Contract No:

This document was prepared in conjunction with work accomplished under Contract No. DE-AC09-08SR22470 with the U.S. Department of Energy (DOE) Office of Environmental Management (EM).

Disclaimer:

AUTHENTICATED SENSOR INTERFACE DEVICE FOR SECURING SENSORS AND DATA TRANSMISSION

RICHARD W. POLAND
Savannah River National Laboratory
Aiken, SC, USA
Email: Richard.Poland@srnl.doe.gov

NICHOLAS F. DEROLLER
Savannah River National Laboratory
Aiken, SC, USA

Abstract

The paper will discuss the features of Savannah River National Laboratory's (SRNL) Authenticated Sensor Interface Device (ASID) which provides the ability to authenticate data from critical sensors and other data streams, share that data among a number of parties, and protect the sensor and each party's network from outside cyber-attack or cyber-attack from other parties receiving the data. In addition, the paper will discuss the development of the prototype to date as well as the future plans for the ASID. As industrial sensor data is increasingly transmitted over networks which are ultimately connected to the internet the likelihood that this data, critical to the protection and operation of nuclear and other facilities, will suffer a successful cyber-attack has greatly increased. The risk of unreliable data, either through manipulation or denial of service, being relied upon for physical security systems poses a tremendous security risk. Additionally, unreliable data due to a cyber-attack on industrial control systems poses unacceptable safety and operational risks. The risk of unreliable sensor data must be mitigated to ensure the safety, security, and reliability of nuclear and other critical infrastructure facilities throughout the world. The ASID, fully implemented, can be a key component in the protection of critical infrastructure from malicious cyber-attacks. The ASID's modular concept allows for interfacing to numerous sensor types including digital protocols as well as analog sensors with voltage, milliamp, and temperature outputs. The sensor signal is authenticated and encrypted by the primary embedded controller, then communicated to each party's transmission module where additional private encryption may be applied to the data stream. An integral and key feature of the ASID is the data diode functions that ensure no communication flows backward to the sensor interface module which ensures that both the sensor and every network is protected from cyber-attack.

1. INTRODUCTION

Cyber connectivity and pipelines have quickly become a primary attack vector for those who may desire to access, alter, or inject information into a network, for those who may desire to disrupt operations of critical infrastructure and manufacturing facilities, and for those who may desire to misinform security forces to aid in gaining access to protected materials and facilities. Recent attacks range from the collection of sensitive personal data, to the ransom of information and systems required to provide critical medical and financial services, to the disruption of the operations of critical infrastructure, among other examples. No nation, no corporation, and no person is exempt from potential attack.

Enticed by the exponential expansion of devices connected to the internet as nations, organizations, and individuals strive to benefit from the efficiencies and knowledge that can be realized through this connectivity, adversaries have taken the opportunity to exploit weaknesses in interconnection technologies and security defences. Due to this rapid demand for connectivity and the financial benefits of being quick to market, implementation of adequate cybersecurity to counter the attacks for new cyber-physical products has not always been the primary focus of manufacturers. Additionally, interconnected legacy cyber-physical devices provide additional attack vectors that may not have "patches" available. The risk of unreliable data, either through manipulation or denial of service, being relied upon for physical security systems poses a tremendous security risk. Additionally, unreliable data due to a cyber-attack on industrial control systems poses unacceptable safety and operational risks. The risk of unreliable sensor data must be mitigated to ensure the safety, security, and reliability of nuclear and other critical infrastructure facilities throughout the world.

The Savannah River National Laboratory (SRNL) has developed industrial control systems (ICS) and industrial data acquisition systems for many years in support of nuclear facilities. These systems have traditionally been isolated systems, however ever increasingly the systems are required to be interconnected to permit remote control and monitoring. SRNL has studied the application of and developed instrumentation to enhance the capability of international organizations to more effectively and efficiently monitor the production and storage of nuclear materials around the world. These applications, including joint-use applications, require that critical sensors be secured, data be authenticated, and networks be protected. SRNL has thus developed the Authenticated Sensor Interface Device (ASID) which is designed to authenticate data from critical sensors and other data streams, share that data among a number of parties, and protect the sensor and each party's network from outside cyber-attack or cyber-attack from other parties receiving the data. Further, the ASID can be adapted to many other applications, including the securing of interconnected ICS and security devices. The ASID, fully implemented, can be a key component in the protection of critical infrastructure from malicious cyber-attacks.

