 https://doi.org/10.3011/ESARDA.IJNSNP.2017.12

Field Trial of the Enhanced Data Authentication System (EDAS)

M. Thomas, R. Hymel, G. Baldwin

Global Security Programs, Sandia National Laboratories
P.O. Box 5800
Albuquerque, NM 87185, USA
Email: mthomas@sandia.gov; gtbaldw@sandia.gov; rwhymel@sandia.gov

A. Smejkal, R. Linnebach

Nuclear Safeguards Directorate
European Commission Directorate-General for Energy
Luxembourg
andreas.smejkal@ec.europa.eu; ralf.linnebach@ec.europa.eu

Abstract:

The Enhanced Data Authentication System (EDAS) is a means to securely branch information from an existing measurement system or data stream to a secondary observer. In an international nuclear safeguards context, the EDAS connects to operator instrumentation, and provides a cryptographically secure copy of the information for a safeguards inspectorate. This novel capability could be a complement to inspector-owned safeguards instrumentation, offering context that is valuable for anomaly resolution and contingency.

Sandia National Laboratories gathered operator and inspector requirements, and designed, developed, and fabricated prototype EDAS software and hardware. In partnership with Euratom, we performed an extended EDAS field trial at the Westinghouse Springfields nuclear fuel manufacturing facility in the United Kingdom. We inserted EDAS prototypes in operator instrumentation lines for a barcode scanner and weight scale at a portal where UF_6 *cylinders enter and exit the facility. The goal of the field trial was to demonstrate the utility of secure branching of operator instrumentation for nuclear safeguards, identify any unforeseen implementation and application issues, and confirm whether the approach is compatible with operator concerns and constraints.*

During the field trial, the data streams were collected for nine months, and the EDASs branched 698 barcode and 663 weight scale events. Our analysis found that both EDAS units accurately branched 100% of the data that flowed through the instrumentation lines when we compared them to the recorded operator data. With multiple deployed EDASs we found that it is possible to correlate the branched data and create a more holistic narrative of facility activities. Euratom reported the field trial as a full success due to the continuous, correct, and secure branching of safeguards relevant data. At the same time, the operator is satisfied that EDAS did not interfere with plant operations in any way. The success of this field trial is an important step toward illustrating the potential and utility of EDAS as a safeguards tool.

Keywords: secure branching; data collection, field trial; operator instrumentation; unattended monitoring; minimally intrusive

1. Introduction

EDAS is a means to securely branch information from an existing measurement system or data stream to a secondary observer, as illustrated in Figure 1. An EDAS junction box creates a “branch” of the main communication path data and transmits the replicated data to the secondary observer from a tap-off point close to the measurement system sensor. In an international nuclear safeguards deployment, the primary observer represents the facility operator system while the secondary observer is the safeguards inspectorate system. The EDAS junction box connects to the output of existing operator instrumentation and sends a copy of the information to the safeguards inspectorate EDAS computer. The junction box cryptographically secures the branched data using encryption for confidentiality and authentication to provide data integrity. This branching capability could be a complement to inspector-owned safeguards instrumentation, offering context that is valuable for anomaly resolution and contingency.

The EDAS development project is a collaborative effort between the U.S. DOE Sandia National Laboratories in the United States, the European Commission Directorate General for Energy (DG-ENER) in Luxembourg, and the European Commission Joint Research Centre (JRC) in Italy. The original project began in May 2008 under the auspices of a DOE-Euratom agreement[1] as Action Sheet (AS) 32,

[1] “Agreement between the European Atomic Energy Community represented by the Commission of the European Communities and the United States Department of Energy in the field of Nuclear Material Safeguards Research and Development,” 6 Jan 1995. That agreement was superseded in November 2010 with one of expanded scope, “Agreement between the European Atomic Energy Community represented by the European Commission and the United States Department of Energy in the field of Nuclear Material Safeguards and Security Research and Development.”

