SAND2009-4260C

Next Generation Remote Monitoring Systems Program Development of the Secure Sensor Platform for International Safeguards

INMM 50th Annual Meeting
16 July 2009

Barry Schoeneman
Sandia National Laboratories
Albuquerque, New Mexico, USA
bdschoe@sandia.gov

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.

SAND Number: XXXXXX

Acknowledgements

- **Michele Smith - Program Manager**
  - NNSA, NA 241 - Warhead Fissile Material Transparency
- **Troy Ross - IT and Software Engineer**
  - Sandia National Labs
- **Keith Tolk - Systems Vulnerabilities**
  - Sandia National Labs
- **Vicki Bruch and Kevin Seager - Program Managers**
  - Sandia National Labs

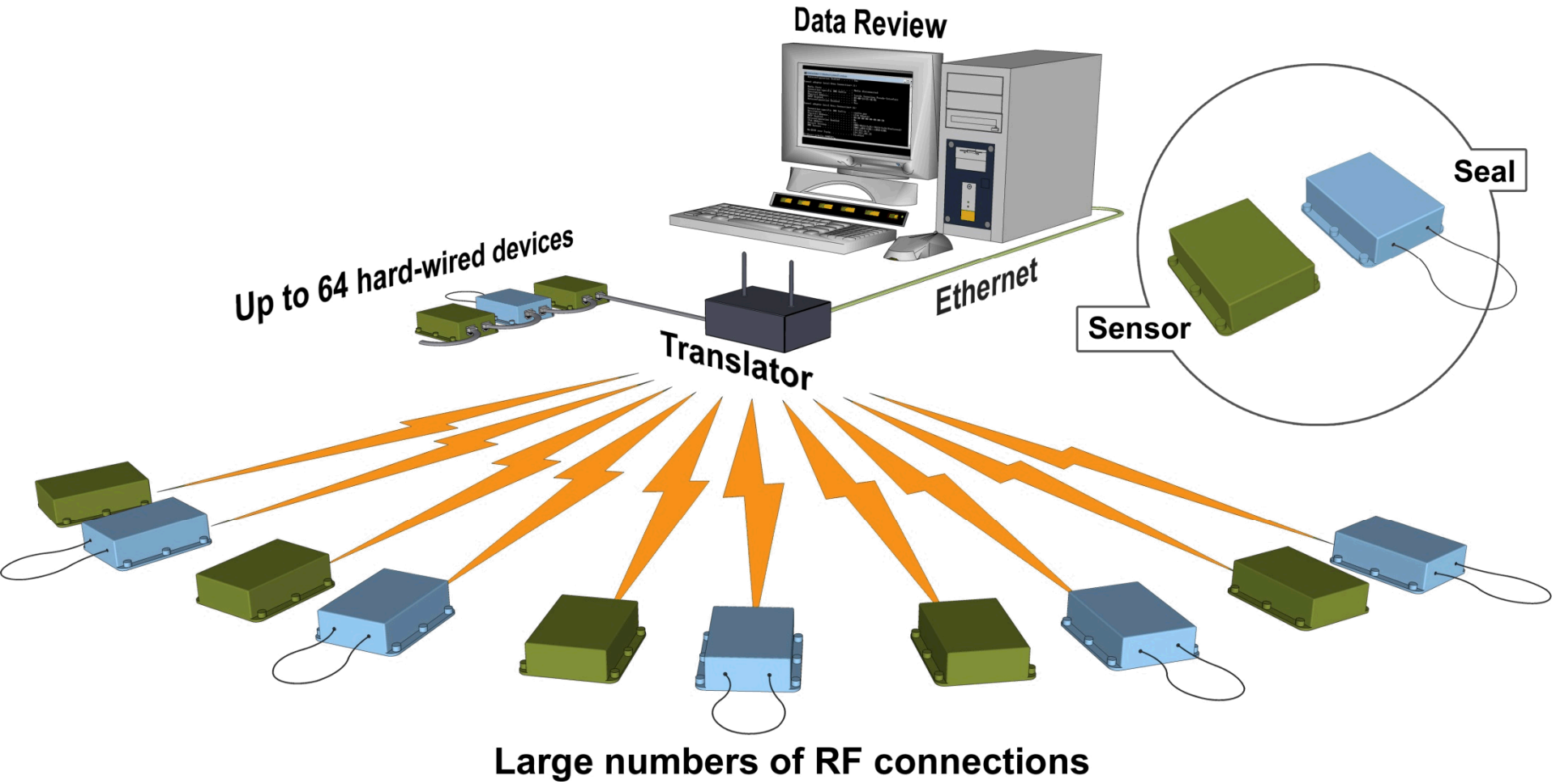
Goals of this Presentation

- Provide a high level understanding of the SSP technology
- Briefly discuss a specific application of SSP technology
- Briefly discuss future goals for SSP technology

