SAND2014-17722C

Testing the Enhanced Data Authentication System (EDAS)

Maikael Thomas[a], G. Baldwin[a], J.G.M. Gonçalves[c], A. Smejkal[b], R. Hymel[a], R. Linnebach[b], L. Dechamp[c], S. Johnson[d], M. Rue[b]

[a] Sandia National Laboratories
Albuquerque, NM USA
[b] European Commission Directorate-General for Energy
Luxembourg
[c] European Commission Joint Research Centre
Ispra, Italy
[d] Westinghouse Springfields
Preston, UK

Corresponding author email: mthomas@sandia.gov

Abstract. The Enhanced Data Authentication System (EDAS) is a secure branching concept that provides to a safeguards inspectorate a copy of measurement data from operator instrumentation. Both safeguards inspector and facility operator requirements for secure branching have been established in previous work. These dictated the design and development of EDAS hardware and software. This paper presents the test plan for the EDAS prototypes, which need to demonstrate performance against the identified requirements.

Sandia National Laboratories (SNL), Directorate-General for Energy (DG-Energy) in Luxembourg, and the Joint Research Centre (JRC) in Ispra will each perform different tests on the EDAS prototypes. Sandia, the developer, will perform comprehensive testing of functionality, robustness, and reliability. The JRC, as an independent technical organization, will evaluate electrical safety and other environmental factors important to facility operator acceptance. The JRC is also able to simulate field trial conditions using equipment similar to what will be used in the field trial. DG-Energy will confirm the Sandia tests and also test the interface of the EDAS prototype to the RADAR data acquisition and analysis system used by the Euratom inspectorate.

The EDAS prototypes will be tested in a comprehensive field trial at the Westinghouse Springfields facility in a collaboration between Euratom inspectors and the facility operator. The field trial will support barcode and weight measurements taken related to the movements of nuclear material items entering and exiting the facility. One EDAS prototype will branch barcode scanner data, while the other will branch facility weight scale data. The branched data will be sent securely to an inspector computer, accessible to a Euratom inspector for data analysis. The field trial will test operational factors and environmental conditions. A critical outcome will be to ascertain whether the inspectorate gains an accurate picture of the facility operation via the branched information channel.

1. INTRODUCTION

Many nuclear facilities are not optimized for safeguards implementation. The Enhanced Data Authentication System (EDAS) is a secure branching concept that seeks to complement safeguards verification measurements in facilities in a low-cost manner. It can be connected to an operator instrumentation signal line, preferably as close to the sensor as possible. The EDAS provides a safeguards inspectorate with a secure copy of measurement and control data, while guaranteeing not to interfere with the operator instrumentation signal line in any way. In previous work, we have established both safeguards inspector and facility operator requirements for secure branching [1].

These requirements have dictated the design and development of EDAS hardware and software, and have culminated in prototype units. This paper discusses the testing for these prototypes, which must demonstrate performance against the identified requirements. The EDAS collaborators Sandia National Laboratories (SNL), Directorate-General for Energy (DG-Energy) in Luxembourg, and the Joint Research Centre (JRC) in Ispra have each performed and participated in different tests of the EDAS prototypes. The testing is divided in two phases: 1) EDAS prototypes requirements and integration testing and 2) a medium-duration field trial of EDAS prototypes at the Springfields nuclear fuel fabrication facility in the United Kingdom.

2. REQUIREMENTS FOR TESTING

The overall goal of EDAS prototype testing is to ensure it meets both the operator and inspector requirements and is ready for the field trial. To give context to the testing, a summary of the operator and inspector requirements are given in Table 1 and Table 2.

Table 1: Operator Requirements for EDAS

Requirement	Explanation
Noninterfering	During operations, the inspector branch cannot interfere in any way with the signal line between the sensor and the rest of the operator's instrumentation.
Fail-safe	If the inspector branch should fail (e.g., EDAS loses power), the operator's signal line must not be affected in any way.
Benign	An inspector must 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. EDAS must be able to branch from these standards.
Provided with Bypass Option	The operator must be able to physically bypass the inspector branch point if and when desired, for any reason.

Table 2: Inspector Requirements for EDAS

Requirement	Explanation
Accurate	The branched data is identical, on a byte-for-byte basis, to the information passed to the operator by the primary signal line.
Complete	All of the information passed in the signal line between the sensor and the operator must be branched, even if the information is bi-directional.
Authentic	The branched data cannot be tampered with in any way—whether by unintentional interference, loss of integrity, or deliberate manipulation.
Meaningful	The branched data stream of bytes is meaningless out of context. An inspector needs to be able to interpret the data stream in the same way that the operator does.