Thomas, M., Hymel, R., Baldwin, G., Smejkal, A., & Linnebach, R. (2017). Field Trial of the Enhanced Data Authentication System (EDAS). *ESARDA Bulletin - The International Journal of Nuclear Safeguards and Non-proliferation*, 54, 88-96. https://doi.org/10.3011/ ESARDA.IJNSNP.2017.12

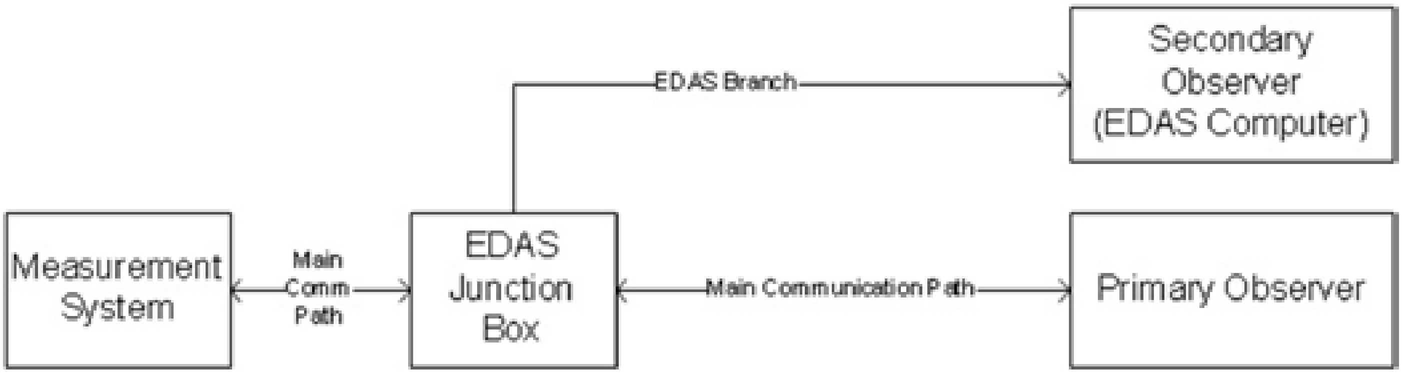

Figure 1: EDAS Branching Diagram

"Enhanced Data Authenticity via an Electronics Platform for the Secure Transmission and Recording of Sensors." That work focused on the inspector requirements for secure branching. The project team designed, built and demonstrated an initial prototype of EDAS to key stakeholders [1]. The project continued under AS 41, "Application of the Enhanced Data Authentication System to Operator Instrumentation." In this second phase, we adapted the concept to meet operator requirements as well; that is, to ensure that EDAS is non-interfering to facility operations, fail-safe, and conforms to instrumentation interface standards [2, 3]. Sandia incorporated the combined inspector and operator requirements into redesigned hardware and software for EDAS [4]. The new prototypes have been tested extensively, culminating in an extended field trial at an operational nuclear facility subject to Euratom safeguards [5].

The goal of the EDAS field trial was to demonstrate the utility of secure branching of operator instrumentation for nuclear safeguards, identify any unforeseen implementation and application issues, and confirm whether the approach is compatible with operator concerns and constraints. Euratom arranged to conduct the field trial at the Westinghouse Springfields nuclear fuel manufacturing facility in Lancashire, United Kingdom. We inserted EDAS junction boxes in two operator instrumentation lines, a barcode scanner and a weight scale, at a portal where Model 30B UF_6 cylinders enter (full) and exit (empty) the facility. Data collection occurred for approximately nine months, from March through November 2015. The branched data transmitted continuously to an inspector computer and was collected by the Euratom Remote Acquisition of Data and Review (RADAR) [6] data acquisition software for subsequent analysis by inspectors.

2. EDAS Prototypes

Sandia designed, developed, and manufactured prototype EDAS software and hardware to meet both operator and inspector requirements, incorporating commercial off-the-shelf (COTS) and custom hardware, as well as open source and custom software. The EDAS junction box features a modular design, which separates its general branching functionality from that which is specific to a particular instrumentation interface. The junction box prototypes interface to the operator main communication path via standard 9-pin RS232 serial, which matches the field trial barcode scanner and weight scale interfaces. The branched data is sent from the junction box to the inspector (EDAS computer) via a RJ45 Ethernet interface and, when employing network extenders, there is no practical distance limit, allowing for a variety of installation configurations. Figure 2 is a picture of the EDAS junction box, which is approximately 9.5 x 6.3 x 4.0 cm. Power is supplied either via a barrel adapter or USB.

