IAEA-CN-184/ 118

Verifiable Process Monitoring Through Enhanced Data Authentication

Troy Ross, Sandia National Laboratories, Albuquerque, New Mexico, USA
George Baldwin, Sandia National Laboratories, Albuquerque, New Mexico, USA
Barry Schoeneman, Sandia National Laboratories, Albuquerque, New Mexico, USA
João G.M. Gonçalves, European Commission Joint Research Centre, Ispra, Italy
Peter Schwalbach, European Commission Directorate General—Energy, Luxembourg

tdross@sandia.gov

To ensure the peaceful intent for production and processing of nuclear fuel, verifiable process monitoring of the fuel production cycle is required. As part of a U.S. Department of Energy (DOE)-EURATOM collaboration in the field of international nuclear safeguards, the DOE Sandia National Laboratories (SNL), the European Commission Joint Research Centre (JRC) and Directorate General-Energy (DG-ENER) developed and demonstrated a new concept in process monitoring, enabling the use of operator process information by branching a second, authenticated data stream to the Safeguards inspectorate. This information would be complementary to independent safeguards data, improving the understanding of the plant's operation. The concept is called the Enhanced Data Authentication System (EDAS). EDAS transparently captures, authenticates, and encrypts communication data that is transmitted between operator control computers and connected analytical equipment utilized in nuclear processes controls. The intent is to capture information as close to the sensor point as possible to assure the highest possible confidence in the branched data. Data must be collected transparently by the EDAS: Operator processes should not be altered or disrupted by the insertion of the EDAS as a monitoring system for safeguards. EDAS employs public key authentication providing `jointly verifiable' data and private key encryption for confidentiality. Timestamps and data source are also added to the collected data for analysis. The core of the system hardware is in a security enclosure with both active and passive tamper indication. Further, the system has the ability to monitor seals or other security devices in close proximity. This paper will discuss the EDAS concept, recent technical developments, intended application philosophy and the planned future progression of this system.

1. Intended Application Philosophy

The same equipment that is used for facility operations can be of interest also for safeguards purposes. Unfortunately equipment such as scales, pressure sensors, and gamma counters cannot currently be used to serve both purposes, because the data coming from these devices is not authenticated and therefore cannot be fully trusted by a safeguards inspectorate. Duplicate systems, separately owned and operated by the facility operator and inspectorate, would in principle solve the issue. However, these not only require additional resources and add to system complexity, duplication of sensors is also frequently impossible for limitations of space, operational safety considerations, accessibility issues etc...

EDAS addresses the problem by providing a second, authenticated branch of the data generated by monitoring equipment, as close as possible to the source of the data. EDAS will allow both the facility operator and safeguards inspectorates to use a single piece of analytical equipment to meet both of their monitoring requirements. For the operator, the signal coming from the equipment will be completely unaffected by EDAS and the operator will be able to use existing infrastructure without modification. The separate signal used by the safeguards inspectorate will indicate the source device of the data, be time-stamped, authenticated, and encrypted. The authentication mechanism used by EDAS employs symmetric key cryptography. All of these operations will occur in the closest proximity possible to the point where the actual measurements are taken.

2. EDAS Concept

The design goals of EDAS can be broken down into four fundamental principles: branch the data as close as possible to the source, do not interfere with data communications between the operator and the equipment, employ a modular design for ease of application, and enable both parties to be confident that the two branches provide identical information.

2.1. Source Proximity

Once a measurement is taken the data associated with the measurement has a binary representation that can easily be manipulated when transferred over communications lines. To ensure that this data is not altered it is ideal to begin protecting it at the soonest moment possible. Ideally EDAS would be running on the same microcontroller or DSP that acquires the data, but for the short term this is not possible within close proximity to the serial communications port is thus the chosen compromise. To retain the greatest amount of confidence in the measurement data the serial communications cable connecting the analytical equipment to EDAS should be as short as possible and protected using tamper sensing or indicating conduit [1].

