SAND2016-12532PE

National Nuclear Security Administration

OFFICE OF
NONPROLIFERATION AND
ARMS CONTROL (NPAC)

EDAS Technology and Commercialization

December 14-15, 2016

SAFEGUARD NUCLEAR MATERIALS TO PREVENT THEIR DIVERSION OR THEFT

CONTROL THE SPREAD OF WMD-RELATED MATERIAL, EQUIPMENT AND TECHNOLOGY

NEGOTIATE, MONITOR AND VERIFY COMPLIANCE WITH INTERNATIONAL NONPROLIFERATION AND ARMS CONTROL TREATIES AND AGREEMENTS

DEVELOP PROGRAMS AND STRATEGIES TO ADDRESS EMERGING NONPROLIFERATION AND ARMS CONTROL THREATS AND CHALLENGES

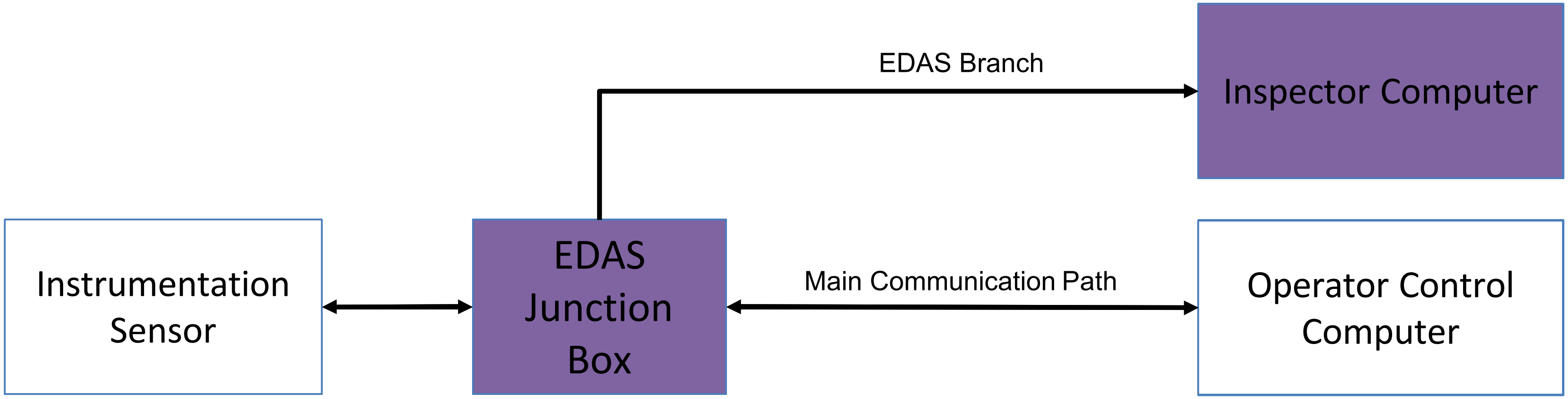
Ross Hymel
Maikael Thomas
Global Security Programs,
Sandia National Laboratories
Albuquerque NM USA

SNL SAND 2016-XXXXX

Outline

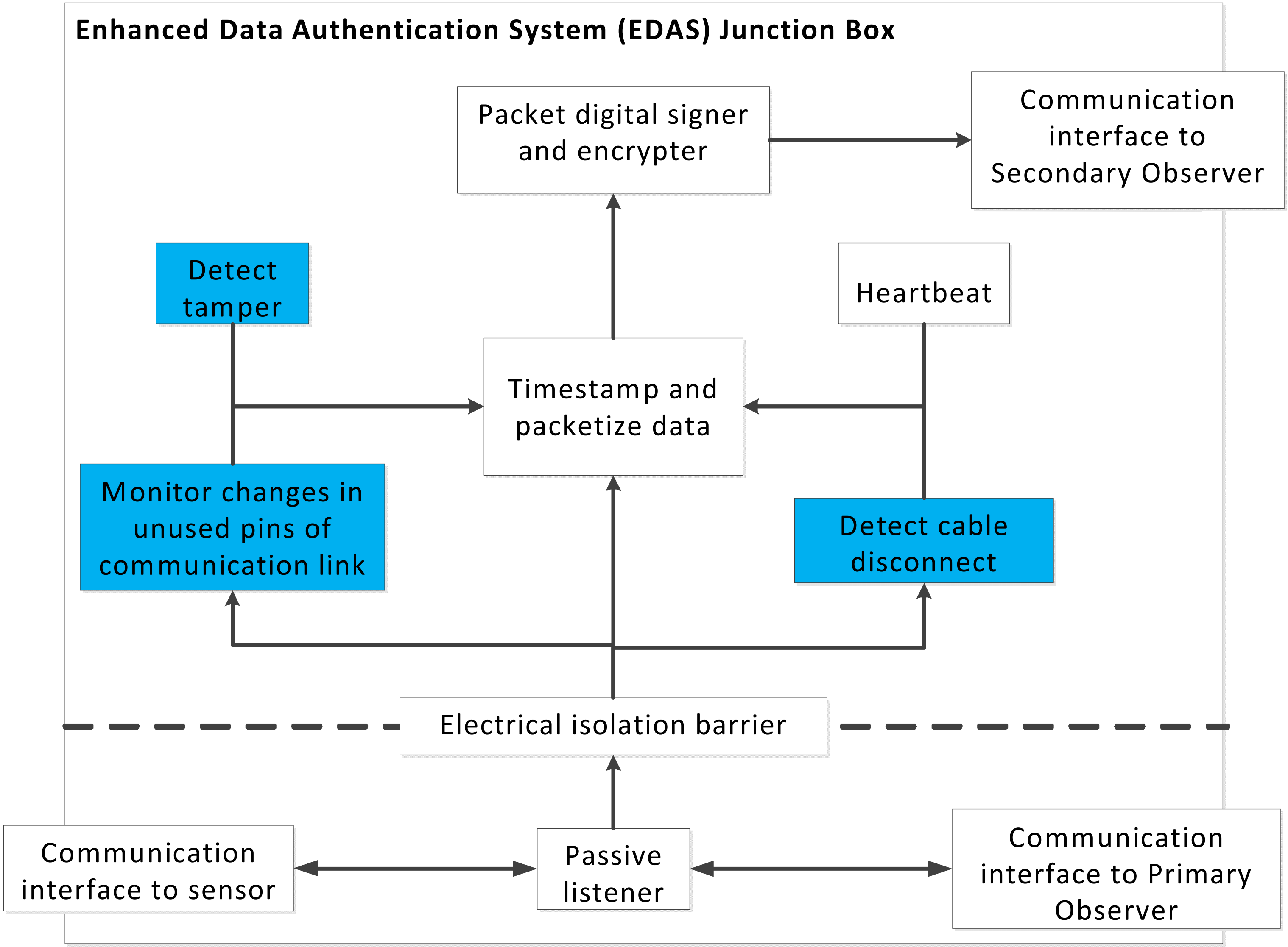
- EDAS implementation specifics and rationale
  - Hardware
  - Software
- Comparison of the EDAS Prototypes
  - Generation 2 (field trial)
  - Generation 3 (commercialization)
- Parts cost
- Cryptography and key protection
- Junction box and Inspector computer software
- Commercialization status

