Current Research on Containment Technologies for Verification Activities: Advanced Tools for Maintaining Continuity of Knowledge

Heidi A. Smartt[a], Daniel Krementz[b], Michael J. Kuhn[c]

[a]Sandia National Laboratories
Albuquerque, New Mexico, USA

[b]Savannah River National Laboratory
Aiken, South Carolina, USA

[c]Oak Ridge National Laboratory
Oak Ridge, Tennessee, USA

Abstract. The US National Nuclear Security Administration (NNSA) Office of Nonproliferation and Verification Research and Development currently funds research on advanced containment technologies to support Continuity of Knowledge (CoK) objectives for verification regimes. One effort in this area is the Advanced Tools for Maintaining Continuity of Knowledge (ATCK) project. Recognizing that CoK assurances must withstand potential threats from sophisticated adversaries, and that containment options must therefore keep pace with technology advances, the NNSA research and development on advanced containment tools is an important investment. The two ATCK efforts underway at present address the technical containment requirements for securing access points (loop seals) and protecting defined volumes. Multiple US national laboratories are supporting this project: Sandia National Laboratories (SNL), Savannah River National Laboratory (SRNL), and Oak Ridge National Laboratory (ORNL). SNL and SRNL have developed and are now fabricating the "Ceramic Seal," a loop seal that integrates multiple advanced security capabilities and improved efficiency housed within a small-volume ceramic body. The project includes development of an associated handheld reader. Currently at the prototype stage, the Ceramic Seal will undergo a series of tests to determine operational readiness. It will be field tested in a representative verification trial in 2016. ORNL is developing the Whole Container Seal (WCS), a flexible conductive fabric capable of enclosing various sizes and shapes of monitored items. The WCS includes a distributed resistance measurement system for imaging the fabric surface area. With the expected technology advances from the Ceramic Seal and WCS, the ATCK project takes significant steps in advancing containment technologies to help maintain CoK for various verification regimes, including international nuclear safeguards.

1. Introduction

Containment/Surveillance (C/S) measures are critical to any verification regime in order to monitor declared activities, detect undeclared activities, verify the integrity of equipment or items, reduce inspector burden, and most important, to maintain CoK between inspections [1]. Equipment used in C/S can include tags, seals, tamper-indicating enclosures, optical surveillance, and radiation detectors, and this equipment currently exists at varying levels of technological sophistication and maturity. Some C/S equipment, such as the metal cup seal, has been fielded for 50 years. The legacy optical surveillance equipment, based on the DCM-14 camera module, is currently undergoing replacement. It is critical that C/S equipment evolve given the continuing advances in the threats posed by and the capabilities of potential adversaries as well as to take advantage of technology advances for continued efficiency and effectiveness gains for inspectors and to reduce burden on operators.

The two NNSA-funded ATCK efforts underway at present address the technical containment requirements for securing access points (loop seals) and protecting defined volumes. Loop seals are common equipment used for C/S measures, as reflected by the tens of thousands of metal cup seals deployed globally, in addition to the Electronic Optical Sealing System (EOSS), the electronic Variable Coding Seal System (VACOSS), the passive Cobra seal, and the electronic/wireless Remotely Monitored Sealing Array (RMSA).

The Ceramic Seal has been in development at SNL and SRNL for more than 3 years, and prototypes for operational testing are now in fabrication. The Ceramic Seal can provide an advanced and modernized alternative to the metal cup seal or other single use seals. The metal cup seal, although environmentally robust, inexpensive, and small in size, is operationally burdensome, and its integrity is not able to be verified in situ. The Ceramic Seal addresses issues with the metal cup seal and makes additional security advancements (tamper indication and unique identification) and efficiency improvements (in situ verification and ease of application). Its innovation is the integration of these advanced capabilities in a small volume, including a self-securing wire feature; multiple levels of tamper indication via a frangible seal body, surface coatings, and active detection of state through low-power electronics; electronic identification number verified in situ through a contact reader; and physical identification via non-reproducible surface features.