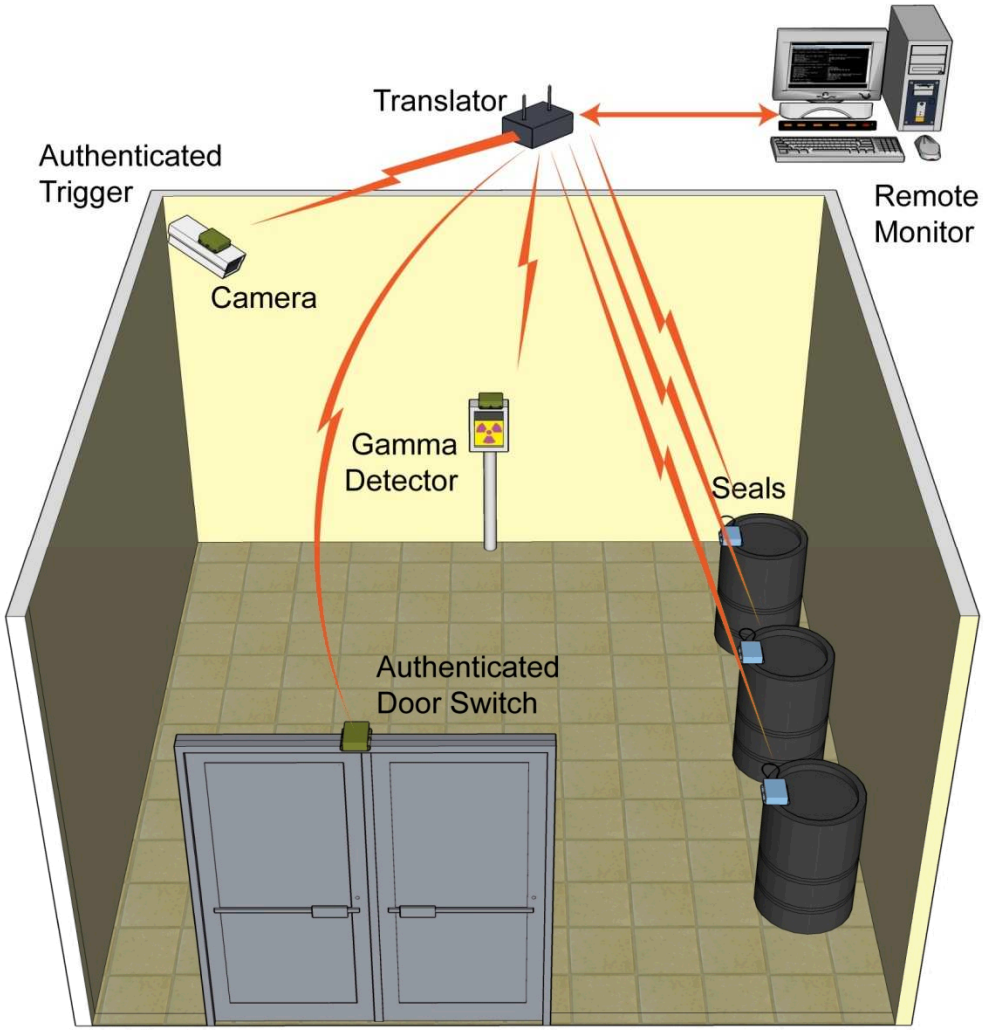
Secure Sensor Platform (SSP) - A Definition

- The SSP is a technology structure that provides for common security, communication, and cryptography capabilities.
- These capabilities are designed to be versatile for monitoring a wide variety of sensors on an application specific platform which provides secure collection and reporting of sensor data.

