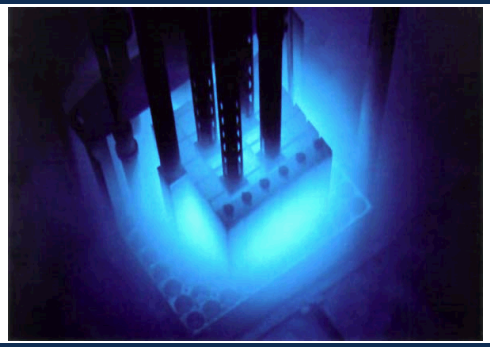
SAND2014-15870PE

Exceptional service in the national interest

Sandia National Laboratories



Prototype Hardware and Software for the Secure Branching of Facility Instrumentation

Maikael Thomas, George Baldwin, Ross Hymel, and Jay Brotz
Sandia National Laboratories

INMM Annual Meeting
Atlanta, GA USA
July 24, 2014

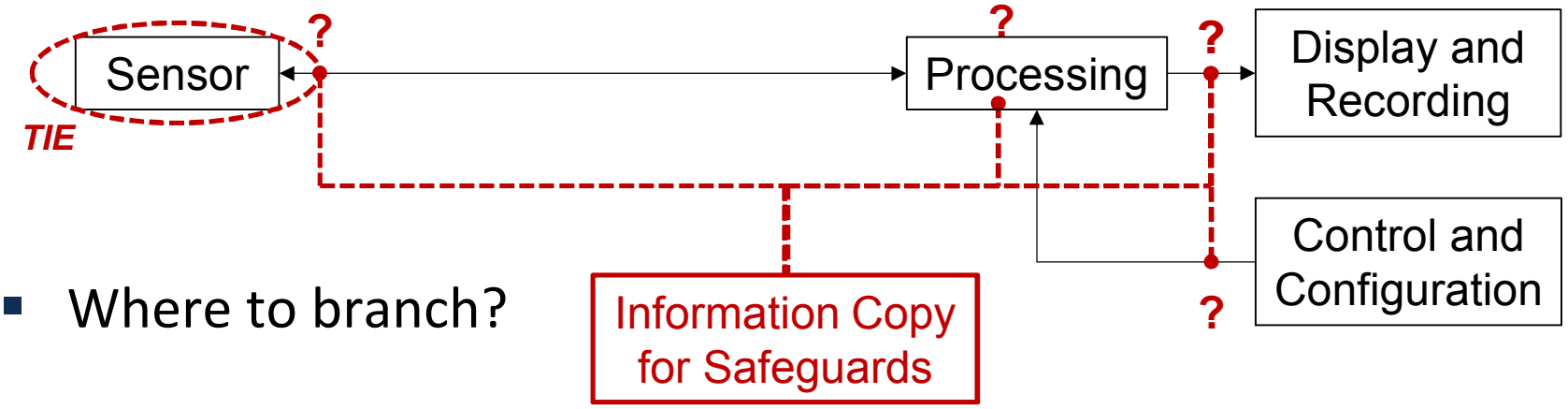
U.S. DEPARTMENT OF ENERGY

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.

Branching approach: “listen” to the operator instrumentation, close to the sensor

