Contract No:

This document was prepared in conjunction with work accomplished under Contract No. DE-AC09-08SR22470 with the U.S. Department of Energy.

Disclaimer:

Authenticated Sensor Interface Device for Joint Use Safeguards Applications – Concepts and Challenges

Richard W. Poland, Robert Drayer, J. Rusty Coleman, Jason Wilson, PhD
Savannah River National Laboratory
Aiken, SC 29808

Abstract

This paper will discuss the key features of the Authenticated Sensor Interface Device that collectively provide the ability to share data among a number of parties while ensuring the authentication of data and protecting both the operator's and the IAEA's interests. The paper will also discuss the development of the prototype, the initial testing with an accountancy scale, and future plans and challenges to implementation into the joint use and remote monitoring applications.

As nuclear fuel cycle technology becomes more prevalent throughout the world and the capacity of plants increases, limited resources of the IAEA are being stretched near a breaking point. A strategy is to increase efficiency in safeguards monitoring using "joint use" equipment that will provide the facility operator process data while also providing the IAEA key safeguards data. The data, however, must be authenticated and validated to ensure the data have not been tampered with. The Authenticated Sensor Interface Device provides the capability to share data and can be a valuable component in the IAEA's ability to collect accountancy data from scales in Uranium conversion and enrichment plants, as well as nuclear fuel fabrication plants. Likewise, the Authenticated Sensor Interface Device can be configured to accept a diverse array of input signals, ranging from analog voltage, to current, to digital interfaces and more. These modular capabilities provide the ability to collect authenticated, joint-use, data streams from various process monitoring sensors.

Introduction

The International Atomic Energy Agency's (IAEA) need to collect authenticated safeguards information from joint use equipment is needed more now than ever with the increase in data obtained through remote monitoring. In the past ten years the number of systems remotely monitored by the IAEA has greatly increased. As of August 2011, there were 263 systems connected remotely. This resulted in over 3.5 Gigabytes of data per day being transferred to the IAEA offices in Vienna, Tokyo, and Toronto. The expected growth rate of the number of remote monitoring systems increasing by 10-15% per year indicates the need for a way to cut the amount of data that needs processing. Through the joint use of safeguards equipment the safeguards data may be more easily obtained, but it may also raise some disadvantages. To help minimize the disadvantages while keeping all of the advantages of joint use equipment, engineers at the Savannah river National Laboratory (SRNL) has developed the Authenticated Sensor Interface Device (ASID). The main features are to provide the ability to share data among a

number of parties while ensuring data authentication and protecting both the operator's and the IAEA's interests.

Concepts and Challenges

There are a number of factors that drive the IAEA toward the implementation of joint-use equipment. An increase in the number of nuclear facilities throughout the world and the larger capacities of those new nuclear fuel cycle facilities is a primary consideration. To meet the additional inspection load, the IAEA must improve efficiencies for inspections and data analysis while essentially maintaining their budget with no year to year increases. Additionally, as the IAEA transitions to Information Driven Safeguards valuable information from operator owned process monitoring equipment can corroborate other data and/or add an additional layer of deterrence to material diversion.

There are several potential benefits to be gained by the IAEA remotely monitoring key processes within plants. These include:

- Safeguards data may be more easily obtained by the Agency with equipment provided by the operator or the state,
- The Agency may save resources by sharing costs of acquiring, maintaining, and operating safeguards equipment,
- Facility operators may find Agency safeguards less burdensome, and
- Inspector and technician radiation exposure may be reduced.

On the other hand, there are several potential disadvantages of joint use equipment. These include:

- Independence of the Agency's safeguards conclusions may come into doubt,
- Integrity and authenticity of data obtained from this equipment may be difficult to ensure,
- Safeguards measures may be easier to defeat when:
    - Operator/State know performance characteristics of the instrument,
    - Operator/State has direct access to the data,
- Addition costs of IAEA authentication methods may be unacceptable.

Further, there are a number of implementation challenges for joint use equipment. Joint use equipment must be kept under adequate Agency control after the authentication procedures are performed. The implementation of this requirement may be viewed differently depending on whether the equipment is a "use each time" equipment that is stored away for use by the Agency and the operator, or whether the equipment is a process monitoring instrument in the operator's process that provides the operator vital data for process control. This paper focuses on challenges relating to implementing joint use process monitoring equipment, which practically is more challenging than the former scenario. Agency "control" of process monitoring joint use equipment may come in the form of a sealed tamper indicating enclosure with additional electronic assurance that sensor data is independent of operator manipulation and authenticated as close as possible to the sensor.

