SAND2016-12534PE

OFFICE OF NONPROLIFERATION AND ARMS CONTROL (NPAC)

Function and Purpose of EDAS in a Safeguards Context

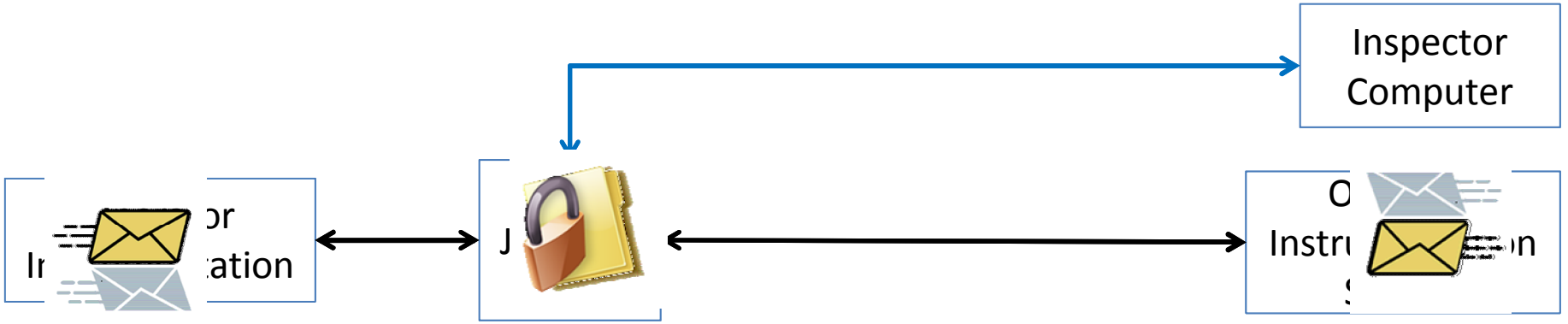
December 14-15, 2016

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

SNL SAND 2016-XXXXX

The Enhanced Data Authentication System (EDAS)

- Create a branch of operator instrumentation data streams
- Transmit secure and authenticated branched data to inspector
- Minimally intrusive to operator instrumentation data stream



EDAS in Safeguards Context

- Typically the instrumentation used by the operator and inspector are distinct
  - Practical cost and space limitations
- EDAS is intended for the shared-use equipment concept
  - Not to replace independent safeguards instruments
- EDAS could be a valuable complement to independent safeguards instrumentation
  - Make available large amounts of plant information
  - A better understanding of the operations of the plant and nuclear material flow
  - Offers redundancy and context that is valuable for anomaly resolution and contingency
- EDAS may apply well in nuclear facilities that are not optimized for safeguards implementation
  - Legacy operator instrumentation

EDAS in Safeguards Context (cont.)

- EDAS designed and tested in collaboration with Euratom Safeguards

COMMISSION EUROPÉENNE
Direction générale de l'énergie

- EDAS may apply well to IAEA safeguards:
  - *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

IAEA

History of EDAS

Date	Event	Stakeholder/Location
June 2006	First draft of DOE – EURATOM action sheet	DG-ENERGY
April 2010	Technical demonstration of EDAS concept	JRC, Ispra
June 2012	Develop operator requirements	UK Springfields
Mar 2015 - Nov 2015	End of field trial	UK Springfields
Ongoing	Commercialization of EDAS	Sandia

