SAND2011-0105P

Louisiana Enrichment Services Gas Centrifuge Enrichment Plant Authentication Issues

Joe Damico
Senior Member of the Technical Staff
Sandia National Laboratories
Albuquerque, New Mexico, USA

Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company for the
United States Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

Topics

- Draft Safeguards approach for Louisiana Enrichment Services (LES) Plant
- Proposed data transfer system
- Potential issues with data transfer system
- Similarities with K-Area Material Storage (KAMS) data transfer system
- Authentication approaches for load cells and scales
- Conclusions

LES Draft SG Approach Overview

- Draft LES Safeguards approach relies on information sharing
  - Facility will periodically download data from
    - All load cells and authenticated accountancy scales
    - On-line mass spectrometers
    - Mailbox Declarations
  - Data transfer system may include an “air gap” between facility & IAEA
    - Data Diode provides security while allowing near real-time transfers

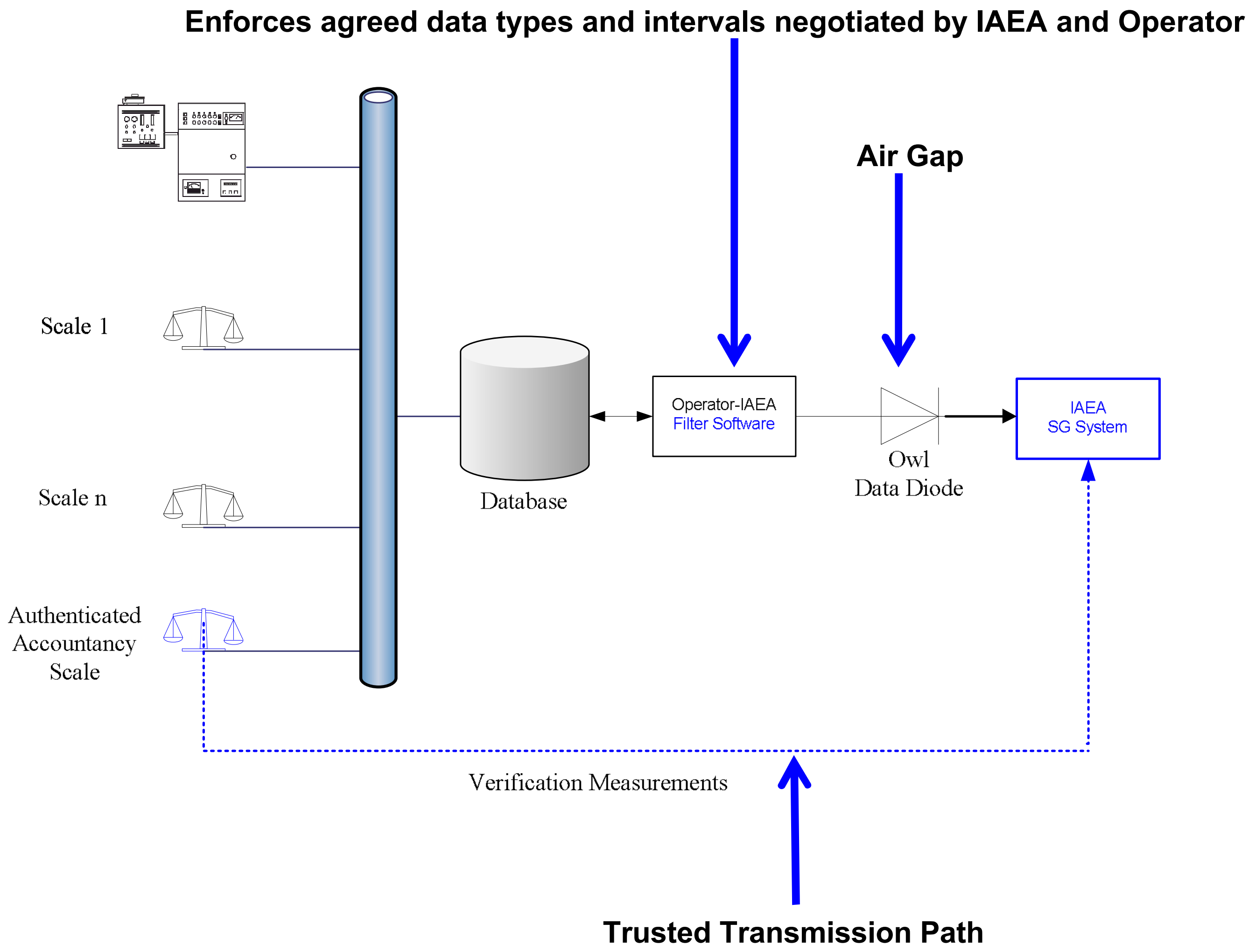
LES Draft SG Approach Issues

- Operator concerns include
  - Disclosure of proprietary and/or classified data to IAEA
  - Data and system security: IAEA connection introduces vulnerabilities
