SAND2013-4036C

Enhanced Data Authentication System: Converting Requirements to a Functional Prototype

Maikael Thomas, George Baldwin, Ross Hymel,

Global Security Programs, Sandia National Laboratories
Albuquerque NM USA
mthomas@sandia.gov; gtbaldw@sandia.gov; rwhymel@sandia.gov

Andreas Smejkal, Peter Schwalbach, Morgan Rue,

Nuclear Safeguards Directorate
European Commission Directorate-General for Energy
Luxembourg
andreas.smejkal@ec.europa.eu; peter.schwalbach@ec.europa.eu,
morgan.rue@ec.europa.eu

Luc Dechamp and João G.M. Gonçalves

Institute for Transuranium Elements, European Commission Joint Research Centre
Ispra, Italy
luc.dechamp@jrc.ec.europa.eu; joao.goncalves@jrc.ec.europa.eu

Abstract:

The Enhanced Data Authentication System (EDAS) is a technical concept to securely "branch" measurement data from operator-owned instrumentation to a Safeguards inspectorate, while guaranteeing the integrity of the operator communication link. While Safeguards normally depend on measurements that are fully independent from those of the operator, certain situations may call for the sharing of information from facility systems for both operations and verification purposes. An inspector must be confident that this branched information is a secure, true, and complete replica of the operator instrumentation. At the same time, an operator must have the assurance that the branching does not introduce an unacceptable risk to facility operations.

The EDAS project is a joint collaboration between the European Commission Directorate-General for Energy, the Institute for Transuranium Elements of the European Commission Joint Research Centre, the U.S. Department of Energy, and Sandia National Laboratories. Recognizing the special and conflicting requirements of the inspector and the operator, we have broken EDAS development into two phases. An initial EDAS prototype, focused on inspector requirements, was tested in a laboratory setting using representative instrumentation based on serial (RS232) communication. Results of these tests show that EDAS is able to meet inspector requirements. Current development emphasizes the operator concerns: establishing the complete set of requirements, designing and implementing a solution, and testing performance.

In this paper we focus on the second phase. We have developed an improved functional prototype that incorporates operator requirements. Considering these requirements, we show how they motivated the selection of our chosen embedded platform and accompanying Linux operating system. For software, we used open source libraries for communications and to encrypt and authenticate the data. We plan an installation and field test of the EDAS prototype at a facility in the United Kingdom in late 2013 to demonstrate the EDAS concept.

Keywords: branching, measurement, operator, safeguards, authentication

1. Introduction

The process monitoring of safeguarded nuclear fuel cycle facilities has a history of technical and policy challenges. Typically, the instrumentation used for safeguards inspections and that used for facility operations are distinct, using separate inspector and operator equipment, which can reconcile the differing needs of the inspector and facility operator. However, there can be practical cost and space limitations to this approach. Due to these constraints, it could provide additional confidence to an inspector to supplement dedicated safeguards implementations with other measures that provide complementary information directly from operator instrumentation.

We present the Enhanced Data Authentication System (EDAS) as a minimally intrusive technology that could provide inspectors with complementary safeguards information and more comprehensive view of a facility [1,2]. The concept of EDAS is to tap, or "branch," an operator's existing instrumentation to provide the inspector a secure and identical copy of the information flowing to/from the sensor. A conceptual example of EDAS is illustrated in Figure 1. Examples of sensors could include temperature probe, a flow monitor, a weight scale, a switch, or any other instrument.