EDAS Major Components

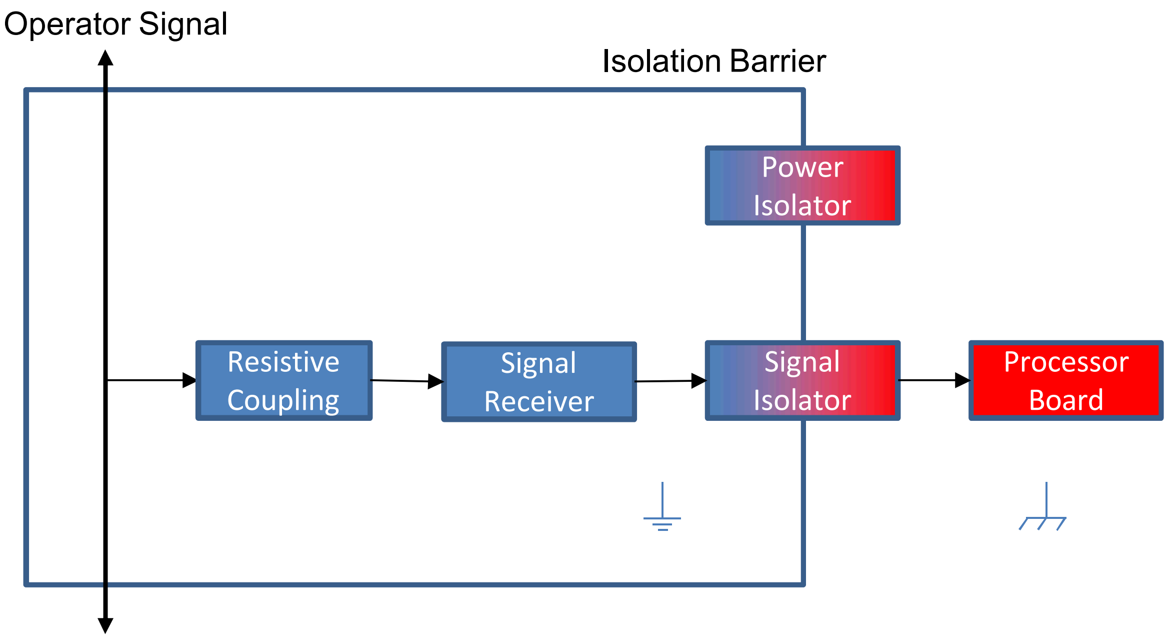


- EDAS Junction Box
  - Case
  - Custom printed circuit board (PCB) for branching and cryptography
  - COTS single-board computer with custom software for data packet formation and forwarding
- Inspector Computer
  - Custom software to receive packets, authenticate, and store data