Confidential	The branched data must be communicated confidentially, preventing third parties from eavesdropping.

3. SYSTEM AND INTEGRATION TESTING

The EDAS prototypes have undergone a multiple-month period of system and integration testing as part of the first testing phase. Each of the EDAS collaborators has performed different aspects of this testing. Many of the tests described in this paper are derived directly from the inspector and operator requirements. The testing also focuses on longevity, robustness, electrical safety, and integration of the EDAS prototype into a larger system.

3.1. Requirements, Robustness, and Stress Testing

The majority of inspector and operator requirement testing was performed at SNL. SNL created the EDAS Data Simulator software to simulate representative operator instrumentation and control computer data to an EDAS prototype. Data sent out by the simulator can be configured at a variety of baud rates (from 300 to 115,200 bits per second) and simulate a variety of instrumentation data patterns (i.e., bursts or continuously) and operational scenarios.

A test matrix, shown below in Table 3, was created to ensure all requirements, robustness, and longevity testing is adequately performed. The EDAS Data Simulator was installed on a test workstation. The EDAS was connected to the test workstation via two serial cables and the branched signal line was also connected to the test workstation via USB. For each test, the simulator sent data to the EDAS over the serial cable connections, simulating the bidirectional communications of the operator signal line. At the conclusion of a test, a software script was used to analyze and compare the simulator output and EDAS branch data on a byte-by-byte basis.

Table 3: SNL Test Matrix for EDAS System Testing

Test Name	Description
Noninterference Integrity Test	The purpose of this test is to prove EDAS does not interfere with the operator signal line while the EDAS is operating normally. Send the same test data over the serial cables, once with the EDAS attached and once removed. Ensure the data from the two tests are equivalent.
Failsafe Requirement Test	The purpose of this test is to prove EDAS does not interfere with the operator signal line in the event of an EDAS failure. Send the same test data over the serial cables, once with the EDAS operating normally and once powered off. Ensure the data from the two tests are equivalent.
Benign Requirement Test	The purpose of this test is to prove that an inspector cannot use EDAS to intentionally introduce data on the operator signal line. Send data from the EDAS over the serial interfaces and verify that none of this data was received on the operator signal line.
Instrumentation Standards Test	The purpose of this test is to prove that EDAS complies with standard instrumentation interfaces. This test is considered complete if the Accuracy and Completeness test passes since that test uses the standard EDAS RS-232 serial interface.
Bypass Option Test	The purpose of this test is to prove that the operator can bypass the EDAS if and when necessary. Disconnect the two serial cables from

	the EDAS and plug them in to each other and verify that communication correctly continues on the operator signal line.
Accuracy and Completeness Test	The purpose of this test is to prove the branched EDAS data is a byte-by-byte replica of the operator signal lines. Send test data on both serial ports. Ensure the simulator output is equivalent to the EDAS branch output by checking that no data has been altered and that the data is complete.
Cryptographic Authentication Test	The purpose of this test is to prove the branched EDAS data is digitally signed and therefore authentic. Send test data on both serial ports. Ensure that all entries in the EDAS branched output are verified as authentic.
Cryptographic Encryption Test	The purpose of this test is to prove the branched EDAS data is encrypted and therefore confidential. Send test data on both serial ports. Ensure that all entries in the EDAS branched output are decrypted successfully.
Longevity Test	The purpose of this test is to prove the EDAS continuously and correctly operates under normal stressing conditions. This test is similar to the Accuracy and Completeness Test except run for periods of weeks or months.
Robustness Test	The purpose of this test is to prove the EDAS continuously and correctly operates under stressing data conditions. This test is similar to the Accuracy and Completeness Test except the simulator will send data at high baud rates in bursts and continuously.

3.2. Electrical Safety Testing

In order to ensure electrical safety compliance of the EDAS, JRC will perform several tests using as reference the UL standard 60335 [2]. Testing will focus on the leakage current and electric strength at operating temperature, transient overvoltage, moisture resistance, leakage current and electric strength and abnormal operation. Abnormal operation could be short-circuit of the EDAS serial acquisition lines, injection of perturbation signal (high frequency signal) on the EDAS acquisition line, and injection of DC signal on the EDAS acquisition line.