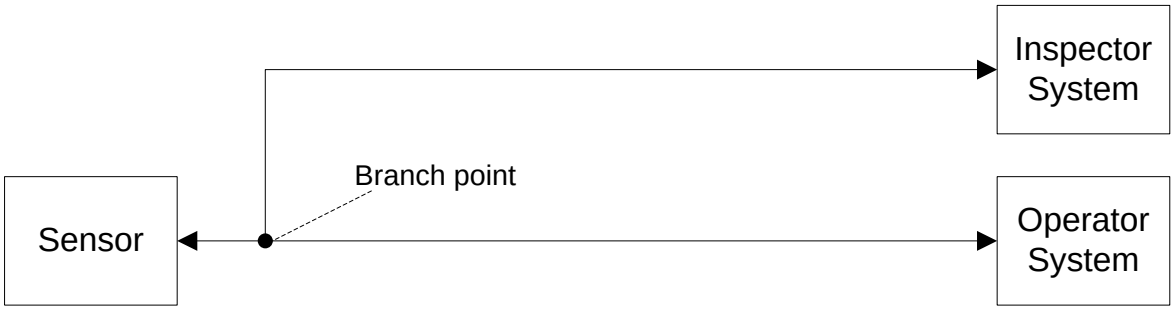

Figure 1: EDAS Branching Concept

For EDAS to be trusted and accepted by inspectors and operators, it is important to address the requirements of both parties. As part of a first phase in the development of EDAS, our team collected the inspector requirements and developed a first generation prototype that was demonstrated to members of the DG-Energy, the IAEA, and the Joint Research Centre. EDAS is now in a second phase of development that focuses on collecting operator requirements and creating a second generation prototype that combines both inspector and operator requirements. This paper focuses on converting these requirements into a functional prototype, and describing our architecture and design in greater detail.

2. Inspector and Operator Requirements

It is important to enumerate the inspector and operator requirements as it motivates the EDAS architecture and design.

2.1. Inspector Requirements

As listed in Baldwin [1], the requirements collected for inspectors are as follows:

Accurate
By accurate, we mean identical, on a bit-for-bit basis, to the information passed to the operator by the primary signal chain.

Complete
The inspector wants to see all of the information passed in the signal chain between the sensor and the operator. The signal chain may be bidirectional—with control signals being passed to the sensor—

so a branching solution would want to capture both data streams. If there should be multiple (parallel) data paths, each would need to be branched in duplicate.

Authentic
The inspector wants assurance that the information indeed comes from the agreed branch point without change—whether by unintentional interference, loss of integrity, or deliberate manipulation. For digital signals, this requirement generally calls for cryptographic signing of the branched data ("authentication").

Meaningful
At its most basic level, the branched data stream of 0's and 1's is meaningless out of context. An inspector needs to be able to interpret the data stream in the same way that the operator does. To use an exaggerated example: It does no good for the inspector to observe the messages "off" and "on" confidently, if the operator instead interprets these messages to instead mean their opposites, "on" and "off." The data stream is interpreted literally; the operator must not be talking in secret code.

Confidential
As a general rule, an inspectorate is expected to treat safeguards information as confidential. Third parties should not be able to eavesdrop. Thus the information branched to the inspector typically requires encryption.

2.2. Operator Requirements

The operator requirements were collected more recently as part of a second project cycle with EDAS. For an operator to feel comfortable allowing EDAS inside of a facility, our team assumes the following operator requirements:

Noninterfering
Once in place, an inspector branch cannot interfere in any way with the signal chain between the sensor and the rest of the operator's instrumentation. Data cannot be dropped, delayed, or altered. In every respect, the original signal chain must function exactly as it did without the inserted branch point. Essentially, noninterference is the single overriding requirement, but we mention two variants explicitly in the next two requirements:

Fail-safe
Noninterference must be the rule *whatever* the condition of the inspector signal branch. In particular, if the inspector branch should fail (e.g., EDAS loses power), the operator's signal chain must not be affected. Detailed requirements must anticipate and explore *all* conceivable modes of failure.

Benign
Noninterference also implies that an inspector could never *intentionally* manipulate the operator's sensor and instrumentation through the branch. The branch is strictly passive (unidirectional).

Consistent with Instrumentation Standards
Operator instrumentation may be compelled to comply with particular instrumentation standards, or satisfy specific performance criteria. For example, a measurement might function as part of an automated safety system. Instrumentation standards such as the Open Connectivity Standard (OPC) Unified Architecture are becoming more widely adopted. Any modifications for branching would need to satisfy such requirements, but these could vary depending on the particular measurement and on the facility.

Provided with Bypass Option
The operator must be able to physically bypass the inspector branch point if and when desired, for any reason, thereby leaving no question that the operator system had been restored fully to its original uninterrupted state.