Block Diagram

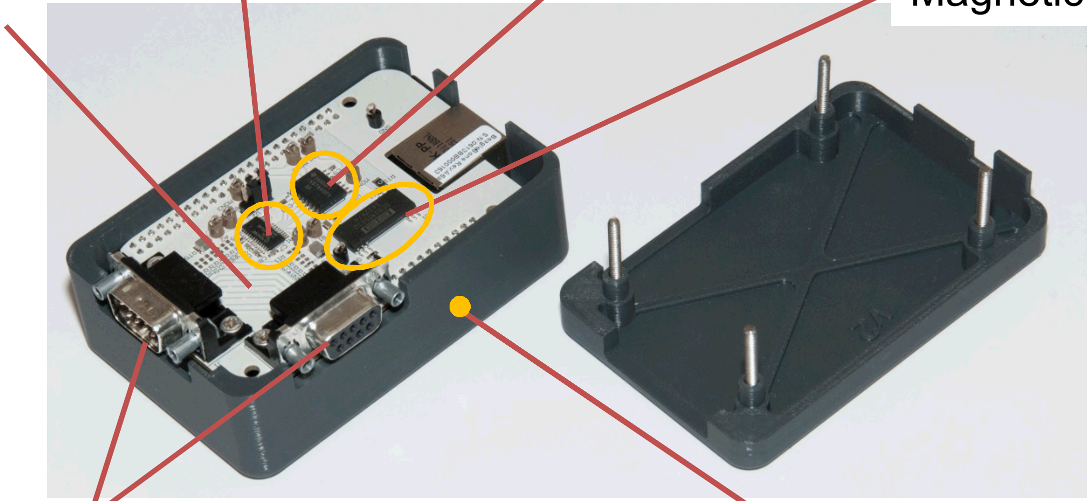

Enhanced Data Authentication System (EDAS) Junction Box
Packet digital signer and encrypter
Communication interface to Secondary Observer
Detect tamper
Heartbeat
Timestamp and packetize data
Monitor changes in unused pins of communication link
Detect cable disconnect
Electrical isolation barrier
Communication interface to sensor
Passive listener
Communication interface to Primary Observer

EDAS Branching Electronics Architecture



- Resistive coupling isolates EDAS from the operator system (fault condition)
- Signal receiver enables compatibility with RS-232 (or other standard)
- Signal isolation breaks ground loops and ensures transmission is only to, and not from, the inspector
- Power and ground isolation for immunity to power transients

EDAS is non-interfering



Signal lines are continuous between the connectors

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

Capacitive data isolator

Magnetic power isolator

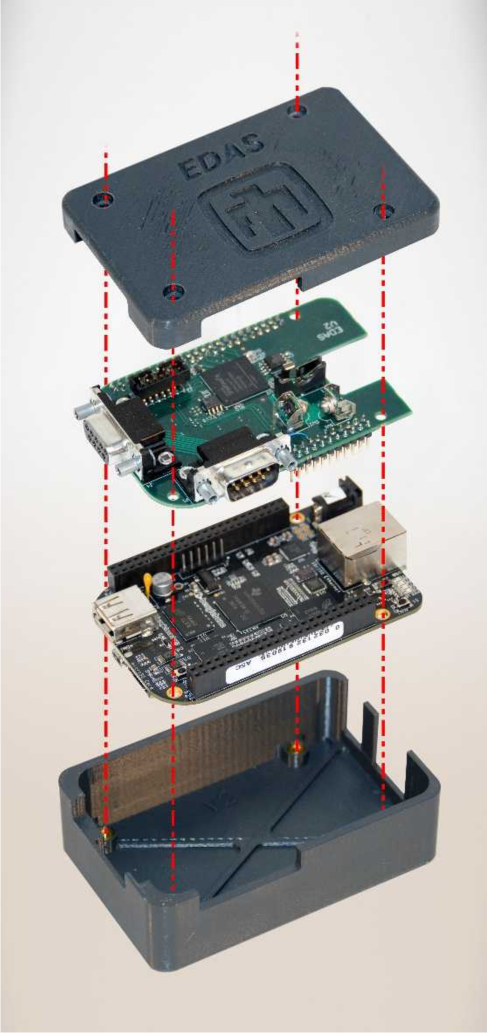
9-pin RS-232 connectors for operator signal in / out

