SAND2016-5425PE

Exceptional service in the national interest

Sandia National Laboratories

AS41: Development of the EDAS Prototype
June 10, 2016

Maikael Thomas and Ross Hymel
Global Security Programs, Sandia National Laboratories,
Albuquerque NM USA

SAND2016-XXXX PE

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.

AS32 & AS41: Bilateral Agreement Between US DOE and Euratom

Sandia National Laboratories

June 2006	First draft of DOE – EURATOM action sheet	DG-ENERGY
May 2008	Action Sheet 32 approved	
April 2010	Technical demonstration of EDAS concept:	JRC, Ispra
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
Dec 2013	EDAS Prototypes	Sandia
Dec 2014	IAEA Symposium: Poster presentation	Vienna
Nov 2015	End of field trial	UK Springfields
Ongoing	Create Commercialization Prototypes	Sandia

Safeguards Objective

- The objective of this Action Sheet is to further develop and demonstrate a secure branching capability for facility instrumentation to meet operator, as well as inspector, requirements
- The enhanced data authentication system (EDAS) secure branching capability is seen as a valuable complement to independent safeguards instrumentation, offering redundancy and context that is valuable for anomaly resolution and contingency
- Envisioned use is for Euratom Safeguards, yet there is also significant interest by the IAEA for wider application:
  - *IAEA Department of Safeguards Long-Term R&D Plan, 2012-2023, STR375, January 2013, Milestone 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."*

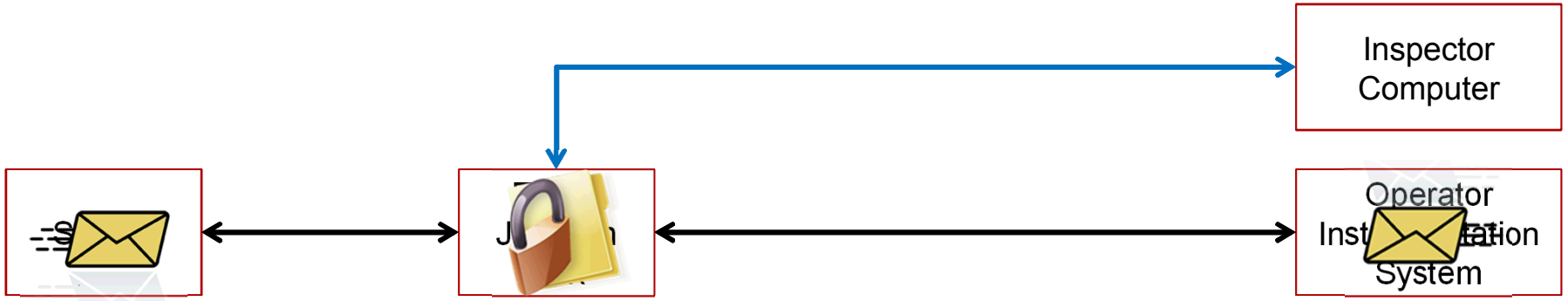
    Urgency: High

Action Sheet Status

- Task 1: Identify facility and facility representative for the field test application. [COMPLETE]
- Task 2: Develop operator requirements for EDAS. [COMPLETE]
- Task 3: Modify EDAS design to address operator requirements. [COMPLETE]
- Task 4: Plan and execute a field test. [COMPLETE]
- Task 5: Identify appropriate safeguards application scenarios for EDAS. [COMPLETE – On agenda for close-out meeting discussion.]
- Task 6: Produce prototypes. [COMPLETE]
- Task 7: Produce final report. [In Progress]

EDAS Technical Concept

- Branched data is a complete, accurate, and confidential replica of operator signal line
- Protects operator system by isolating instrumentation signal line from EDAS electronics
- Designed for low cost deployment, employs mainly commercially available hardware
- Conforms to standard communication interfaces



