SAND2011-8429C

Secure Sensor Platform (SSP) Authenticated Switch

IAEA Workshop on Sealing, Containment, and Authentication Technologies

9-11 November 2011, Vienna, Austria

Heidi Smartt – Sandia National Laboratories

Natacha Peter-Stein – AREVA BUNM / CANBERRA

SAND-2011-XXXXP

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.

Overview (1/2)

- Authentication/encryption of data generated by unattended safeguards systems essential for IAEA safeguards conclusions
- Currently, IAEA can use balanced magnetic switches to monitor doors, hatches, and access points, but has no means to authenticate the trigger signal
- Solution: the SSP Authenticated Switch
  - Track any movement of access points (surveillance cabinets, building doors, etc.)
  - Capable of remote monitoring
  - Reduce cost of safeguards operations while increasing effectiveness and response time

Overview (2/2)

- Canberra and Sandia National Laboratories (SNL) have teamed together to create the next product in the SSP family evolution, the new Authenticated Switch
- SSP Authenticated Switch creates family of products for IAEA using same building blocks (hardware and security protocol)
- Since work to develop Authenticated Switch is performed under Canberra / SNL CRADA, it comes at no cost to IAEA or Member State Support Programs
- To ensure that actual implementation is in line with IAEA needs, feedback on technology is required to be incorporated into final design