  - Operator systems may not be able to transmit IAEA authentication data
    - Operator data collection systems & database designs not easily modified
- Possible IAEA concerns include
  - Detecting missing or spoofed data
  - IAEA could need independently verified data to trust plant data.
  - Authentication of operator systems and data
    - How to transmit authentication data from in-plant systems

LES Draft SG Approach Issues (2)

- Shared concerns
  - Data Filter is a key concern
    - Identification and negotiation of data and sampling rates for transfer
    - Both parties need to trust system
      - Operator would probably develop this since it runs on their network
      - IAEA would need to trust that filter delivers all negotiated data
- Shared benefits
  - IAEA access to plant data could benefit both IAEA and Operator
    - IAEA has lower equipment & maintenance costs with more information
    - Operator possibly benefits from smaller IAEA footprint at plant

Key Data Transfer System Features



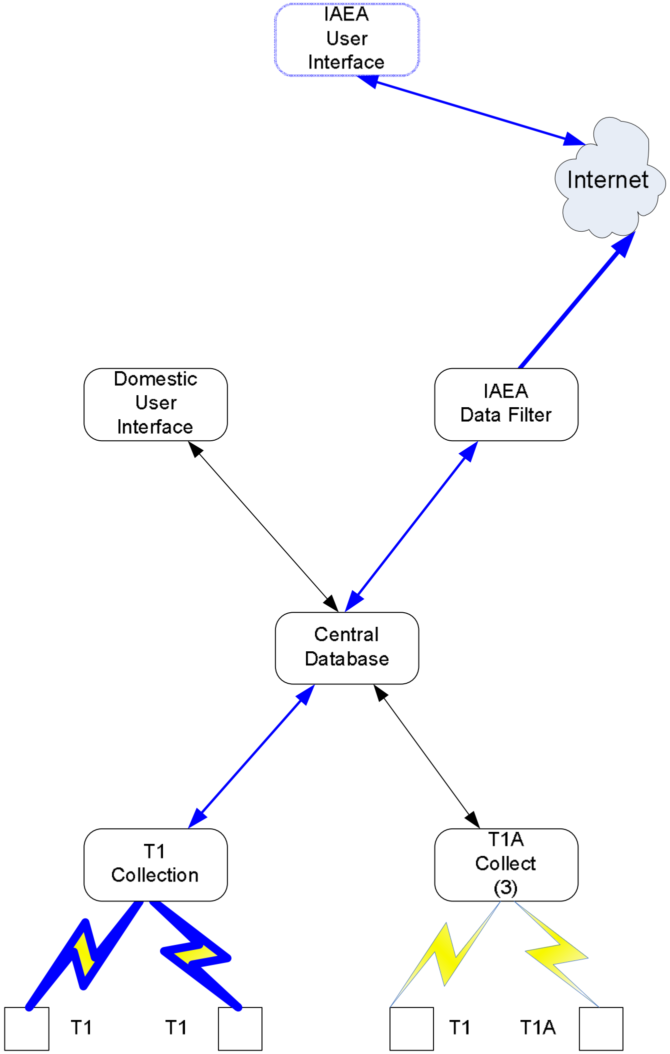
Enforces agreed data types and intervals negotiated by IAEA and Operator
Air Gap
Scale 1
Scale n
Authenticated Accountancy Scale
Database
Operator-IAEA Filter Software
Owl Data Diode
IAEA SG System
Verification Measurements
Trusted Transmission Path

