities
  – Attacks can have severe consequences on the operations of a facility or the validity of safeguards data

• Many cybersecurity challenges must be considered when designing a networked industrial monitoring and control system
  – Securing the networks, sensors, controllers, and data transmissions is vital

ASID can be a key component in ensuring the cybersecurity of a critical system and ensuring the validity of vital sensor data

“Secure, Authenticate, Share”
Thank You
Authenticated Sensor Interface Device

- **Secure**
  - Each Party from attack or intrusion from all other parties
  - The Sensor from manipulation from any party
- **Authenticate Data**
  transmitted to each party
- **Share Data**
  among a number of parties

**Security Features**
- Data Diode
- Segregation
- Sensor Integrity
- Authentication
- Confidentiality

**Functional Features**
- Data Diode
- Micro-Computer Core
- Sensor Interface
- Modular Design
- On-board Memory