The EDAS junction box employs a low-cost commercial BeagleBone™ Black embedded processor and a custom accessory board, called a "cape," that is mounted on top of the BeagleBone™ Black board. The Sandia-developed cape is interface-specific; it performs the branching function for both the "transmit" and "receive" signals in the RS-232 serial specification. Figure 3 is a picture of the EDAS cape inside the case. It links the primary instrumentation signal path between the in and out serial connectors, and includes sensing electronics to generate an isolated copy of the signal. The isolation acts as a diode and

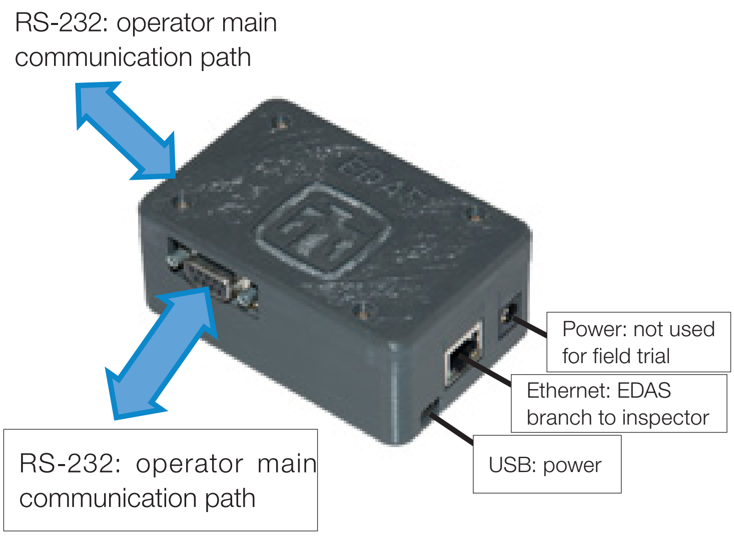

Figure 2: The EDAS Junction Box

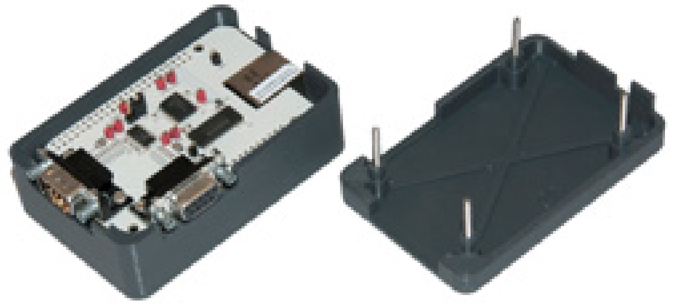

Figure 3: EDAS Cape (the white-colored board with mounted electronics)

prevents any information from the inspector being introduced onto the operator main communication path. DB-9 serial connectors on the cape use different genders, so that the primary instrumentation cables could be disconnected from the EDAS junction box and mated directly to each other, should the operator have a reason to bypass the EDAS entirely.

The EDAS uses a streamlined version of Linux, created for embedded systems, called Yocto. We eliminated any functionality from the operating system not needed by EDAS by removing software functions that may consume processor and memory resources. We also made the EDAS junction box more secure by disabling access to ports not used for normal operation (e.g., FTP).

The custom firmware directs the embedded processor to collect and buffer all branched data from the main instrumentation signal path. The data are then compiled into discrete packets; digitally signed using a public key cryptographic algorithm; encrypted; and finally pushed over an Ethernet connection to the inspector computer. The firmware also periodically creates and sends state of health "heartbeat" messages to confirm that EDAS is operating normally. The inspector computer runs custom software that receives and decrypts the EDAS packets, verifies their authenticity, and writes the data to an output file for post-processing and analysis.

3. RADAR Integration

The EDAS junction box has no *a priori* understanding of, or expectation for, the meaning of the data it branches. Rather, it forms data into packets based on preset configuration settings and sends each via TCP/IP over Ethernet to the inspector computer. The EDAS inspector computer software receives all EDAS packets from the EDAS branch and writes these to a log file. In order for these EDAS packets to be interpreted equivalently for the facility operator and inspector, we used the Remote Acquisition of Data and Review (RADAR) software package.

RADAR, developed by Euratom, is a modular and standardized software platform for data acquisition from different sensors. Typical sensors (e.g., shift registers or multi-channel analyzers) are configured and operated by RADAR Data Acquisition Modules (DAM). In order to use EDAS field trail data in the RADAR framework, EDAS DAMs were developed for both the field trial barcode scanner and weight scale. The EDAS DAMs are fully integrated into the RADAR system like other, already existing, DAMs.

Euratom configured and activated the EDAS modules to derive meaning from the barcode and weight scale branched bytes so that they are identically interpretable for the inspector and the facility operator. During the field trial, the inspector computer continually ran the EDAS RADAR software modules, which scanned the EDAS log files for new records. The modules converted the branched signals into event records containing a time stamp, the scanned barcode ID or weight measurement, and cryptographic authentication status.

