SANDIA REPORT
SAND2017-9716
Unclassified Unlimited Release
Printed September 2017

Non-RF Chain of Custody Item Monitor (CoCIM) Development Report

Jay K Brotz
Ross W Hymel
J. Rokwel Wade
Steven Schwartz

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

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International, Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

Sandia National Laboratories

Issued by Sandia National Laboratories, operated for the United States Department of Energy by National Technology and Engineering Solutions of Sandia, LLC.

Available to DOE and DOE contractors from
U.S. Department of Energy
Office of Scientific and Technical Information
P.O. Box 62
Oak Ridge, TN 37831

Telephone: (865) 576-8401
Facsimile: (865) 576-5728
E-Mail: reports@osti.gov
Online ordering: http://www.osti.gov/scitech

Available to the public from
U.S. Department of Commerce
National Technical Information Service
5301 Shawnee Rd
Alexandria, VA 22312

Telephone: (800) 553-6847
Facsimile: (703) 605-6900
E-Mail: orders@ntis.gov
Online order: http://www.ntis.gov/search

SAND2017-9716
Unclassified Unlimited Release
Printed September 2017

Non-RF Chain of Custody Item Monitor (CoCIM) Development Report

Jay K. Brotz
Ross W. Hymel
J. Rokwel Wade
Steven Schwartz
Global Monitoring and Verification Research and Development Department
Sandia National Laboratories
P.O. Box 5800
Albuquerque, New Mexico 87185-MS1374

Abstract

The Chain of Custody Item Monitor (CoCIM) developed by Sandia National Laboratories is one of the most mature and well-studied active seals for use in containment applications for arms control treaty verification and international nuclear safeguards. However, its typical design includes wireless communications provided by a radio frequency (RF) transmitter and receiver. While this provides flexibility of movement for many applications, it is unnecessary and undesired for some treaty verification applications. This report details the design and construction of two variants of the CoCIM that remove the RF transmission capability in favor of directly connected wired and short-range infrared communications, as well as a new coordinator that is used to interface the CoCIM to a computer, and new interface software that is simplified for a likely inspection use case.

ACKNOWLEDGMENTS

The authors would like to acknowledge the National Nuclear Security Administration (NNSA) Defense Nuclear Nonproliferation (DNN) Office of Nuclear Verification (ONV) for their generous support of this effort.

CONTENTS

FIGURES

ACRONYMS AND ABBREVIATIONS

CoC	chain of custody
CoCIM	Chain of Custody Item Monitor
DNN	Defense Nuclear Nonproliferation
DOE	Department of Energy
ECDSA	Elliptic Curve Digital Signature Algorithm
IR	infrared
New START	New Strategic Arms Reduction Treaty
NNSA	National Nuclear Security Administration
ONV	Office of Nuclear Verification
PoE	Power-over-Ethernet
RF	radio frequency
RJ-11	Registered Jack 11 (telecommunications standard)
RTTA	request to associate (command)
RTTD	request to dissociate (command)
SNL	Sandia National Laboratories
SOH	state of health
START	Strategic Arms Reduction Treaty
UART	universal asynchronous receiver/transmitter
USB	Universal Serial Bus

1. INTRODUCTION

In FY2015, a gap was identified in the Office of Nuclear Verification (ONV)-sponsored Chain of Custody Technology Mapping Study concerning active seals for use in a monitored dismantlement scenario. The gap consisted of a mature active seal that did not use radio frequency (RF) communications, which was seen as unnecessary and undesirable in the vicinity of nuclear weapons. Since the Sandia-developed Chain of Custody Item Monitor (CoCIM) was assessed to be a mature active seal that met all requirements other than the absence of an RF transmitter, ONV sponsored development of a modified CoCIM to communicate in a mode that would not have the nuclear safety implications of RF and that would conform to the simplified use case described in that study. In response, Sandia has developed two Non-RF CoCIM variants, each of which implements the same use case (described below) with two different communications methods: wired and infrared (IR). In addition, a new (and much simpler) coordinator has been developed to allow an inspector to retrieve messages from a CoCIM, and a new simple user interface has been developed to allow an inspector to quickly make verification determinations within the described use case.

While these versions of the CoCIM have been designed to meet the requirements of a specific use case (described in the next section), the wired and IR CoCIM represent capabilities for active seals in several other use cases that are relevant to research in arms control.