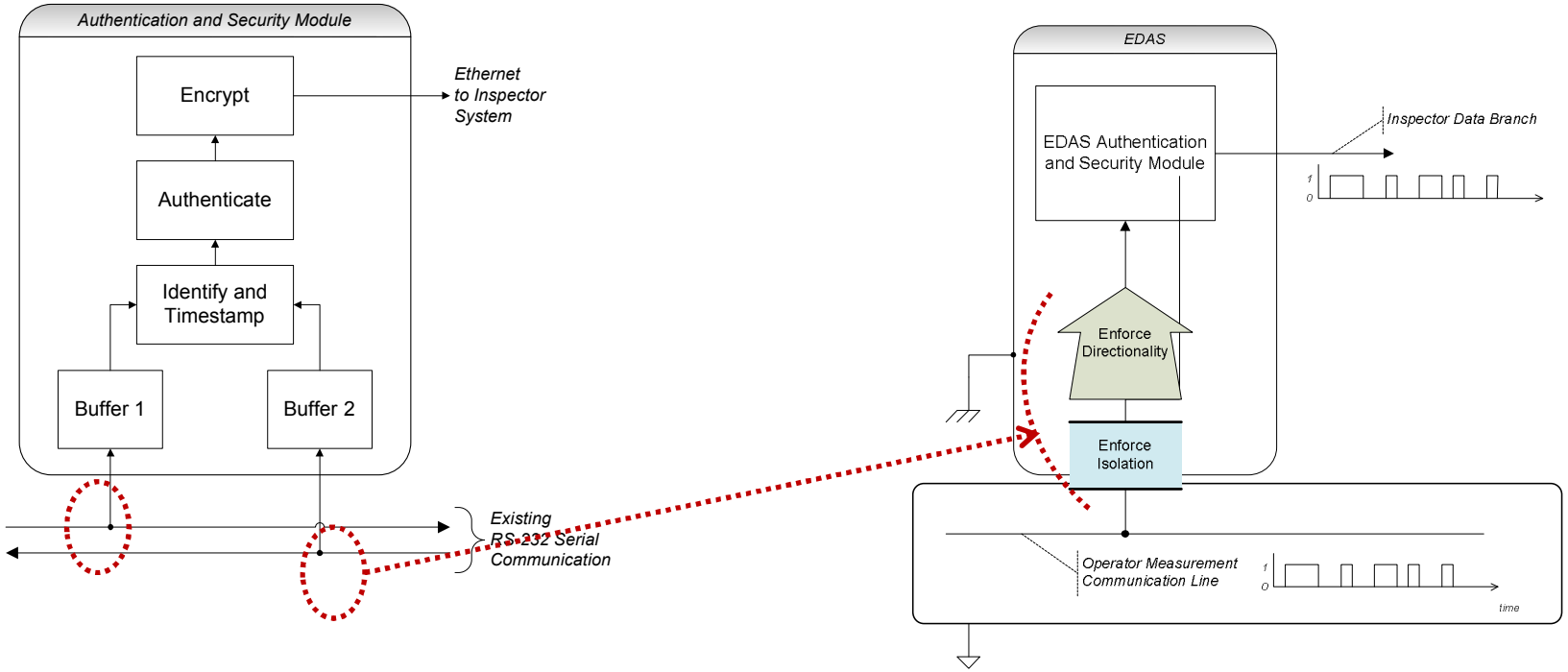
Requirements

Sandia National Laboratories

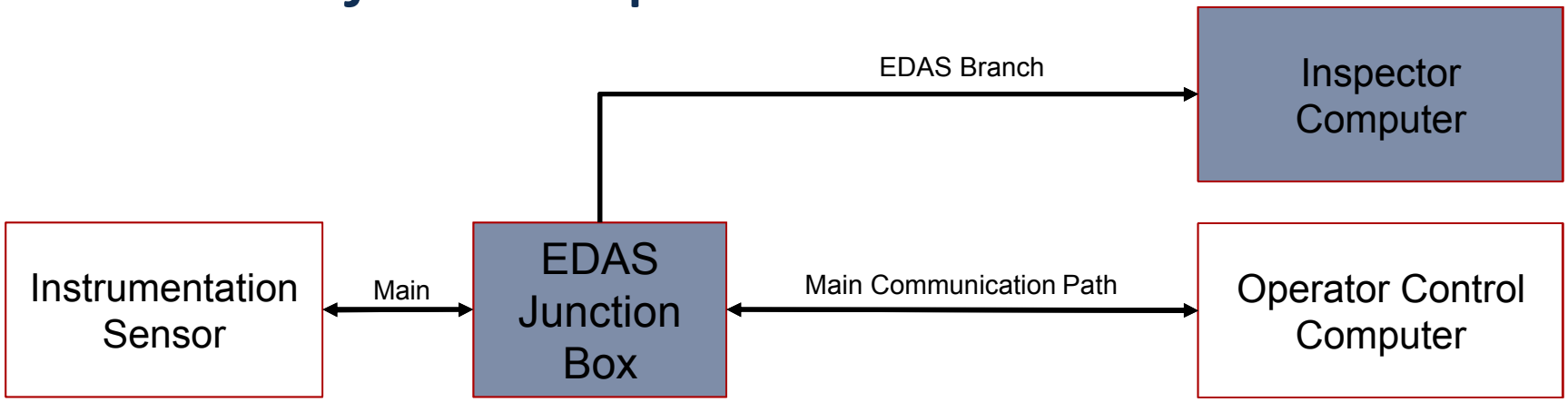
- Isolation of EDAS from the operator signal line
  - Operator signal does not depend on, nor is affected by EDAS
- Fail-safe operation
  - EDAS starts up and recovers automatically; operation is asynchronous
- Accurate, complete and meaningful branched data
  - Prescriptive logic can optimize formation of data packets, but data stream can be reassembled faithfully however the time/size limits are set
  - What those bytes actually *mean* must be determined separately
- Data confidentiality and authentication
  - Encryption prevents an eavesdropper from obtaining the branched data
  - Encryption does *not* prevent an eavesdropper from detecting operation
  - Authentication assures both the source and integrity of the branched data