The development of the RADAR EDAS modules represents an important phase of the collaboration between Euratom and Sandia. Sandia shipped several EDAS junction boxes and software to Euratom headquarters in Luxembourg where EDAS RADAR software modules were developed and tested in a test bed using representative field trial equipment and simulators. EDAS integration with RADAR greatly facilitated our ability to analyze data from the field trial because much of the analysis involved the comparison of operator records to the interpreted barcode and weight scale records in the RADAR files. With development of the field trial RADAR EDAS modules complete, it would be simple to develop new EDAS modules for RADAR to support branching signals from other types of instrumentation.

A further benefit is that RADAR converts EDAS data to a standard format that can be analyzed by an automated review and analysis tool, such as the integrated Review & Analysis Platform (iRAP). iRAP, originally developed by Euratom, has been made available to the International Atomic Energy Agency (IAEA), and is now the subject of a software collaboration between both organizations. Under a license agreement between the IAEA and EURATOM, iRAP will be developed jointly towards an "all-in-one review platform." [7]

4. Field Trial Setup

The field trial took place at a UF_6 cylinder portal at the Springfields nuclear fuel manufacturing facility. During operations, full Model 30B cylinders enter the portal staging area one at a time and are placed on a scale. Per the facility procedure, an operator must scan the cylinder identification number with a barcode scanner and measure its weight. These two operations can happen in either order. To measure a weight, an operator must enter a command into the operator system, which triggers three consecutive weight commands. The operator weight scale control unit subsequently sends three successive weight measurements, in kilograms, to the operator system. The operator system then averages these three weights, which becomes the final weight measurement record. Both the barcode scan and weight scale measurements are recorded in an operator log file. The cylinder then enters the facility for processing. After processing, the cylinder reenters the portal and its identification number and weight measurement are recorded. The empty cylinder then leaves the facility. For the field trial, EDAS junction boxes formed branch points in the barcode scanner and weight scale communication lines.

In early March 2015, the Sandia EDAS developers, Euratom inspectors, and operator representatives met at the Springfields facility to install the EDAS system and commence the field trial. The Sandia team installed, configured, and initialized the EDAS prototypes. Euratom provided the inspector computer to acquire the field trial data, and configured and activated the EDAS inspector computer software and RADAR EDAS DAMs. The Springfields operator installed a lockable custom cabinet, pictured in Figure 4, to house both the EDAS junction boxes and the inspector computer. The cabinet was fitted with feedthrough connectors for both signal and power lines.

The EDAS was configured for a standard 9-pin RS-232 interface for the barcode scanner, but we discovered during the installation visit that the installed barcode scanner used a pen interface. The operator promptly replaced that barcode scanner with a new one that uses a 25-pin interface. To obtain the correct signal on the EDAS, the operator installed a Datalogic CBX800 adapter, shown in Figure 5, in the signal line between the barcode scanner and operator system. It is important to note that the Datalogic adapter split the barcode signal, with one portion going to the operator system and the other to the barcode EDAS. In other words, the EDAS received data that was already branched by the CBX800 adapter.

The operator classified the continuous and direct output from the scale as part of the facility safety system; branching here would have required a prohibitively long and uncertain approval process. Therefore, the EDAS branch point for the weight scale was installed at the output of the control unit for the scale, not at the scale itself. The control unit was a Mettler Toledo model IND690 weighing terminal. EDAS, therefore, did not sense weight continuously. Both the operator and EDAS received weight data only when the facility instrumentation control system triggered the IND690 to send a reading.

Figure 6 shows the installed EDAS junction boxes and the Euratom inspector computer. The inspector computer was a ruggedized Windows computer with several redundant

Figure 5: Datalogic CBX800 adapter that split the barcode scanner communication path

Figure 4: EDAS Cabinet provided by the Operator

Figure 6: EDAS System installed in operator cabinet, showing the Euratom computer (left), network switch (middle), and two EDAS branching units (right)

components for increased reliability. A switch directed EDAS network traffic between the EDAS junction boxes and inspector computer. We verified the successful branching of several facility barcode and weight events over several days before the system ran unattended for the duration of the field trial.

5. Field Trial Analysis

The field trial collected data for nine months, between March 5, 2015 and November 26, 2015. EDAS data were collected by RADAR on the installed inspector computer, and Euratom inspectors retrieved the complete datasets on November 26 when the field trial system was decommissioned. Euratom obtained a separate transcript from the Springfields operator of timestamped system logs of barcode and weight scale data over the same period. Sandia analyzed these data using custom analysis software to compare and correlate the data.

