SAND2015-6832PE

Exceptional service in the national interest

Sandia National Laboratories

Data Authentication for the Nondestructive Assay of Spent Fuel

George Baldwin

August 2015

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.

Context

- We support the Next Generation Safeguards Initiative Spent Fuel (NGSI-SF) project to develop advanced nondestructive assay (NDA) instrumentation for spent reactor fuel
  - All project work by U.S. national laboratory participants is funded by the U.S. National Nuclear Security Administration (NNSA)
  - Sandia has responsibility for the data authentication task
- SKB also collaborates with the NGSI-SF project
  - In particular, SKB has been providing field test opportunities at Clab for prototype instruments: Passive Gamma, DDSI, DDA…

Why are we here?

- This visit differs from others by the project team
  - We are not here to do (or plan for) measurements at Clab
  - We are looking ahead to the possibility for a deployed safeguards instrument to support spent fuel encapsulation (e.g., at CLINK)
- Our goals
  - We wish to understand better the *operational environment* for routine use, both physical and procedural
  - We wish to understand better the *stakeholder requirements* for routine use, both interests and constraints
  - Encourage communication with SKB about helping design controls for the CLINK facility

Motivation: Safeguards by Design

- During their development, NDA systems for spent fuel assemblies (SFAs) are “attended” systems
- Their use in an eventual routine application would likely be as “unattended” systems, either
  - Fully automated, e.g., as part of a robotic system
  - Operated by the facility

- The “data authentication” task poses the question:

What (else) is necessary for a safeguards inspectorate to trust the information from the spent fuel NDA system(s) when operated in unattended mode?

Unattended (or remote) operation: What does an inspector need to know?

Sandia National Laboratories

- The measurement information is indeed from the NDA instrument
- The information pertains to the particular SFA in question
- The information has not been altered since the measurement was performed
- All measurement conditions were in fact as reported
- No complicating factors were present
- Continuity of knowledge for this SFA can be maintained reliably

All of this must be assured by the unattended system
without any reliance on trust

Trust cannot be a factor in accepting the truth of the measurement results

Sandia National Laboratories

- Technical security measures (such as data authentication and tamper indication) ensure the faithful reporting of measurement results
  - No accidental corruption
  - No malicious manipulation
- Other measures may be necessary to establish the truth of the measurement results
  - Instrument calibration
  - Instrument diagnostics

- NOT an acceptable basis for accepting the results:
  - “These are the numbers I was expecting…”

Assumptions: Routine Use

- The instrument must be capable of operating in *unattended mode*
- The measurement will be essential to the IAEA Safeguards objective for *independent verification of* material accountancy declarations
- Other entities also have an interest in the measurement results
  - Operator (SKB)
  - National Authority (SSM)
  - Regional Authority (Euratom)
- Encapsulation: the measurement is likely the *last* one that will be possible for each particular SFA

Joint use greatly complicates unattended measurements

Sandia National Laboratories

- A new potential threat now exists within the secure perimeter: the other party
- At least two issues:
  - Another party may be able to *manipulate* the information
  - Another party is able to *know* the same information
- For cryptographic authentication of digital data
  - Public key cryptography is necessary: only one secret key able to "sign" the data; multiple public keys able to validate the signature
  - Key management is critical: only the trusted source of the data should know the secret key
  - Ideally, the private/public key pair is generated within the trusted source itself
- All parties must accept that the instrument is secure/impartial