1.1. Use Case

The Chain of Custody Technology Mapping Study constructed a monitoring system for each of three technology constraint cases in a monitored dismantlement scenario. The three constraint cases were: a) equipment already accepted for use in START and New START treaty verification, b) equipment that is currently fieldable, and c) equipment that will be fieldable within the next five years. The scenario begins with receipt of a containerized warhead or bomb in its cradle at the dismantlement facility and ends with verification of dismantlement. While the monitoring scenario could use monitor presence in the facility to gain confidence, the study team recognized that using technology to provide chain of custody (CoC) of the warhead and of equipment during off-shifts and any time they are unattended could reduce the personnel burden on both the monitor and the host. In the first constraint case (a), the study team concluded that CoC tools were inadequate and relied heavily on monitor presence, which drove up cost and intrusiveness. While the current RF CoCIM did find use in the second constraint case (b), it was limited to application in areas that are not near warheads, such as on equipment storage room doors, due to the concern about nuclear explosive safety. So for the third constraint case (c), the study team decided that a variant of the CoCIM without RF capabilities would be usable both on equipment and on warheads, and that it was feasible to be developed within the next five years.

The CoCIM is used to maintain chain of custody of warheads, cameras, and equipment storage rooms during a monitored dismantlement process at times when inspectors are not present. The dismantlement process begins when a weapon enters the dismantlement facility in its handling gear. It then is staged until ready, is removed from its handling gear and placed into a plant-specific container, is removed for radiography, and enters the dismantlement. The dismantlement has several stages. Following each of these container accesses, the weapon is sealed in its container with the CoCIM, and prior to each access the CoCIM seal is opened. Both of these

actions are logged internally on the CoCIM seal unit. The inspectors note in a notebook the time of each container access and container sealing. In addition, the inspectors visually inspect the CoCIM for proper sealing (that is, the fiber optic loop seal is actually threaded through the seal points on the container) and evidence of case tamper following all seal applications and prior to all container accesses. Following the entire dismantlement process (a total duration of approximately two weeks with approximately ten applications and removals of the same seal unit), the inspector takes the CoCIM to a station where its data can be read out. The inspector then compares the collected data on the CoCIM with the collected notes and verifies the chain of custody, post hoc, for the entire duration of the dismantlement. The CoCIM is initialized in a joint fashion prior to its first application, is only handled by the host following initialization and until dismantlement is completed, and only communicates with the coordinator (a module that connects to a computer by Ethernet) once it is done being used for sealing the weapon under dismantlement. A similar process is conducted for CoCIMs that seal cameras to the wall or ceiling and CoCIMs that seal the doors to rooms, although the frequency with which they are brought to the inspector station for data readout may vary, as they will be used continuously throughout the regime in these locations.

2. COCIM DESIGN AND OPERATION

The CoCIM consists of a printed circuit board inside a double-wall tamper-indicating enclosure with a fiber optic loop connected at both ends to the seal body by means of ferrules that tighten the fiber in place by screwing onto a connector on the board. In all instantiations of the CoCIM, the battery-powered seal monitors the fiber optic loop on a regular basis for opening and closing of the seal, generates state-of-health (SOH) messages on a regular (and configurable) basis, monitors the case for tamper (opening of the two parts of the case), has the capability to digitally sign and encrypt all messages created, and has a means of communicating those messages to a coordinator. The Non-RF CoCIM differs from the previous RF CoCIM in the way that it communicates. The two variants of the Non-RF CoCIM created in this work include wired communications by means spring-loaded "pogo" pins embedded in the enclosure and short-range infrared communications through a transparent enclosure.

The complete sealing system consists of Non-RF CoCIMs, a computer for a human interface, a coordinator for transferring messages to the computer, and a programming interface for initialization. The system has two modes: Programming Mode (illustrated in Figure 1) in which the open CoCIM is given configuration parameters and initialized, and Monitoring Mode (illustrated in Figure 2) in which the closed CoCIM can be used to seal an item under containment and communicate to a computer connected through the coordinator.

