SAND2013-3942C

Sandia National Laboratories

Development of an Advanced Ceramic Seal for Maintaining Continuity of Knowledge in Treaty Verification and Safeguards Applications

Heidi A. Smartt

May 2013

SAND

U.S. DEPARTMENT OF ENERGY

NNSA 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.

Acknowledgements

- Savannah River National Laboratory (SRNL)
- NA-22 Office of Defense Nuclear Nonproliferation Research and Development

Outline

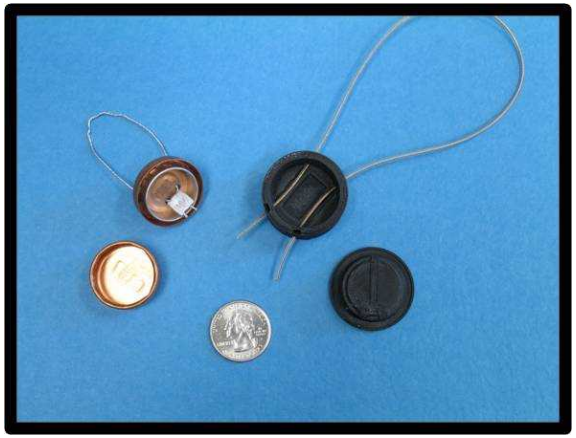
- Introduction
- Advanced security
- Improved efficiency
- Next steps

Seals and lifecycle

- Seals provide Continuity of Knowledge (CoK) in treaty verification regimes
- Require continuous improvement as:
  - Adversary advances
  - Requirements change
  - Technology advances, providing new options
- Ceramic Seal improves
  - Security features
    - Tamper indication
    - Unique identification
  - Efficiency
    - In-situ verification
    - Self-securing wire

Goals and objectives

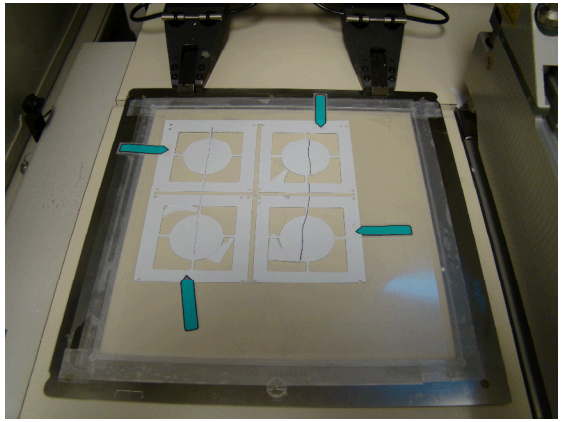
- Integrate multiple advanced technologies into prototype next generation loop seal
- Advance seal capabilities
  - Improve efficiency
    - In-situ verification
    - Self-securing wire
  - Create multiple levels of tamper indication
    - Frangible seal body
    - Surface coatings
    - Active detection of state
  - Create unique identification
    - Electronic ID
    - Non-reproducible surface features
- Innovation of Ceramic Seal is advanced capabilities in small volume



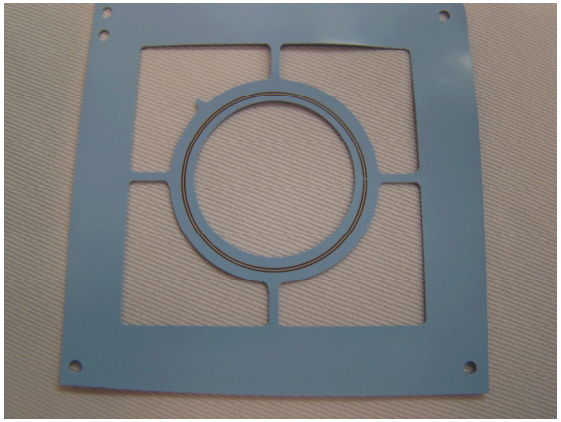
Picture courtesy SNL

Advanced security: seal body

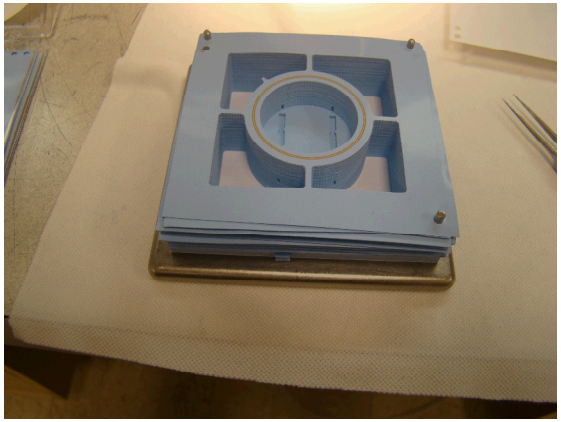
- Low-temperature co-fired ceramic (LTCC)
  - Meets frangibility requirements
  - Allows integration of electronic components/line traces