2.2. Non-interference

The facility operator cannot risk any malfunction or misconfiguration of critical process monitoring equipment and the safeguard authorities cannot run a liability risk in case of malfunction. EDAS must be fail-safe, and cannot be capable of making any changes to the operator system. Just as important, it must be possible to convince an operator that EDAS is sufficiently low risk.

2.3. Modularity

EDAS is a concept--not a set of hardware or software; any system realization should be flexible enough to allow hardware implementations of subsystems to replace software implementation and vice versa. Modular design enables such flexibility. For example, a hardware-based cryptographic module could handle authentication and encryption rather than writing software. Modularity enables an upgrade of the currently implemented serial splitter to something more advanced, such as a data diode, without modification to the rest of the system.

2.4. Identical Information

EDAS is of no use if the data that it generates can be repudiated by either the facility operator or the inspectorate. For this reason public-key authentication is preferred: the operator would be able to verify the signature of data transmissions independently, and neither party can create measurement data that can be authenticated by the other party.

3. System Components

In order to support the greatest amount of existing equipment, EDAS currently can capture data from a variety of serial interfaces including RS-485 and RS-232 at several baud rates up to 1.152 kbps. Because data from different devices can arrive either in bursts or continuously, the data stream from a device can be divided into blocks based upon a set number of bytes, divided into transmission bursts based upon the delay between bursts, or some combination of a maximum number of bytes as well as a maximum delay between data bursts.

The authentication approach employed by EDAS uses asymmetric RSA cryptography by default. However, EDAS uses a pipelining mechanism to transfer bytes between various subsystems, so the authentication approach can be changed to symmetric or even one based upon a Hash Machine Authentication Code (HMAC) depending upon application. The encryption mechanism is currently based upon AES, but it can also be substituted with any other block cipher, as required.

Finally the subsystem that stores the data stream into files to be transferred over the network is also flexible enough to divide data by size or by date (e.g. to create day file)s. By design EDAS is implemented to be as straight forward as possible to facilitate integration into and implementation on various types of process monitoring equipment.

4. Recent Technical Achievements

A conceptual prototype of EDAS was demonstrated in April, 2010 at the European Commission Joint Research Centre, attended also by representatives from the IAEA. The hardware components of this system

consisted of a readily available PC104 computer and a serial communications splitting device that is commercially available. The primary EDAS software modules implemented data pipelining techniques that made it possible to optionally encrypt, authenticate and divide captured serial communications into various sized blocks. The PC104 system was programmed to demonstrate the real-time capture of serial data transmitted from a Mettler Toledo Mass Scale, a Mensor Pressure sensor, and a Sick laser range finder. The tests demonstrated the serial capture, authentication, encryption, and secure transmission features. Other software was written to interpret the inspectorate data stream coming from the EDAS system. The visualization readily confirmed that EDAS captured all of the serial communications of interest accurately.

5. Planned Future Progress of System

Since the EDAS system today is still in the experimental prototype phase, there are several areas that can be improved in the near term. The first improvement is to design a system board that completely isolates the EDAS serial capture from the operator serial pass through.

In this configuration, the serial capture module utilizes two input buffers that support high data rate requirements. The serial capture module is designed to allow transparent tapping of bi-directional digital data travelling between the analytical equipment and the operator processes. It utilizes active buffer-drivers that split digital signals without interference and provide those to the serial capture module and the respective intended destination. The serial capture module also incorporates a power-fail functionality that allows communication to continue uninterrupted, from the perspective of the operator, and provides an indication to the inspectorate that the state of the serial capture module communications has changed. This process occurs without the knowledge of the operator.

A second improvement will integrate tamper indicating functionality in the next EDAS prototype. These improvements are detailed in the included figure. EDAS will also incorporate tamper sensor monitoring for both internal and external sensors. The external tamper sensors will be applied to the analytical equipment as possible based upon the specific application.