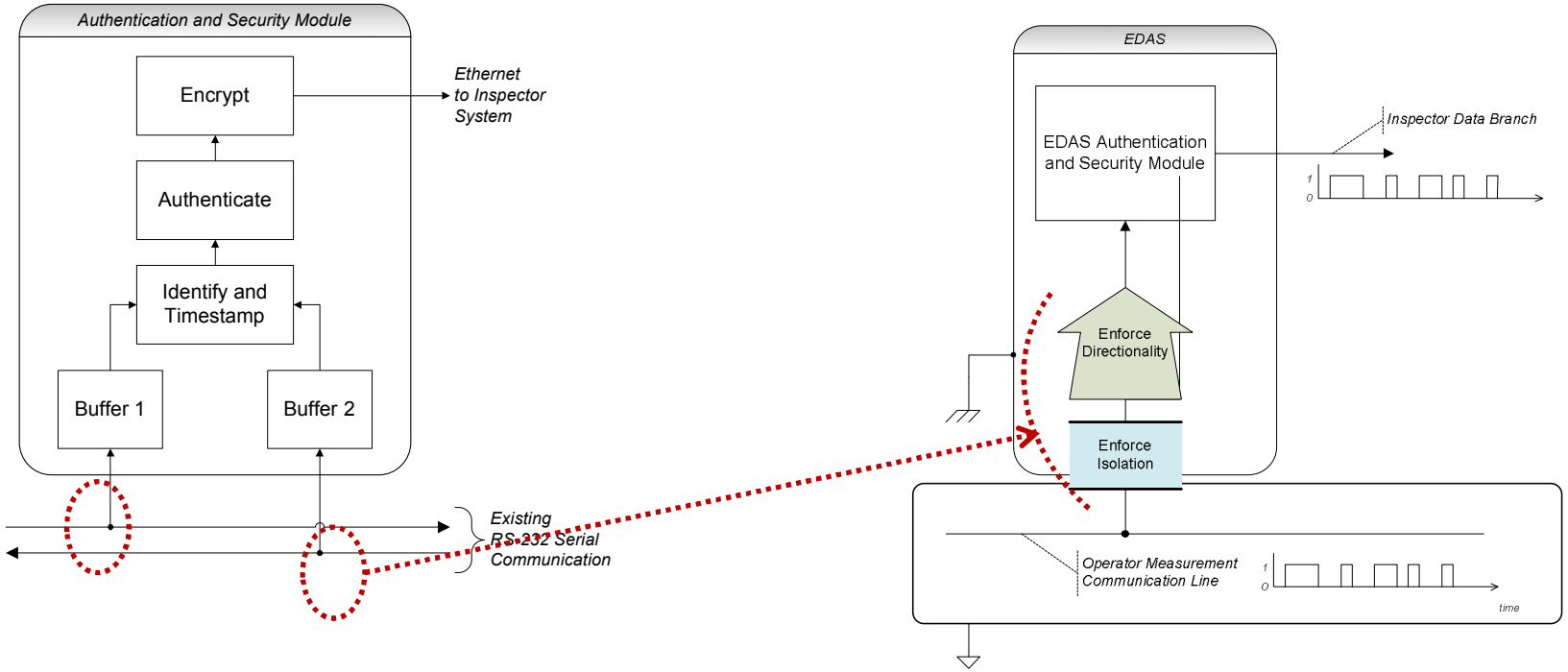
- Operator instrumentation system:



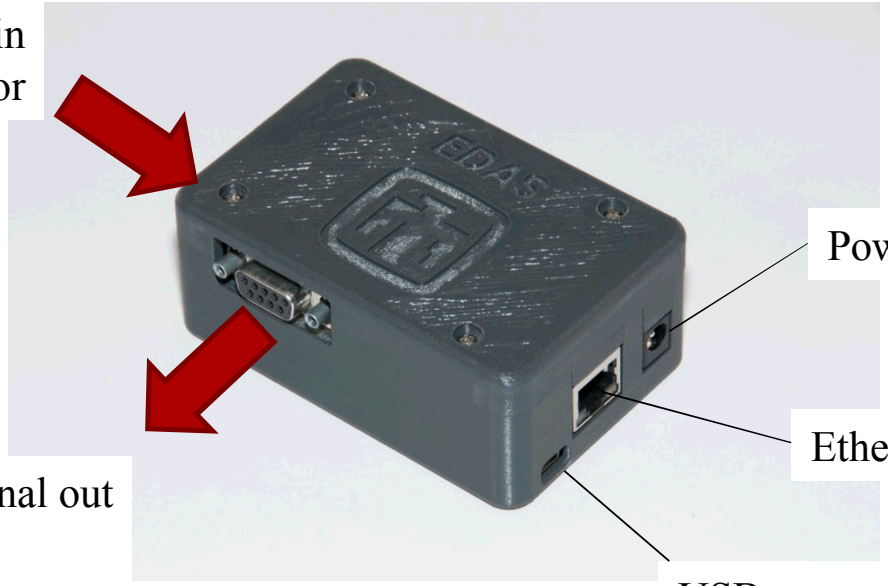
- Where to branch?
- EDAS: “Enhanced Data Authentication System”
- The EDAS design philosophy is
  - 1) faithful replication of operator data
  - 2) meet trust and security requirements of both inspector and operator
- Requirements can be met by blindly copying data bits as close as possible to the data source