The EDAS redesign extends previous work

- Branching originally used simple signal line “splitters”
- The latest design assures non-interference

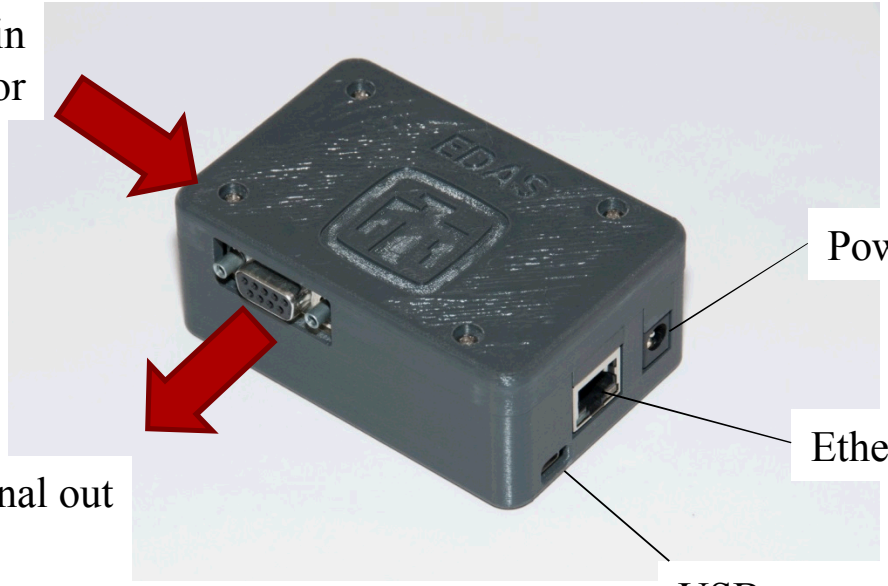


EDAS Major Components



- EDAS Junction Box
  - Case
  - Custom Printed Circuit Board for branching and cryptography
  - COTS Single Board Computer with Custom Software for data packet formation and forwarding
- Inspector Computer
  - Custom Software to receive packets, authenticate, and store data

Connections to the EDAS Junction Box



EDAS is non-interfering: A custom circuit board isolates the operator signals from EDAS