3. System Architecture

The EDAS architecture can be divided into hardware/electronics and software components. By dividing the EDAS in this fashion, it will be easier to illustrate how the architecture and design meet the inspector and operator requirements.

3.1. Electronics Architecture

The EDAS electronics architecture is illustrated in Figure 2. This diagram includes several important architectural features starting at the tap off point of the operator instrumentation line and continues to the processor board that runs the EDAS software. Each major component of the electronics addresses either a requirement or a feature to enhance EDAS robustness.

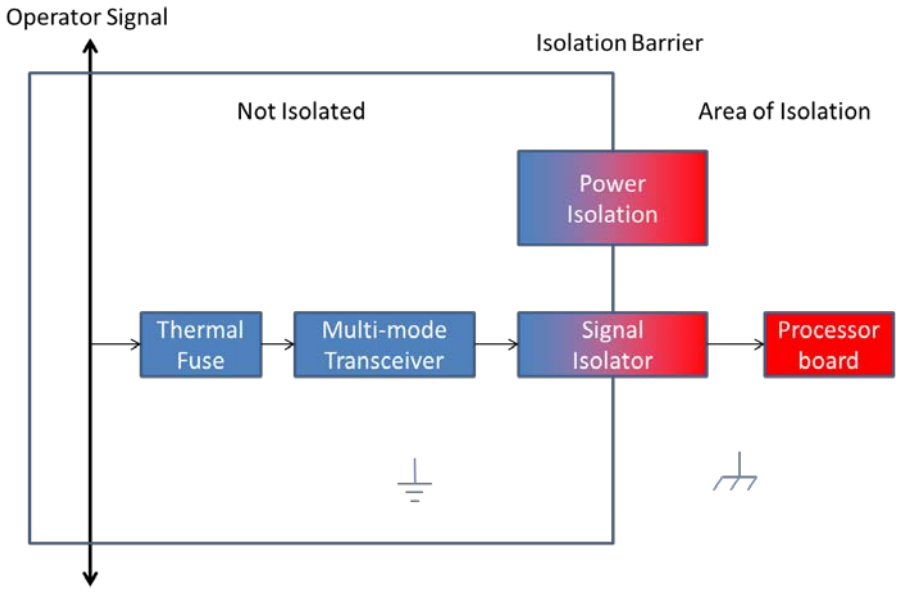

Figure 2: Electronics Architecture

The major electronics component that interfaces to the operator signal line is the thermal fuse. The thermal fuse addresses the noninterference operator requirement for fail-safe operations. In the case that the multi-mode transceiver or signal isolator electronics were to fail (e.g., due to overvoltage or incorrect polarity) and thereby interfere with the operator signal line, these fuses change their properties to become highly resistive, thus effectively isolating the signal line from the rest of EDAS. Similarly, if the EDAS electronics were to lose power, the electronics will act as an open circuit, preventing noise from reaching the operator signal. These steps help prevent potential corruption of data on the operator signal line in the case of multiple EDAS failure scenarios.

The multi-mode transceiver allows the processing of multiple types of signal inputs to make the EDAS more extensible. For example, such a transceiver could support RS-232 or RS-485 signals, so that the same EDAS could be deployed to tap instrumentation that uses either of these signal types.

Another important feature of the electronics is the various isolation features. All signals tapped from the operator signal line are passed through a signal isolator. An isolator ensures that EDAS is functionally benign as it allows for the operator signals to pass to the EDAS processor board while preventing any EDAS (and, by extension, inspector) signal from entering the operator signal line. A power isolator also provides isolated power for electronics inside of the EDAS to prevent power surges from destroying the components. Without a power isolator, in the worst case, a power surge could destroy the signal isolator, rendering it ineffective.

3.2. Software Architecture

The EDAS software architecture is shown in Figure 3. This diagram represents the major software blocks of the processor board block of Figure 2. As with the electronics, each major software component addresses a major inspector or operator requirement.