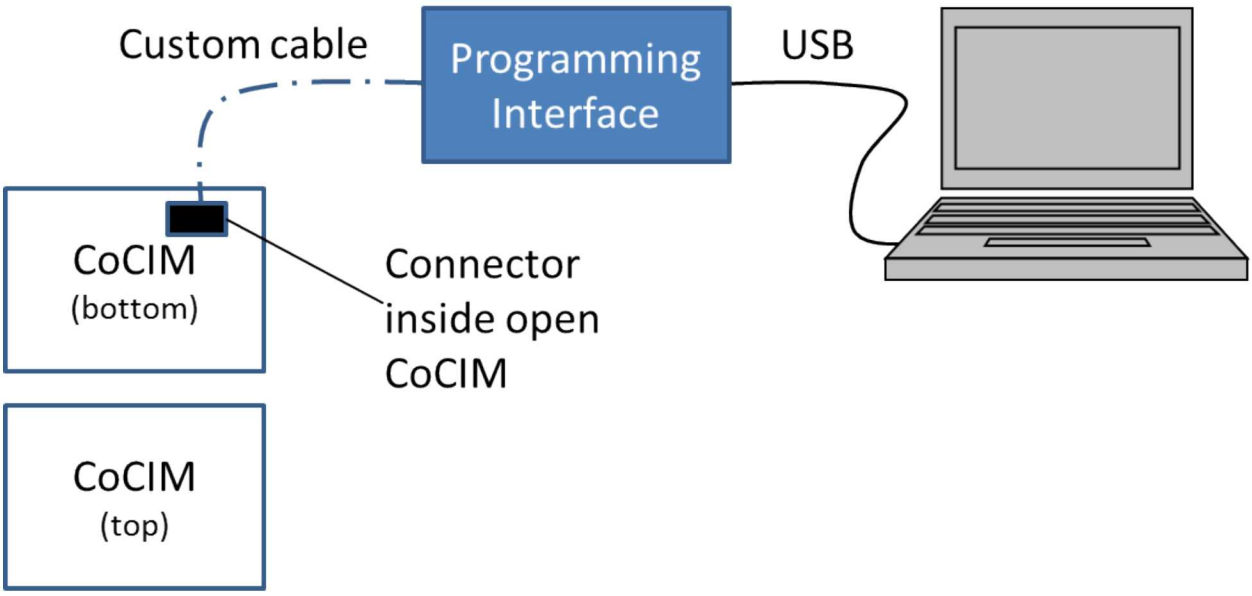

Figure 1. Programming Mode

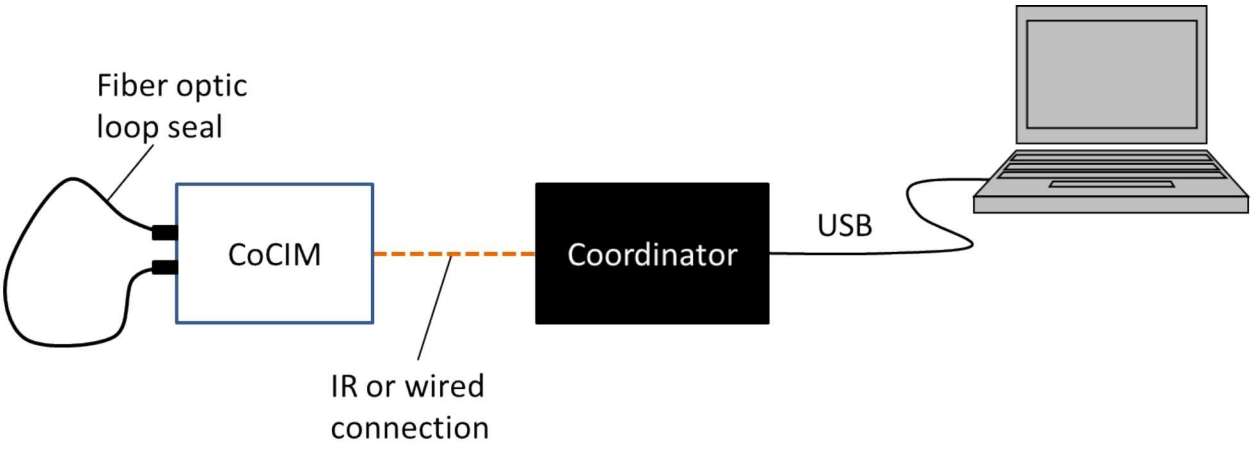

Figure 2. Monitoring Mode

Programming Mode

In the Programming Mode, a CoCIM is initialized for use by setting the configuration of the device in a step referred to as “personality programming”. In this activity, the CoCIM is open and the custom programming cable is connected to the programing connector on the CoCIM main board. This is illustrated in Figure 3 below, with an open CoCIM and a programming interface.