BeagleBone Black processor board

A custom PCB that transforms and isolates the operator signals from EDAS

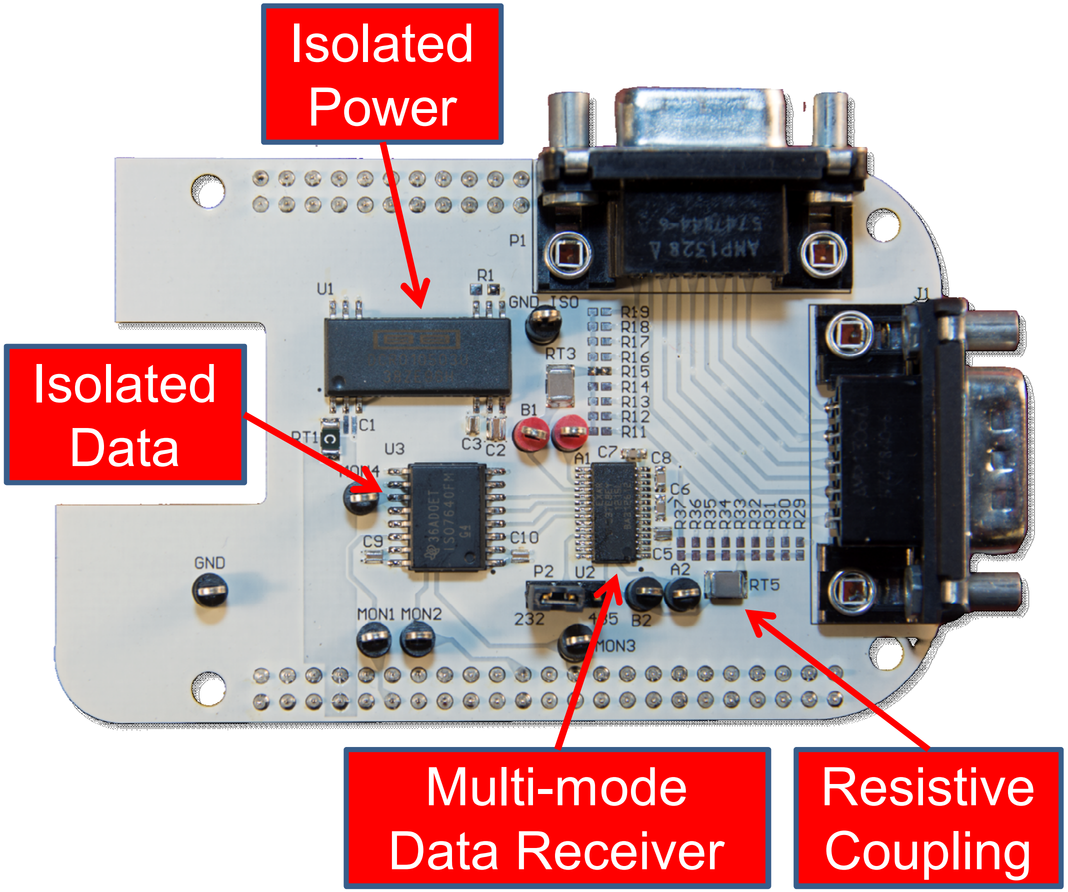
The EDAS Junction Box

- COTS single-board computer
  - BeagleBone Black (BBB)
  - Interface to inspector computer
  - Power for entire junction box
- Custom PCB
  - BeagleBone cape interface
  - Modular design for different instrumentation interfaces
- 3D-printed enclosure
  - Plastic jet printing
- Optional rechargeable Li-ion battery



EDAS Generation 2

- Version used for field trial
- RS-232 or RS-485
  - 250 kbps/15 Mbps
- Configurable signal tap-off
  - Limit of 4
- 1kV power isolation
- 4kV data isolation



Isolated Power

Isolated Data

Multi-mode Data Receiver

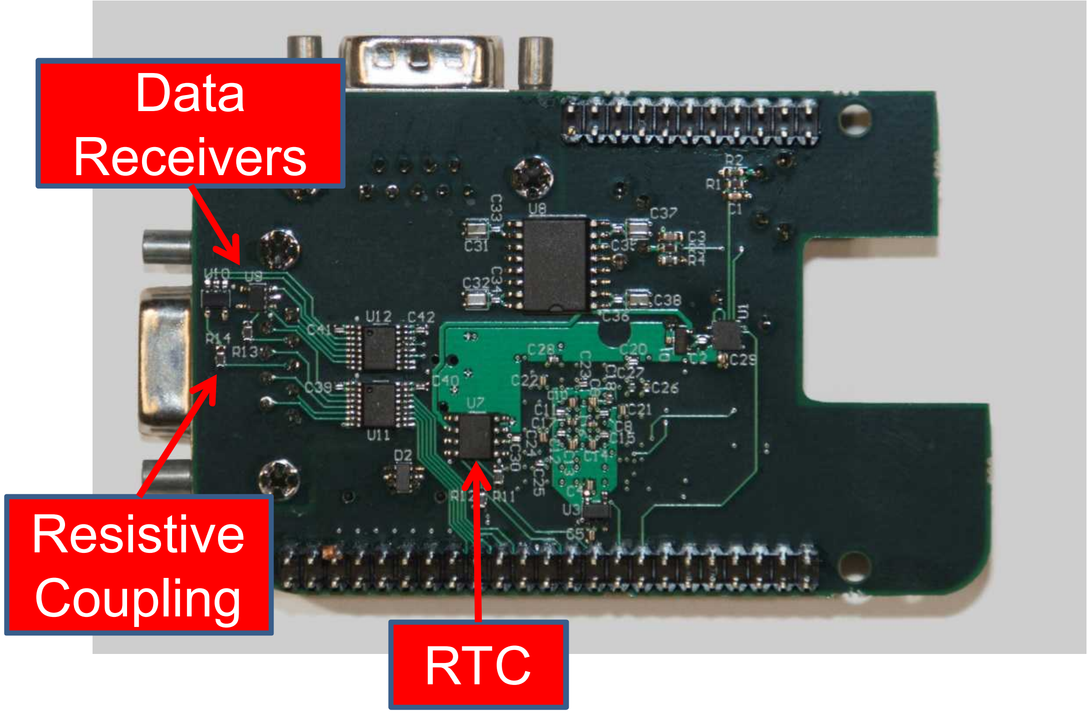
Resistive Coupling

Lessons Learned from Field Trial

- The EDAS Junction Box did not keep accurate time
  - Time reset when power is lost
- Junction box could not detect if operator signal cable was disconnected and/or if data was being transmitted on unused conductors
- Cryptographic schema could be improved
- Need tamper-indicating enclosure to protect cryptographic keys

EDAS Generation 3

- Current version for commercialization
- RS-232 only
  - 1.5 Mbps max data rate
- 2.5kV power isolation
- 5kV data isolation
- Cable disconnect detection
- Unused signal line monitoring
- Extremely accurate (±5ppm) RTC