The WCS is a flexible conductive fabric capable of enclosing various sizes and shapes of monitored items. The WCS includes a distributed resistance measurement system for imaging the fabric surface area. WCS is a unique approach because when securing a container using traditional C/S equipment, it may be difficult to visually inspect the back side and bottom of a container and furthermore difficult to verify the integrity of the entire container. The WCS could function as both a seal and an active monitoring system in regards to the integrity of the container.

2. Whole Container Seal (WCS)

2.1. *Conceptual Design*

A conceptual design of a WCS is shown in Figure 1. Various fabric pieces are connected together either with zippers or conductive Velcro. Conductivity must be maintained across the entire WCS to ensure tamper detection over the whole container. As shown in Figure 1 (right), each fabric piece is composed of multiple layers including outer insulating layers and an inner sensing layer. The inner sensing layer is composed of a continuous sheet of conductive fabric and a grid of sensors that are used in capturing the distributed resistance measurements. In addition to the concept outlined in Figure ***1***, an inner liner design and a free-form blanket design are also being explored.

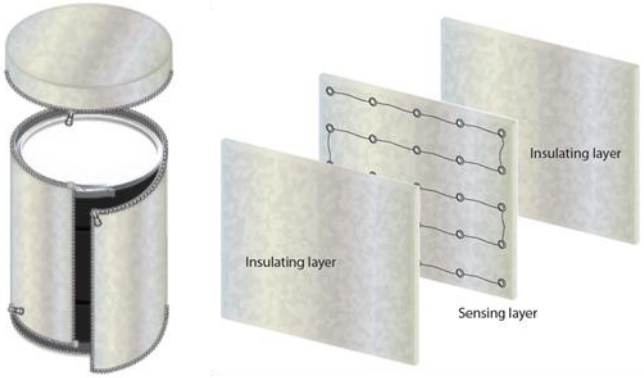

Figure 1: (Left) Conceptual design of the WCS where the sensing system is embedded into the fabric comprising the seal. The seal is scalable for use in sealing containers of various sizes. (Right) Multilayer fabric structure.

2.2. *Conductive Fabric*

The WCS utilizes commercially available conductive fabric as a distributed sensor for real-time tamper detection. Various intrinsic properties of conductive fabrics can be measured for sensing purposes. As outlined in [2], we have focused on building a measurement system to monitor the distributed resistance of a conductive fabric sheet. By measuring the resistance between various points across the fabric, the distributed resistance of the fabric sheet can be mapped into an image. Image processing techniques can then be used to continuously monitor the status of the conductive fabric seal and automatically detect breach or tampering of the conductive fabric distributed sensor.

2.3. *Hardware*

The main hardware components are shown in Figure 2. The main hardware components include a computer or tablet running the main software application that is connected through a USB cable to the main controller, which is housed within the WCS. The main controller includes a microcontroller-based system on a chip and interfaces with the smart node sensing network through an I^2C digital bus.