LTCC Green Tape™ punching process



Conductive trace screen printing



Green Tape™ stacking prior to lamination

Pictures courtesy SNL

Advanced security: tamper planes

Sandia National Laboratories

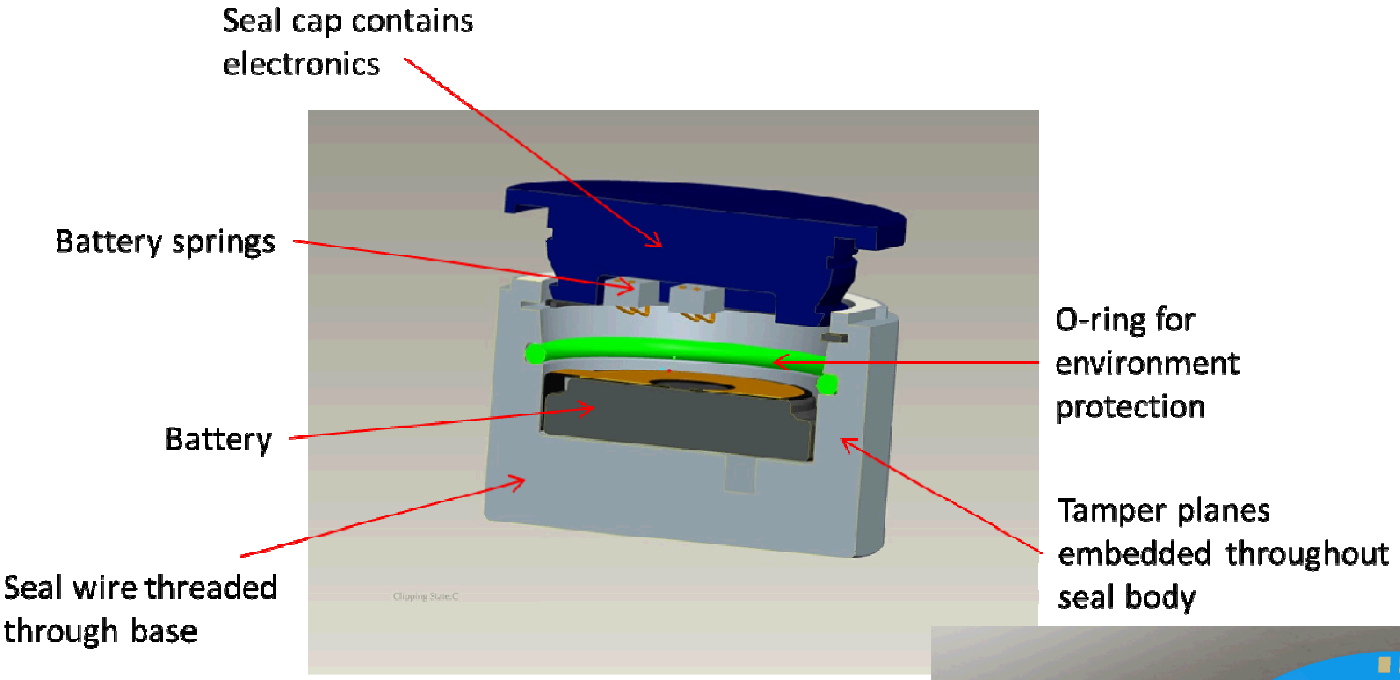
- Conductive line traces integrated into LTCC
- Tamper planes throughout body walls, cap, and base
  - Connected to electronics
  - If disrupted, seal performance affected