SSP – System Perspective



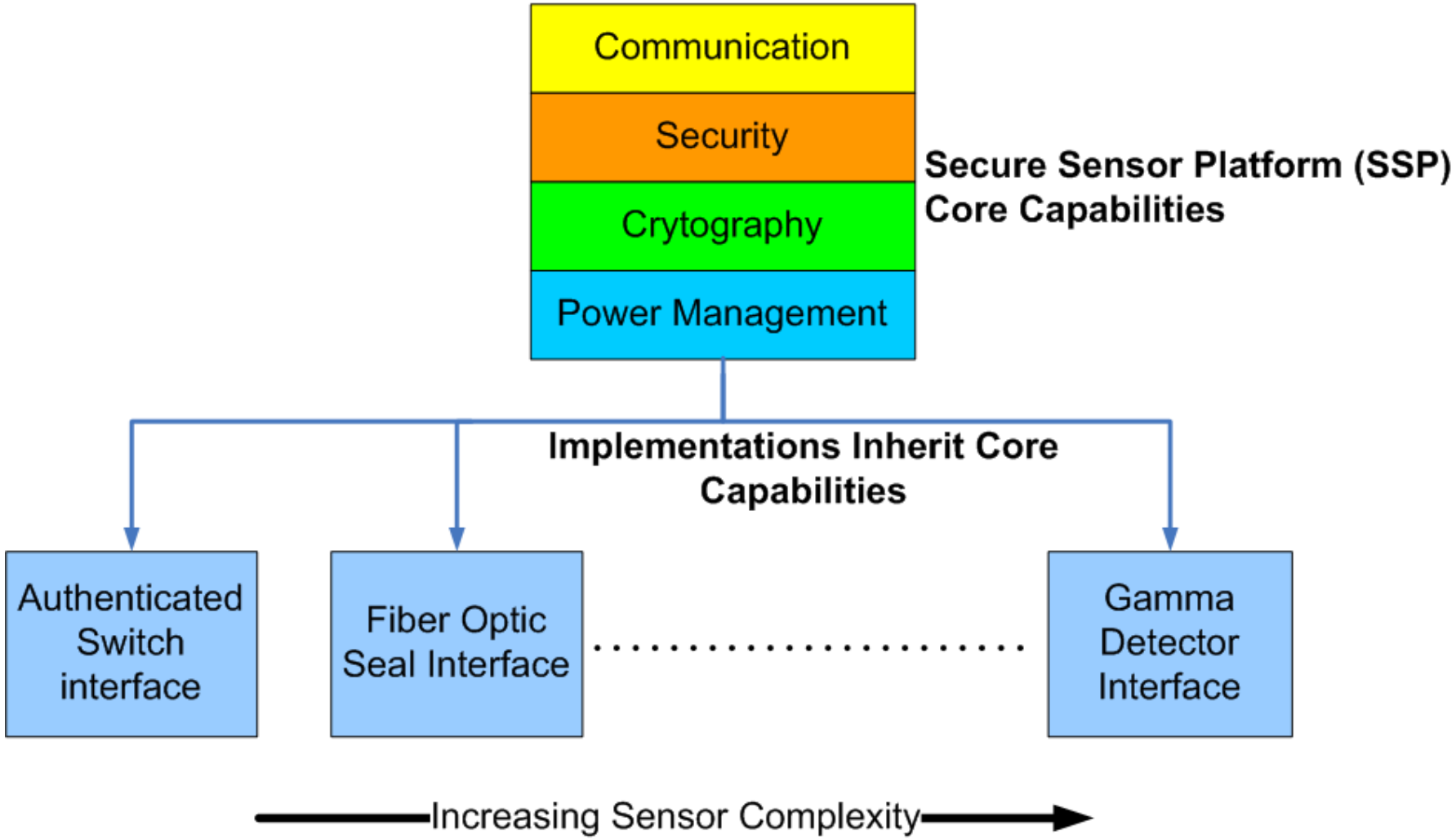
SSP Based Deployment



SSP - Core Capabilities

- Communications
  - Sensor protocol stack that supports hardwire and RF
  - Versatile data representation
- Security
  - Active/passive/intrinsic tamper with crypto key protection for sensors
  - Time variants and strict message format
- Cryptography
  - Authentication and encryption based upon NIST standards
- Sensor Power Management
  - MCU and peripheral sleep
  - Multiplexed sensors
  - High energy density battery technologies
  - Wake on radio features

SSP Capability and Implementation Relation Diagram for Sensors



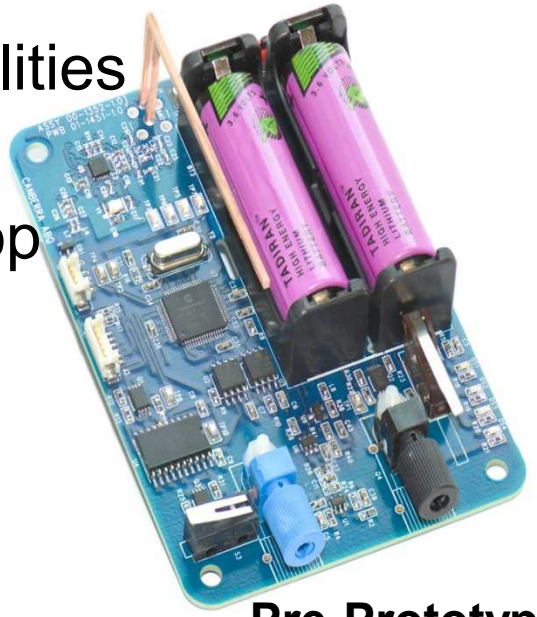
SSP Concept Advantages

- Shorten design cycle for new sensor types
- Easily add new data types
- Interoperability of SSP based sensors
- Common components
- Vulnerability assessments can be shortened
- Interface options – Hardwire or low-power RF
- Cost effective security implementations