If authentication of data is to be maintained, an IAEA representative must be present during installation, repair, maintenance, and upgrade of critical components. This is a natural argument from the above statement regarding the Agency maintaining control of the equipment.

Finally, the sharing of data between the parties, potentially the operator, the State, and the Agency presents a number of implementation challenges. Data sharing must not compromise the Agency's capability to draw independent safeguards conclusions. This is vital to the successful and useful implementation of any joint use effort. Additionally, data sharing shall not give outside parties unrestricted access to Agency computing or data collection networks. Finally, only the Agency should have access to the joint use equipment data before the Agency receives the operator's declarations. In cases where this cannot be avoided (such as operator process monitoring data), additional measures must be specified to address this problem.

Authenticated Sensor Interface Device

The collection, sharing, and authentication of joint use data continue to be a challenge. Protection of the IAEA data transmission and network from operator manipulation or attack is a primary concern for the IAEA, while the operator has similar concerns regarding the IAEA's access to operator proprietary data. The ASID provides a comprehensive solution to this challenge. The ASID can be configured to accept a diverse array of input signals, ranging from analog voltage, to current, to digital and more. These expanded capabilities provide a much greater market opportunity in safeguards as the IAEA intends to jointly monitor process instruments such as accountancy scales, load cells, and possibly assay instrumentation.

The goal of the ASID is to:

- Share data among a number of parties,
- Authenticate data transmitted to each party,
- Protect each party from attack or intrusion from all other parties, and
- Protect the sensor and the ASID from electronic manipulation from any party.

Additionally, the ASID will aid in the standardization of data transfer protocols and data security, and provide a uniform interface for remote monitoring devices to communicate with IAEA collection devices.

Functional Attributes of ASID

Safeguards data collected using "joint use" equipment will provide the facility operator process data while also providing the IAEA key safeguards data. The data, however, must be authenticated and validated to ensure the data have not been altered. The Authenticated Sensor Interface Device provides the capability to share data and can be a valuable component in the IAEA's ability to collect accountancy data from scales in Uranium conversion and enrichment plants, as well as nuclear fuel fabrication plants. Likewise, the Authenticated Sensor Interface Device can be configured to accept a diverse array of input signals, ranging from analog voltage, to current, to digital

interfaces and more. These modular capabilities provide the ability to collect authenticated, joint-use data streams from various process monitoring sensors. The ASID modular functionality is shown in Figure 1.

Sharing and authenticating this data, however, continues to be a challenge. Protection of the IAEA data transmission and network from operator manipulation or attack is a primary concern for the IAEA, while the operator has similar concerns regarding the IAEA's access to operator proprietary data. The ASID provides a comprehensive solution to this challenge.

Current "data diode" type devices provide only unidirectional protection leaving one party's network vulnerable to attack or other interrogation by an untrusted party. Further, currently available systems do not provide encryption, data authentication, storage, or other desired features in a single unit, and the systems are very expensive to purchase and operate. The ASID is a compact, inexpensive solution that will provide all the features required by both the IAEA and the commercial nuclear operators monitored by the IAEA.

At its core, the ASID is based on a micro-computer. This core functionality provides for the adaptation of the ASID to a considerable number of applications. Most notably, the micro-computer (shown as the "Data Aggregate" in Figure 1) offers ASID the ability for diverse sensor interfaces. The input options for ASID include digital protocols, both standard and proprietary as well as bi-directional communication to sensors that require a request to collect data. Additionally the ASID accepts analog input signals to include voltages, currents, thermocouple, and other analog sensors. The ASID can also communicate directly with a PLC.