The EDAS Concept

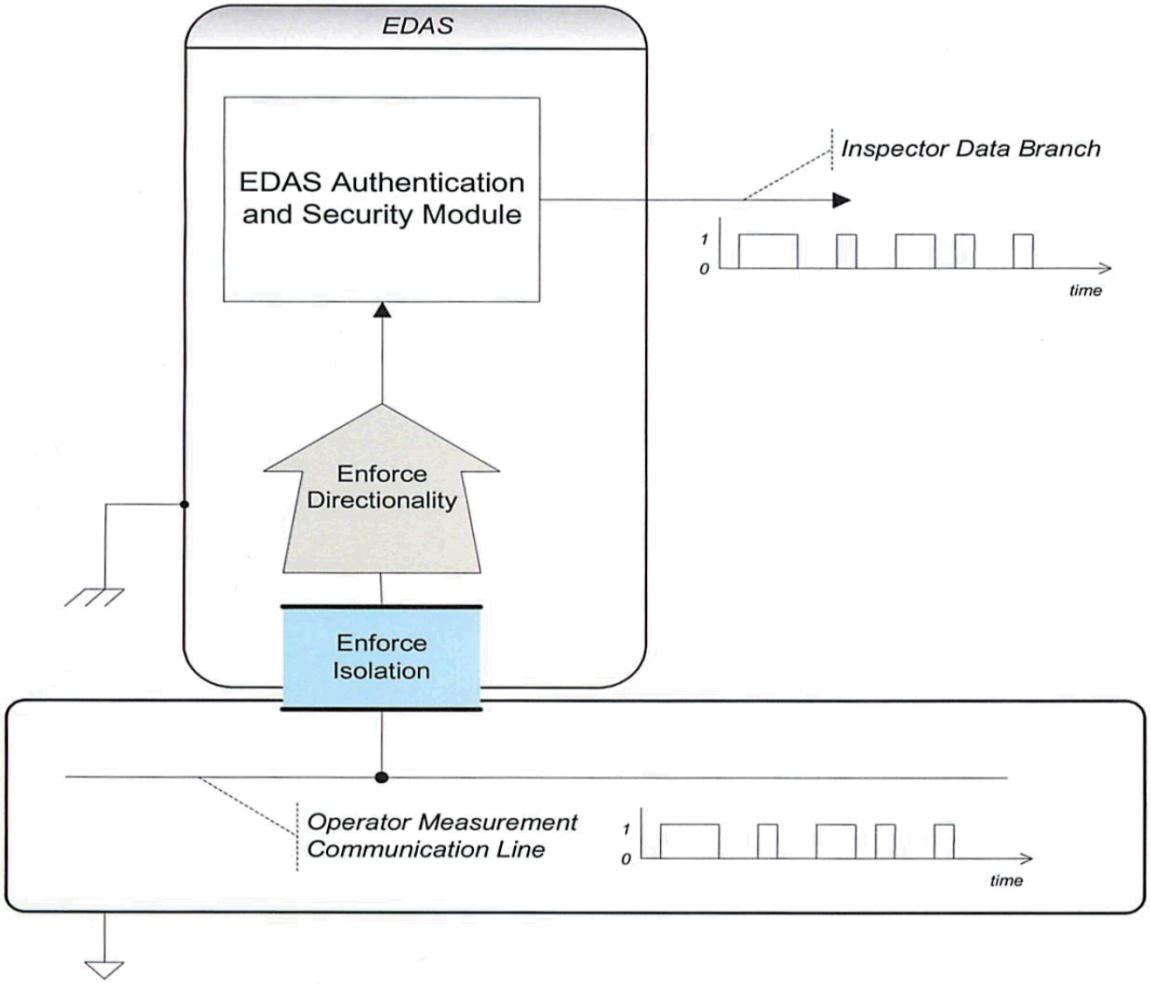
- Branched data is a complete, accurate, and confidential replica of operator signal line
- Protects operator system by isolating instrumentation signal line from EDAS electronics and easy to install
- Designed for low-cost deployment, employs mainly commercially available hardware
- Conforms to standard communication interfaces
- Requirements collected from stakeholders in safeguards community
  - Inspectors, operators, safeguards researchers

