SAFEGUARD SYSTEM

RMSA™

Remotely Monitored Sealing Array

Versatile, low-power active sealing solution that can support multiple sealing and containment verification disciplines.

FEATURES

- Portable, active and reusable sealing system
- Monitors and records tamper events, inspection data and seal status
- Provides requested or periodic State of Health updates
- Provides intrinsic tamper indication
- No external power required, battery operated
- 4+ years surveillance between battery replacement
- Secures Seal data with encryption and authentication techniques
- Communicates all relevant data to a data Translator station via RF communication link
- Requires no license for its low power 900 MHz ISM band RF communication
- Many seals (hundreds) can be linked to a single translator station
- Allows remote transmission of Seals and Seals events for off-site review

DESCRIPTION

The ‘Remotely Monitored Sealing Array’ or RMSA system is a versatile, low-power active sealing solution that can support multiple sealing and containment verification disciplines. The RMSA system introduces an electronics platform that is designed to monitor a fiber optic loop seal and to communicate the results to a data consolidation Translator via secure radio frequency communication. At the Translator station, data can be stored locally or retrieve from a remote host computer for analysis.

Based upon the Secure Sensor Platform (SSP) technology developed by Sandia National Laboratories (SNL), the RMSA Fiber Optic Seal is a low-cost active fiber optic loop seal that stores, forwards and communicates data (tamper events, open/close events, seal status) via a customized data communication protocol over a no-license, low power RF link. The data can be stored and transferred remotely and securely (authenticated and encrypted) to the RMSA Translator that collects data from all the RMSA seals in a particular location. The data is made available on the RMSA Translator in an easily accessible format either for data retrieval by an authorized inspector (SD Card) or for remote data communication via Ethernet and VPN link. The data collected by the RMSA seals can then be verified and analyzed on-site or worldwide with the RMSA Review Software. The RMSA Programmer serves as the tool for initial set up of the RMSA seals (loading keys).
The RMSA Fiber Optic Seal is rugged and resistant to tampering. Its electronics are in a tamper indicating anodized aluminum or plastic housing. A pair of tamper switches is used to detect any opening of the seal housing. The seal can be easily installed and reused indefinitely with no external power required; the seal housing may be opened to replace the internal batteries. Openings are recorded as tamper events. The Seal is contained in an overlapping two-piece case that contains an O-ring Sealing system for environmental protection. The Seal stores data and then forwards this data securely to a local Translator via a low power RF communication. Thousands of normal State of Health messages are stored locally in the Seal in a non-volatile circular memory buffer. This locally stored data can be retrieved by the user when following the Send Message Protocol should RF transmission be interrupted during normal operation. Three versions of the seal are available: Aluminum enclosure with external antenna, plastic enclosure with external antenna and plastic enclosure with internal antenna.

The RMSA Translator is the device used to initialize the seal. Only one translator is needed per location. The Translator collects, stores, and then forwards data from the Seals, local or remote. All data is encrypted by the Seals before transmission, though some portions of the data frame such as Seal ID is sent in the clear (no encryption). An authentication signature is part of the overall Seal message. The Translator sends the encrypted Seal messages as well as non-encrypted information regarding the Seal address, the number of bytes in the encrypted messages, received signal strength as seen by the Translator, and other information.

The RMSA Review Software Application includes the ability to decrypt and authenticate Seal data and facilitates review of data both in a batch processing mode and in a live update mode. Review Software can be run on any PC so that data can verified and analyzed at the installation site or remotely. A TCP/IP (Ethernet) connection between the Translator and the Remote Review Application host facilitates the transfer of data from the Translator to the Review Software Application. In addition to remote review, this network connection is used to allow the inspector to interrogate specific Seals for state-of-health or to request re-send of a specific Seal message.

The RMSA Programmer is used to program the microcontroller code and Seal personality information that is unique to each Seal. It also provides the interface between an external USB device, such as a PC, and the UART on the Seal, for personality programming and debugging.