LES Data Transfer Resembles KAMS

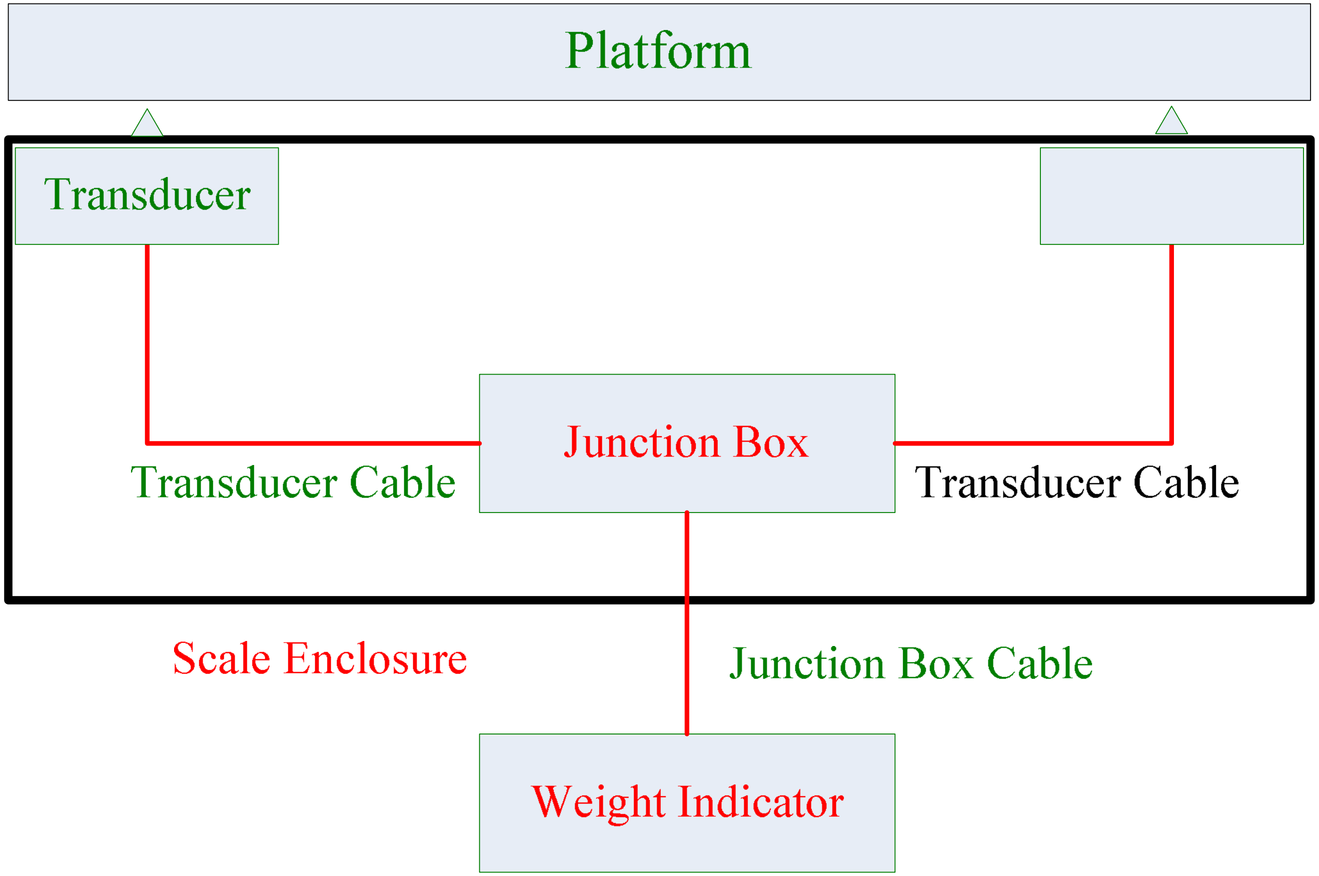
- Operator owned KAMS data system processes IAEA seal data
- IAEA data stored in the same database as operator data
- Operator filter SW extracts and formats IAEA data from system
- Data transferred to IAEA system on-site
  - Data transferred from on-site IAEA system to IAEA Headquarters
- Data transfers to IAEA require significant network security
- Key difference: KAMS scheme has sensor level authentication
  - IAEA authentication data collected and stored by domestic system
  - Authenticated IAEA seals provide tamper indication
  - Message and event counters reveal missing data