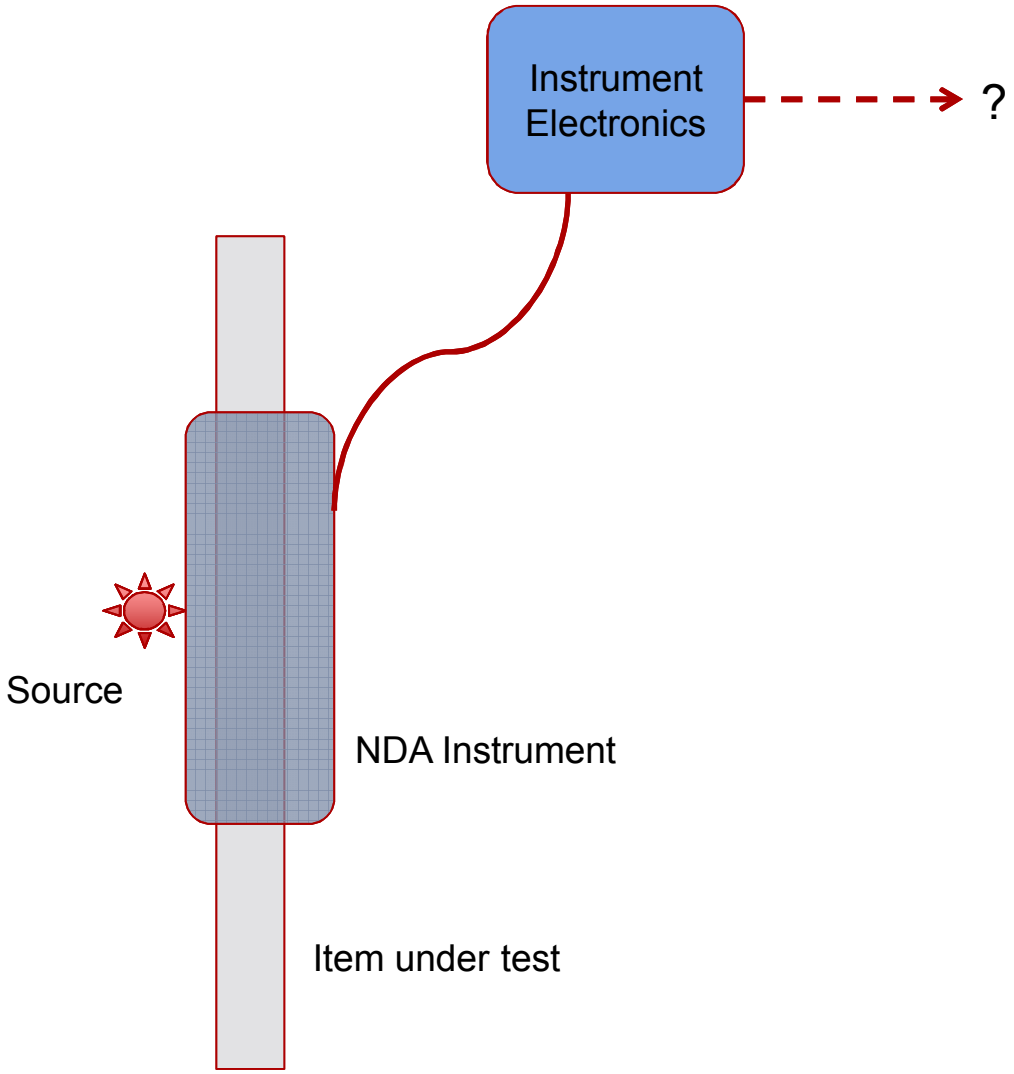
Joint use (continued)

- IAEA requirements for joint use are governed by internal policy paper 20
- Operator would need to declare a SFA *before* the measurement results could be shared
  - (the SFNDA measurement results could not inform the operator declaration)
  - Mailbox system for operator declarations?
- After measurement
  - How does the IAEA verification conclusion affect the encapsulation process? Must the operator wait for a go / no-go indication from IAEA? From Euratom?
  - How do the measurement results affect the operator decisions concerning that SFA? What options does the operator need?