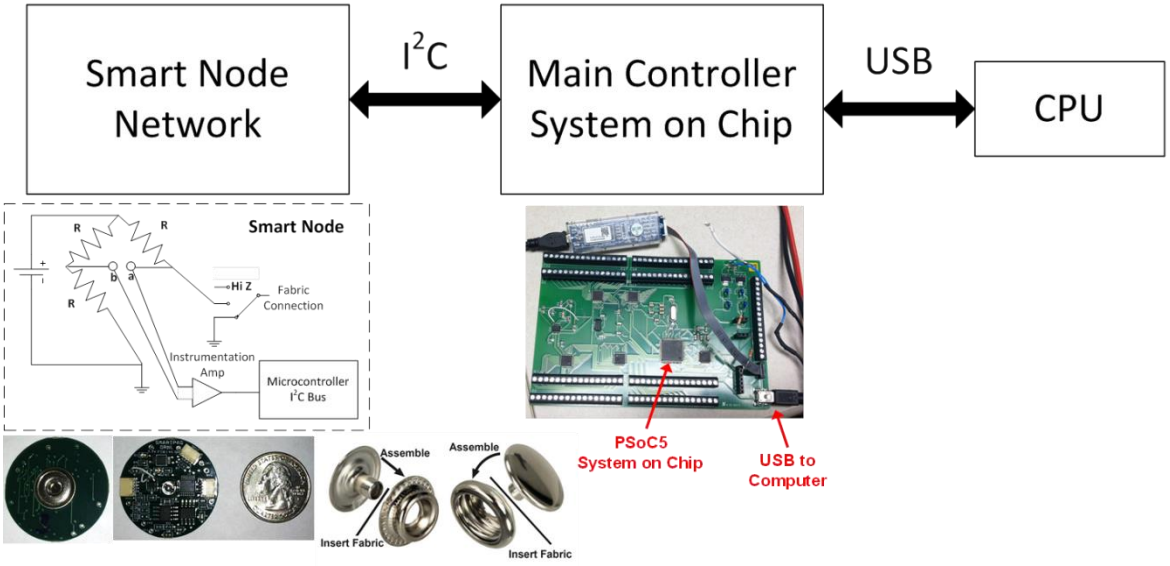

Figure 2: Smart nodes (embedded within fabric snaps) are used at each sensing point on the conductive fabric sensing layer to provide a means for making resistance measurements and relaying the resistance data back to the main controller. A front-end instrumentation amplifier connected to a Wheatstone bridge provides stable resistance measurements across the surface area of the WCS.

Each smart node contains a microcontroller that is connected to power and the I^2C bus via a thin cable that is run from the main controller and daisy chained between each smart node, ultimately connecting all of the smart nodes to the I^2C bus. A fabric snap is soldered to the smart node circuit board and used to secure it to the conductive fabric sheet. Each smart node contains an instrumentation amplifier and Wheatstone bridge circuit. The smart node can be switched to either provide a connection to ground or to perform the Wheatstone bridge measurement for calculating the resistance between any two smart nodes. The smart node can also be put into a high-impedance state, which is needed when the smart node is not being used so that other point-to-point resistance measurements can be performed without the inactive smart nodes interfering with the measurement. The main controller communicates with the network of smart nodes to loop through the entire resistance measurement sequence needed to map out the distributed resistance of the conductive fabric sheet. Figure 3 (right) shows a nine-node network of smart nodes set up in a 3×3 grid on an ~ 0.60 m × 0.60 m piece of conductive ripstop fabric. Low-profile four-wire cables are daisy chained to power the smart nodes and connect them to the I^2C bus. Testing is under way to determine the optimal spacing between the smart nodes in terms of the needed sensitivity of the overall system in detecting tamper and providing a secure WCS.

2.4. *Software*

The software interface for the WCS is shown in Figure 3. The software application has been developed in Microsoft Visual Studio using the Visual C# programming language. The main functions of the software application include the following: (1) connecting to the main controller through a USB cabled connection, (2) initializing the main controller, (3) getting information on the current smart node network from the main controller, (4) defining the spatial arrangement of the smart node network, (5) calculating and sending the resistance measurement sequence to the main controller given the spatial arrangement of the connected smart node network, (6) streaming real-time resistance data from the main controller and displaying that data on the Resistance Map display in the main window, (7) saving and logging resistance data, (8) performing baseline calibrations and saving calibration data

for specific fabric sheets and specific smart node network configurations, and (9) detecting and logging tamper events.

The software application is currently operational and can stream and visualize resistance data across the fabric sheet in real-time. The algorithms used in providing a baseline calibration of the fabric sensor and smartly detecting tamper events will continue to be refined as we conduct formal test campaigns of WCS prototypes. This includes understanding how the resistance measurements change due to environmental effects including temperature and humidity.