The EDAS redesign extends previous work

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



Connections to the EDAS Junction Box



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

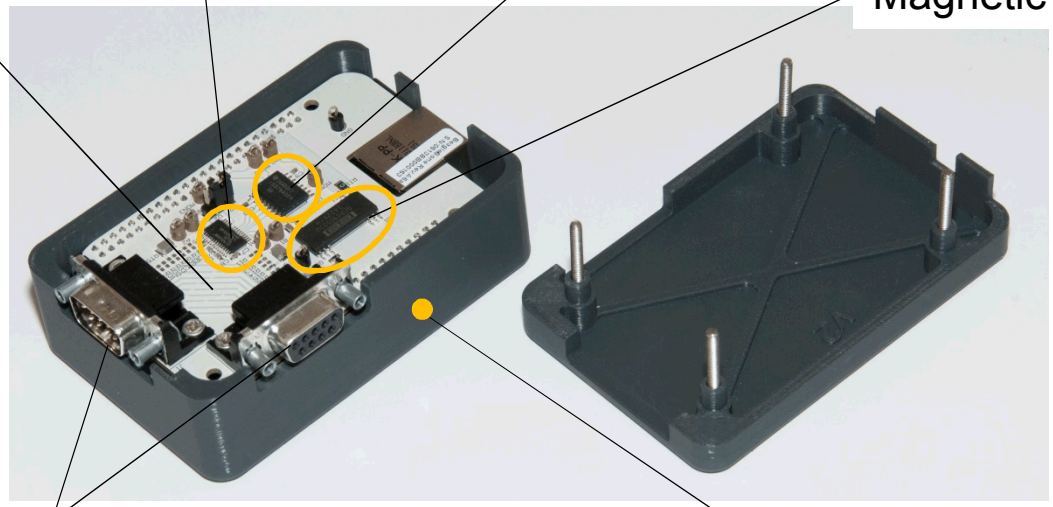
Sandia National Laboratories

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)

How EDAS “listens” to the operator instrumentation:

Sandia National Laboratories

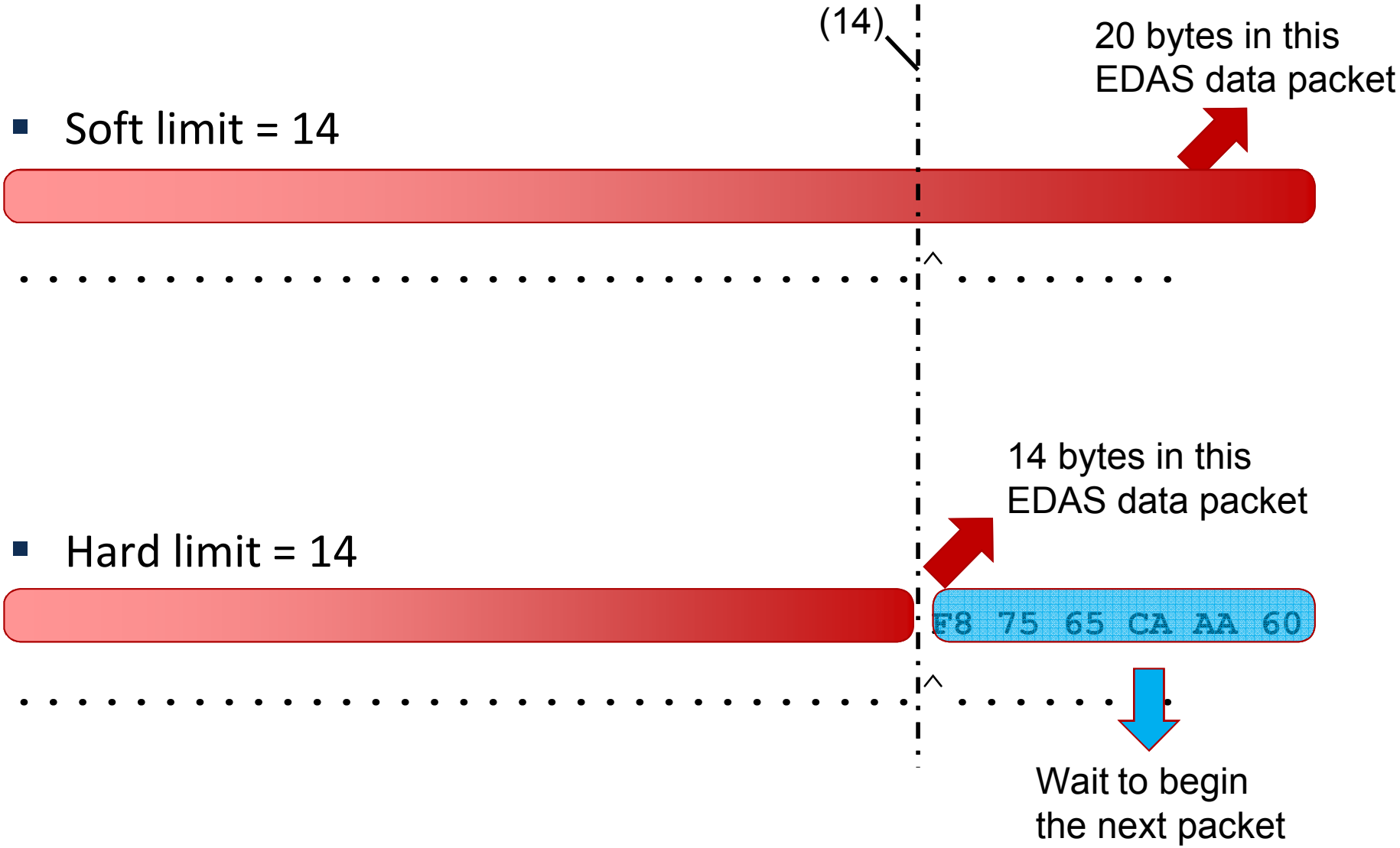
- Transceiver detects the RS232 data levels (0’s and 1’s)
  - Receive (Rx)
  - Transmit (Tx)
- The data levels pass across a one-way isolation barrier
- EDAS buffers accumulate a copy of the RS232 data
- EDAS decides how to group the data into packets
- Each data packet is
  - Identified and time-stamped
  - Authenticated
  - Encrypted
  - Pushed out over TCP/IP to an inspector computer