In order to gauge the success of the EDAS field trial against our original goals, we posed the following questions:

- Did each EDAS operate continuously for the field trial duration?
- Do the EDAS and operator barcode scanner and weight datasets match? Did the EDAS miss any events with respect to the operator? Did the EDAS capture any events not contained in the operator logs?
- For every barcode scan is there a corresponding weight measurement, and does every weight measurement have an associated barcode scan?
- Are all weight scale data preceded by associated “send weight” commands? Conversely, is any command missing a weight scale response?
- Were other anomalies discovered?

The field trial analysis specifically addresses these questions, and the following sections report the results of the analysis. Additional interpretation is deferred to the Discussion section.

5.1 Analysis Methodology

We wrote software to automate the analysis of the field trial data. The software was coded to apply several rules and assumptions that define the continuous operation of EDAS, correct format of a record, and tolerances for expected differences between the EDAS and operator system data. The following are the rules and assumptions we used for the field trial analysis:

- The barcode scanner EDAS junction box will hereafter be referred to as “EDAS-B.”
- The weight scale EDAS junction box will hereafter be referred to as “EDAS-W.”
- A barcode ID is an alphanumeric string.
- A weight sent by the Mettler-Toledo IND690 is measured in kilograms and has two digits of precision after the decimal point.
- A weight scale command is considered valid if it matches the Mettler-Toledo IND690 control sequence: S<CR><LF><ACK>. Note that any variations are flagged as anomalies.
- Packets sent from the EDAS junction box to the inspector computer are digitally signed and encrypted. For a received packet to be classified as authentic, the packet must correctly decrypt and authenticate.
- To prove that the EDAS junction boxes were continuously operating, we configured them to periodically send heartbeat messages, and expected to observe contiguous heartbeat messages at a rate of at least once every two minutes.
- For comparing the EDAS-B and operator barcode data, a match is recorded when the values are identical AND occur within four minutes of each other.
- For comparing the EDAS-W and operator weight scale data, a match is recorded if the values vary by less than 0.1 kg AND occur within four minutes of each other. Note that slight precision differences in measurement values are expected since three weight values are averaged independently by the operator and the RADAR EDAS weight scale module on the inspector computer.
- Per the operator’s cylinder entry/exit procedure, we expect the barcode scan and weight scale measurements for a cylinder to occur within one minute of each other.
- An operator weight command to the IND690 (weight scale terminal) immediately and automatically triggers a weight measurement. We create an association if a weight command precedes a weight measurement AND the timestamps are within two seconds of each other. Note that this analysis is only possible with EDAS data because the operator does not keep a record of commands in the operator system logs.

Note that all selected time thresholds to compare values are heuristics selected by the authors. These values were selected via analysis of the data as they afforded enough flexibility to identify all true matches. At the same time, the chosen thresholds had a tight enough tolerance to not conflate incorrect events. In the case of EDAS heartbeat messages, we selected a two-minute threshold as sufficiently frequent to prove the junction boxes were continuously operating. When comparing EDAS junction box and operator barcode or weight scale data, we selected a four-minute threshold to account for observed clock drift over the course of the field trial between the operator and EDAS systems. This value allowed our analysis to identify all true positives while eliminating the possibility of incorrect matches since containers are processed at the portal at a much slower rate.

5.2 Test for Continuous EDAS Operation

Both the EDAS-B and EDAS-W units operated continuously for the nine-month duration of the field trial. To assess continuous operation, we first checked that there were no interruptions in heartbeat messages from either EDAS junction box. There was no time during the field trial where more than two minutes passed between these messages. We also searched the inspector computer log files for evidence of a network disconnect between an EDAS junction box and the inspector computer. The only recorded instance of establishing a network connection was the initial connection at the beginning of the field trial.

5.3 Test for EDAS and Operator Dataset Equality

Our analysis software compared the EDAS measurements collected by RADAR with the operator system data files to check whether either of the EDAS junction boxes missed any records captured by the operator system. A match of a barcode or weight is determined according to rules set in the Analysis Methodology section. A discrepancy, or difference, is any deviation from the above conditions, or any missing or additional EDAS data with respect to the operator system. Table 1 illustrates the total number of barcode and weight data points analyzed for the field trial.

Measurement Type	Operator	Operator Manual Bypass	EDAS
Barcode Scanner	705	7	698
Weight Scale	664	1	663

Table 1: Total Barcode and Weight Events. Some operator barcode and weight data were manually entered into the system, effectively bypassing the EDAS.