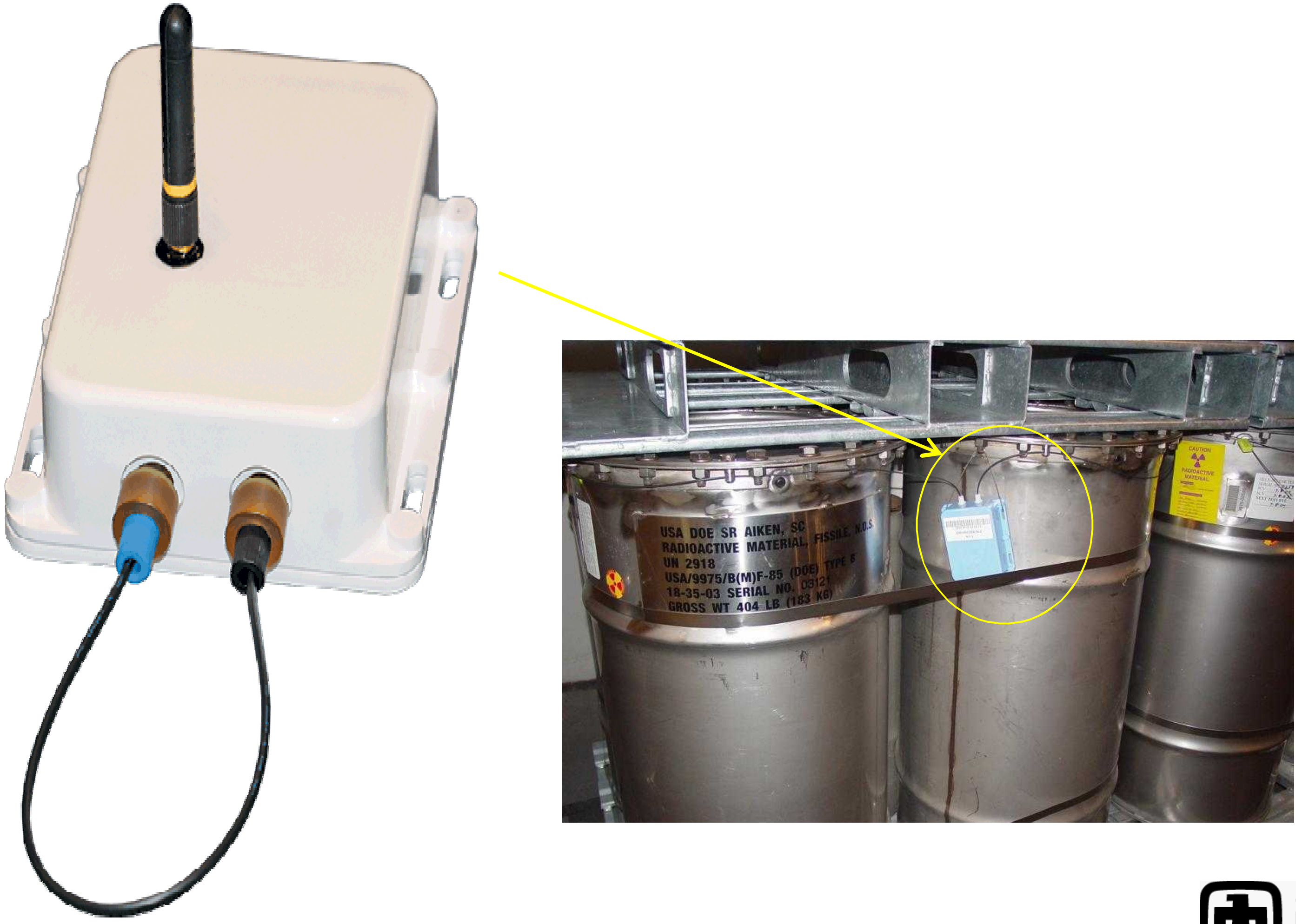
The Need

- IAEA needs to monitor doors and gates in material balance areas
- Open/close events generated by balanced magnetic switches cannot be authenticated with today's means
- Makeshift and expensive workaround solutions prompt IAEA to request solutions
- Since SSP framework has been evaluated and accepted by IAEA for use in field, SSP-based Authenticated Switch can be quickly implemented