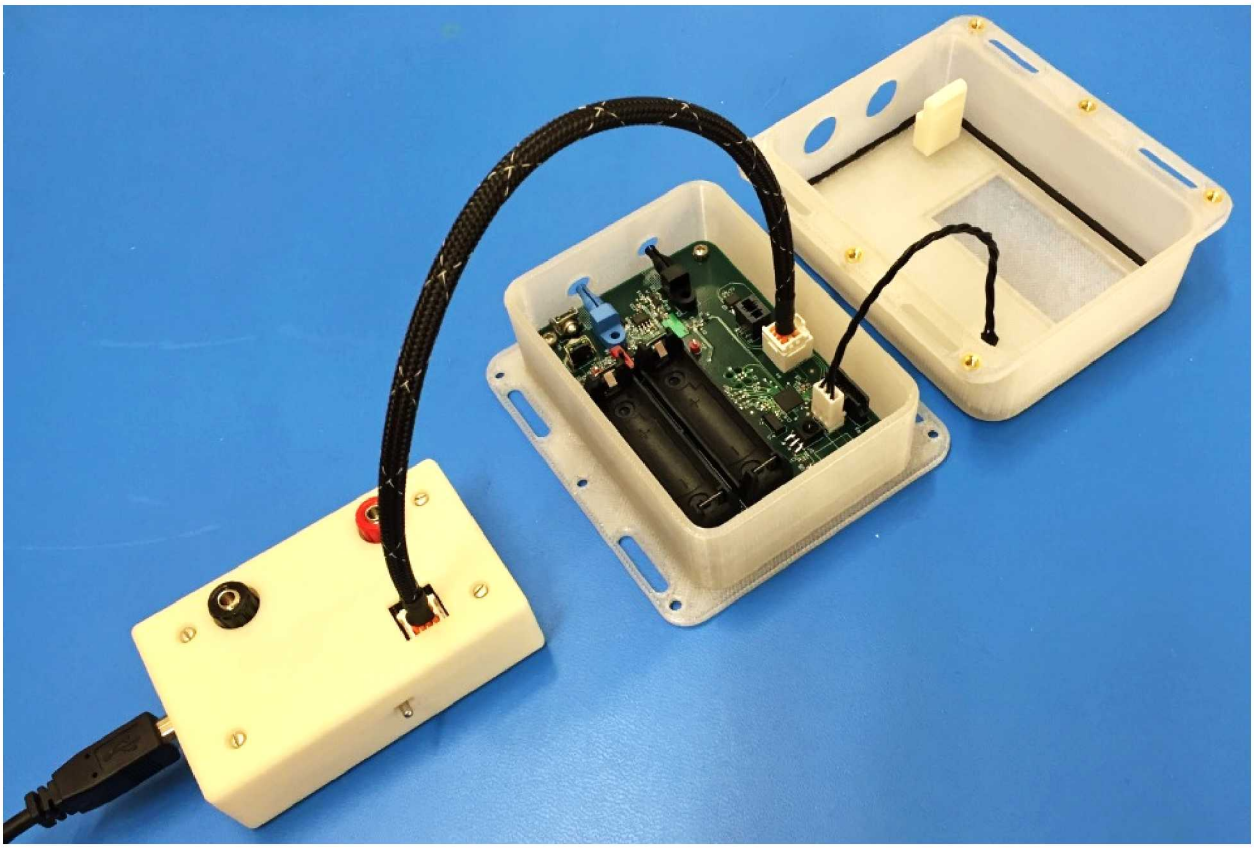

Figure 3. Illustration of Programming Mode

The other end of the custom programming cable is connected to the programming interface and the programming interface is connected to the computer by USB. The Personality Programmer (software program) is run on the computer and the configuration in a configuration file is loaded onto the CoCIM. The configurable parameters are frequency of SOH message generation and the current date and time.[1]

The programming mode should be used in a joint initialization of each CoCIM in the presence of the host and monitor parties. Since the computer used to configure the CoCIMs will be either a host or a monitor computer, and authenticating or certifying that computer will be difficult, it would be preferable for each party to have adequate confidence in the configuration file and in the programming interface (and for the initialization to occur in a non-sensitive area). Specifically, both parties should trust that the programming interface is incapable of using any data transferred to it by the computer via USB that is not specifically formatted for configuration of a CoCIM, and that the configuration file that is loaded onto the CoCIM is as agreed.

---

[1] Historically, this configuration included more parameters, including authentication and encryption keys used in symmetric algorithms. The CoCIM (all forms) uses public key cryptography supported by a custom FPGA cryptoprocessor within the unit, which creates the keys in hardware upon power up and initialization. In theory, the SOH frequency could be hard-coded in the firmware, but the date and time should still be loaded during initialization so that the first message has a valid date and time stamp.

Improvements could be made to the programming interface hardware to generate this confidence.

Monitoring Mode

In the Monitoring Mode, the CoCIM has been initialized and records all seal and tamper events, as well as a SOH every four hours (or as often as configured).

The Message Viewer software allows the user to request and to receive messages from the CoCIM through the coordinator. The coordinator, whether wired or infrared, is a small PCB in an enclosure that interfaces to the CoCIM, either with spring-loaded "pogo" pins or with an infrared transmitter and receiver (through transparent enclosures). Two commands are sent to the CoCIM when messages are requested (with the Download button) – one command that causes the CoCIM to send all seal messages and one command that causes the CoCIM to send all non-seal messages. This results in the CoCIM sending every message in its memory through the coordinator to the Message Viewer software on the computer every time that messages are requested.