EDAS-B did not branch seven events of the 705 found in the operator log files over the course of the field trial. These events transpired on four different occasions spread over the field trial duration. After speaking with the facility operator, we determined that these seven anomalous events were manually entered into the operator system because the cylinder label was damaged, and was unreadable by the barcode scanner. In other words, the operator bypassed EDAS-B since the barcode scanner was not used for these seven events. Of the 664 operator weight events, we identified one additional empty weight measurement of 0.0 kg in the operator log file that does not show up in the EDAS-W data. The operator determined that this anomalous weight entry is an artifact created by their control system when initially powering the IND690, and is not generated by the scale itself. Since this data did not derive from the scale or travel along the weight scale instrumentation line, it was not branched by EDAS-W. In summary, both EDAS-B and EDAS-W correctly branched 100% of events that passed through each instrumentation line from the measurement device.

We also compared the EDAS measurements collected by RADAR with the operator system data files to check whether either EDAS-B or EDAS-W observed any measurements not recorded by the operator system. Our analysis found that of the 698 and 663 events recorded by each junction box, there was a 100% match with the operator files, indicating that each EDAS junction box did not branch any extra events not reported by the operator.

5.4 Test for Barcode / Weight Correlation

Since each cylinder must have both its barcode scanned and weight measured when entering or exiting, we looked for correlation between these events captured by EDAS-B and EDAS-W. Of the 698 barcode and 663 weight events, 654 of them correlated. This leaves 44 bar code scans that did not have associated weight data. Further analysis discovered several reasons for these discrepancies: (1) operator scanning a test pattern rather than a cylinder barcode, (2) inadvertently scanning the same barcode identification number multiple times in rapid succession, or (3) accidentally scanning a barcode on a UF_6 cylinder intended for autoclave processing (i.e., not the portal). Note that for this last case, a second barcode scanner, connected to a different operator system, scans the cylinder identification number for subsequent processing in the autoclave. There were nine instances of weight data without corresponding barcode scans. As discussed earlier, many of these discrepancies are attributable to the seven barcode identification numbers that were manually entered by the operator, and not branched by EDAS-B. The remainder consist of weights that are outside the range expected for a UF_6 cylinder in that they are less than the typical tare weight. The operator confirmed that these extra weight events were for scale testing purposes.

We also analyzed the operator records for correlation between barcode and weight data events, and found the discrepancies to be the same as the EDAS data. There were 705 barcode and 664 weight events from the operator record. We would initially expect the discrepancies between the operator and EDAS records to match. However, when backing out the seven manual barcode scan entries, where EDAS-B was bypassed, and the single empty weight entry, where EDAS-W was bypassed, we measure 698 barcode and 663 weight events, and found that 654 of them correlated, identical to the EDAS data.

5.5 Test for Weight Command / Data Correlation

Of the 663 weight readings branched by EDAS-W, 100% were correlated to a weight command that immediately preceded the event. We did not perform this test on the operator data since commands are not included in their log files. Also note that this analysis does not apply to the barcode scanner data, since a human operator must squeeze the barcode scanner trigger to command the device; so, there is no command signal for EDAS-W to branch.

5.6 Test for Other Anomalies

During field trial setup, it became clear that the EDAS junction box electronics do not keep time well. The BeagleBone™ Black has an inaccurate system clock. For this reason, we relied instead on the inspector computer time: the inspector computer affixes its own timestamp to each EDAS message it receives. However, even using this timestamp in lieu of the EDAS timestamp was not without issues. We observed a dozen occasions when the inspector computer timestamps on successive EDAS heartbeat messages were spaced only a few seconds apart, rather than the configured separation of once per minute. We believe that these heartbeat messages, sent by the EDAS junction box, were queued while the inspector computer was otherwise busy and unable to process them, causing a backlog of messages. At a later point, the inspector computer processed them in rapid succession, resulting in a cluster of closely spaced timestamps for these messages. Analyzing the EDAS timestamps, even though incorrect in an absolute sense, revealed they were sufficiently accurate on smaller timescales to confirm that the heartbeat messages were generated at the expected frequency.

Another issue was the assignment of the local time zone to the timestamped EDAS data packets. Two daylight savings transitions occurred during the course of the field trial, causing timestamps to suddenly skip or move backwards an hour. An appropriate time correction factor was applied to the analysis software to rectify this issue for data analysis.

6. Discussion

The field trial analysis has shown that EDAS and the inspector computer operated continuously and correctly over the nine-month duration of the field trial, showing that EDAS can run unattended in an operational nuclear facility for long periods of time. There was never an interruption in heartbeat messages in either EDAS-B or EDAS-W, and no network connectivity issues or errors occurred in the log files. In addition, the data were secure in that they were free of decryption and authentication errors, which satisfies the inspector requirements for the data being both confidential and trustworthy, respectively, from the branch point forward. Further, it is noteworthy that the RADAR EDAS modules ran continually for the entire field trial without any data interpretation issues or interruption.