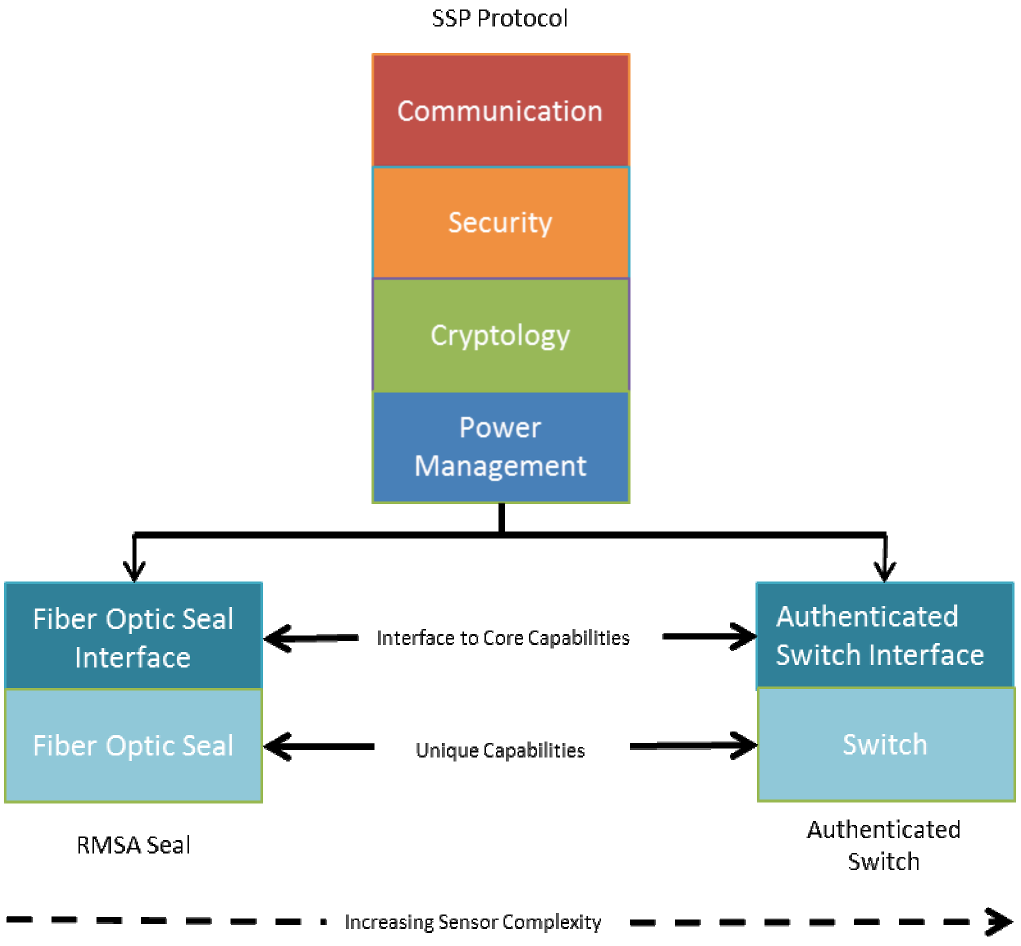
The Solution

- Door switch is suitable approach to need as it will indicate open/close position while not resulting in a mechanical breakage every time it is triggered
- Message will be transmitted remotely to safeguards agency headquarters every time switch is triggered and will allow operator to conduct operations on behalf of the safeguards agency without physical intervention of inspector
- Using standardized solution (built on RMSA) with approved data communication/security protocol will shorten approval/evaluation process and lower associated costs for IAEA
- Triggering of other sensors is possible

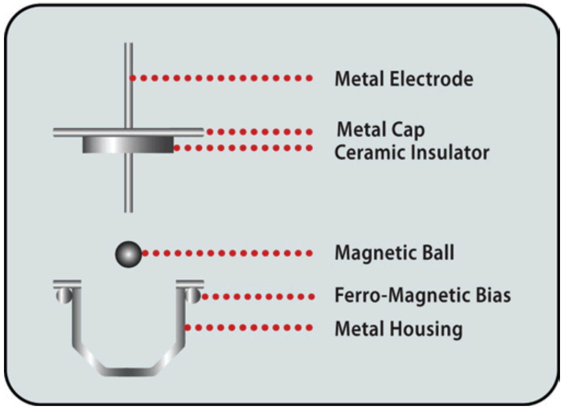
SSP Sensor Framework


USA DOE SR AIKEN, SC
RADIOACTIVE MATERIAL, FISSILE, N.O.S.
UN 2918
USA/9975/B(M)F-85 (DOE) TYPE 6
18-35-03 SERIAL NO. 03121
GROSS WT 404 LB (183 KG)
CAUTION
RADIOACTIVE MATERIAL