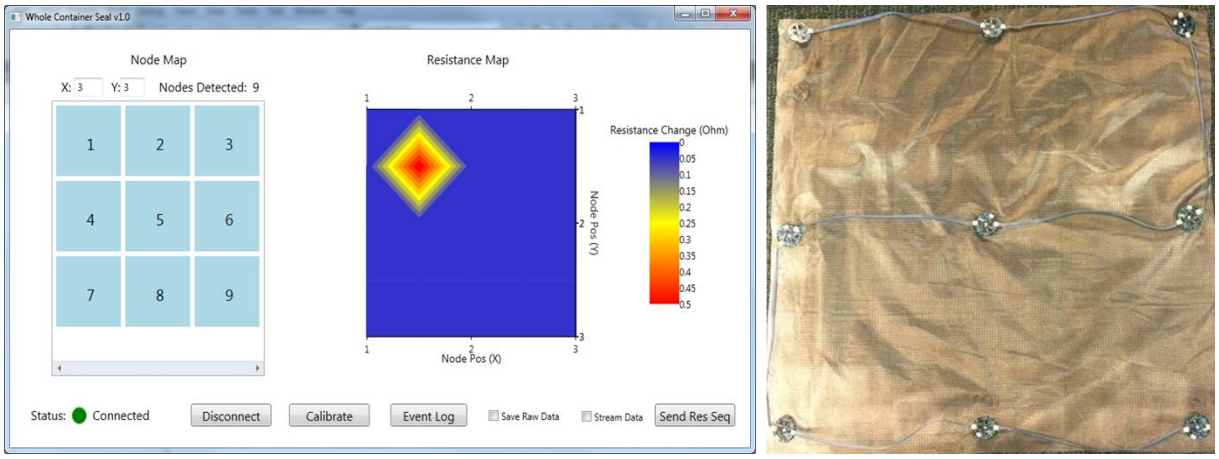

Figure 3: (Left) Software interface for communicating with the WCS, interfacing with the smart nodes, visualizing data, and logging data and alarms. (Right) Nine smart nodes connected in a grid pattern where one cable is strung between the smart nodes and connected to the main controller.

2.5. *Experimental Results*

Two smart nodes were placed on the left and right sides of a ~ 0.30 m × 0.30 m conductive ripstop sheet of fabric, and a cut was introduced down the middle of the sheet. Resistance is measured between the two smart nodes over a 25 second time period in which the cut is made during the time interval from 6–20 seconds. The measured *baseline* resistance increases from 5.29 Ω to 5.42 Ω (increase of 133 mΩ) when comparing the measured resistance at 5 seconds versus 19 seconds. The large spiking in resistance values from 5 Ω to 30 Ω (the maximum value allowed as an output) is caused by the complete separation of the fabric sheet into two halves. Once the two fabric sheets are completed separated, an open circuit with very high resistance is created (MΩ to near infinite resistance between the two smart nodes). Resistance measurements can change slightly based on changes in the fabric temperature or smart node electronics temperature; however, calibration of resistance measurements with an on-board precision resistor at each smart node provides an accurate baseline over long time periods and in varying temperatures.