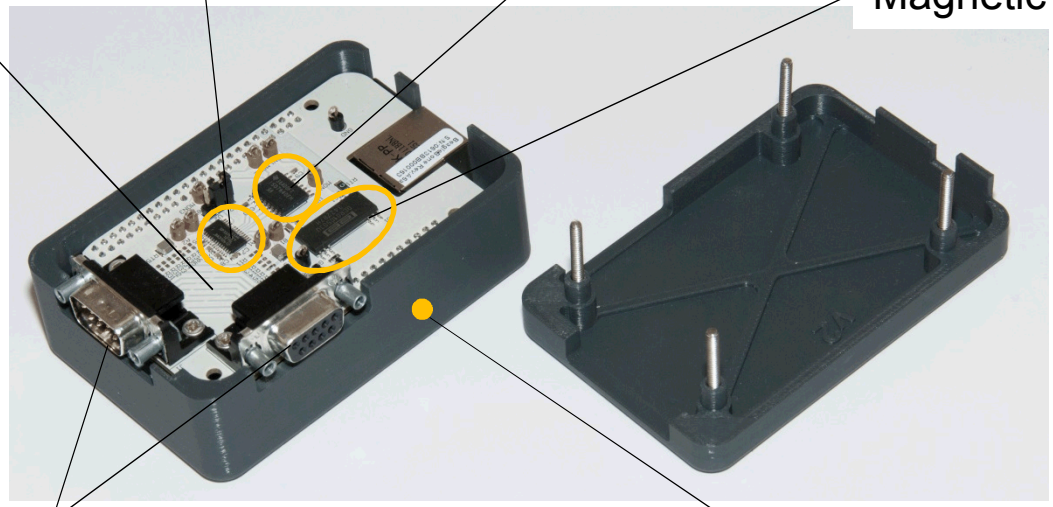
Sandia National Laboratories

Transceiver interprets the RS-232 signals as 0's or 1's

Capacitive data isolator

Signal lines are continuous between the connectors

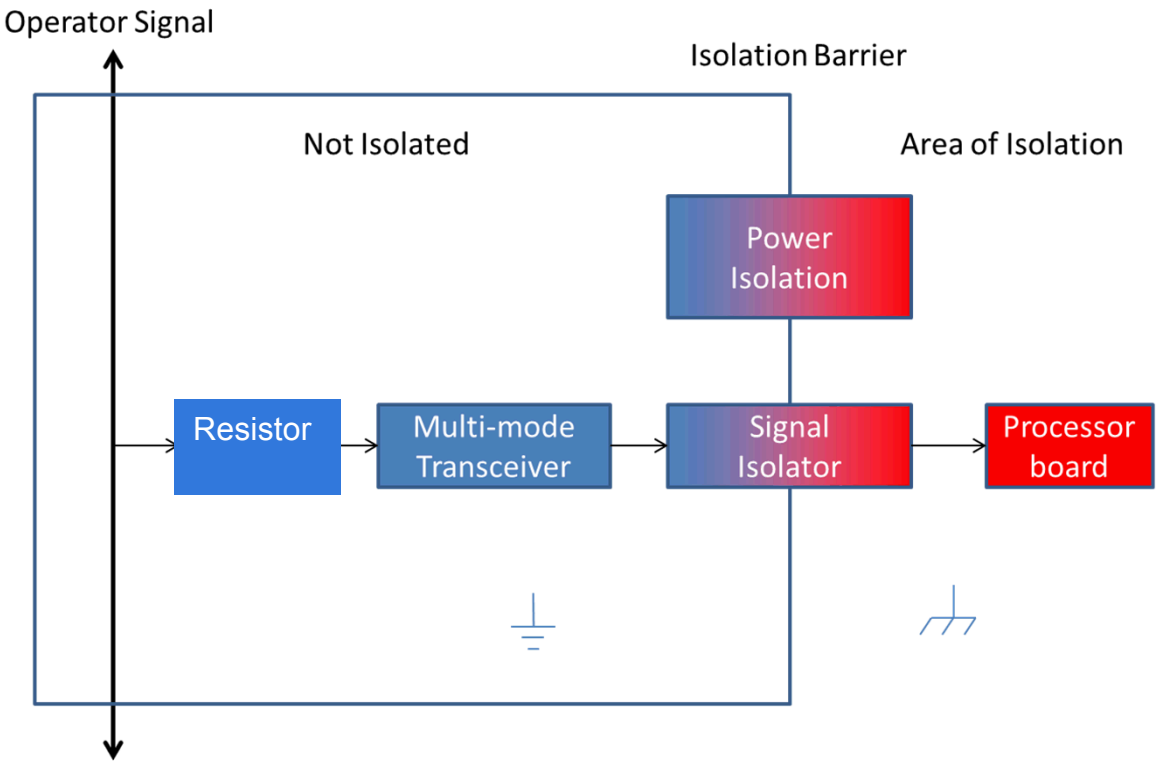
Magnetic power isolator



9-pin RS-232 connectors for operator signal in / out
(able to be bypassed manually if operator chooses)

BeagleBone Black processor (underneath the custom board)