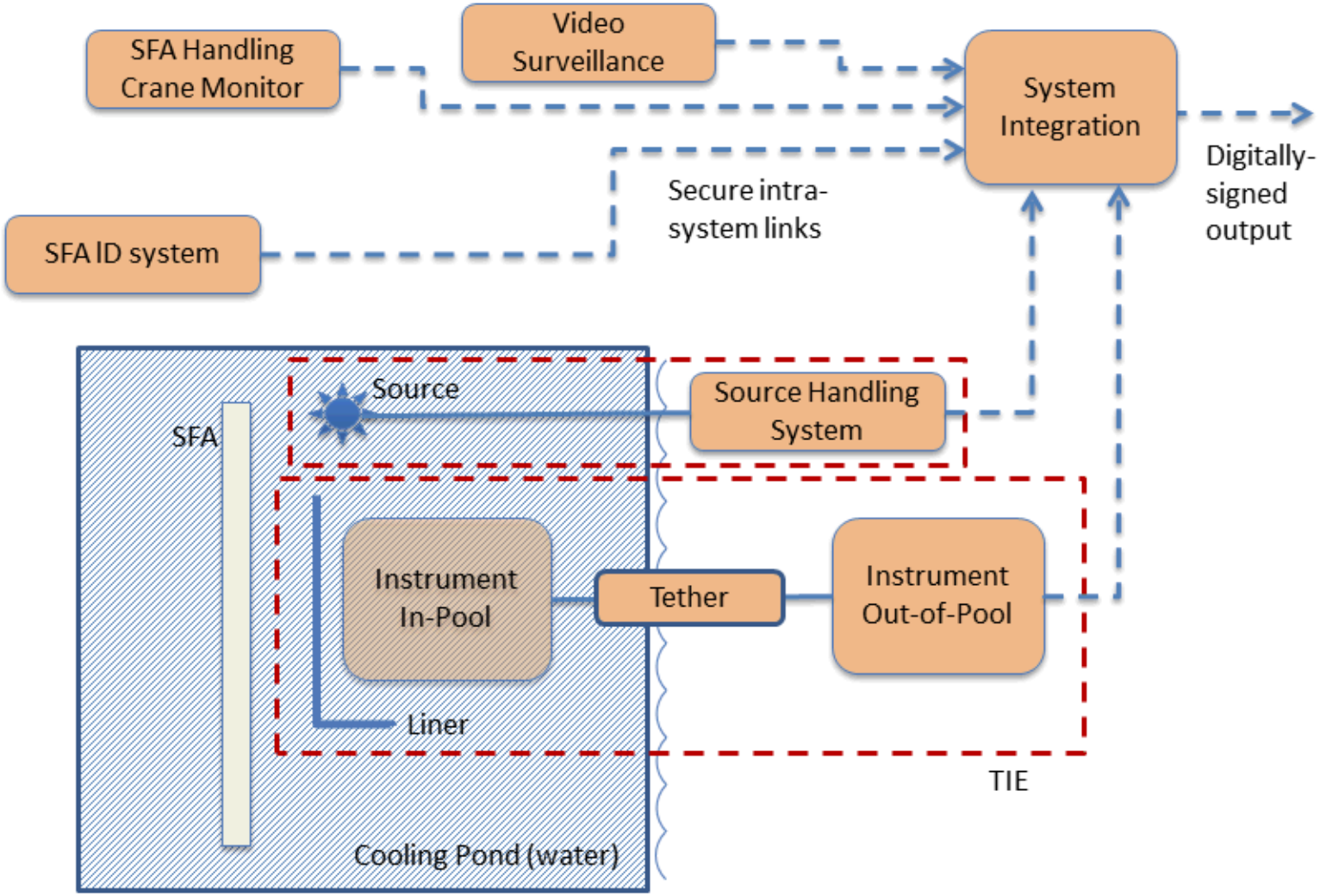
Generalized measurement scenario

Factors:

Interrogating source (if required)
Position of that source (if required)
Item being measured
Position of that item
Environment
Instrument configuration
Instrument integrity
Instrument-measured data
Timing



Notional system configuration



The notional system is only a guess: What is *actually* necessary or planned?