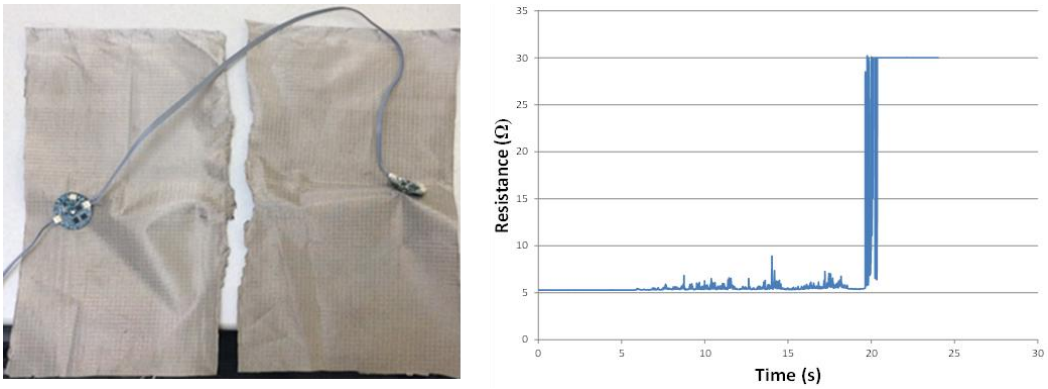

Figure 4: (Left) A ~ 0.30 m × 0.30 m fabric sheet in which two smart nodes are placed on the left and right sides of the sheet, and a cut is made down the middle of the sheet. (Right) Resistance measured between the two smart nodes over a 25 second time period in which the cut is made during the time interval from 6–20 seconds.

3. Ceramic Seal

The Ceramic Seal [3–6] integrates multiple advanced security features and efficiency improvements within a small volume (25 mm height by 24 mm diameter). Prototype seals are currently undergoing fabrication for insertion into various testing scenarios, and associated readers are under development.

3.1. *Ceramic Seal Concept of Operation*

The Ceramic Seal (Figure 5) notionally operates as follows: the Ceramic Seal wire is looped around the item to be monitored and secured within self-securing grooves in the seal base. The battery is inserted into the seal base, and the seal cap is snapped onto the seal base, secured by a snap ring. The Ceramic Seal will now require "personality programming". Personality programming assigns ID, State of Health (SOH) reporting interval, loads cryptographic keys, and sets seal time. A cable connects the Ceramic Seal to a reader with the personality programming application. The cable has a "tag-connect" connector on one side, attached to the outside of the Ceramic Seal cap, and an RS-232 connector attached to a reader. The seal is now ready for use. Note: expected seal lifetime under stressed conditions in 12 years. It is expected that the seal would be periodically inspected physically and electronically. An inspector would attach a reader to download SOH and events. Physical inspection (visual or instrumentation) would reveal deformations in structure or coatings.

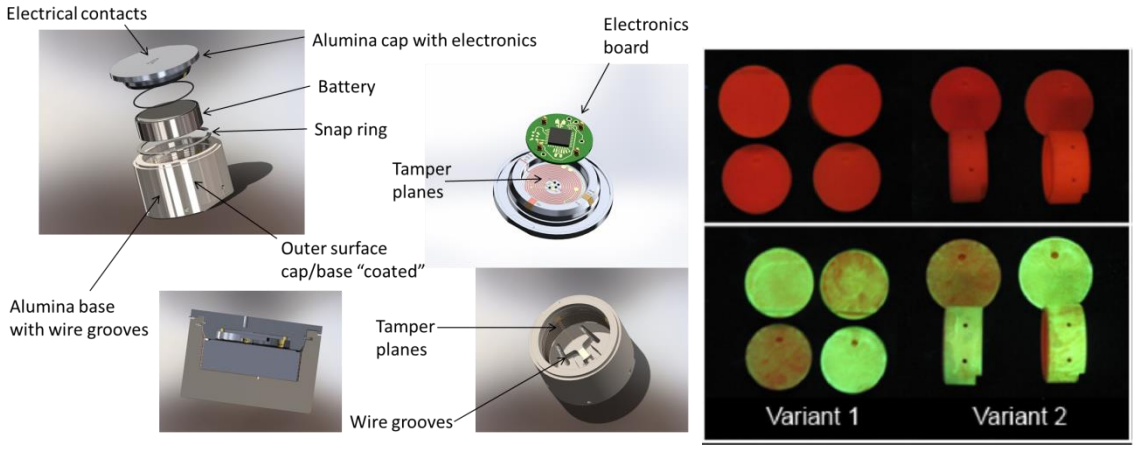

Figure 5: (Left) The Ceramic Seal design features. (Right) Ceramic Seals are shown on top uncoated, with Alumina-based sol gel doped with terbium coatings on the bottom. Excited by 254 nm UV. Images courtesy Tetramer Technologies.

