SAND2012-3933 C
SAND2012-3933C

Exceptional service in the national interest

Sandia National Laboratories

Enhanced Data Authentication System (EDAS): Concept, Requirements, and Applications

Maikael Thomas

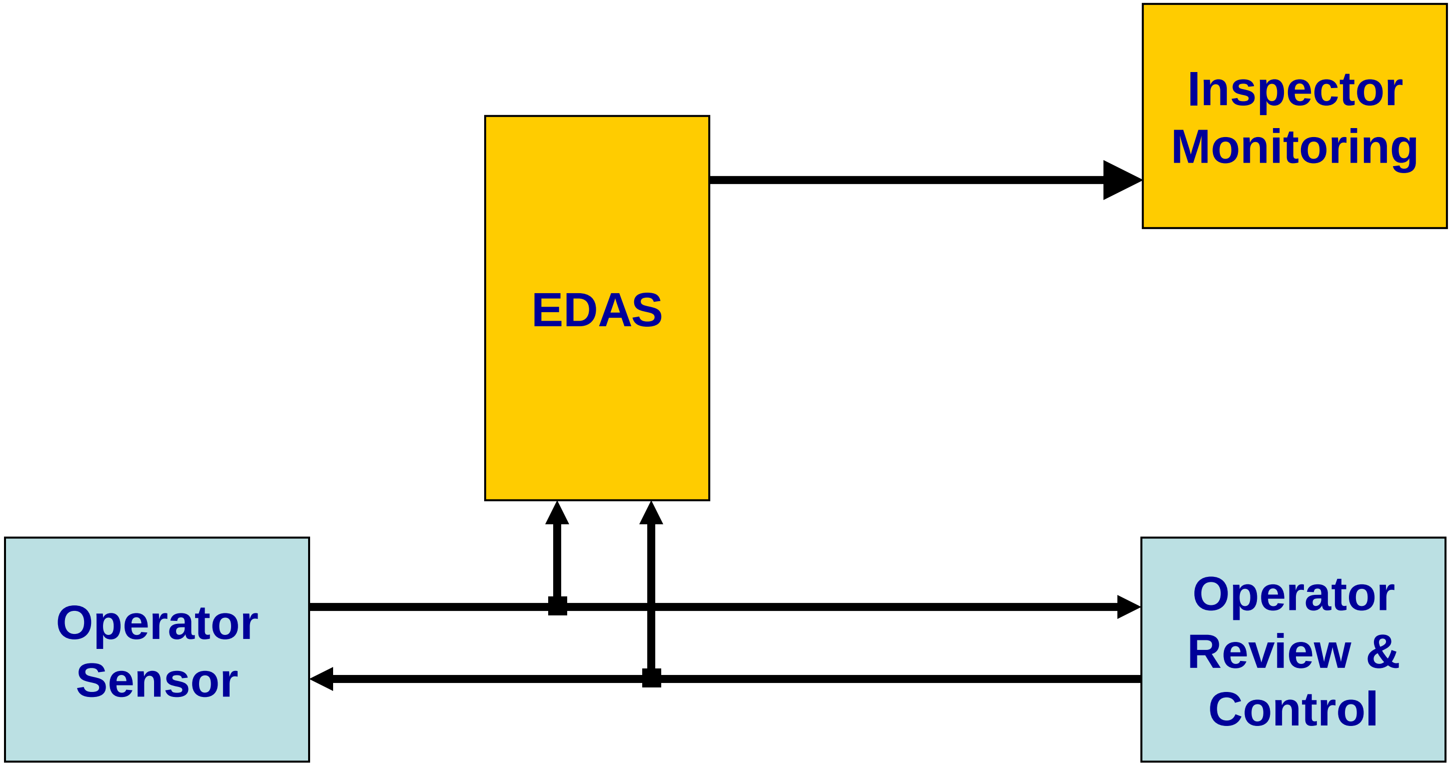
May 14, 2012

U.S. DEPARTMENT OF ENERGY

NNSA National Nuclear Security Administration

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.