Sandia National Laboratories

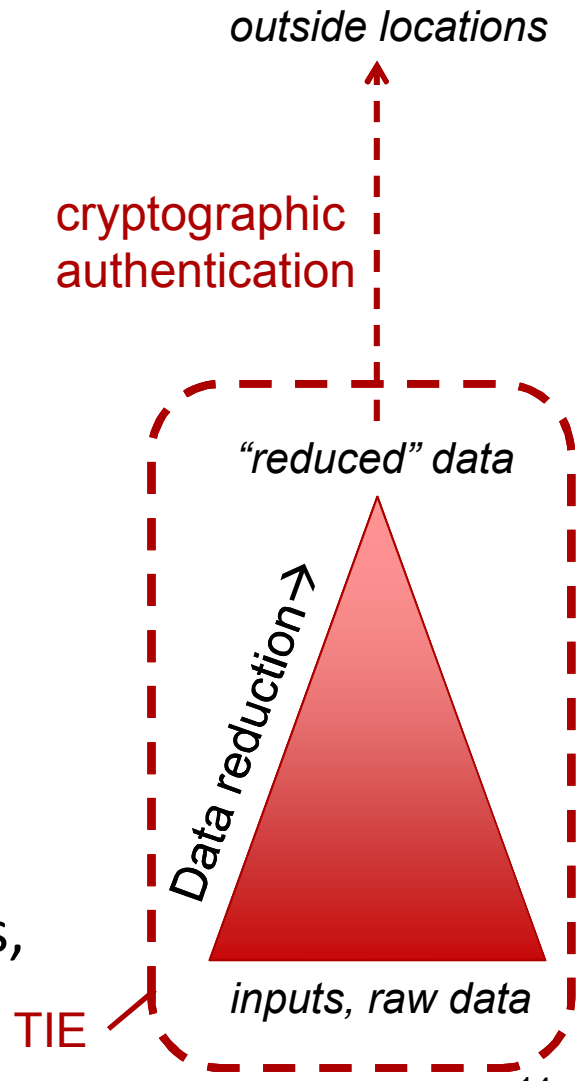
- The physical layout and design of the facility
- What is the process of moving SFAs from wet storage to encapsulation?
  - Where does the process permit temporary storage of assemblies?
  - What are the conditions that allow a SFA to proceed to encapsulation?
  - What is the system that maintains a continuity of knowledge of SFAs?
- How are SFAs identified?
  - By the operator
  - By the safeguards inspectorate
- How are both normal and off-normal events handled?
  - SFA that might be returned to storage?
  - Situation where the SFNDA instrument isn't working?
  - Other situations that might be anticipated?

Procedural considerations

- What is the role for the safeguards measurement in the encapsulation process?
  - Information only; encapsulation proceeds regardless of the results
  - Measurement results dictate the next steps for the operator
- What are the requirements/expectations for the measurement data and results?
  - Immediate use only (e.g., pass/fail partial defect verification)
  - Archive forever (e.g., historical record of repository content)
  - How are measurement data analyzed & abstracted to yield “results”?
- Are measurement data and/or results shared?
  - Joint use by IAEA and Euratom
  - With the operator as well?