3.2. *Advanced Security*

The most critical element of a seal applied in a treaty verification regime is its tamper-indicating features. A loop seal will employ a wire or fiber-optic cable (FOC) threaded through a monitored item's hasp or otherwise secured, and the wire or FOC will terminate within the seal body. In single use seals such as the Ceramic Seal and metal cup seal (versus multiple use seals in which the seal wire can be removed and reattached), confidence must be maintained that the wire is unable to be removed from the seal body once secured without detection and that the seal body has remained intact such that the seal body has not been opened and the wire removed/replaced. Tamper-indicating features on the seal body serve the role of providing this confidence. It is important to note that a vulnerability review (VR) team iteratively worked with the design team to evaluate and guide the tamper-indicating features of the seal.

The properties of the material used in the Ceramic Seal body, alumina (99.8% Al_2O_3), meet the requirements of "frangibility" – that is, upon deformation it tends to break into fragments rather than retaining cohesion, yet the material is strong enough to withstand the operational environment. Frangibility is important so that a tamper attempt might result in difficult-to-reassemble fragments.

The Ceramic Seal will be coated with spray coatings developed in partnership with Tetramer Technologies. These exterior fluorescent coatings act as a tamper-indicating feature [7–9] as

modification/tampering of the seal will be visible under UV illumination. The coatings are transparent to allow Laser Surface Authentication (LSA) for unique physical identification of the seal body.

The Ceramic Seal provides active tamper indication by monitoring both "tamper planes" embedded in the interior of the seal, as well as monitoring connectivity between the cap and base of the seal (to determine if the seal has been opened). The tamper planes are connected to the electronics and if disrupted, i.e., signals cannot pass, software within the electronics impacts performance.

Seal firmware is programmed prior to deployment; however, the Ceramic Seal requires personality programming in situ, meaning configuration must happen via the RS-232 serial communication link located on the cap of the seal. Personality programming loads the secret keys onto the seal, sets message creation interval, and sets absolute time. The electronics will not be powered until the seal cap and base is connected, so personality programming the seal must happen after it has been closed. However, for added security, we have designed the seal to accept personality programming only one time; i.e., cryptographic keys can only be loaded a single time.

The seal creates several message types – State of Health (configurable), anomalous events, and the seal interrogation history. As messages are created, we append a message authentication code (MAC) using the 128-bit CMAC algorithm with AES cipher (and optionally encrypted using 128-bit AES) before storing in flash memory. The MAC derives its uniqueness from the secret key, the seal's 8 byte ID, a non-repeating message count, and a clock. The 8 byte ID is assigned during firmware programming and can be a unique number by procedure. The MAC ensures that the seal itself can be uniquely identified due to the combination of the 8 byte ID with the cryptographic key.

A seal reader (two variations are currently under development and described later in this paper), which will also have the secret keys, will be able to send an authenticated command to the seal (over the serial port), receive the requested message(s), and authenticate them using its copy of the secret key.

3.3. *Improved Efficiency*

The capability of self-securing wire not only improves efficiency but touches upon security as well. The wire ends must securely terminate in the seal body in such a manner that they cannot be easily removed, and must do so in an efficient manner. In the Ceramic Seal design, the wire is routed through the monitored item and into the seal base, where it is secured by a tortuous path. The design team and SNL VR team iterated on several designs before choosing a final design.

The wire itself is important as well. Active research in identifying appropriate wires is ongoing, and commercial candidates have been identified. The current seal prototype does not have the capability to monitor the integrity of the wire using the internal electronics; however, such a capability is anticipated in future research. There are instruments available to externally connect to the wire after deployment and subsequently during verification to determine if the wire has been tampered with.