EDAS correctly branched 698 barcode scanner and 663 weight scale events over the course of the field trial without interfering with the operator system. It is notable that neither EDAS junction box recorded any events that were absent from the operator system. Also, neither EDAS missed any unexplained barcode or weight scale events when compared to the operator record. While the operator did manually bypass EDAS-B several times, both junction boxes branched 100% of the data that flowed through each for the entire field trial duration. The cases where the operator manually bypassed EDAS-B, due to damaged cylinder labels, highlights a tenet of the EDAS non-interference requirement and illustrates one reason a facility operator might bypass a junction box, without much affecting the overall safeguards narrative.

With multiple EDASs installed in a facility, there are other first-order analyses that can correlate data to look for consistency. When a UF_6 cylinder enters or exits the facility, one would expect the cylinder to be both barcode scanned and weighed at approximately the same time. Yet comparing barcode scans to weights between the EDAS junction boxes showed over 40 discrepancies. As discussed earlier, all of these differences can be explained by operator tests and errors in procedure. In other words, correlation between barcode and weight scale data is not possible for these artifacts since they are not attributable to an actual cylinder entry or exit measurement. The operator barcode and weight log file data were also compared, and the discrepancies matched those of the analysis between the EDASs, showing equivalency in narratives between both systems.

Another analysis found 100% correlation of EDAS weight commands and data, which proves that, in every case, a command immediately preceded a weight measurement. More generally, the installation of multiple EDASs independently observing various aspects of a process can increase context for the safeguards inspector to draw conclusions on declarations since they can correlate more data streams to confirm agreement in the data. The ability to check data consistency across multiple EDASs makes undeclared operations on a process more complex and difficult to perform without detection.

The decision to build a lockable custom cabinet to house the field trial equipment affected setup and installation. While such a cabinet is advantageous for an inspectorate to house the inspector computer, there are downsides to placing the EDAS junction boxes inside. For one, it makes it difficult for the small form-factor EDAS junction box to be installed as close to an instrumentation sensor as possible. In addition, the pass through connectors, built into the cabinet wall, add more capacitance to the instrumentation signal path, which will affect data transmission and integrity for both the operator and inspectorate. Another point is that the operator created an external bypass path at the connectors of the cabinet itself, foregoing the bypass option designed into the EDAS junction box.

The field trial exposed several issues with timing. The built-in EDAS clock, included with the BeagleBone™ processor, is not very accurate and resets to a default value if it loses power. A low-cost, high-accuracy, real-time clock with battery backup can be added to future versions of the EDAS junction box to fix the problem. It is also essential to standardize the time zone used by the EDAS and inspector computer, irrespective of installation location. A universal time zone such as UTC (Coordinated Universal Time), which does not observe daylight savings transitions, is recommended. Clock drift between EDAS and the operator system is another important concern for the future since the inspector does not have the ability to regulate time on the operator system. The time drift between these systems is an issue that could impact event correlation and should be given further consideration.

More sophisticated field trial analyses could yield patterns of facility operations for the branched instrumentation by correlating multiple measurements over time. For this field trial, it may be possible to calculate the net weight difference of cylinders, get a sense of the residence time of each cylinder within the facility, and the direction of cylinder movement. Such data can yield an indication of uranium hexafluoride mass processed at the facility per unit time as well as how many and which cylinders are currently inside the facility, or were recently processed and shipped. The types of patterns extracted by an EDAS installation can be extrapolated to other areas of the nuclear fuel cycle.

7. Conclusions

Euratom reported the field trial as a full success due to the continuous, correct, and secure branching of safeguards-relevant data. More generally, it is advantageous that EDAS allows the use of existing operator instrumentation to collect operator-owned instrumentation data. The EDAS supports various installation configurations and could branch data from a wide array of instruments used for nuclear safeguards in different parts of the fuel cycle, such as monitoring material flow in nuclear facilities by branching operator-owned NDA instruments in material balance areas. An overview of nuclear safeguards instrumentation can be found here [8]. Another point is that EDAS could reduce cost by decreasing the installation of redundant safeguards instrumentation in facilities. Such duplicate equipment uses facility real estate and can decrease facility throughput (e.g., the extra time to weigh a UF_6 cylinder on both operator- and inspector-owned weight scales).