KAMS Data Transfer System

Mass Spec

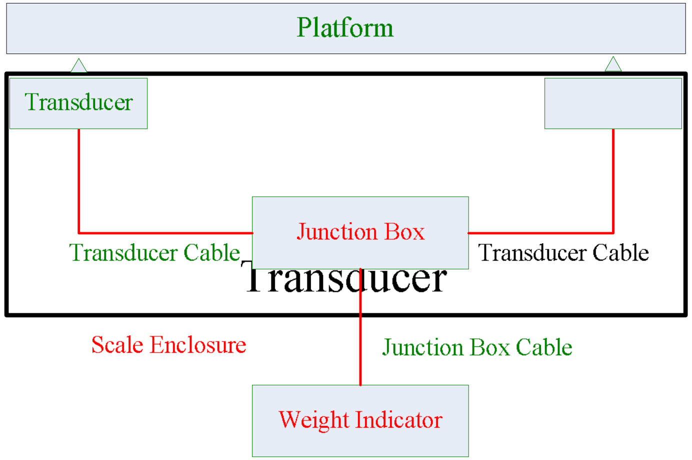


Scale Authentication: Simple Schematic



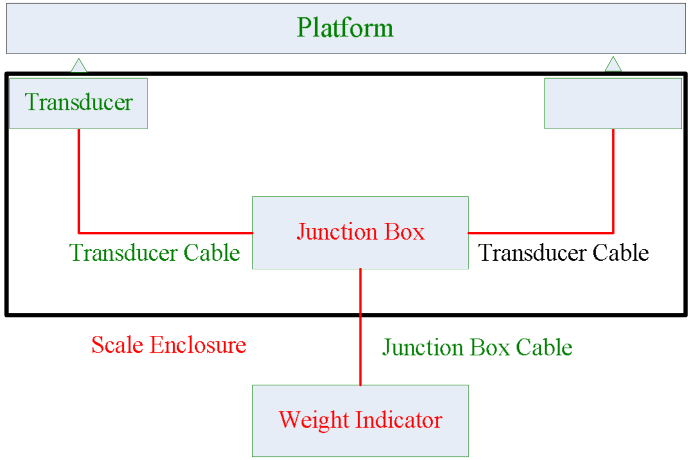
A

Scale Authentication Issues: Mechanical



- Mechanical Issues
  - Mechanical tampering (thumb on the scale)
  - Mechanical parts must move freely
    - Requires careful application of Tamper Indicating Enclosure (TIE)
  - Environmental factors bias measurements
    - Drafts, fans, building heating and cooling
    - Convection from cylinder cooling/heating

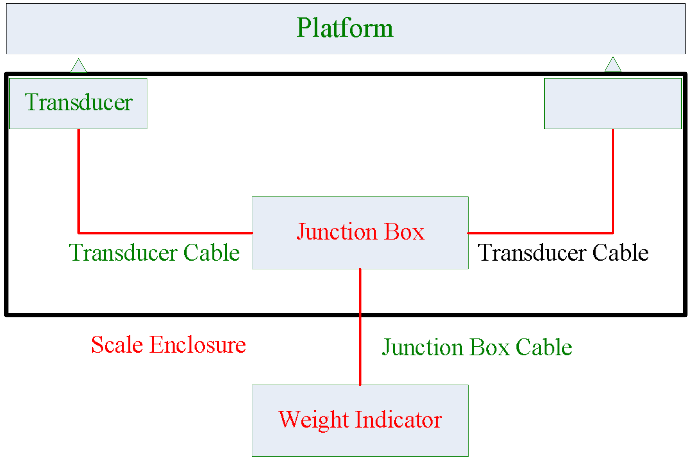
Scale Authentication Issues: Electronic



Electronic Issues

- Low level load cell signals
  - Signal level proportional to excitation voltage (mV/V)
  - Cables may need shielding from noise and possible tampering
- Signal conversion electronics complex and often proprietary
  - Difficult to authenticate