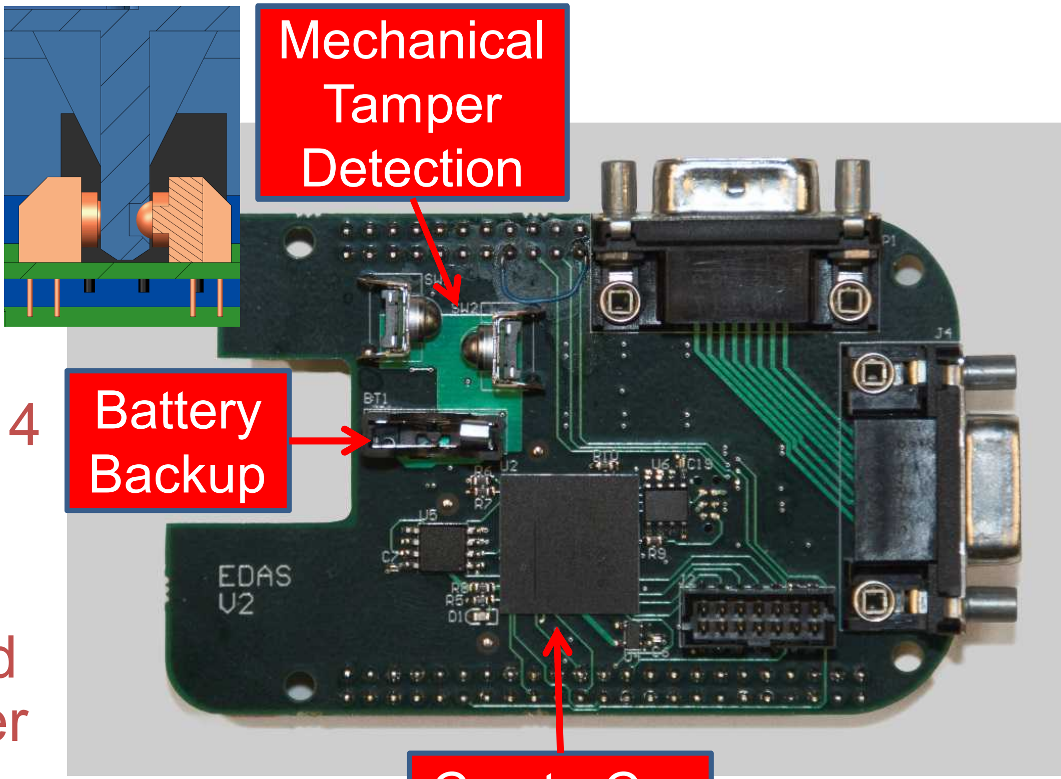
Data Receivers

Resistive Coupling

RTC

EDAS Generation 3 (cont.)

- Tamper detection
  - Mechanical scheme identical to RMSA
  - Environmental monitoring
  - FIPS-140 security level 4 (with foil)
- Battery Backup
  - Maintains RTC time and private key during power outage
- Dedicated hardware cryptography



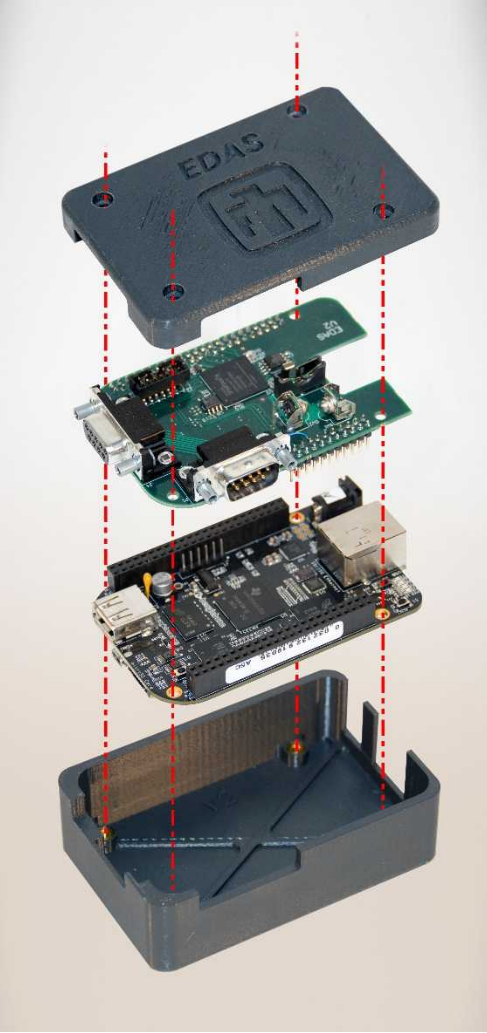
Mechanical Tamper Detection

Battery Backup

Crypto Co-processor

Junction Box Prototype Unit Cost (Quantity 10)

- Single Board Computer: $56
  - BeagleBone Green: $39
- Enclosure: $150
- Generation 2 Cape
  - PCB: ~$25
  - Parts: ~$36
- Generation 3 Cape
  - PCB: ~$50
  - Parts: ~$110
- Costs will vary based on features and quantity



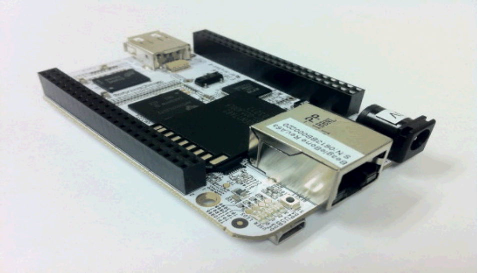
Cryptography

- Elliptic Curve Digital Signature Algorithm (EC-DSA)
  - FIPS 186-4 / NSA Suite B
  - Signing of data (and verification of commands if desired)
  - 233-bit key size (Koblitz curve, polynomial basis)
- Elliptic Curve Fully Hashed Menezes-Qu-Vanstone (EC-FHMQV)
  - Authenticated key agreement protocol
  - Generates 128-bit shared session secret key
  - Protection against active attacker
- Hardware (true) Random Number Generator
  - Satisfies NIST SP 800-22

Cryptography (cont.)