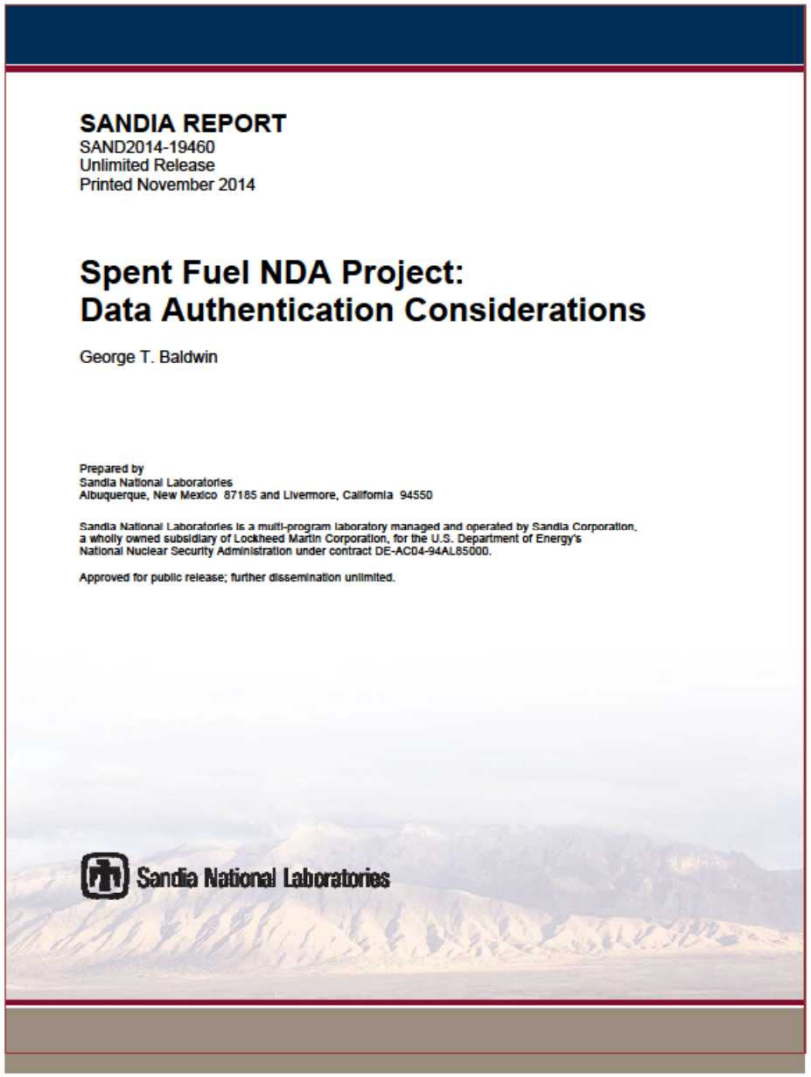
Data Reduction

- Various data streams may be consolidated to generate a measurement result
  - May be automated or done manually
- Where does that consolidation take place?
  - Within a tamper indicating enclosure (TIE)…
    - At the measurement station? Elsewhere at the facility?
    - Offsite?
- When does that consolidation take place?
  - In real time?
  - At the discretion of the inspectorate
- If multiple parties are to receive the results, do all receive the same information?



Recommendations from our initial report

- Develop use cases for these measurements
- Develop readily-verifiable tamper indicating enclosures for submerged NDA instruments to be used in unattended mode
- Define the individual ancillary instruments needed for systems implementation.
- Develop the system implementation for automated, unattended measurements
- Operate the NDA instrument continuously: self-monitoring to detect and deter tampering and report state of health.



SANDIA REPORT
SAND2014-19460
Unlimited Release
Printed November 2014

Spent Fuel NDA Project:
Data Authentication Considerations

George T. Baldwin

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico 87185 and Livermore, California 94550

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.

Approved for public release; further dissemination unlimited.

Sandia National Laboratories

Task 12: Data Authentication
Revised FY15 Milestones/ Deliverables

1) Finalize, and validate with stakeholders, the equipment and information security requirements for the NGSI-SF project

- Work with stakeholders to define the use cases
- Compare and contrast data authentication issues for the various NDA technical options

~~2) Explore potential solutions to ensure information security of instruments for unattended operation.~~

~~3) Downselect/rank among technical options and draft a proposed approach for the project.~~

~~4) Review the proposed approach with stakeholders (IAEA, Euratom, SKB, SSM, LANL, and possibly others) and revise as necessary.~~

5) Write a concluding, summary report with recommendations.

Conclusions

- The “data authentication” task effectively takes a systems engineering approach to evaluate what is required to trust information from NDA instrument
- At this stage, we wish to
  - understand the concept for routine operation
  - identify the trust issues that will inform system requirements
- These issues still need better definition, which requires stakeholder engagement
- Results from the data authentication task can inform
  - NDA instrument selection
  - Instrument engineering design
  - Implementation procedures
  - Safeguards approach