Advanced security: active tamper

Sandia National Laboratories

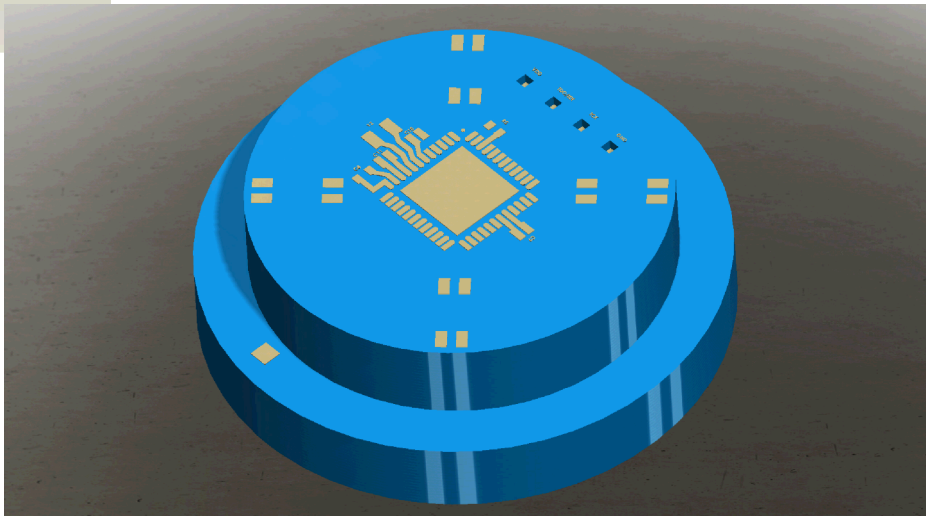
- Electronics recessed underneath seal cap
  - Attached to embedded line traces in LTCC
- Single microcontroller
- One-time personality programming in-situ
  - Loads secret keys onto seal, sets message creation interval and absolute time
- Messages
  - State-of-health, anomalous events, seal interrogation history
  - Stored in flash memory
  - Message authentication code (MAC) appended to messages using 128-bit CMAC algorithm with AES cipher
    - Based on secret key, 8 byte ID, non-repeating message count, clock

Advanced security: active tamper



Picture courtesy SRNL

Picture courtesy SNL



Advanced security: ID

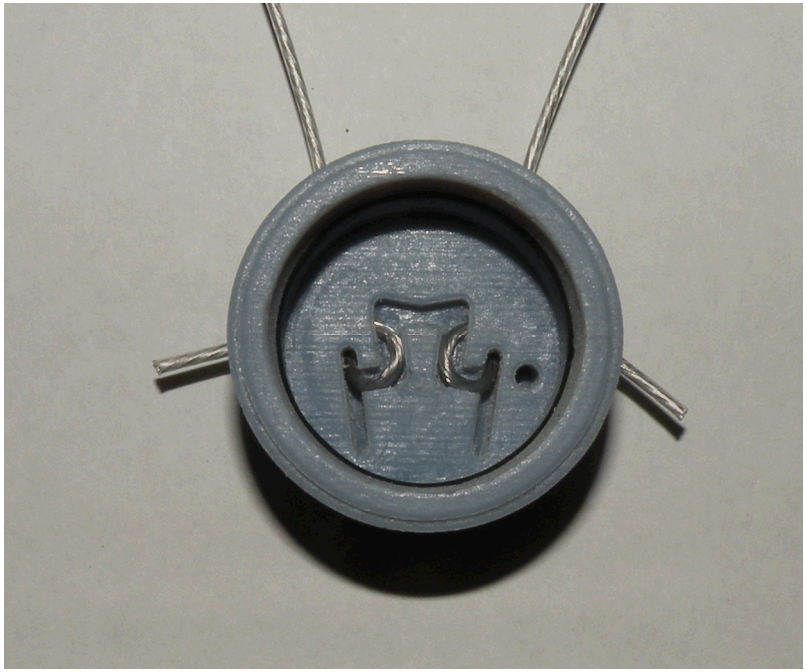
Sandia National Laboratories

- 8 byte number
- Assigned when firmware programmed
- Ensuring unique ID number procedural
- Seal electronic uniqueness (authenticity) based on MAC

Improved efficiency: self-securing wire

- Wire follows tortuous path within seal body
- Design increases difficultly of removing wire
- Active research on wire
  - Commercial candidates identified

Picture courtesy SRNL



Improved efficiency: in-situ verification

Sandia National Laboratories

- Contact reader has same secret keys as seal
- Supports following authenticated commands over serial port:
  - Request latest sensor state-of-health
  - Request specific message number from seal
  - Request that seal send latest anomalous/tamper message
  - Request that seal send all anomalous/tamper messages
  - One-time personality programming
- Authenticates received messages
- Currently implemented as laptop

Next steps

- Complete software development
- Vulnerability review of electronics and software
- Fabrication of seal prototype with LTCC, tamper planes, electronics, battery, coatings
- Functional testing
- Comprehensive vulnerability review