- Performance
  - Can sign up to 128 kB at a time (~700 ms of data at 1.5 Mbps)
  - Signature Time: ~5 ms
  - Communication over SPI bus: 2 Mbps
- Security
  - Over (4.0V) / under (2.1V) voltage detection
  - Over (95C) / under (-35C) temperature detection
  - All-analog tamper circuit, key destruction in ~50 µs
  - Anti-remanent key storage

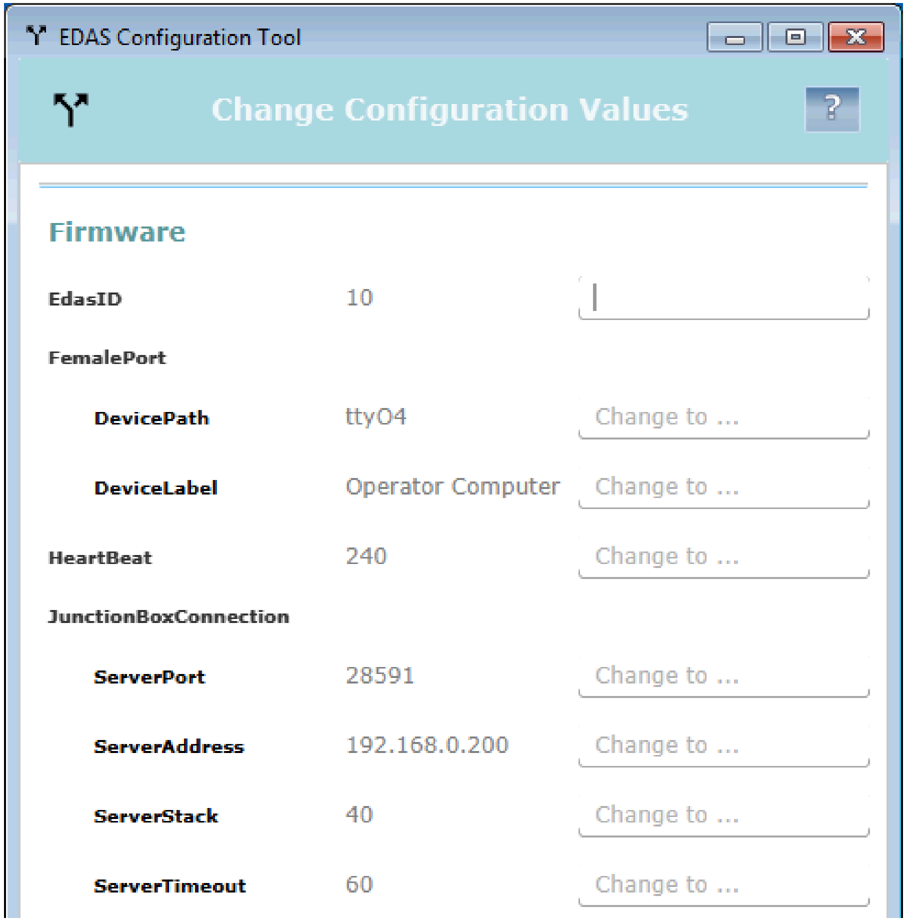
EDAS Software



- All software written in Java
- Junction Box
  - Runs on BeagleBone Black processor
  - Linux operating system starts as soon as power is available and starts EDAS software service
  - Junction box sends various packets types to inspector computer
  - Robust: can recover from power lapses, breaks in signal connections, etc.
- Inspector Computer
  - Operating system loads as soon as power is available and starts EDAS software service
  - Cryptographic operations performed using BouncyCastle open-source software library