**MODES OF OPERATION**

The RMSA system is capable of supporting three configuration modes of operation: standalone mode, local host supported mode and remote monitoring mode. In the standalone configuration, the system hardware may consist of many active RMSA Fiber Optic Seals and one RMSA Translator, which sits unmonitored for long periods of time. The local host supported configuration is via an Ethernet interface connected directly to a local host computer. The remote monitoring mode is similar to the local host mode but is via the internet to allow monitoring by a host computer of the RMSA system over the internet.

**BENEFITS**

- Efficiency – Less time needed to inspect and interrogate seal in the field. No more need to visit and check each individual seal
- Security/Reliability – Fulfill IAEA Safeguards standards to provide a platform with authenticated and encrypted communication channels, tamper indications and sealing capabilities
- Versatile – Easily installed and maintained with two types of seal antennas available, large (hundreds) number of seals deployed at one location and manageable remotely. No special tooling to terminate sealing cable required

Overview of the RMSA system.
RMSA FIBER OPTIC SEAL

- Power: One or two lithium, 3.6 V AA Batteries
- Expected operational life: 4+ years (two lithium batteries)
- Non-volatile memory: Thousands of messages
- Fiber seal: 1 mm Plastic Fiber ≤50 m Length
- Security: Active/Passive/Intrinsic
- Other features: Clock accurate to two minutes/year, battery monitor, temperature monitor
- Environmental: -40 °C to +85 °C (operation or storage)
- Humidity: 5% to 95%
- Case: IP54 minimum
- Case material: White PVC plastic
- RF frequency operation: 900 MHz ISM Band (902 to 928 MHz) (other ISM/SRD bands available)
- RF sensitivity: -110 dB (typical)
- RF power output: -30 to +7 dBm typical at antenna input (internal or external) +10 dB ERP improvement with 1/4 wave vertical external antenna (transmit and receive)
- Antenna: Internal F or External SMA connection
- Communications protocol: SSP/Sandia TLV
- Encryption: AES 128-bit cipher
- Authentication: AES 128-bit cipher
- Dimensions and weight:
  - Metal: 5.125 x 4.135 x 1.590 in. (1.26 lb)
  - Plastic: 4.640 x 4.125 x 1.560 (0.75 lb)
- Communication range with translator: 500 meters with external antenna, 200 meters with internal antenna – * based on outdoor test with no obstacles

RMSA TRANSLATOR (Plastic Housing)

- Power source: AC Power (universal 120 V/220 V, 50/60 Hz)/POE
- Power dissipation: 6 W maximum, 4 W typical
- Environmental: -40 °C to +85 °C (operation or storage)
- Humidity: 5% to 95%
- Case: IP54 minimum
- Case material: Polycarbonate
- Security: Active
- Memory: Removable SD Card, 128 MB SDRAM, 512 MB Flash
- Software: Debian Linux 2.6.21 based application
- RF frequency operation: 900 MHz ISM Band (902 to 928 MHz) (other ISM/SRD bands available)
- RF sensitivity: -110 dB (typical)
- RF power output: -30 to +7 dBm
- Antenna ports: Dual SMA Female connectors, only one active
- Communication: Compatible with SSP/Sandia TLV protocol
- Ports: Gigabit Ethernet, 10/100/1000 speeds
- Weight: Four pounds (includes AC power adaptor and one antenna)
- Dimensions: 9.8 x 6.8 x 3.7 inch

RMSA REVIEW SOFTWARE

- Operating system: Windows XP 32-bit required
- Hard drive: 500 MB minimum
- Memory: 1 GB minimum plus hard drive swap space
- Other: Ethernet port, Microsoft .Net Framework 3.5 SP-1 required
- Encryption: AES 128-bit Cipher
- Authentication: AES 128-bit Cipher
- Features: Add/Subtract Categories, Sort on Category, Sort on Seal, Color coded alerts

CERTIFICATIONS

- TUV
- FCC