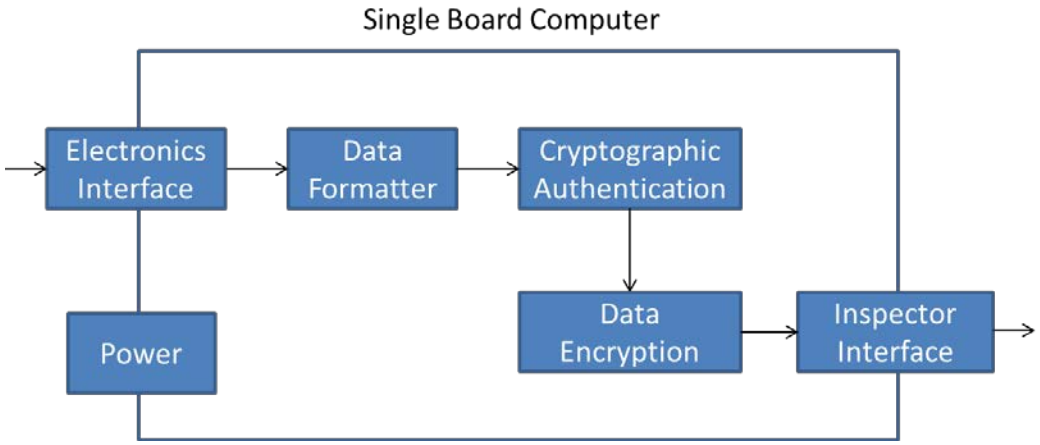

Figure 3: EDAS Software Architecture

Data from the operator signal line will first pass through a data formatter, whose function is to add a metadata tag to all incoming data packets. To simplify the EDAS architecture, the EDAS does not have an understanding of the underlying data passing through it. This task is left for subsequent processing by the inspectorate computer. However, to aid with downstream processing, the EDAS will add the following metadata tags: time stamp of first received packet, time stamp of last received packet, ID of input port, ID of EDAS, ID of tapped pin (e.g., Rx or Tx of RS-232 connection), and the number of bytes in the data block. The use of two timestamps implies variable length output messages from the EDAS, but this solves the issue where input data could be continuous or in bursts. The data formatter addresses the inspector requirements that the data be complete and meaningful as data packets will be formatted with helpful header information. The packets shall also be formatted to meet the operator requirement that data will be consistent with instrumentation standards. More information is given in the next section as to which specific standard our prototypes comply.

The EDAS will cryptographically authenticate all data packets to ensure that the inspector authentic requirement is met. The software will be configurable to allow a selection from various authentication algorithms that meet the stringent NSA Suite B standards for data security. After the authentication block, data packets are encrypted to the same NSA standards to meet the inspector requirement for data confidentiality. After these steps, all data packets are pushed to an inspector system, where the operator instrumentation data can be further analyzed.

4. Prototype Design

Our design of an EDAS prototype is influenced in part by an anticipated field trial deployment. We will support branching either four RS-232 pins or two RS-485 pins on the prototype to interface and tap data from the selected field trial equipment. All data are passed through a capacitive SiO_2 signal isolator rated to 6kV. We use a magnetic power isolator to provide power to the isolated electronics in the EDAS. These electronic components will be fabricated on a custom printed circuit board, which will interface to the software processor board.

As shown in Figure 4, we have selected the low cost, credit card-sized BeagleBone as the processor platform to run the EDAS software [3]. The BeagleBone is powered through the USB port and will push output data to the inspectorate computer via its Ethernet port. The EDAS prototype runs a variant of the Linux operating system on the BeagleBone computer.