Junction Box Configuration Tool

- Tool to configure junction box before deployment

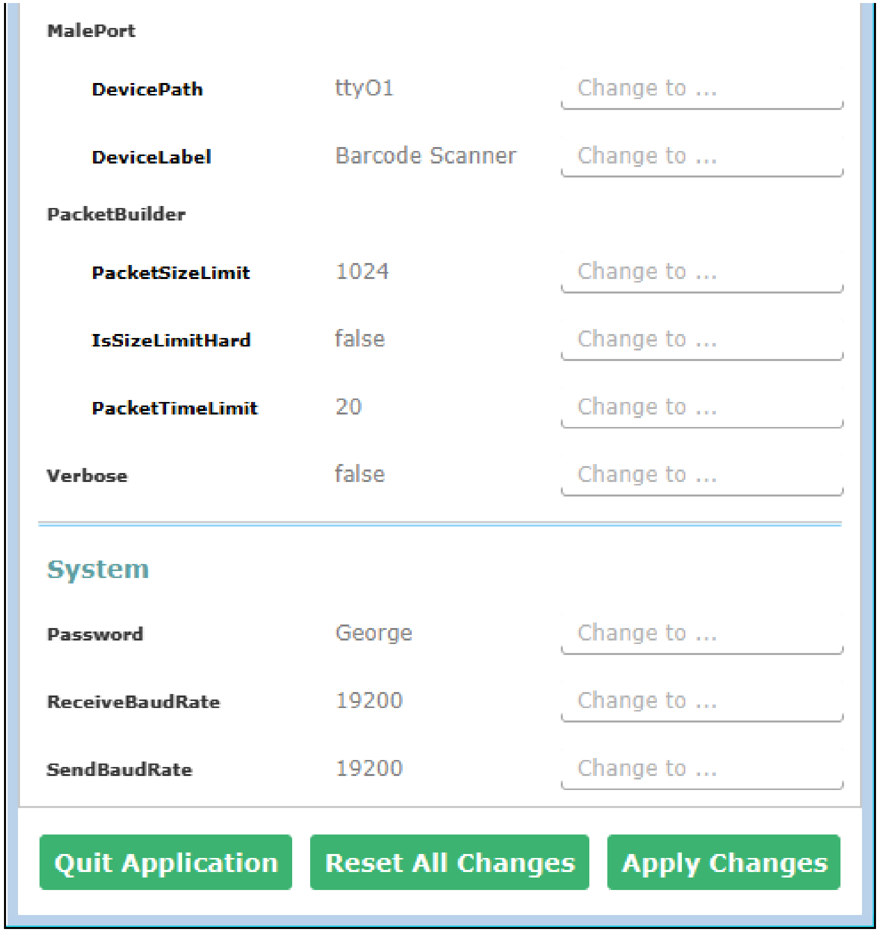


Firmware

EdasID	10	
FemalePort		
DevicePath	tty04	Change to ...
DeviceLabel	Operator Computer	Change to ...
HeartBeat	240	Change to ...
JunctionBoxConnection		
ServerPort	28591	Change to ...
ServerAddress	192.168.0.200	Change to ...
ServerStack	40	Change to ...
ServerTimeout	60	Change to ...

Junction Box Configuration Tool (cont.)

- Tool to configure junction box before deployment



MalePort

DevicePath	ttyO1	Change to ...
DeviceLabel	Barcode Scanner	Change to ...

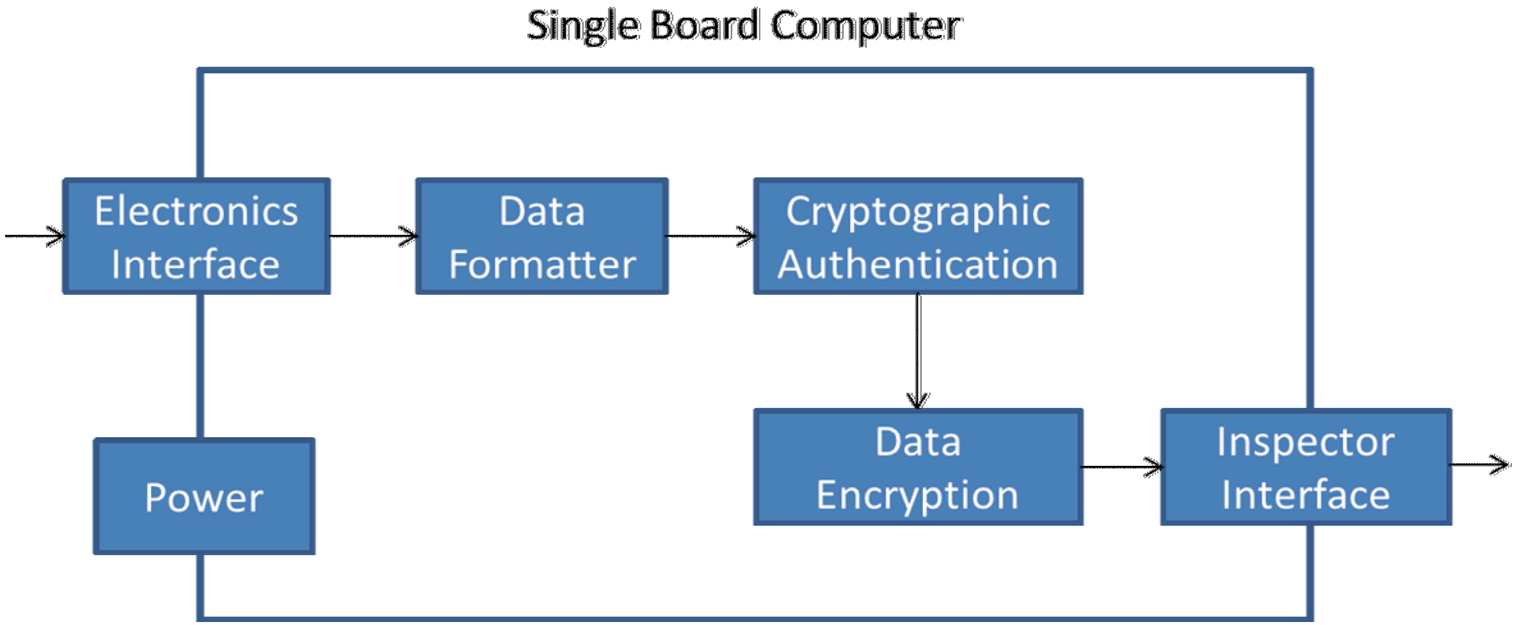
PacketBuilder

PacketSizeLimit	1024	Change to ...
IsSizeLimitHard	false	Change to ...
PacketTimeLimit	20	Change to ...
Verbose	false	Change to ...