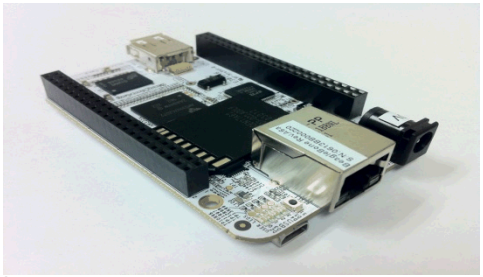
EDAS Branching Electronics Architecture



- A resistor isolates EDAS from the operator system (fault condition)
- Multimode transceiver enables compatibility with either RS-232 or RS-485
- Signal isolator ensures transmission is only *to,* and not from, the inspector
- Power and ground isolation for immunity to power transients

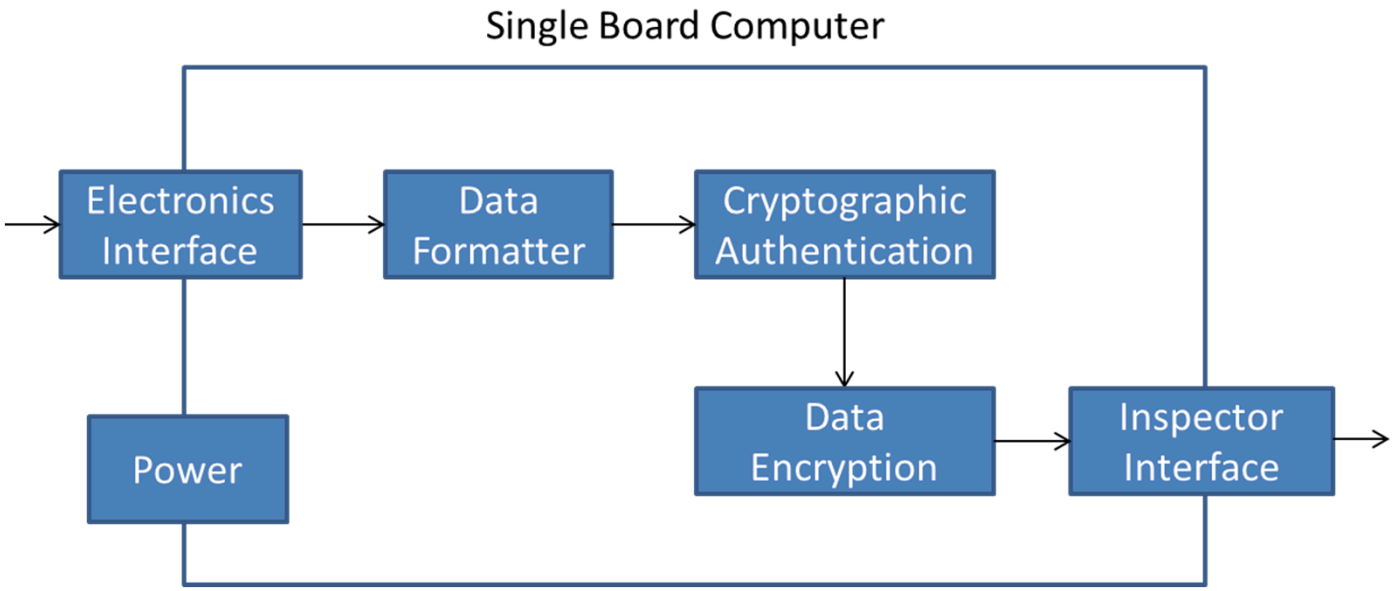
EDAS operations are implemented with custom software on a commercial platform

Sandia National Laboratories



- BeagleBone Black commercial processor
- Linux operating system
- Software written in Java
- Bouncy Castle cryptographic library for authentication and encryption (open source)
- Inspector computer software runs on Windows 7
- Automatic operation
  - Linux operating system starts as soon as power is available over USB
  - Operating system loads and runs the EDAS software immediately
  - EDAS software is designed to begin asynchronously
  - EDAS sends “heartbeat” state-of-health messages as well as data packets
  - Robust: can recover from power lapses, breaks in signal connections, etc.