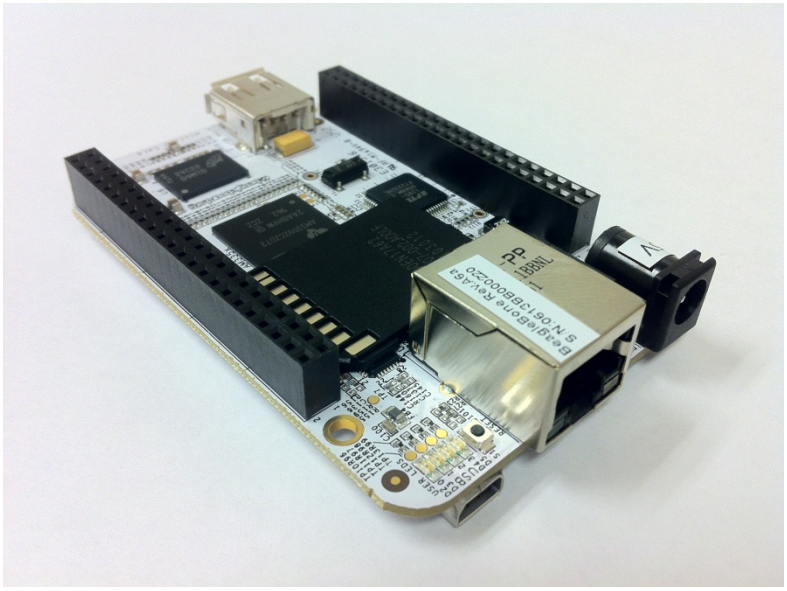

Figure 4: The BeagleBone Computer

All software is written in Java to support easy interface to available open-source libraries that support cryptography. As such, the EDAS prototype will support the selection of several NSA Suite-B cryptographic algorithms, such as the Advanced Encryption Standard (AES) for encryption and the public key Elliptic Curve Digital Signature Algorithm (ECDSA) for generating digital signatures.

To conform to data standards, the EDAS will output data that conforms to a format expected by the Remote Acquisition of Data and Review (RADAR) software package employed by the Euratom inspectorate for the automated acquisition of nuclear data [4]. The RADAR software will be hosted on an inspectorate computer connected to the EDAS via a network connection. As the EDAS pushes data to the inspectorate computer, a Data Acquisition Module (DAM), the entry point to RADAR, will automatically acquire, decrypt, and translate the data into a format understandable by the RADAR framework.

5. Testing and Field Trials

After completion of the EDAS prototype, we will perform a variety of tests to ensure it performs to functional requirements. The Joint Research Centre (JRC) in Italy will define and carry out specific tests consistent with the high-level test matrix detailed in Table 1. The tests by the JRC further will assure a European operator of acceptability for field trial deployment.

Table 1: EDAS Prototype: Test Matrix

Test Set	Purpose
Branch correctness	Verify that the inspector and operator branches produce identical data.
Normal operations	Verify that the EDAS perform as required against several operational use cases.
Failure scenarios	Verify that the EDAS never interferes with the operator signal line based on various failure scenarios.
Tamper scenarios	Verify that the operator and inspector data paths cannot be manipulated by the other party.

Once the JRC testing is has been satisfactorily completed, the Euratom safeguards inspectorate will work together with a facility in the United Kingdom to conduct a field trial of the EDAS prototype. We are planning an application that would share operator weight measurements of nuclear material cylinders. Two EDAS prototype units would be required. One branches the data from a weight scale; a second branches the data from an associated bar code reader used to identify the cylinders. The field trial will be an excellent opportunity to identify unexpected issues and better understand how EDAS could be most useful as a safeguards tool.

6. Conclusion

The EDAS is a secure branching concept that could provide complementary safeguards information to inspectors to create a more complete picture of facility activities. The design meets the requirements of both inspectors and facility operators. The upcoming testing and field trials of the EDAS prototypes will provide several opportunities to learn and further improve on the EDAS concept.

7. Acknowledgements

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000. Support to Sandia National Laboratories provided by the NNSA International Nuclear Safeguards and Engagement Program is gratefully acknowledged.

SAND2013-4036 C

8. References

[1] George Baldwin, et al; Secure Branching of Facility Instrumentation for Safeguards; American Nuclear Society / Institute of Nuclear Materials Management 9th International Conference on Facility Operations - Safeguards Interface; Savannah, Georgia, USA, September 23-28, 2012.

[2] João G.M. Gonçalves, et al; *Enhanced Data Authentication System (EDAS): Concept, Demonstration and Applications*; proceedings of the Institute of Nuclear Materials Management 52nd Annual Meeting, Palm Desert, California, July 2011.

[3] http://beagleboard.org/

[4] Andreas Smejkal, et al; *Improvements for Spent Fuel Verifications by Safeguards Inspectors*; proceedings of the Institute of Nuclear Materials Management 53rd Annual Meeting, Orlando, Florida, July 2012.