2. APPLICATIONS

The Authenticated Sensor Interface Device was originally developed to aid the International Atomic Energy Agency (IAEA) in the implementation of joint-use equipment for the monitoring of nuclear materials safeguarding activities. Driven by the increasing number of nuclear facilities and constrained IAEA budgets, the IAEA actively pursues innovative and cost effective methods to reduce the number of inspector days at facilities yet maintain the ability to draw credible conclusion for each state. To this end, the IAEA must ensure that data collected is credible, ensure the integrity of sensors and information systems, and ensure that any joint-use devices installed have no adverse impact on the process being monitored. The facility operator will require no adverse impact to the process and that all proprietary information and systems are protected.

The expectation is that implementation of joint-use equipment will yield several advantages that will be realized by both the IAEA and the operator. These include:

- Cost effectiveness through remote collection of data and a reduction in the number of inspector days at a given facility;
- Cost sharing between the operator and the IAEA through the joint-use of equipment and thus the elimination of the purchase, installation, and maintenance of duplicative sensors;
- The opportunity to collect additional process monitoring data that otherwise would require a far too costly installation for either party.

Sharing data from critical safeguards sensors, however, comes with a number of potential disadvantages and risks to the IAEA if the joint-use program is not implemented with thorough consideration of all risks and an effective mitigation strategy. These disadvantages and risks include, but are not limited to:

- A risk that the IAEA's safeguards conclusion may be compromised;
- A risk that the data collected from the sensor cannot be authenticated;
- A risk that the IAEA's network may be breached due to the need for interconnectivity.

The remainder of this paper will not only focus only on the application of ASID to mitigate the risks associated with the interconnectivity of these joint-use sensors, but also on the application of the ASID to the protection of nuclear facilities' ICS, security systems, computer and interconnection systems, and data collection and transmission systems.

3. AUTHENTICATED SENSOR INTERFACE DEVICE

There are three primary goals of the Authenticated Sensor Interface Device which, when effectively implemented, will help ensure secure collection and transmission of sensor data. These goals are:

- **Share** data among parties.
- **Authenticate** data transmitted to each party;
- **Protect**:
  - the network of each party from attack or intrusion from all other parties;

- the sensor, an ICS device, and the ASID from cyber-attack;

3.1. Functional Features of ASID

The Authenticated Sensor Interface Device, to provide the above listed benefits, is designed as a modular platform that has interchangeable modules allowing the ASID to be configured to meet the challenges of many safeguards, security, and industrial manufacturing applications. The major functions of the ASID are the Sensor Interface, the Digital Controller, and the Data Output modules as shown in Fig. 1.

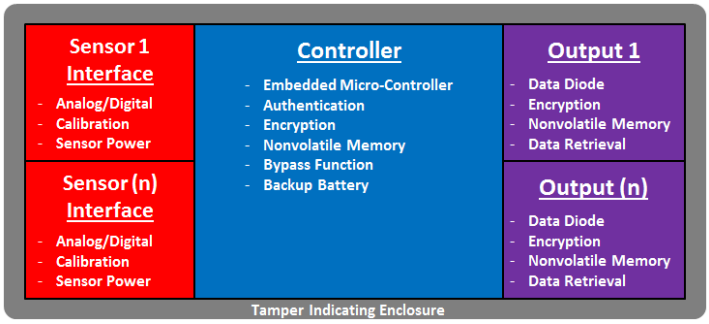

Fig. 1 Modular Functions of the ASID

The prototype ASID was designed to work with a digital interface from an accountancy scale, however the vision is that enhanced versions of ASID will incorporate a modular design which will permit the ASID to be configured by selecting from a diverse selection sensor interface modules. The modules will include analog voltage, analog current, temperature (thermocouple and RTD), or other sensor interfaces. Sensor interface modules that collect data from sensors with digital outputs such as serial and tcp-ip will also be available. This wide range of inputs permits the ASID to collect data from essentially any process sensor, including radiation monitors, pressure sensors, load cells, security cameras, and numerous other devices. Because the ASID is a “smart” interface, it will have the ability to calibrate each sensor to ensure valid and accurate data is collected. Additionally, the ASID will accept any number of these inputs, so the modular design of the ASID allows for an increase in the number of sensors monitored as an application grows.

The central function of the ASID is the microcontroller core which provides the capability for adaptation to diverse applications. The Controller collects the data from each of the sensor interface modules, applies an authentication strategy to the data to ensure the data can be validated at the destination. To execute this function, the Controller module will have a data source available such as a clock or other predictable data source to aid in the implementation of a sign and forward strategy. The Controller then encrypts the data, if required, prior to forwarding the data stream to the appropriate Output module. The functional data flow is shown in Fig. 2.