EDAS Junction Box

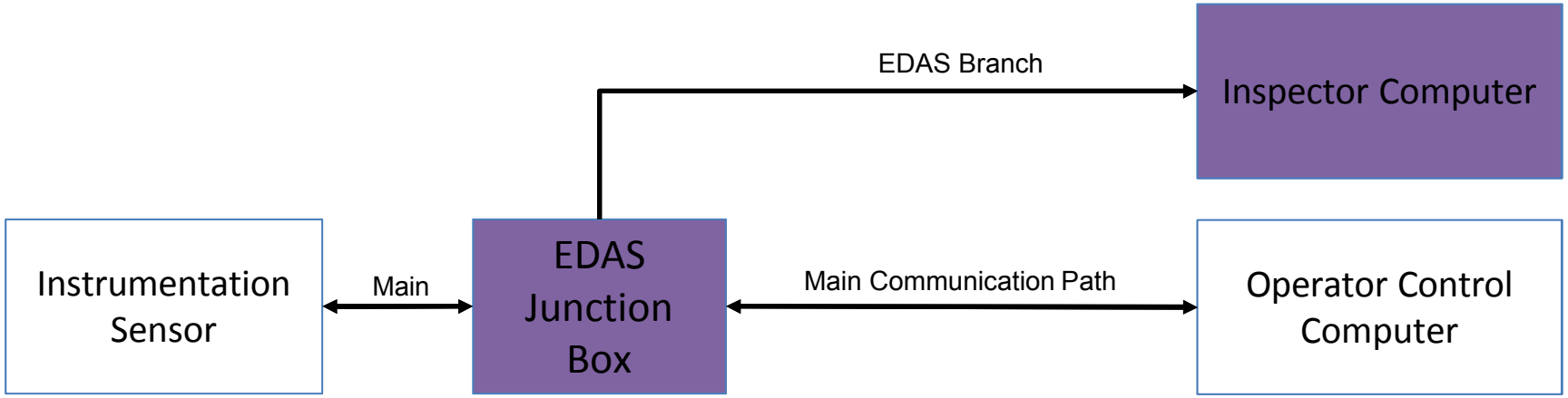
Designed for Inspector and Operator Requirements