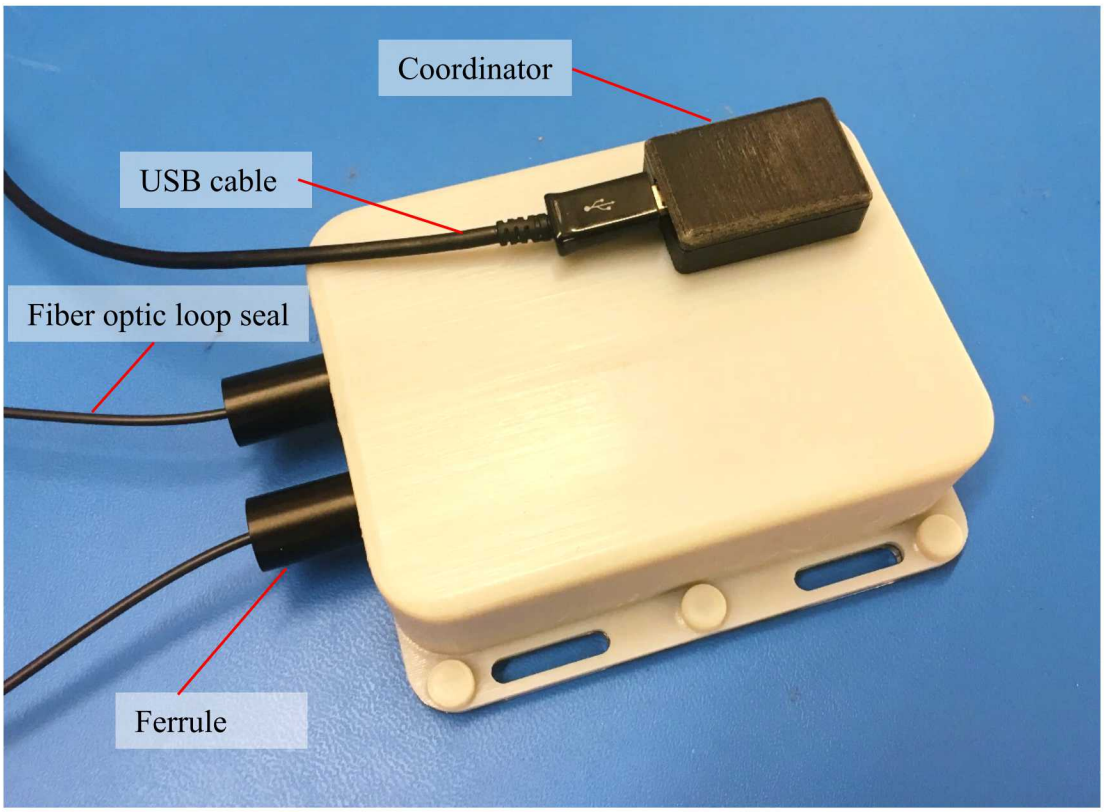

Figure 4. Wired Coordinator attached to Wired CoCIM Seal

The behavior of the Non-RF CoCIM is simplified with respect to previous RF versions. A Non-RF CoCIM creates a Public Key message immediately after initialization, which includes the CoCIM's public key as a data field. It then creates a SOH message, and after every preset

interval it creates another SOH message. Any seal opening will immediately create a timestamped Seal Event message and a seal closing will create (after a few second de-bounce period) another Seal Event message indicating closure. The only commands that the Non-RF CoCIM will respond to are the two commands that result in all messages being sent to the coordinator.

The Message Viewer software has one primary screen with two sections and four buttons, as seen in Figure 4. The Download button will cause the two commands to be sent to the CoCIM to send all messages, and the Message Viewer software will receive and display all messages in the message table section. This can be done multiple times with the same CoCIM – each time it is done, the messages that have already been collected will be ignored, so that duplicate messages are not displayed in the table. Messages can be filtered by type or any text contained within using the filter section. The main data fields displayed in the table are message number, message type, date and time of creation, an authentication flag (described in the next section), and an expandable list showing all contained data fields.[2] The use of the Message Viewer software is described in more detail in the Non-RF CoCIM User Manual.