System

Password	George	Change to ...
ReceiveBaudRate	19200	Change to ...
SendBaudRate	19200	Change to ...

EDAS Junction Box 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
- Digital signing of data packets to ensure data integrity
- Encryption for data confidentiality
- Processed data are pushed via TCP/IP interface to inspector system

EDAS Junction Box Packets

Packet Type	Packet Function
DATA	Branched operator instrumentation data
HEARTBEAT	Junction box state of health
TAMPER	Tamper indicating enclosure
SERIAL	Instrumentation cable disconnect
LEVEL_CHANGE	Signal activity on unused conductors in operator instrumentation cable
WARN	Junction box warning or error

Data Packet Formation

- Junction box has no a priori understanding of operator instrumentation data passing through junction box
- Packets are “built” using a combination of data size and time
  - Time: accumulate bytes until timer expires
  - Size: specify minimum or maximum packet size, in bytes
  - Can be combined, but time takes priority

Inspector Computer Software

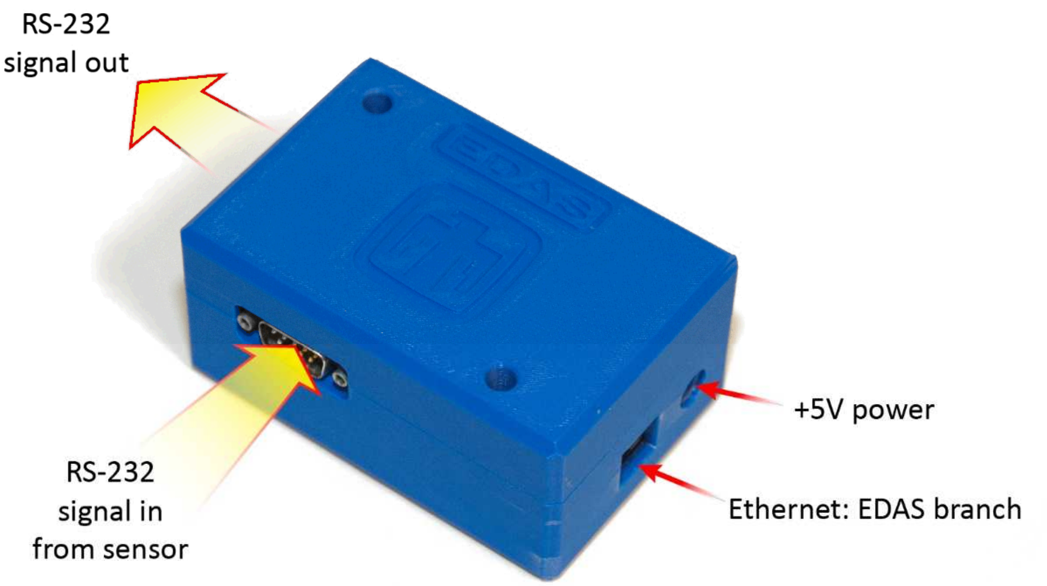
- Simultaneous connection to multiple EDAS junction boxes
- Decryption of data packets
- Verification of digital signature for data integrity
- Store data to a CSV file in ASCII format
- No *a priori* understanding of data passing through
  - Interface to Euratom RADAR Software to format packets in the same way as the operator interprets them

EDAS Commercialization

Goal:
Create a commercially-available version of EDAS

- Manufacture new EDAS Junction Box prototypes and update software
  - Incorporating lessons learned from the field trial
- Protect EDAS intellectual property via patent and copyright
- Currently in discussions with vendors

Prototype Status



- ✓ Designed and fabricated hardware prototypes
- ✓ Completed new Junction Box firmware and inspector computer software
- ✓ Created Junction Box configuration tool
- ✓ Currently performing functional, robustness, and longevity testing

Commercial Vendor Status

- We are in talks with commercial vendors familiar with safeguards applications under non-disclosure agreement
  - Executing a Test & Evaluation license, and vendor is evaluating EDAS
  - Next step: Non-exclusive license and tech transfer
- Protection of intellectual property to make EDAS more attractive to a commercial vendor
- Provisional patent filed in Nov. 2016
  - Application Serial No. 62/423,714
  - Patent application to be filed in early 2017

Summary

- EDAS is a low-cost option for branching and authenticating operator data
  - Mitigates operator concerns with isolation and directionality
  - Standards-based public key cryptography with sufficient key length
  - Currently RS-232, but extension to other standards is simple due to modular design
  - Software interface allows for simple integration with RADAR or other analysis programs
- Commercialization ongoing

Questions?

Additional Cost Information

- Time Keeping
  - RTC: $5.40
  - Battery: $1.62
  - Battery Holder: $0.69
- Cryptography
  - Crypto FPGA: $70
  - RNG: $15
- Quantity of 100: Parts are 75% of cost
  - BB and enclosure same cost
  - PCB: $25
- Injection molded case has large upfront cost to create molds