- 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

EDAS Design Requirements

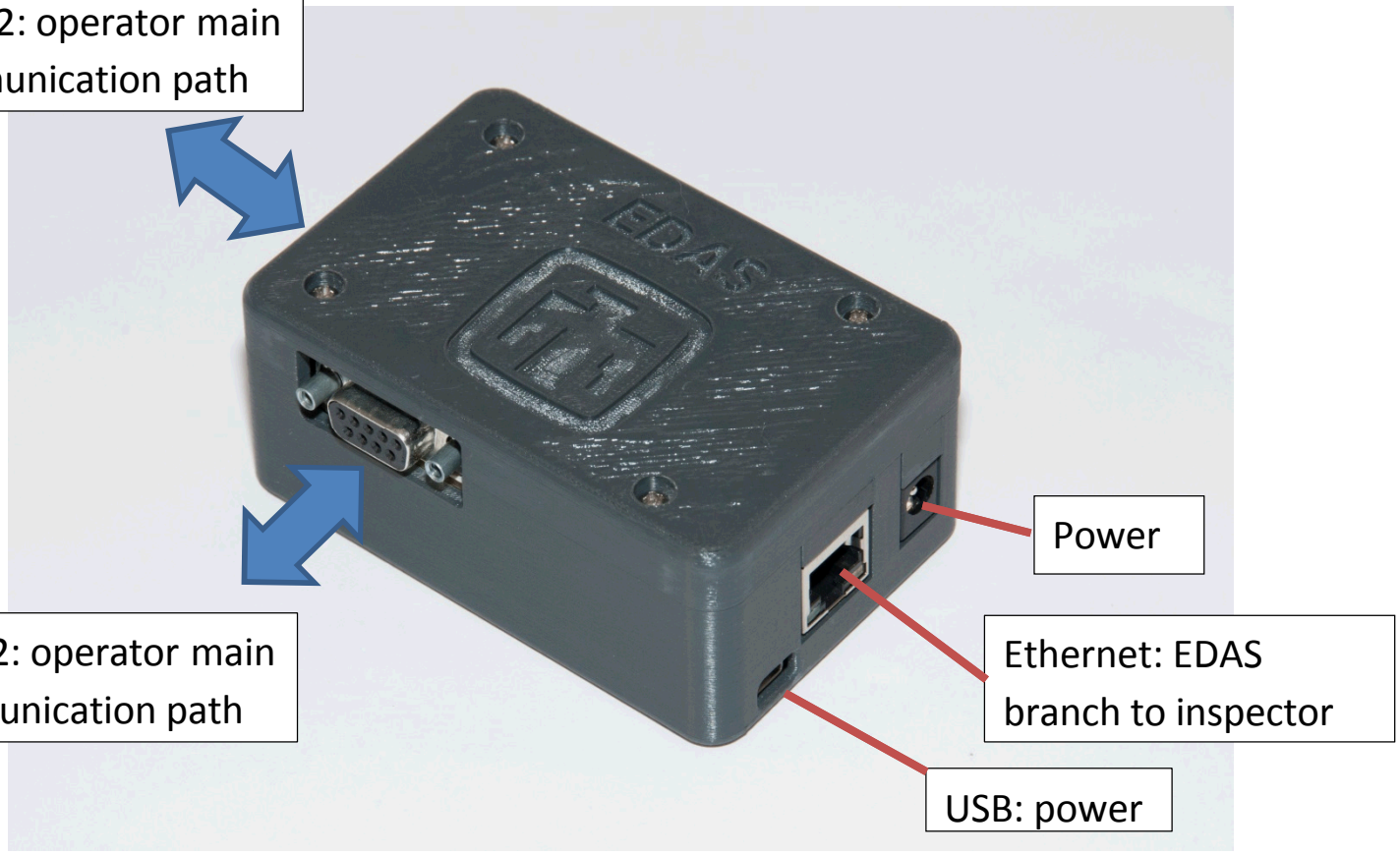


The EDAS System



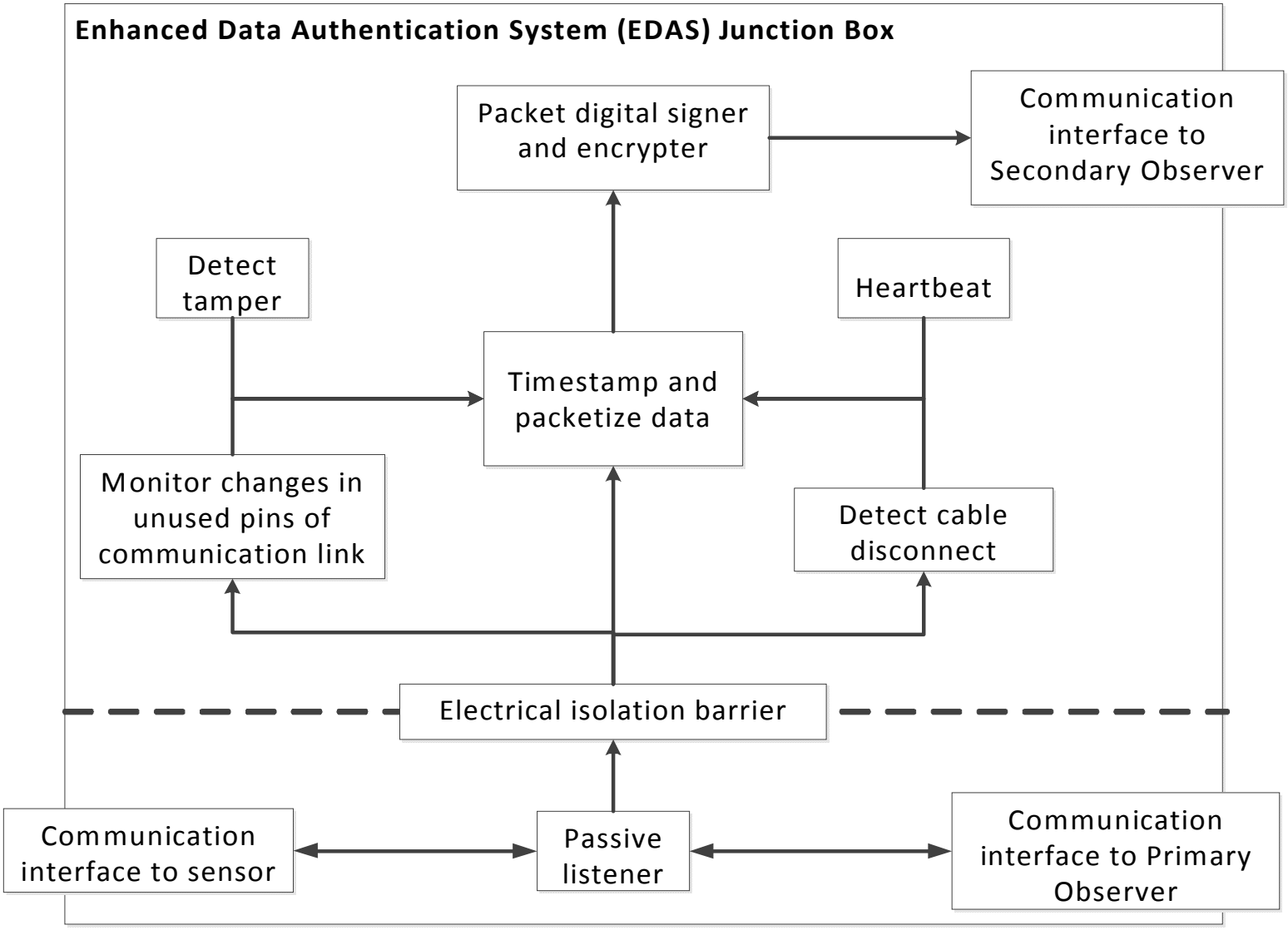
- EDAS Junction Box
  - Case
  - Custom Printed Circuit Board for branching and cryptography
  - COTS Single Board Computer with Custom Software for data packet formation and forwarding
- Inspector Computer
  - Custom Software to receive packets, authenticate, and store data