Any field trial at a facility can represent a challenge for an operator, due to potential interference with standard operations and additional work required to establish an acceptable solution that complies with the plant operational and safety systems. The installation of the EDAS junction boxes and the associated Euratom computer was completed relatively easily. The main observation from the operator is that the EDAS system was, in effect, invisible to plant operations. That is, there were no instances of interference with use or operation of the weight scale, barcode scanner, or associated operator systems.

There are several field trial takeaways that can be integrated into a future version of EDAS. These include incorporating better time keeping with a battery backup, and using a universal time zone to timestamp data. The junction box RS232 serial interface is compatible with a significant portion of legacy instrumentation. For broader interface compatibility we recommend that future EDAS hardware be compatible with 25-pin RS-232 (e.g., a standard 25- to 9-pin adapter), and potentially other instrumentation interfaces, such as USB or Ethernet. In addition, a tamper indicating enclosure is a recommended addition to protect the EDAS cryptographic keys.

The EDAS junction box should be installed as close to the sensor as possible as the data is cryptographically confidential and authentic starting from the tap-off point until it reaches the inspector computer. Since the data between the sensor and junction box are unsecured, it is important that EDAS is deployed as part of a comprehensive safeguards solution. For example, tamper indicating conduit could be installed to secure the sensor to junction box communication path and/or surveillance could be used to monitor the instrumentation. Looking forward, the safeguards community could work with manufacturers to integrate EDAS directly into the sensors of new instrumentation.

The success of the EDAS field trial is a critical step in addressing the IAEA Long Term R&D plan item 7.1, “Develop minimally intrusive techniques that are both secure and authenticated to enable the use of operator’s systems, instruments and process monitoring for cost effective safeguards implementation.” EDAS is a useful tool for the nuclear safeguards inspection community to securely monitor processes using operator instrumentation without undue burden on the facility operator — not to mention reducing the burden on IAEA’s budget for new unattended monitoring systems. More generally, EDAS could be a useful tool in other areas where a secondary observer has the need to monitor a measurement system or data stream.

8. Acknowledgments

This field trial represents work performed under Action Sheet 41 for the U.S. DOE – Euratom collaboration sponsored by the NNSA International Nuclear Safeguards Engagement Program (INSEP). The EDAS collaboration comprises Sandia National Laboratories in the United States, the European Commission Directorate General for Energy (DG-ENER) in Luxembourg, and the European Commission Joint Research Centre (JRC) in Italy. We wish to acknowledge the participation of the Westinghouse Springfields nuclear fuel manufacturing facility in Lancashire, United Kingdom, for providing the operational facility for the EDAS field trial.

Sandia National Laboratories is a multi-mission laboratory managed and operated by National Technology and Engineering Solutions of Sandia LLC, a wholly owned subsidiary of Honeywell International Inc. for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

SAND2016-11899 J

9. References

[1] 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 CA, July 2011.

[2] George Baldwin, et al; *Secure Branching of Facility Instrumentation for Safeguards*; American Nuclear Society 9th International Conference on Facility Operations – Safeguards Interface, Savannah, Georgia, September 2012.

[3] Maikael Thomas, et al; *Enhanced Data Authentication System: Converting Requirements to a Functional Prototype*; proceedings of the European Safeguards Research & Development Association 35th Annual Meeting, Bruges, Belgium, May 2013.

[4] Maikael Thomas, et al; *Prototype Hardware and Software for the Secure Branching of Facility Instrumentation*; proceedings of the Institute of Nuclear Materials Management 55th Annual Meeting, Atlanta, Georgia, July 2014.

[5] Maikael Thomas, et al; *Testing the Enhanced Data Authentication System (EDAS)*; proceedings of the International Atomic Energy Agency Symposium on International Safeguards: Linking Strategy, Implementation, and People, Vienna, Austria, October 2014.

[6] P. Schwalbach, et al; *RADAR and CRISP - Standard tools of the European Commission for remote and unattended data acquisition and analysis for nuclear safeguards;* proceedings of the International Atomic Energy Agency Symposium on International Safeguards, Vienna, Austria, 2006.

[7] A. Smejkal, et al; *Automated processing of safeguards data: Perspectives on software requirements for a future "All-in-one Review Platform" based on iRAP*, 37th ESARDA Symposium, Manchester, England, 2015.

[8] *Safeguards Techniques and Equipment: 2011 Edition*, International Nuclear Verification Series No. 1 (Rev. 2), International Atomic Energy Agency, Vienna, Austria, 2011.