The JRC will further test for correct EDAS connectivity using safeguards instrumentation that is representative of that to be used during the field trial. The JRC has a similar barcode reader as well as a weight scale from the Mettler-Toledo family. This testing will be especially important to avoid EDAS connectivity issues during the field trial.

3.3. EDAS Integration with RADAR

EDAS appends its own metadata for each packet it sends to the inspector computer. This metadata includes a date/time stamp for the packet, the unique identification number (ID) of the EDAS junction box, the direction of the data on the operator signal line, and the packet number. Additionally, each EDAS packet contains a digital signature so that the packet can be authenticated by the inspector computer. Each data packet from an EDAS is represented as a single line of comma separated values (CSV). As illustrated in Figure 1, this list will contain entries for each branched data stream.

The EDAS branch data on the inspector computer has been integrated with the Euratom data acquisition system, known as RADAR (Remote Acquisition of Data and Review) [2], via the output file shown in Figure 1. Integration with RADAR allows branched EDAS data to be analyzed by the standard tool used by the Euratom inspectorate. DG-Energy has been working with a subcontractor to implement the interface software so that RADAR may ingest EDAS data.

	A	B	C	D	E	F	G	H	I	J	K
1	Received Date/T	Message	Message	EDAS ID	EDAS Date/Time	Data Source	Data Size	Data	Authentication Status	Encryption Status	
2	7/22/2014 0:00	DATA	3668508	1	5/24/2014 19:53	operator equipment	856	4F9E3AAF	Passed	Success	
3	7/22/2014 0:00	DATA	3321464	2	10/12/2013 22:16	operator computer	619	19DF971F	Passed	Success	
4	7/22/2014 0:00	DATA	3668509	1	5/24/2014 19:53	operator equipment	829	3AC73801	Passed	Success	
5	7/22/2014 0:00	DATA	3321465	2	10/12/2013 22:16	operator computer	658	AEB87473	Passed	Success	
6	7/22/2014 0:00	DATA	3668510	1	5/24/2014 19:53	operator equipment	860	D8CF7C34	Passed	Success	
7	7/22/2014 0:00	DATA	3321466	2	10/12/2013 22:16	operator computer	631	F80CEBEC	Passed	Success	
8	7/22/2014 0:00	DATA	3321467	2	10/12/2013 22:16	operator computer	613	4304A580	Passed	Success	
9	7/22/2014 0:00	DATA	3668511	1	5/24/2014 19:53	operator equipment	869	AD1F5944	Passed	Success	
10	7/22/2014 0:00	DATA	3321468	2	10/12/2013 22:16	operator computer	631	83314EED	Passed	Success	
11	7/22/2014 0:00	DATA	3668512	1	5/24/2014 19:53	operator equipment	843	096C56A6	Passed	Success	
12	7/22/2014 0:00	DATA	3321469	2	10/12/2013 22:16	operator computer	629	158F08CA	Passed	Success	
13	7/22/2014 0:00	DATA	3668513	1	5/24/2014 19:53	operator equipment	857	13A783F9	Passed	Success	
14	7/22/2014 0:00	DATA	3321470	2	10/12/2013 22:16	operator computer	623	DEC3E26A	Passed	Success	
15	7/22/2014 0:00	DATA	3321471	2	10/12/2013 22:16	operator computer	634	B10D0AC9	Passed	Success	
16	7/22/2014 0:00	DATA	3668514	1	5/24/2014 19:53	operator equipment	834	6FA5621A	Passed	Success	
17	7/22/2014 0:00	DATA	3321472	2	10/12/2013 22:16	operator computer	616	DFBA7B81	Passed	Success	
18	7/22/2014 0:00	DATA	3668515	1	5/24/2014 19:53	operator equipment	841	AAA0A4FE	Passed	Success	

messages2014-07-22

Figure 1: Output of EDAS branch data

4. RESULTS OF TESTING

At the conclusion of the testing period, the EDAS prototypes have passed all tests outlined above. It successfully branched all test data under a variety of communication patterns and operational scenarios. The inspector is ensured a complete, accurate, and confidential replica of the operator signal line. Testing showed the operator system is protected by isolating the instrumentation line from the EDAS electronics either through purposeful attempts or failure modes. The results of the EDAS testing illustrate that the prototypes meet both the stated operator and inspector requirements.