EDAS Junction Box Interfaces



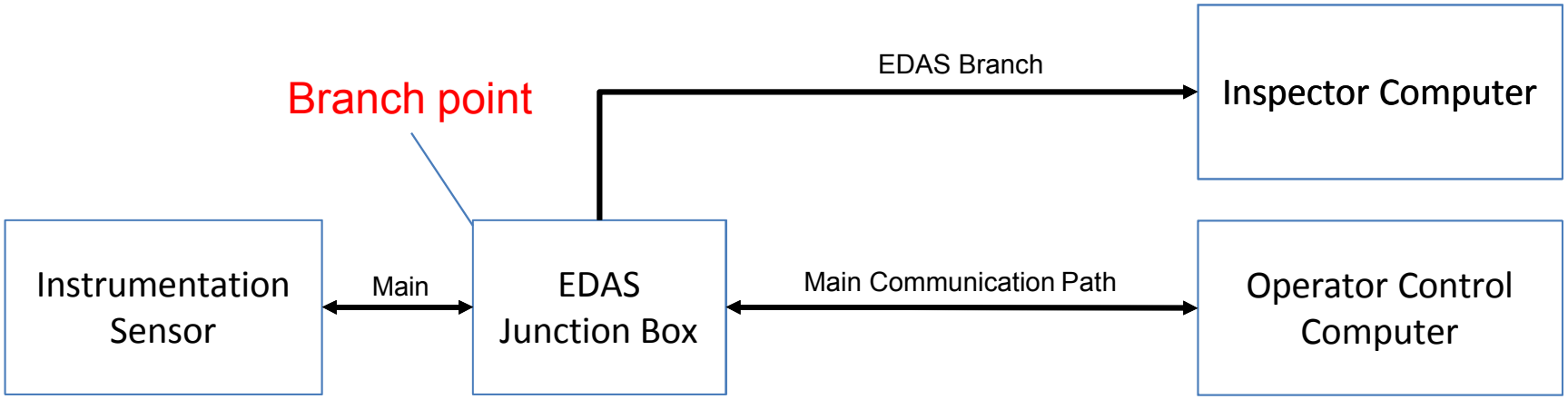
- EDAS supports instrumentation interface standards
- Modular design to support other instrumentation interfaces

EDAS Major Components



Description of an EDAS Deployment

- Configure EDAS Junction Boxes
- Select and install junction box at branch point as close to the sensor as possible
- Setup inspector computer on- or off-site
- Multiple junction boxes transmit to one inspector computer



Use Case Discussion

- Monitoring operator instrumentation in highly complex and large bulk handling facilities
  - e.g., additional information on material movements
- Process monitoring
- Nuclear facilities not optimized for safeguards implementation
    - Legacy instrumentation
    - Not enough real estate to deploy an independent safeguards instrument: cranes, weight scales
    - Impact to operations
- Prohibitive purchase and deployment cost of independent safeguards instrument

Use Case Discussion (Cont.)