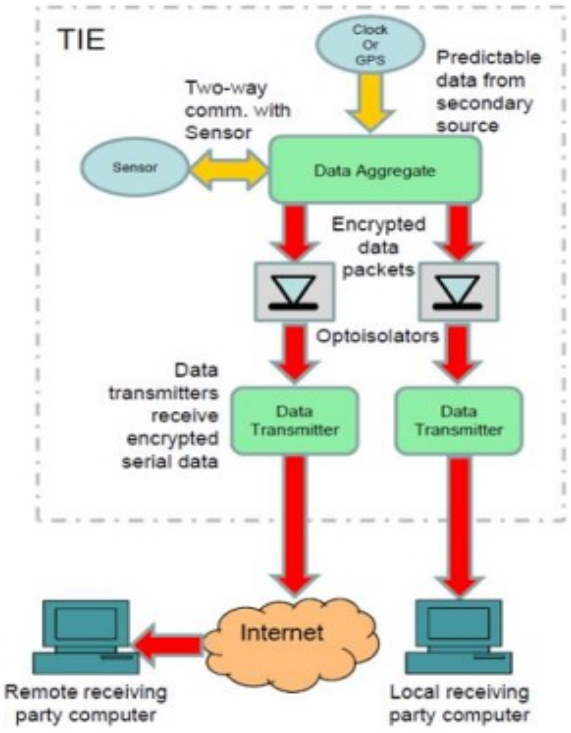

Figure 1

This wide range of inputs permits the ASID to collect, secure, and transmit data from accountancy scales, process load cells, radiation monitors, surveillance equipment, NDA instruments, and many other sensor types.

Protection of data will be assured by the implementation of sign and forward technology and data encryption. The ASID will have available a data source such as a clock or other predictable data source to aid in this feature as required. Although encryption of data will be available for any party, data will be encrypted only for the parties, such as the IAEA,

who require encryption for protection. Typically, the operator will not require encryption of data for in-plant use.

Optoisolators provide a physical barrier to prevent electronic communication from a party into the ASID. The optoisolators essentially provide a data diode function, only permitting data to pass from the ASID to a party. This feature provides protection for the sensor, the ASID, and effectively provides isolation for each party's network, data, and instrumentation.

Additional features not shown in Figure 1 include local memory for the logging of raw sensor data at the micro-computer. If for some reason transmission of data was interrupted, the logged raw data could be physically retrieved from this memory card by an inspector. Memory will also be available at each data transmitter for logging of each party's transmitted data. If communication is lost with the ASID, the IAEA could remotely send a query to retransmit and retrieve the missing encrypted data since this memory is outside the data diode feature.

The ASID is designed on a modular platform. Features can be implemented or eliminated depending on the application. Sensor type can be selected and implemented. Memory can be implemented or eliminated. The ASID can transmit data to one party or up to n parties. Data can be encrypted to a party or not. Battery back-up may be a selected feature. The ASID's modular platform permits it to be cost effective for most any data collection and transmission application.

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.

The IAEA is currently developing the Real-time and Integrated Stream-Oriented Remote Monitoring (RAINSTORM) interface. The motivation of this interface is to standardize data transfer and data security, while providing a uniform interface across all instruments that the IAEA monitors across the world. Currently the IAEA collects data from a wide array of remote interfaces and data security implementations. ASID, having a micro-controller at its core, can implement this chosen standard and provide the standardized remote monitoring interface and the required features of shared and isolated data paths to permit joint use of operator or IAEA equipment.

Future Tasks

A prototype ASID has been fabricated and bench top testing is complete. Initial field testing of the ASID is expected to be completed with the installation of an accountancy scale at a production facility in 2013. The functionality will be evaluated as the ASID is integrated and tested on the operator's network while sharing data with the SRNL collection computer system. SRNL and NNSA intend to continue to communicate with

the IAEA to define requirements and application concepts, and to work with the IAEA to implement RAINSTORM on the ASID.

Conclusions

The ASID provides many features crucial to effectively implement joint-use process instrumentation and authenticated remote data collection. These features include:

- *Sharing Data*
  The ASID provides unidirectional data flow to any number of parties while protecting each party's network from attack or interrogation from all others, allowing the sharing of data while ensuring the security of each party's data and network.
- *Authentication of Data*
  Unidirectional data flow also ensures that no party can manipulate the raw analog or digital data collected from the sensor before the data is signed and/or encrypted and forwarded. Further, integrated signing and encryption capabilities ensure that the data that is collected is the authenticated data received by the IAEA.
- *Protect Each Party's Information*
  The unidirectional data flow ensures that no party can electronically attack the sensor or the ASID, and as stated above provides physical assurance that no party can attack or interrogate another party's network. Therefore, both the sensor and each party's network are protected.
- *Standardization*
  The IAEA is developing RAINSTORM as its standard for data transfer and data security, while providing a uniform interface across all remotely monitored instruments. ASID will incorporate RAINSTORM and provide those standardized features while also standardizing the collection, sharing, and transmission of joint use data.

Acknowledgements

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