Over the course of testing, several software bugs and other issues were discovered. All uncovered software bugs were fixed. Analysis identified another interface-specific issue with the EDAS prototypes where it is theoretically possible to misinterpret a bit when branching. The error can happen in the universal asynchronous receiver/transmitter (UART) hardware in the EDAS, and according to the hardware manufacturer, the probability of occurrence is much less than one percent in even the most stressing case. The fundamental issue is that when any two systems communicate with the serial protocol, data is transmitted and received with UARTs, which are clocked asynchronously with respect to each other. Since the systems' clocks drift with respect to one another, a data bit will occasionally be misinterpreted.

It is important to consider the placement of the bit error in the context of a branched data packet. The error will be insignificant if it is in the least significant digits of a high-precision measurement. A bit error could be significant, however, if a character of a barcode is interpreted incorrectly (e.g., a 'P' turns into a 'Q'). One mitigation strategy is to deploy EDAS as part of a larger system that can detect and correct these errors.

More philosophically, data transmission errors are commonplace with any communication protocol. While some protocols, like serial, do not include much error correction, some protocols like Ethernet and USB have full error correction capabilities. However, this does not mean that an EDAS designed with Ethernet or USB inputs will branch error-free data. Since EDAS has a non-interference requirement, it can only sense data on the operator signal line, and cannot participate in the USB or Ethernet error correction protocol. This discussion illustrates the conflict between the non-interference and accuracy & completeness requirements for EDAS, and the inspectorate and operator would need to negotiate these issues as part of a secure branching deployment in a facility.

We attempted to expose this error using a variety of input test patterns, and have consistently been unable to replicate this error despite testing over several months with large volumes of test data. Nevertheless, this theoretical error is understood well enough to proceed to the field trial.

5. FIELD TRIAL

The upcoming EDAS field trial at the Springfields fuel fabrication facility in the United Kingdom will use EDAS prototypes and software to track the entry and exit of UF_6 cylinders in to and out of the facility. The field trial has three goals:

1. Demonstrate secure branching of representative operator instrumentation for an extended period under realistic operational conditions
2. Derive narrative of facility activity from multiple operator instruments
3. Identify any unanticipated issues with EDAS installation and operation

The field trial is expected to run continuously over a several month period, during which time we will be able to check on the system periodically. It is only possible to attend the system in person during the limited time windows for scheduled Euratom inspections at the facility, which are for a few days each month.

5.1. Field Trial Setup

The upcoming field trial will take place at a facility entry/exit portal for UF_6 cylinders. Two independent data streams will each be monitored by an EDAS. The streams are understood to convey the following attributes of a UF_6 cylinder: 1) scanned bar code ID and 2) weight. The high-level setup for the EDAS field trial is illustrated in Figure 2. The output of the barcode scanner and scale will each interface to an EDAS via RS-232 serial connectors. The branched EDAS output will be securely transmitted over a USB cable to a Euratom inspector computer. USB provides both data transfer over Ethernet to the inspector computer and power to the EDAS prototypes. Additional post-processing of the branched data will be done by the Euratom RADAR software. The inspector computer is connected to the facility mains power, but would run on battery should there be any interruption from the facility mains.

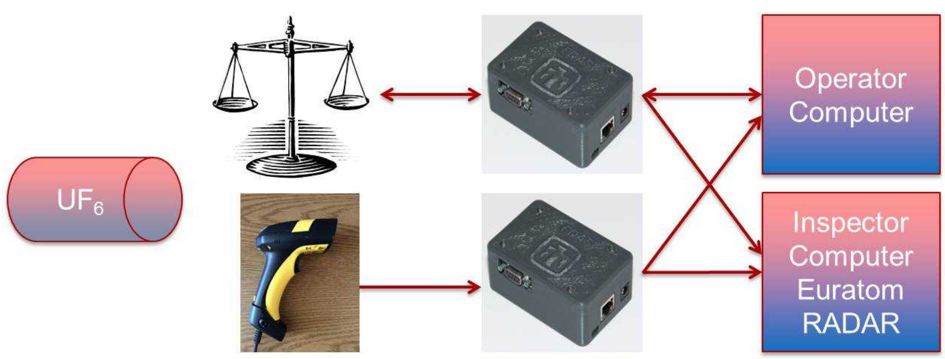

Figure 2: Field Trial Setup

The EDAS branch point for the scale is in the output of the local scale control unit, a Mettler Toledo model IND690 weighing terminal [4]. As a result, EDAS receives weight data only when the IND690 is triggered by the facility instrumentation system to send its current reading. The scale itself is sending weight information to the IND690 continuously. There are various considerations when choosing a branch point and this location was mutually agreed upon with the facility operator