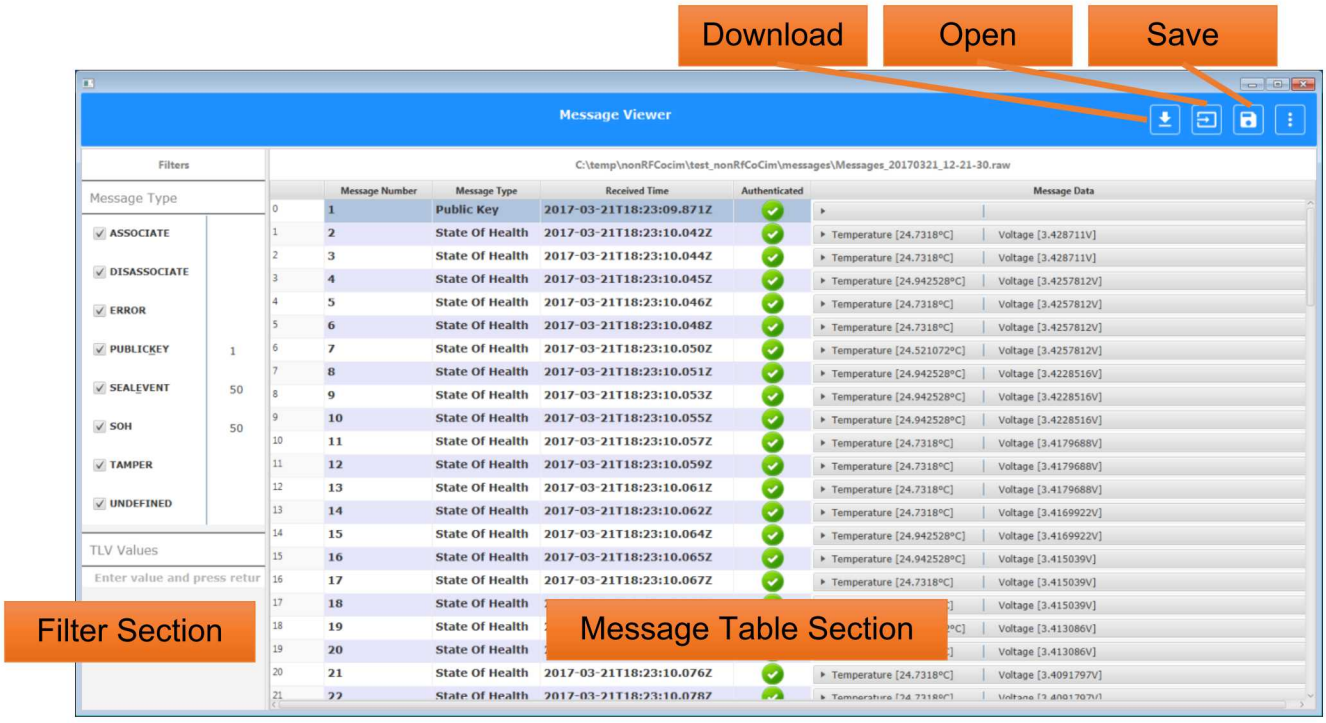

Figure 5. Message Viewer Interface

[2] For diagnostic and backwards-compatibility reasons, there are many data fields in CoCIM messages that are not useful to inspectors in our use case. These are available to view in this expandable list, but probably will not need to be.

Authentication

Digital signatures provide authentication for all messages by an elliptic curve digital signature algorithm (ECDSA) on the public key cryptoprocessor inside the CoCIM. Using the public key from the first CoCIM message, all subsequent messages will be verified for data authentication and the result will be displayed in the Authenticated column of the message table. Since the public key is the most security-critical piece of information, the inspector should read the CoCIM messages immediately after initialization in order to detect tampering of that key in subsequent reads.

Communication between the CoCIM and the Coordinator

There are four communications variants of the CoCIM: an RF variant (the original design and a basis for comparison), a wired pogo pin variant, a wired RJ-11 variant (an early prototype superseded by the pogo pin variant), and an infrared variant. Each sends generated messages and receives commands over a serial connection. The differences between these communications methods are described in this section as are the potential strengths and weaknesses of each communication variant.

RF communications between the CoCIM and the RF coordinator use multiple communication architecture layers. All of the layers are managed by the radio chips: Texas Instruments CC1101 on the CoCIM and Texas Instruments CC430 on the coordinator. This RF communications method uses a mature design and has seen extensive operational testing. The RF variant is the standard to which the other three communication variants were compared. The main advantages of the RF variant are ease of communications provided by an omnidirectional transceiver with a range of tens of meters, allowing not only periodic, on-demand communications, but pervasive communications in an unattended mode. The main disadvantage, which is the reason for this current work, is that RF energy poses a concern for nuclear explosive safety when used near nuclear weapons. It becomes a more serious concern when the RF transceiver is attached to the warhead or its container.