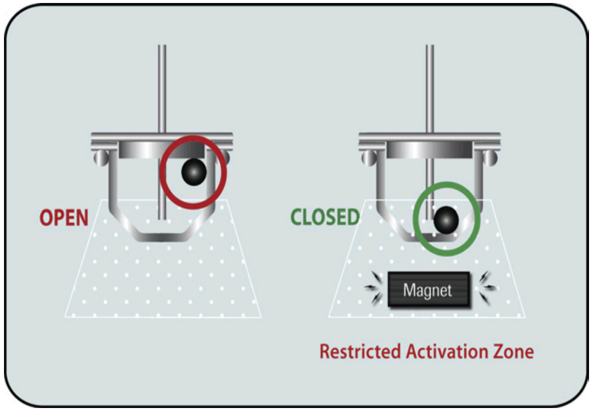
SSP Sensor Framework



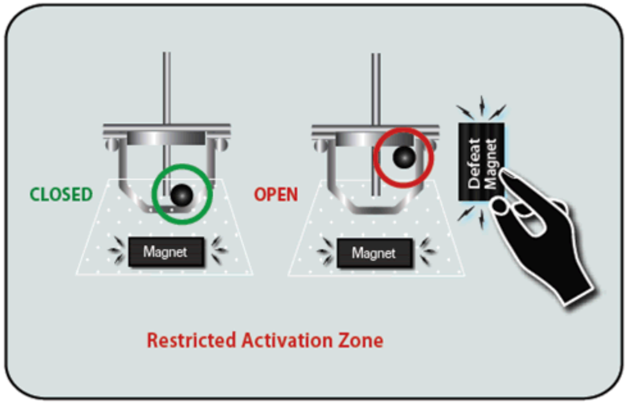
Magnasphere® Technology



Construction of the Magnasphere® Switch

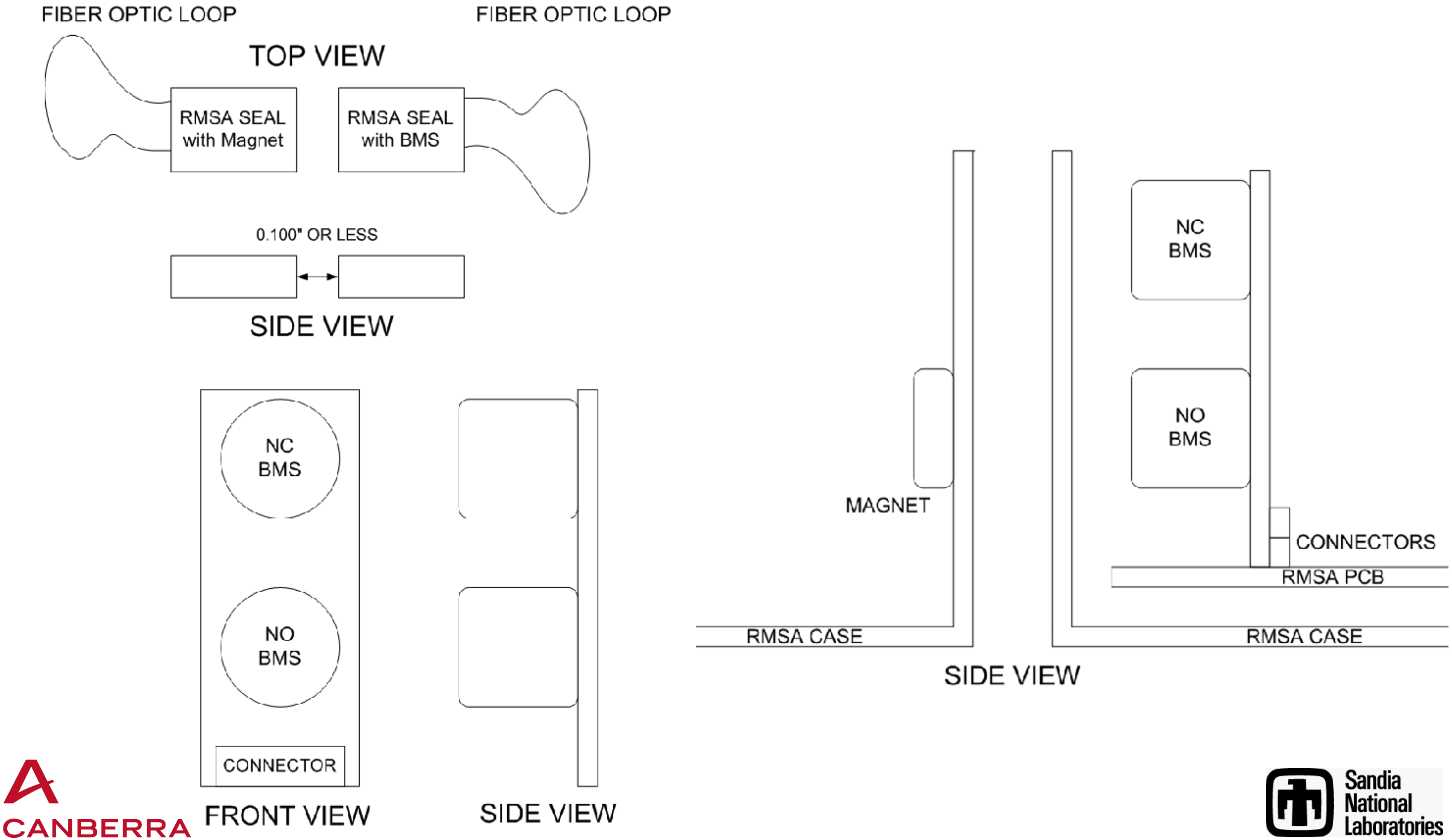


Switch Functionality



Magnetic Tamper Resistance

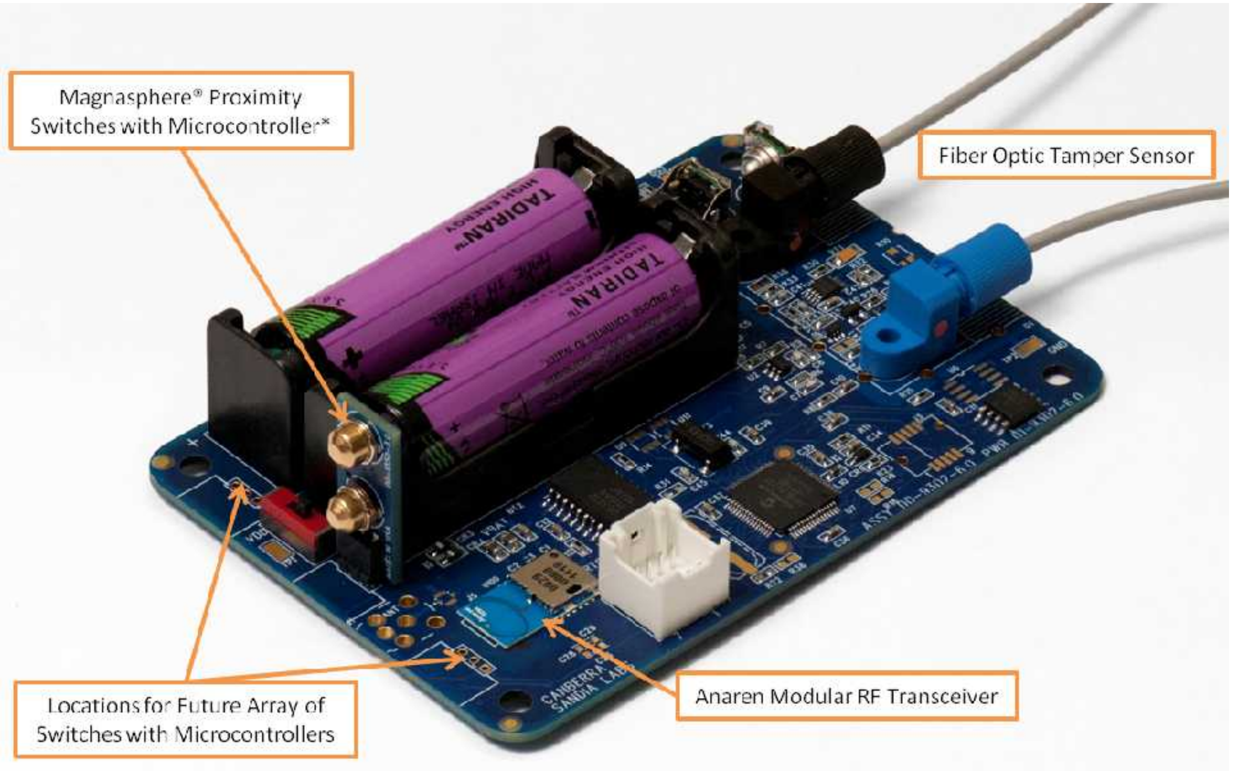
SSP Authenticated Switch Concept (1/2)



SSP Authenticated Switch Concept (2/2)

- Two RMSA seals used in tandem
  - One seal has magnet
  - One seal has two Magnasphere® switches
- Two RMSA seals can be oriented in any direction (gravity has no effect)
- Enclosures should be aligned for the switch to remain in a “Secure State” position