- Monitor configuration ports of deployed safeguards equipment
  - Reconfiguration
  - Modification of firmware
- Dual-use of either operator or inspector safeguards instrument between two safeguards inspectorates
- Encryption and authentication of a legacy data stream that does not transmit securely

Requirements Testing and Results

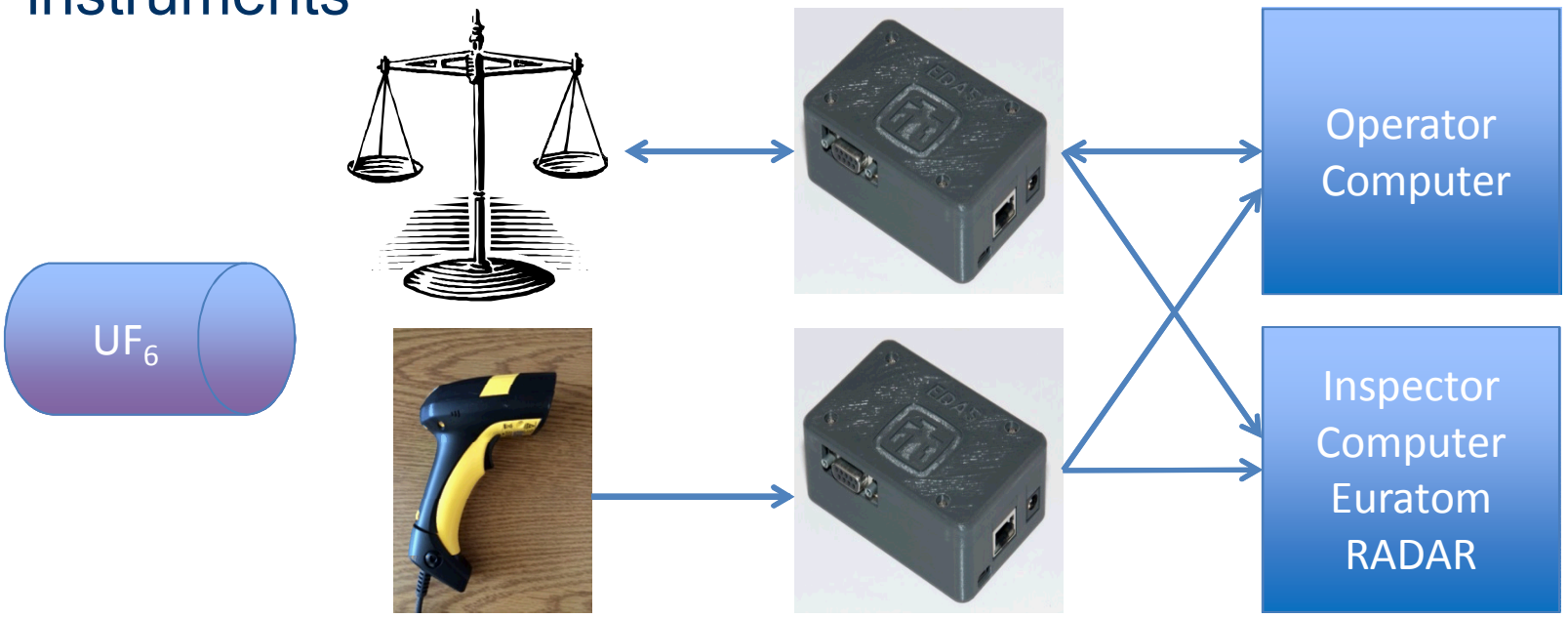
Testing performed with various communication patterns and operational scenarios

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

EDAS Field Trial

- 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



EDAS Commercialization

Goal:
Create a commercially-available version of EDAS

- Incorporate lessons learned from the field trial
- Tamper indicating enclosure
- Protect EDAS intellectual property via patent and copyright
- Currently in discussions with vendors

Questions?