In the second year of this project, we migrated the previous coordinator design from an Ethernet interface to a Universal Serial Bus (USB) interface. This simplification drastically reduced the size of the coordinator, from 10.9 in^2 to 1.2 in^2. It also allows the coordinator to plug directly into any computer that contains a USB port (via a type B micro USB cable) rather than requiring Power-over-Ethernet. To access the coordinator, the only requirement is that the FTDI virtual COM port driver be installed on the host computer, and this driver is freely available from FTDI. Once installed, the coordinator will appear as a standard COM port with configurable baud rate when plugged in. Like the first version, this coordinator supports both wired and IR communication.

The wired variant uses a directly-connected universal asynchronous receiver/transmitter (UART). This is the same UART signal that transfers data between the microcontroller and the radio in the RF variant, simply bypassing the radio on the CoCIM and coordinator. The wired “pogo pin” variant was designed to reduce the size of any case penetrations. Only three pins are necessary for the serial communications between the CoCIM and the coordinator, so we

constructed a custom interface in which three pins are embedded directly into the enclosure material of the CoCIM and three spring-loaded pogo pins are embedded in the underside of the coordinator (see Figure 6 for a close-up view of the pins in both devices). In the CoCIM, the pins are connected to the board inside with a small cable. The coordinator case is designed to fit over the CoCIM such that the pogo pins are lined up with the static pins, as shown in Figure 4. Small magnets are used inside both enclosures to ensure proper pin alignment.

The IR variant uses the same UART with an infrared transmitter (Vishay VSLB3940) and receiver (Vishay TSDP34338) using pulse code modulation at a carrier frequency (a pulse frequency) of 38.4 kHz and a data rate of 4800 bps. The locations of the transmitter and receiver on the CoCIM board are shown in Figure 11. The placement of these IR components in the CoCIM and the coordinator allow the same type of mating to be used for communications as in the pogo pin variant, shown in Figure 10. However, an advantage of the IR CoCIM is that contact is not necessary, which may be a benefit for nuclear explosive safety even without an RF transmitter. The range of the IR transmitter/receiver pair is about two meters, and could be increased or reduced as needed for a particular use. The IR CoCIM and coordinator must have translucent, though not necessarily completely transparent, enclosures (the 3D-printed enclosure shown in Figure 7 performs correctly).

The coordinator achieves infrared communication at 4800 baud using pulse code modulation. The underlying carrier frequency is 38.4 kHz in 8-N-1 format. For wired communication, the coordinator employs a standard UART operating at 4800 baud. Three pins are necessary, receive (RX), transmit (TX), and ground (GND). Because this connection is physical, the pins are protected against both electro-static discharge (ESD) and electromagnetic interference (EMI) via dedicated circuitry. The connection itself uses spring-loaded pogo pins. These pins are directly soldered into the printed circuit board and are long enough that they penetrate three pre-defined holes in the housing while still being able to actuate. A CAD drawing of the printed circuit board layout of the coordinator is shown in Figure 6.

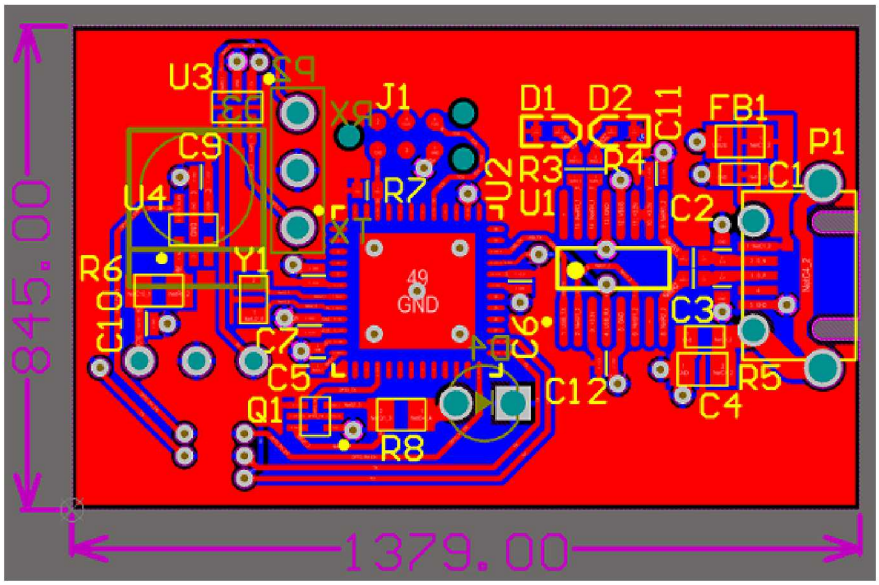

Figure 6. PCB Layout of Coordinator

Figure 7. Static Pins Embedded in CoCIM Enclosure and Pogo Pins Embedded in Coordinator Enclosure