Scale Authentication Issues: Systematic

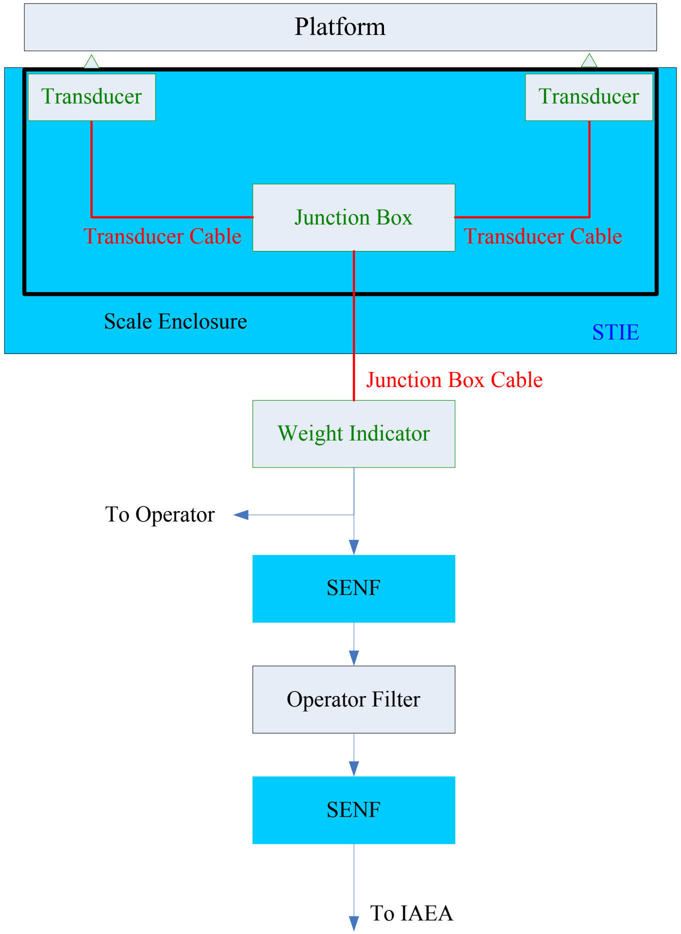


Systematic Issues

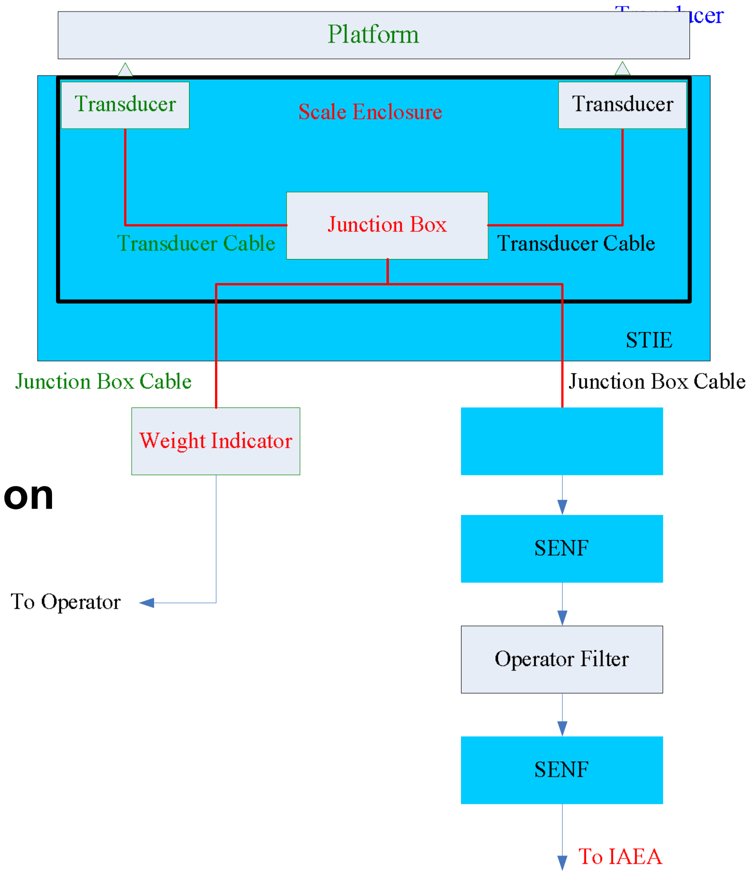
- Mass measurements depend on tare measurements
  - Tare is complex
    - Tare based on cylinder manufacturer's data and tails
      - Difficult to accurately measure tare once cylinder is used
    - Tare easily manipulated by adding/removing weights
- Scales and load cells are part of a larger system
  - Scale integrity not important if system process flow has vulnerabilities

Scale Authentication Concept 1

- Shared Scale with Shared Electronics
  - Less intrusive and easier to implement
    - Signal split after scale electronics
      - No modification to scale
  - Hard to authenticate
    - Must trust complex scale electronics
    - Comparing both outputs does not help
      - System manipulation impacts both outputs