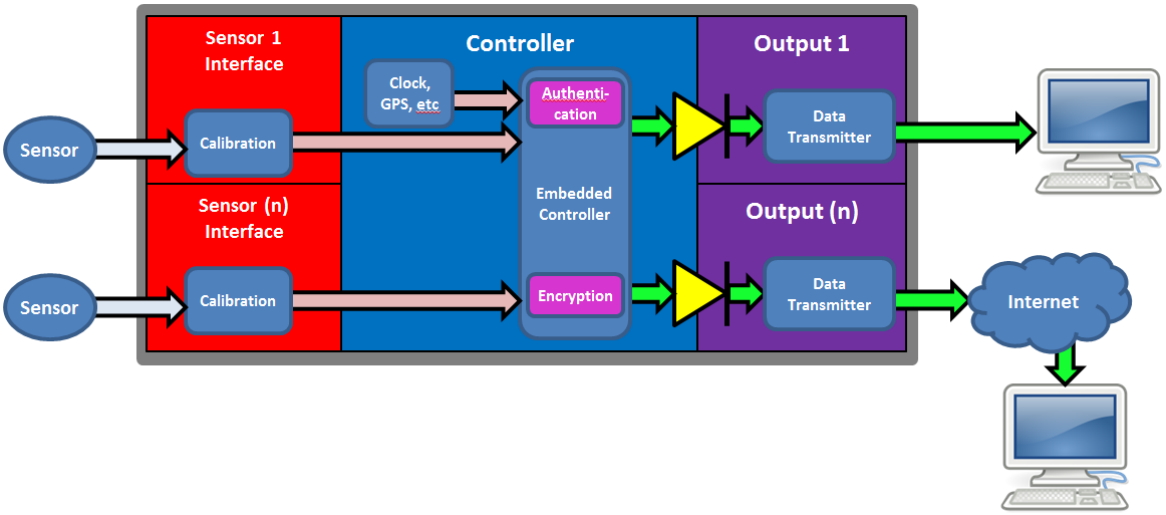

Fig. 2 ASID Data Flow

Several other valuable features, as listed in Fig. 1, are embedded in the functionality of ASID's controller module. These include: non-volatile memory which is used to log the raw sensor data, battery backup to ensure the parties can be alerted if ASID loses power or encounters other issues, and a bypass function which will engage if the ASID malfunctions.

An additional key feature of the ASID is the data diode function that is provided between the controller module and each of the output modules permitting data to be passed only from the controller to each of the output modules. The data diode physically isolates each party from the sensor and from each other. Therefore, no monitoring party has digital access to the sensor, the controller module, or any component beyond their output module.

Also, each output module contains non-volatile memory to log the party's authenticated data stream. This memory permits the monitoring party to remotely retrieve a specified amount of its authenticated data in case the network connection is lost for some period of time. Each output module also has the capability to encrypt its data stream before transmission.

A Tamper Indicating Enclosure (TIE) protects the ASID from physical intrusion. Ideally, to ensure full authentication of data, the sensor will be authenticated and a tamper indicating enclosure will enclose the sensor as well as any electrical connections between the ASID and the sensor

3.2. Security Features of ASID

The ASID provides numerous benefits based on the functional features listed in the previous section. The key security feature is the assurance of data integrity and network security. The data diode function described above ensures sensor *data integrity* because no party, invited or otherwise, can digitally interact with the sensor, raw sensor data, or other client modules. Additionally, the implementation of data authentication in the ASID controller module ensures that the data provided to each party is valid. *Data confidentiality* is ensured by proper implementation of the encryption features. Finally, the ASID provides *network segregation*. No party can attack or manipulate data being received by another party, or another's networked systems.

4. ADDITIONAL APPLICATIONS

Although the ASID was designed for various safeguards applications, it is apparent that the ASID concept is applicable to security, industrial manufacturing, and other interconnected applications. For example, ASID can have a direct and immediate impact on any networked security

sensor, such as surveillance cameras, that have no requirement for bi-directional data flow. Many radiation monitors do not require bi-directional data feeds.

For those sensors that do require bi-directional data feeds, ASID's micro-controller can be customized to autonomously provide those communications to retrieve the data, then transmit that data to the user, thus isolating and segregating the sensor from cyber-attack.

ASID should be considered for these and other applications.

ACKNOWLEDGEMENTS

Funding for this project was provided by Savannah River National Laboratory's Laboratory Directed Research and Development Program.