The Ceramic Seal uses a "tag-connect" electrical contact that can be queried using either a stand-alone reader or interface tablet, depending on the scenario. The stand-alone reader allows direct query, while the intended application of the interface tablet is to connect to a data management backbone. Both the stand-alone reader and interface tablet are currently in development.

3.4. *Testing and Reader Development*

In order to determine operational readiness, the Ceramic Seal has moved to the test and assess phase. As such, batches of Ceramic Seals are currently in fabrication. The Ceramic Seals will be deployed in a final demonstration in 2016 as well as field tested in two earlier scenarios to take place in 2015 – one as an honest game assessment at SRNL and the other as part of a testbed in which seal status is uploaded via an interface to a testbed backbone, and seal status is queried directly with a handheld reader. To accommodate the upload capability, SNL is developing an interface between the seal and a testbed backbone that handles data management (Figure 6). To accommodate applications in which the seal is in a stand-alone configuration, SRNL is developing a handheld reader that can interface to the seal – sending/receiving commands as well as querying seal status for immediate display (Figure 7).

The SNL tablet interface uses a Nexus 10 tablet and USB to serial connection to the Ceramic Seal. When the Ceramic Seal is attached to the tablet, commands can be sent from the tablet to the seal, depending on the user requests (SOH only, all history). The tablet passes the received data via Wi-Fi to a data management system (backbone) that may be responsible for multiple sensors/devices.

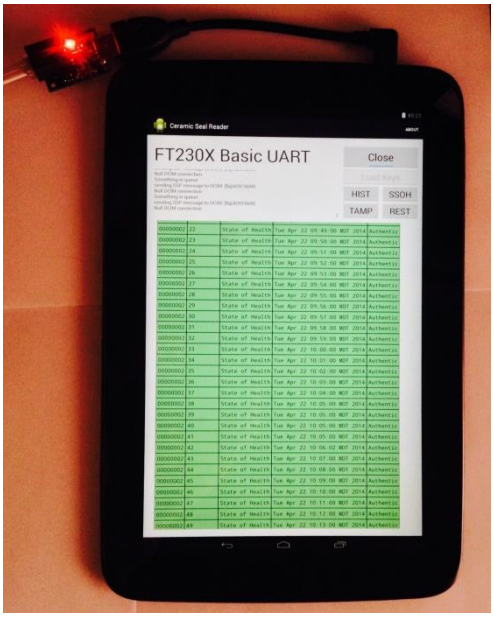

Figure 6: Tablet-based interface capability to a data management backbone. Tablet is connected to Ceramic Seal via "tag-connect" on seal cap, and SOH and events are downloaded to tablet and passed to the data management system.

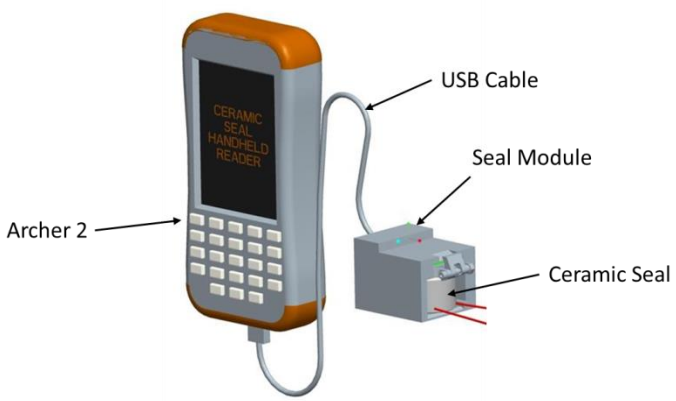

Figure 7: Handheld reader concept. Reader connects to Ceramic Seal via "tag-connect" on seal cap, providing in situ information on seal status such as SOH and events. Image provided by SRNL.