EDAS software architecture



- Data formatter adds a metadata tag to all incoming data packets:
  - e.g., start/stop time stamps, input port, EDAS identifier, size of data block
- Authentication to ensure data integrity
- Encryption for data confidentiality
- Processed data are pushed via TCP/IP interface to inspector system
- Interface to RADAR

Requirements Testing and Results

Sandia National Laboratories

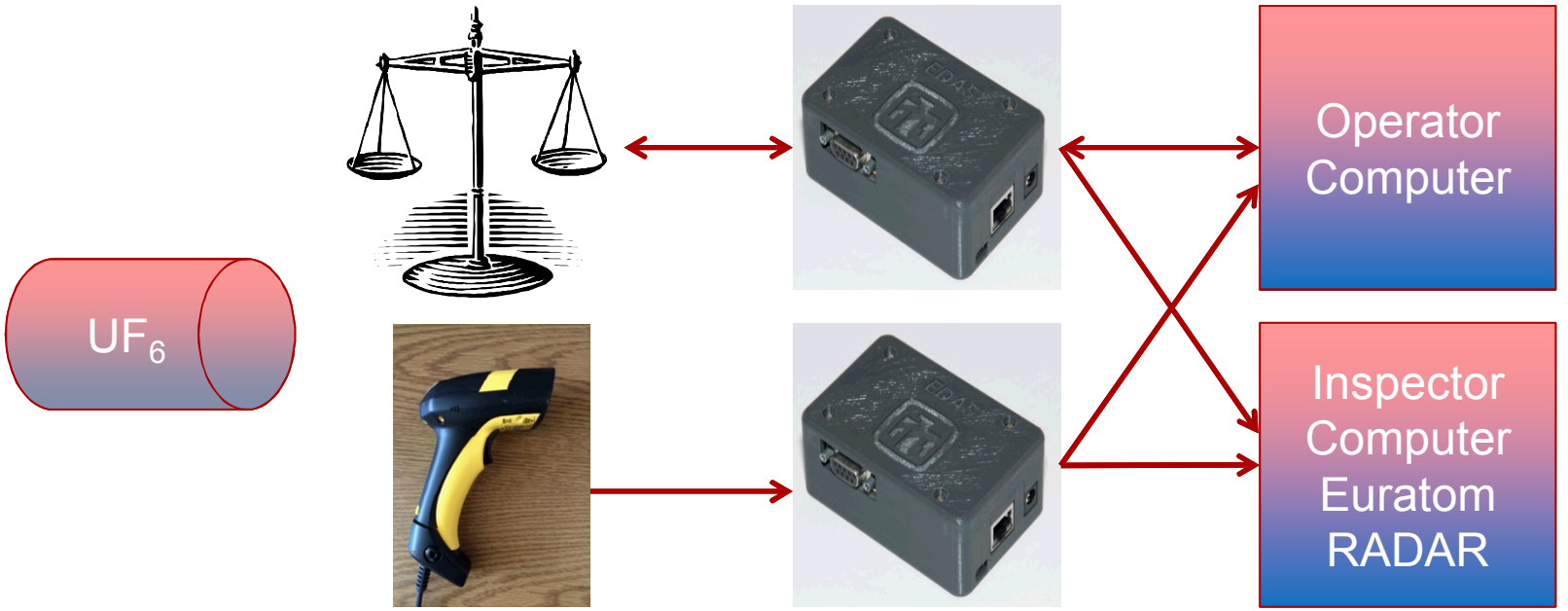
Testing performed with various communication patterns and operational scenarios

Requirement	Test
Non-interfering	Ensure the EDAS cannot corrupt the operator signal line, intentionally or unintentionally, under normal operations and failure modes
Cryptographic	Ensure the branched data line is confidential and authentic
Accuracy and Completeness	Ensure the branched data is a byte-by-byte replica of the operator signal line
Robustness	Ensure EDAS operates correctly under stressing data inputs
Longevity	Ensure EDAS operates correctly with normal data inputs for long time periods

EDAS passed all tests

Field Trial at Springfields Fuel Fabrication Facility

- Demonstrate secure branching under realistic operating conditions
- Identify any unanticipated issues with EDAS operation and installation
- Derive narrative of facility activity from multiple operator instruments



Acknowledgements

- EDAS teams:
  - EC Directorate-General for Energy, Luxembourg
  - EC Joint Research Centre, Ispra, Italy
  - Sandia National Laboratories, USA
- Thank you to:
  - Office for Nuclear Regulation – ONR
  - Westinghouse Springfields Ltd.
  - US National Nuclear Security Administration International Nuclear Safeguards and Engagement Program (INSEP)