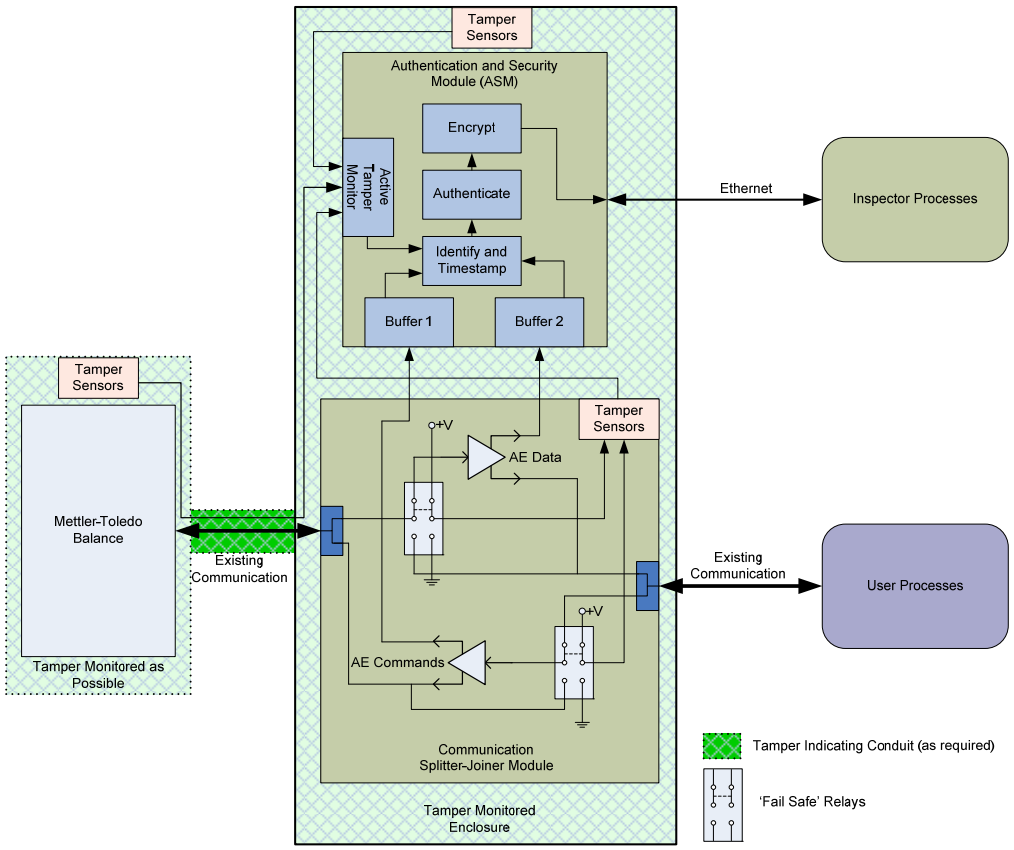

Figure 1 of the proposed concept for demonstrating Enhanced Data Authentication

Operator acceptance of an inspectorate branching capability is essential. Although EDAS already demonstrates the functionality required for the inspectorate to trust the duplicate data stream, it has not yet addressed operator concerns about reliability and non-interference. Not only must EDAS address those concerns, but it must also be possible to demonstrate its fail safe functionality, convincingly.

Finally it is the goal of EDAS to utilize knowledge gained from the near term activities to determine best approaches for the development of safeguards guidance policies and equipment requirements. Work with equipment manufacturers (e.g. Canberra, Honeywell analytical equipment) to provide support for authentication requirements at or near the sensor, whichever is most reasonable. It is envisioned that the verification techniques will gradually envelop the sensor points and the associated analytical equipment. Techniques will eventually add tamper indicating (active and passive) features as well as moving EDAS closer to the sensor points where practical.

6. Acknowledgments

Sandia is a multi-program laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy under contract DE-AC04-94AL85000.

References

[1] Keel, Frances, Chris Pickett, and Keith Tolk. "Conduit." Preliminary Results from the 2010 INMM International Containment and Surveillance Workshop. Proc. of 2010 INMM International Containment and Surveillance Workshop, Oak Ridge. INMM, July 2010. Web. Sept. 2010.