The stand-alone reader, developed by SRNL, uses an Archer 2 handheld computer from Juniper Systems with a custom seal module. The Archer 2 is designed for industrial use, is shock resistant, waterproof, has a high visibility screen for outdoor applications, and can operate up to 20 hours on one charge. Rather than modifying the rugged Archer 2 case, it was decided to design a separate seal module to connect to the Ceramic Seal electrical contacts. This module will communicate with the Archer 2 via USB. To use the seal reader, the seal would be slid into the seal module. The seal module is designed to automatically capture the seal and make electrical contact with the seal once the seal is fully inserted into the module. The module has internal electronics that alert the Archer 2 that a seal is connected. The Archer 2 then processes the data from the seal. If the state of health of the seal is "healthy" and no tamper attempts are registered, the seal module will indicate that the inspection is complete. If the seal is "unhealthy", a tamper attempt is detected, or if there is an error in communicating with the module, the Archer 2 to will direct the seal module to indicate to the inspector that further information is needed. The inspector will then activate the Archer 2 to determine the path

forward based on the information processed by the reader. Once the seal interrogation is complete, a lever on the seal module is pushed to eject the seal from the module.

4. Summary

Containment/Surveillance measures are fundamental for verification regimes and thus must evolve technically to counteract advances from potential adversaries and gain efficiency/effectiveness from technological advances. The US National Nuclear Security Administration (NNSA) recognizes the need for research into containment technologies and currently funds the ATCK project to advance technologies for securing access points and protecting defined volumes.

The Ceramic Seal is a loop seal with advanced security technologies, particularly in tamper indication, and improves efficiency over similar single use seals. The Ceramic Seal has been designed and is currently in fabrication for insertion into several testing scenarios – from an honest game assessment to operation. In addition to the fabrication and testing of the Ceramic Seal, accompanying readers are in design and development.

The WCS is a conductive fabric seal meant to protect an entire volume by monitoring resistance changes across the fabric in real-time. It is in the design and prototype stage. Development efforts thus far have been on designing electrical hardware and software, with future work on demonstrating applicability in operating conditions.

5. References

[1] Texas A&M Nuclear Safeguards Education Portal. http://nsspi.tamu.edu/nsep/courses/containment-and-surveillance/introduction/what-is-cs-and-why-do-we-need-it-%28cont%29 Last accessed 8/28/2014.

[2] S. Holland, C. Mahan, M. Kuhn, N. Rowe, "Utilizing Metalized Fabrics for Liquid and Rip Detection and Localization," Proceedings of the SPIE, Volume 8719, ID. 87190J, May 2013.

[3] H. A. Smartt et al., "Intrinsically Tamper Indicating Ceramic Seal (ITICS)," Proc. Institute Nuclear Materials Management, Palm Desert, CA, 2011.

[4] H. A. Smartt et al., "First Prototype of the Intrinsically Tamper Indicating Ceramic Seal," Proc. Institute Nuclear Materials Management, Orlando, FL, 2012.

[5] D. Krementz, K. S. Brinkman, M. J. Martinez-Rodriguez, A. E. Mendez Torres, G. E. Weeks, "Development of a Ceramic Tamper Indicating Seal: SRNL Contributions" (2013).

[6] D. Krementz, M. J. Martinez-Rodriguez, *Ceramic Tamper Indicating Seal (Ceramic Seal) Final Report* (2013).

[7] A. E. Mendez-Torres et al., "Synthesis and Characterization of Smart Functional Coatings by Chemical Solution Deposition Methods," Proc. Institute Nuclear Materials Management, Palm Desert, CA, 2011.

[8] R. M. Krishna et al., "Characterization of Transparent Conducting Oxide Thin Films Deposited on Ceramic Substrates," *Materials Letters*, Vol. 65 no. 1, 2011.

[9] M. Shaughnessy, S. D. Hudson, J. R. DiMaio, "Photoluminescence Measurement Characterization Report" (2013).