5.2. Field Trial Analysis

Members of the EDAS team will participate in the field trial analysis. The first analysis goal will determine whether EDAS correctly executed its branching function. The analysis team will use a combination of EDAS log files and the RADAR software to perform analysis of the data. Secondly, the team will investigate the utility of EDAS branch data as a complementary safeguards measurement. Operator ground truth, in the form of facility declarations and Euratom inspector notes, will be used to provide the necessary context for this step.

To assess EDAS's ability to perform its branching function, members of the analysis team will check the state of health of the EDAS units during the course of the field trial and perform periodic analysis of the data to assess that each EDAS continues to operate normally. Care will be taken to extract and identify all barcode and weight events so that they may be corroborated with each other to create a narrative of UF_6 cylinder movement at the portal. To the extent possible, the EDAS will further be tested in off-normal conditions (i.e., loss of power to EDAS or inspector computer). The goal is to 1) prove a failure state does not affect the operator signal line and 2) the EDAS units can automatically recover upon return to normal conditions.

Due to the nature of EDAS and the field trial, there will be several analysis challenges. How these respective branched digital signals convert to bar code ID and weight can only be clarified by the context given by the operator. It is unknown, a priori, whether a cylinder is entering or leaving the facility. For scale measurements, it is uncertain whether a given set of branched data is for a new cylinder, or a repeat measurement of the same one. Further, it is unknown whether there may be a variety of cylinder sizes, or even *what* is on the scale when a measurement is made.

Nevertheless, it may be possible to derive certain inferences. Although specific calibration information may not be available, the EDAS will branch a gross weight of a given cylinder at a specific time. From such an isolated measurement, it is not known whether that cylinder is entering or exiting; nor whether the cylinder is full, partially full, or empty. However, after observing the flow without interruption for an extended time, it may be possible to infer additional information. For example, as cylinder bar code IDs repeat over time, it is possible to calculate difference (net) weights, get a sense of the residence time of each cylinder within the facility, and the direction of cylinder movement. From such data can be extracted a fairly good measure of uranium hexafluoride mass processed at the facility per unit time as well as how many and which cylinders are currently inside the facility.

The field trial will be beneficial for both the operator and inspector point-of-view. The analysis will help identify the types of aggregate information that may be inferred by installing multiple EDAS units in a facility. Portions of this aggregate information may be considered sensitive by the facility operator, and it is important to understand how this information could be inferred. More generally, an operator must trust that the EDAS is truly non-interfering to facility operations, and may want to test and analyze several EDAS units before accepting a deployment. Similarly an inspector may want to perform a vulnerability assessment on the EDAS before accepting it as a safeguards tool that meets its requirements. These are some of the important issues that would need to be addressed with a facility and inspectorate before a deployment of EDAS.

6. CONCLUSIONS

The EDAS is a secure branching concept that can provide a copy of operator instrumentation and control system data that complement safeguards verification measurements. Several EDAS prototypes were tested against both the needs of the inspector and facility operator. Testing revealed several issues, the majority of which have been addressed. Despite the discovery of a theoretical bit error when branching, we have never witnessed this issue practically through the rigorous testing period. Testing has helped to characterize the EDAS prototypes, which increases the likelihood for success for the upcoming field trial. The field trial will test the EDAS prototypes in a realistic operating environment. Having the participation of both the Euratom inspectorate and a facility operator for the field trial will be valuable to the continuing evolution of EDAS as an accepted safeguards tool.

REFERENCES

1. 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.
2. http://ulstandardsinfonet.ul.com/scopes/scopes.asp?fn=60335-1.html
3. P. Schwalbach, et al; *RADAR: Euratom's Standard for Unattended Data Acquisition*; proceedings of the International Atomic Energy Agency Symposium for International Safeguards, Wien, Austria, 2001.
4. http://us.mt.com/us/en/home/supportive_content/product_documentation/operating_instructions/IND690_Base_BA/jcr:content/download/file/file.res/22012808F.pdf

ACKNOWLEDGMENT

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.

SAND2014-2827 C