EDAS logic to assemble data packets can be configured as required

Sandia National Laboratories

- Time
  - As soon as data start to accumulate in the buffer, a clock starts
  - As soon as the elapsed clock time reaches a preset time limit, EDAS will packetize the buffered data
- Amount of data (“size”)
  - Soft limit
    - As soon as the number of bytes exceeds a specified size, EDAS will packetize all of the buffered data
  - Hard limit
    - As soon as the buffer exceeds a specified size, EDAS packetizes only that fixed number of bytes
    - bytes beyond the hard limit
      - Are retained in the buffer
      - Start the next data block

Examples of size limits for data packets



EDAS processes its copy of the operator data

Sandia National Laboratories

- Time stamp and identity
  - Transmit (Tx) or Receive (Rx) line
  - Internal clock, set by inspector computer
- Authentication
  - EDAS cryptographically signs the data blocks sent to the inspector computer
  - Ensures both the integrity and the source of the data
- Encryption
  - EDAS ensures the confidentiality of the operator data copy
  - Secret key encryption established by Diffie-Helman key exchange
- Data are “pushed” to the inspector computer using TCP/IP

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.

Discussion

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

Status and Next Steps

- EDAS is currently undergoing extensive testing
  - Sandia: functional and system testing
  - Partners (European Commission) conducting other tests to assess performance
- EDAS integration with inspectorate data collection system
  - DG-ENER is developing software that will interface EDAS with RADAR, used in Euratom safeguards
- Planning is underway for a forthcoming field trial

- Future considerations:
  - Fitting EDAS with a tamper-indicating enclosure
  - Adapting to other instrumentation interfaces
  - Transition from custom to production availability

Conclusion

- EDAS ensures that the branched information is a secure, true, and complete replica of an operator data stream.
- By design, EDAS is intended to minimize risk to an operator system from branching.
- We are now in a testing phase and will soon be ready to consider deployment aspects

We thank the DOE/NNSA International Safeguards and Engagement Program (INSEP) for financial support of the EDAS secure branching project, and appreciate the valuable collaboration of our international partners at the European Commission, DG-ENER, and the Joint Research Centre, ITU.