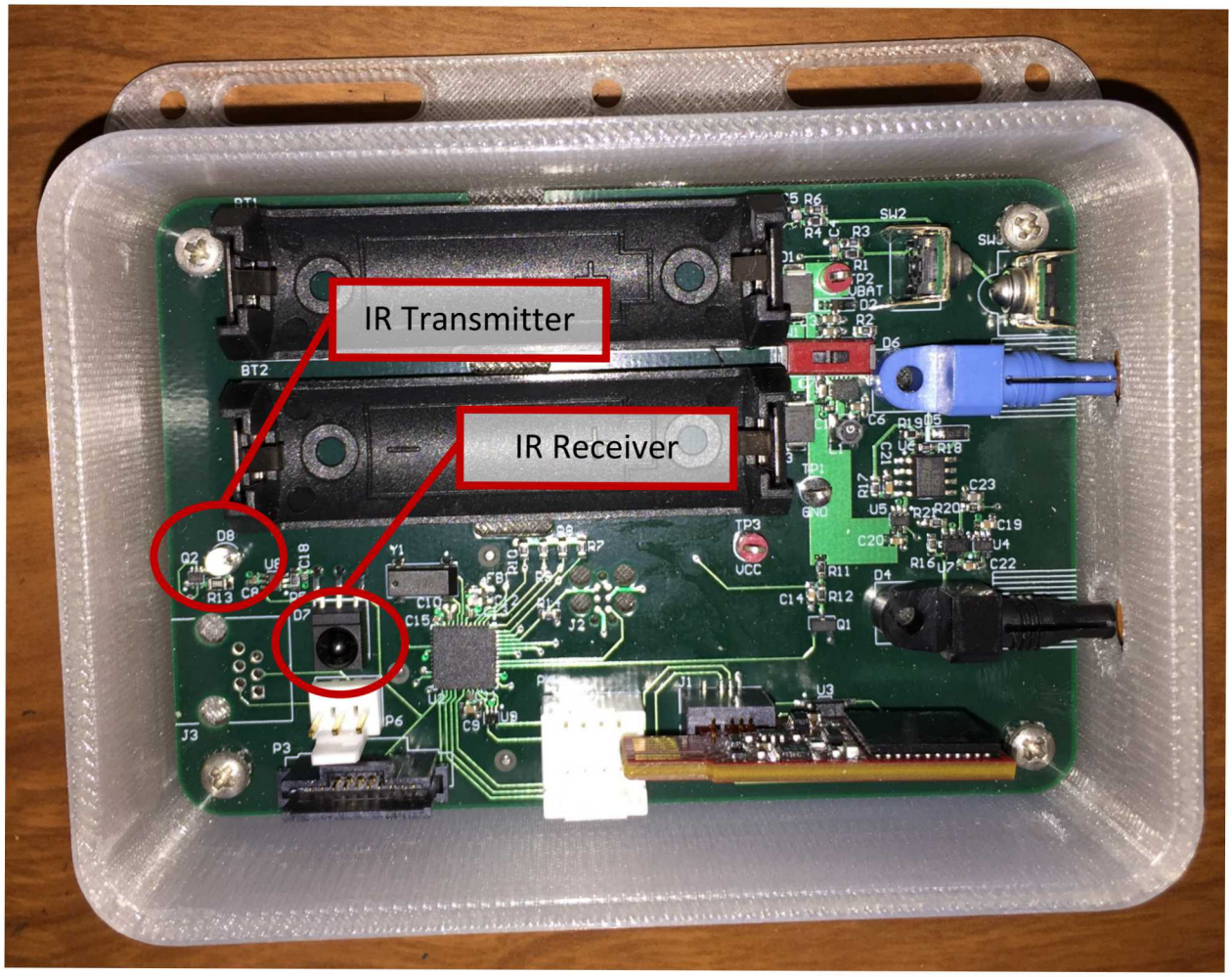

Figure 8. IR Transmitter and Receiver

3. CONCLUSIONS

We have developed two variants of a Non-RF CoCIM with associated coordinator and user interface software. The IR variant is the best option if contact is not desired between the coordinator and the CoCIM. If, for any reason, standoff wireless communications were not desirable (due to information sensitivity in the messages, for instance), the pogo pin CoCIM may be more suitable.

The development of a CoCIM to suit the described use case has been completed, and the wired variant will be used in the LETTERPRESS exercise in October, 2017, as part of the Quad Arms Control Working Group. The design team recommends a vulnerability analysis be performed on the CoCIM system.

DISTRIBUTION

1	MS0899	Technical Library	9536 (electronic copy)
1	MS1374	Jay Brotz	6831
1	MS1374	Mary Clare Stoddard	6831


Sandia National Laboratories