BMS Component



Magnasphere® Proximity Switches with Microcontroller*

Fiber Optic Tamper Sensor

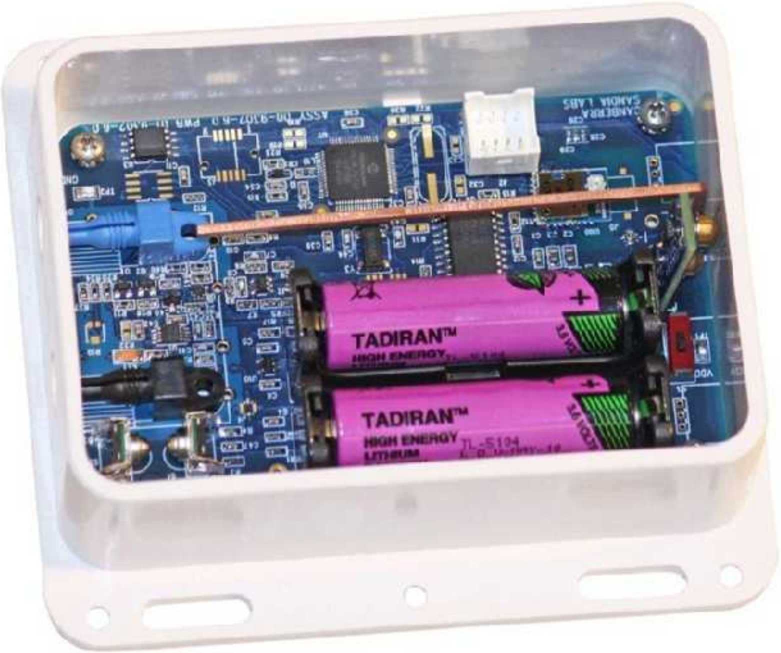
Locations for Future Array of Switches with Microcontrollers

Anaren Modular RF Transceiver

Authenticated Switch (BMS Component) - Concept Version

*Microcontroller allows algorithmic processing of state data

BMS Component with Enclosure



Authenticated Switch (BMS Component) in Enclosure

Functional and Performance Requirements

- New TLV defined to provide "Secured State" or "Non-Secured State" message
- Response time for state change will be in microsecond range
  - Message assembly, authentication, encryption, and transmission may take a few microseconds
- Software filter will minimize false alarms
- Magnetic tamper detection provided by engaging only one Magnasphere® switch with magnet
  - Tampering with a different magnet will be detected by the non-engaged switch and cause "Non-Secured State" message

Benefits

- Share same infrastructure as RMSA seal (translator, hardware, communication protocol)
- Security/Reliability
  - Fulfill IAEA safeguards standards to provide platform with authenticated and encrypted communication channels, tamper indication and sealing capabilities
- Versatile
  - Easily installed and maintained, large (hundreds) number of authenticated switches deployed at one location and manageable remotely
- Limit cost for safeguards
  - One time cost, unlimited lifetime use, maintenance only at the battery level with the same battery life as RMSA (4+ years) and limit visits of inspectors on site
- Development and commercial partners already established who provide complete knowledge and committed resources

Accomplished-to-date

- Hardware
  - Updated RMSA seal hardware built and tested
  - BMS hardware built and tested
- Firmware
  - BMS firmware completed
  - RMSA seal firmware to be completed in November 2011
- Software
  - Review software updated
  - No translator software update required

Current Schedule

- IAEA feedbacks on design by mid-November 2011
- RMSA seal firmware to be completed in November 2011
- Final testing by early December 2011
- Prototype available by end of December 2011
- Documentation by January 2012

Summary

- Authenticated Switch satisfies clear technical need of IAEA and other safeguards authorities
- Existing SSP framework backbone provides optimal conditions to develop this building block in quick and efficient manner
- IAEA acceptance process shortened through earlier acceptance of RMSA
- Authenticated Switch will further establish SSP backbone as IAEA standard, opening avenue for future sensor implementations