Example SSP Application

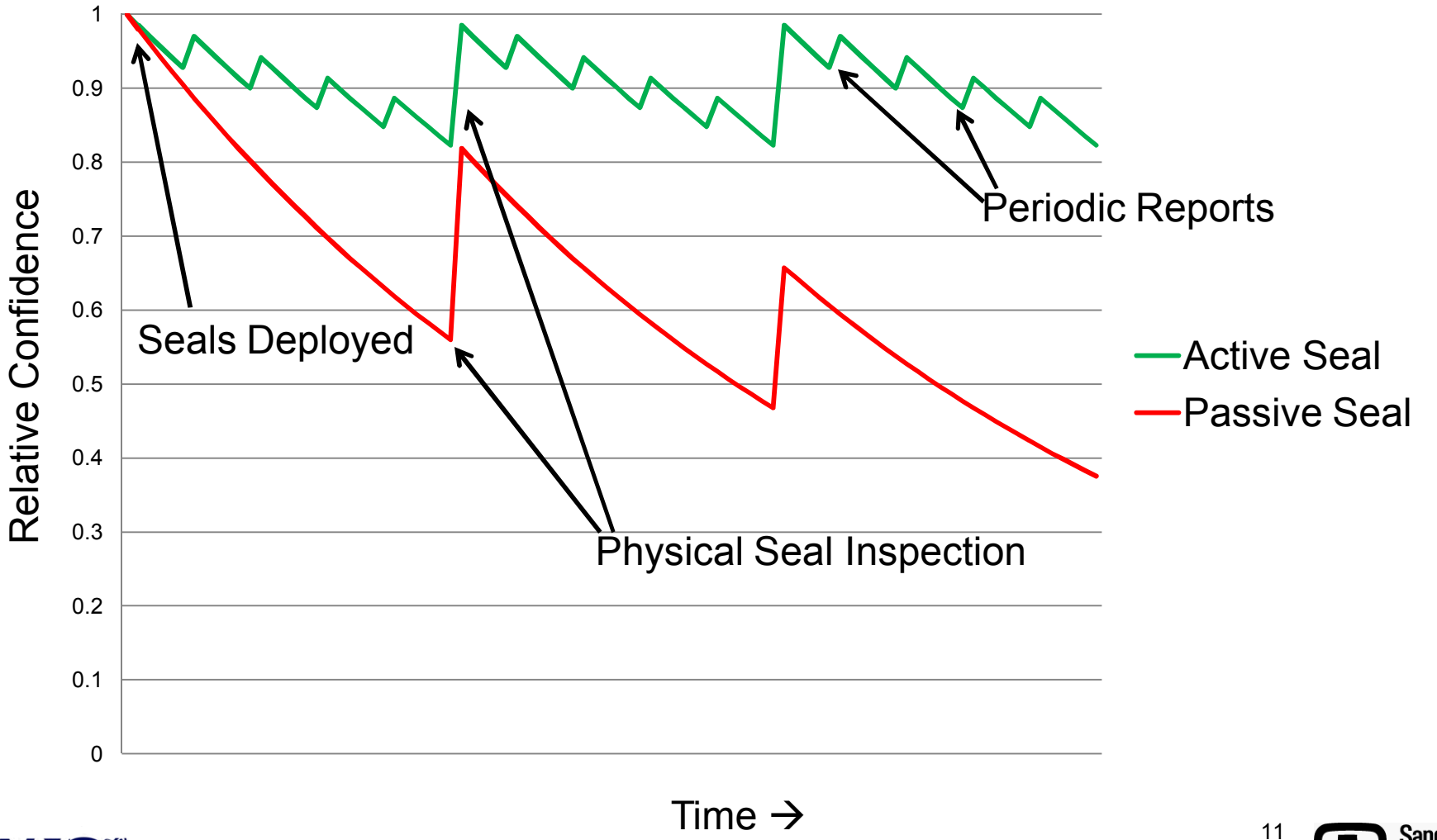
Remotely Monitored Sealing Array

- Provides all of the SSP core capabilities
- Fiber optic seal sensor
- Up to 50 meter length of sealing loop
- Low cost seal (low life-cycle costs)
- Up to 4 year battery life
- Fiber can be cut to length
- Parametric fiber monitoring
- RF communication only
- Years of message storage (typical app.)



Pre-Prototype Development Board

Relative Confidence of Integrity Active vs. Passive Seal



Future Goals of the SSP Project

- Stronger cryptography and reduced key management loads,
- Higher confidence of detection of tamper while still maintaining low cost for wide deployment,
- Longer autonomous operation,
- More sensor technologies supported by the SSP concept, and
- More user interfaces to provide choices for monitoring and review platforms.