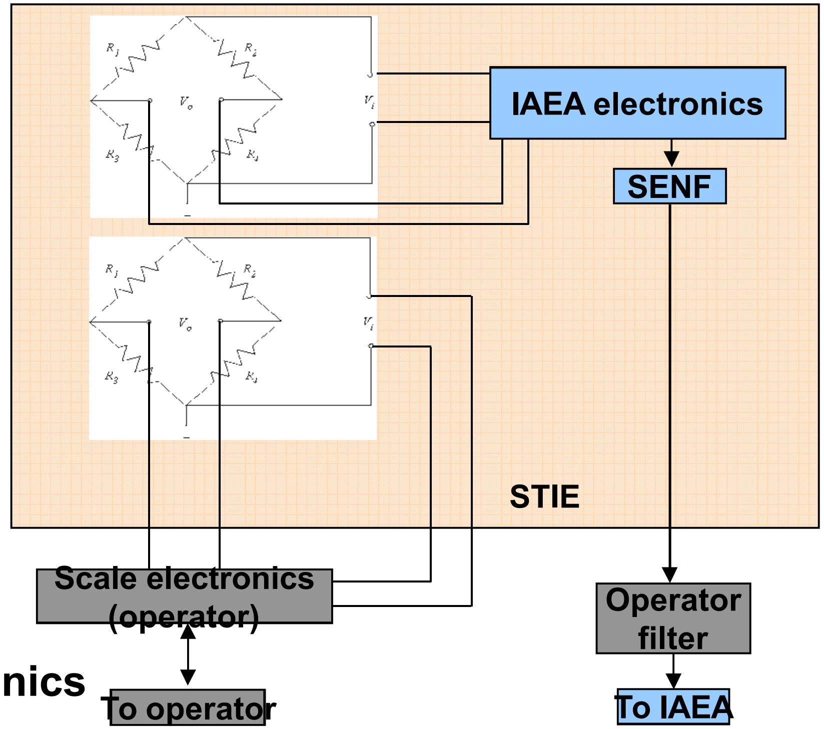


Scale Authentication Concept 2



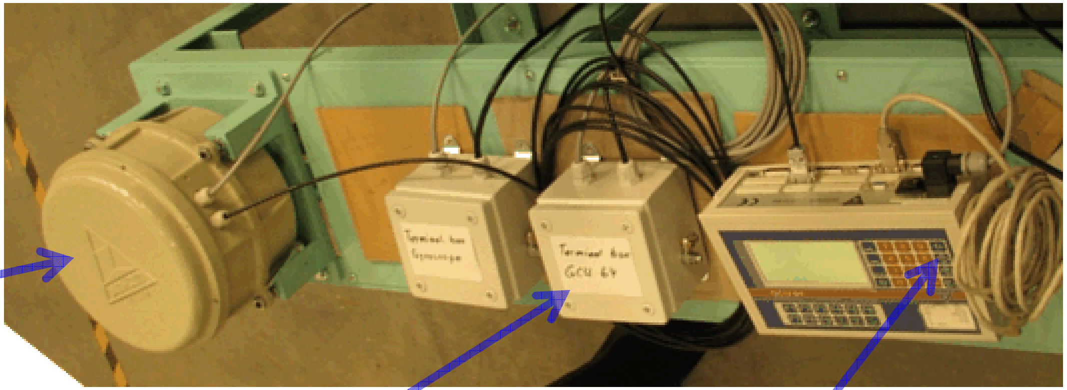
- Shared Scale with Separate Electronics
  - More intrusive and harder to implement
    - IAEA electronics and cables need protection
    - Scale modifications needed
      - Signal splitter and STIEs
  - Harder to authenticate
    - Scale electronics can manipulate signal
    - Independent IAEA electronics can give false sense of security

Scale Authentication Concept 3



- **Dual Transducers**
  - **Independent Data for IAEA**
    - **Separate IAEA transducer and electronics**
  - **More Intrusive**
    - **Requires retrofit on existing equipment or modifications of standard models**
    - **Need TIEs on IAEA electronics and cables**
  - **Best concept identified in Vulnerability Review**

WOHWA Scale Authentication Concepts



- Concept 3
  - Separate Optical Transducers
- Concept 1
  - Split binary data stream
- Concept 2
  - Split Optical Pulse Train Signal
- All concepts require mechanism to deliver authenticated data
  - May need a separate data transmission path
    - Current plant data systems may not work with this data

Conclusions

- Draft Safeguards Approach for LES has benefits & potential issues
  - IAEA benefits from wealth of plant data but needs to trust it
  - Data Filter functionality requires negotiation
  - IAEA needs to trust that filter delivers all negotiated data
    - Spoofed and missing data are possible concerns
  - IAEA needs mechanism to independently verify plant data
- *Authenticate*d scale provide independent verification
  - Several approach concepts available
  - Transmission of authenticated data an important issue
    - Current operator data systems will probably not work
    - May need an independent transmission path