The EDAS Concept



AS32 & AS41: Bilateral Agreement Between US DOE and Euratom

June 2006	First draft of DOE – EURATOM action sheet	DG-ENERGY
May 2008	Action Sheet 32 approved	
April 2010	Technical demonstration of EDAS concept:	at JRC
Nov 2010	IAEA Symposium: Poster presentation	Vienna
	Original goals of Action Sheet 32 have been met	

Nov 2011	Action Sheet 41 approved (2 year period)	
June 2012	Develop operator requirements	UK Springfields
Ongoing	Modify EDAS design per operator requirements	
2013	Execute fields trials	UK Springfields
2013	Produce prototypes	

EDAS Objectives and Design Goals

Objectives:

- Ensure there is no interference with operator owned equipment
- Provide authenticated and secure data to the safeguards inspectorate

Design Goals:

- 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

Inspector concerns: monitored information must be …

1. **Accurate:** EDAS signal duplicates the information flowing between the sensor and the operator (in both directions)

2. **Complete:** All data between the sensor and operator is captured

3. **Authentic:**
   - Confidence that there has been no deliberate tampering
   - Monitored signal is a true representation of the information source being measured by the sensor

4. **Meaningful:** Inspector can interpret what the information means

5. **Confidential:**
   - Information between EDAS and the inspector is encrypted
   - The operator cannot know the status of the monitored branch

Operator concerns: EDAS must be …

1. **Non-interfering**
   - EDAS cannot inadvertently alter, control, delay, or otherwise interfere with existing communication between the sensor and the process system
2. **Fail-safe**
   - If EDAS fails (i.e., any form of abnormal operation), it cannot block or otherwise disrupt the normal communication between sensor and the process system
3. **Benign**
   - An inspector is unable to control or manipulate the sensor through the monitored branch

EDAS: Confidence Measures and Interfaces

Sandia National Laboratories

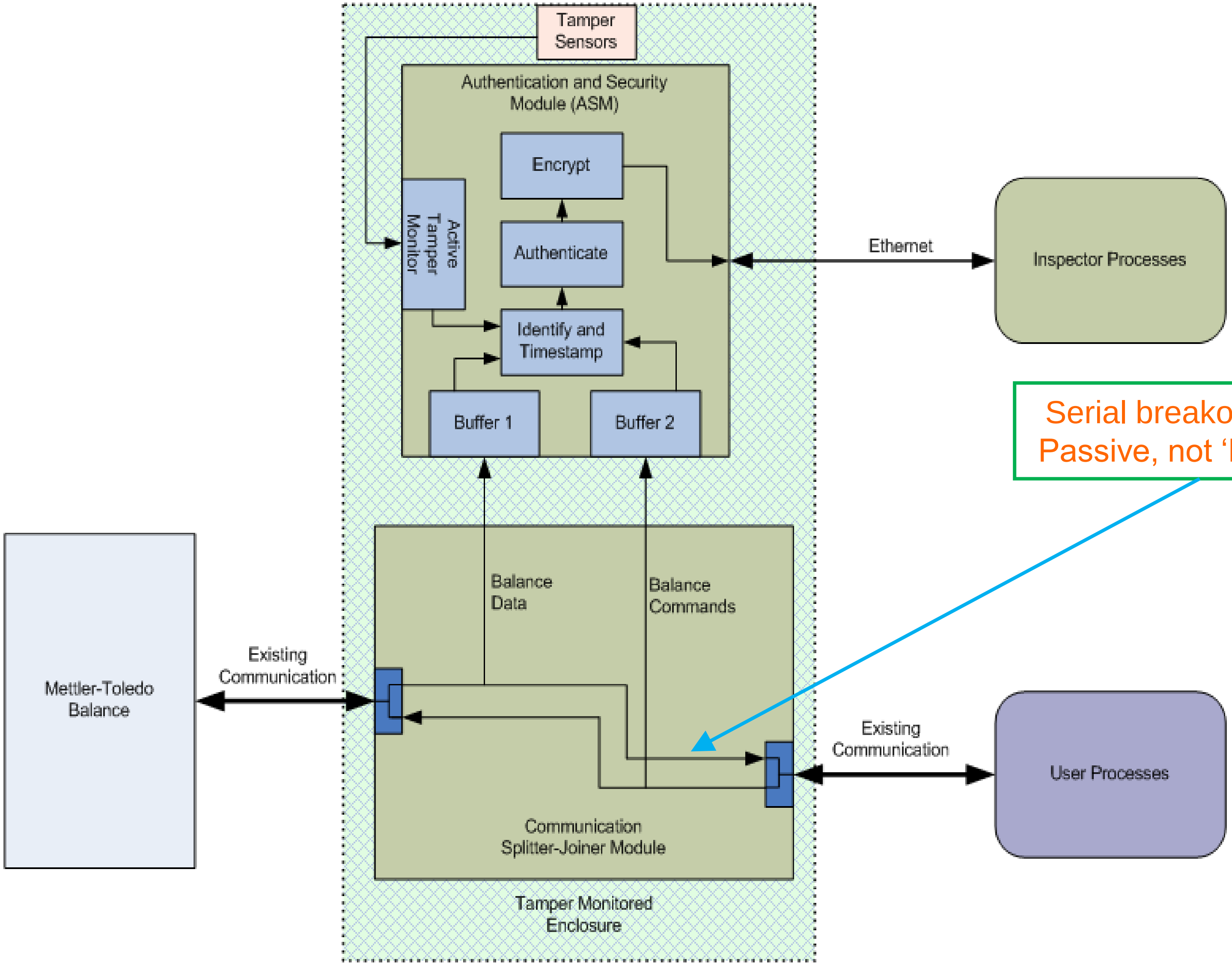
Security and Confidence Measures:

- All acquired data is time-stamped
- Data is identified relative to its direction (flow to or from the sensor)
- Authenticated (i.e., uniquely referred to its source sensor)
  - Currently, employing symmetric key cryptography
- Encrypted
  - Currently based on AES (any other block cipher is possible)

Communications:

► Operator equipment:	Serial interface – RS-232 or RS-485
► Inspectorate:	Ethernet

EDAS Concept Demonstration Block Diagram



Serial breakout cable: Passive, not 'Fail Safe'

Processing EDAS data for Safeguards purposes

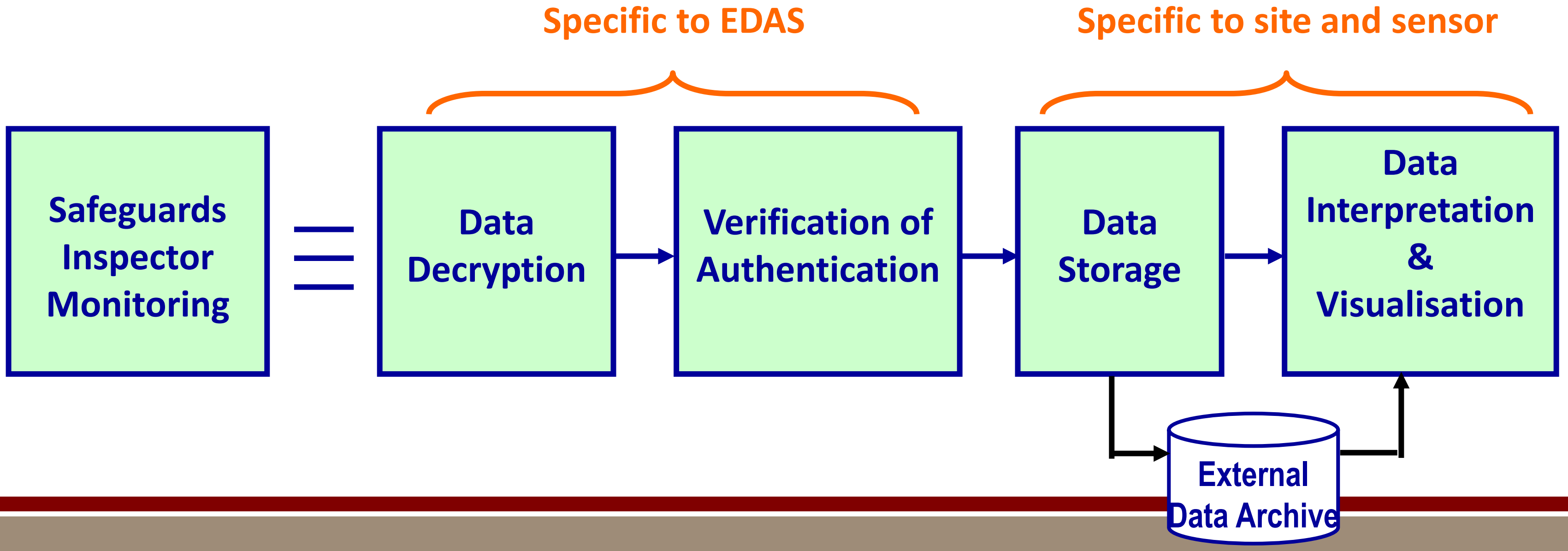
Different Steps:

A. Decryption of EDAS originated data

B. Verification of Authentication

C. Data Archiving

D. Sensor specific data Interpretation and Visualisation module


Specific to EDAS
Specific to site and sensor
Safeguards Inspector Monitoring
≡
Data Decryption
Verification of Authentication
Data Storage
Data Interpretation & Visualisation
External Data Archive

EDAS Next Steps

- AS32: the original goals of the existing Action Sheet have been met to create a design that satisfies the requirements of the inspectorate.

- AS41: work has begun to focus on the requirements of the facility operator and perform field trials with operator participation.
  - Operator collaboration: UK Springfields Oxide Fuel Complex
  - Measurement point: UO2 drum weight station
  - Instrument: Mettler Toledo weighing system

- Improve EDAS technical features:
  - Other communication interfaces e.g., USB
  - Fail-safe operation