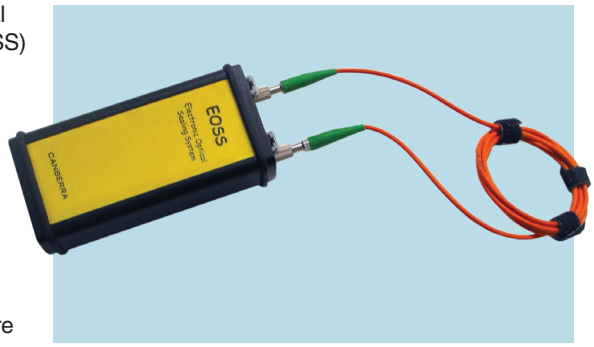
MIRION TECHNOLOGIES

Electronic Optical Sealing System (EOSS)

Features

- Portable, active reusable seal
- Logs tamper events, open/close events, inspection data, and seal status
- Tamper proof enclosure
- Encrypted data storage

Description



The Electronic Optical Sealing System (EOSS) is a re-usable mechanical locking seal for long-term surveillance. The EOSS seal employs an active fiber optic light source and light sensor to record any open/close events. Source and sensor are connected outside the seal housing through a fiber optic cable, which takes the place of the sealing wire used in a typical non-electronic seal. The EOSS seal does not prevent opening and closing; instead, it monitors the FO cable and records any attempt to open, cut, or manipulate the FO cable. In addition, the EOSS seal includes built-in provisions to report any attempt to tamper with the seal body (e.g. trying to drill a hole in the seal body to gain unauthorized access to the seal data or to switch off essential functions). Any attempt to open the seal's case is stored in the seal's memory.

Sealing is achieved by sending light pulses through the fiber optic cable and monitoring the received signal. If the cable is closed, the light pulses are immediately received. If no pulse is received, the seal is considered opened. The seal timestamps all open/close events and stores them in an event log, which is also capable of storing other information including operator activities or state of health information.

The EOSS seal delivers three types of information to the seal reader: status data, event log data, and inspection data. The status data includes information on the current state of the seal such as the state of the seal wire, housing switch, battery voltage and remaining capacity, and hardware failures. The event log stores all openings and closings of the seal wire, certain operator activities (i.e. logon/logoff), and security-relevant data such as battery compartment openings and attacks on the seal electronics and cryptosystem. The event log is secured through a message authentication code that makes it possible to verify that each entry is complete and genuine.

While the seal status and event log are read-only, the inspection data can be read and written to. Here, the seal can store additional information such as seal location or cargo contents. Data is automatically stored in an encrypted database file which can be viewed and analyzed off-line (without connecting to the seal). Data can be exported to a customized XML document, which in turn can be distributed and processed across various computer platforms and database systems.

Electronic Optical Sealing System (EOSS)

COMMUNICATION

A PC/notebook computer connected to the communication port of the seal allows users to view event log entries. Serial (RS-485/RS-232) and Ethernet (IP) are supported. Seal reader software is employed to communicate with the seal itself. The software, which runs on Windows® 2000 and XP, is used to retrieve, store, and display data collected from the seals. It is also used for initializing the seals and for performing diagnostics and maintenance functions.

DATA SECURITY AND STORAGE

The EOSS seal provides all data with authentication tags, which are created by a message authentication code (MAC) that combines the data with a secret key consisting of random numbers. The keys are generated in the seal and are used by the EOSS seal to verify the authorization of operator commands as well as to encrypt data transmitted between the operator and the seal. The various keys are handled as a single unit referred to as a *key-set*. The key-set is created during the initialization of the seal. The security of the seal depends on good key-set management: Seal data cannot be trusted if there is any indication that a key-set or parts of it may have been discovered by unauthorized personnel.

The 8-KBytes EEPROM of the log memory is divided into pages of 64 bytes. Each of the three logs uses a different format for the log entries. However, all pages have the same header format. The page header contains a 64-bit authenticator, the seal serial number (16 bit), the page type (8 bit) as well as the page number (8 bit) and the time at which the authenticator was created (32 bit). The authenticator covers the contents of the whole page. Therefore, a page is the smallest verifiable unit in a log.

ENCRYPTION

The access authorization and data authentication of the EOSS seal is based on the TDES symmetric block cipher. To facilitate the distribution and selection of the keys, the seal reader uses a special utility program, the Key Manager, to automate the handling of keys. The Key Manager encrypts the keys with a user-specific password, holds them at a single, common location and provides required keys on request of the seal reader.

Specifications

- OPERATING ENVIRONMENT – Windows 2000 and XP.
- INTERFACE – RS-485/232 or Ethernet.

POWER

- Main Battery –
  - TYPE – Two internal Lithium batteries.
  - OPERATIONAL LIFETIME – Approximately two years.
- Emergency Battery –
  - TYPE – Internal Lithium battery.
  - OPERATIONAL LIFETIME – Approximately 2000 h.
- External Power –
  - VOLTAGE RANGE – 5 V dc to 18 V dc ±10%.
  - CURRENT CONSUMPTION [peak] – Approximately 6 mA.

PHYSICAL

- DIMENSIONS – 125 x 60 x 35 mm (4.9 x 2.3 x 1.3 in.); excluding seal wire.
- WEIGHT – 260 g (9.1 oz).
- MEMORY – 8 Kbytes EEPROM flash memory segmented into three logbooks. Logbooks organized into 64 byte pages.

SEAL SPECS

- OPERATING AND STORAGE TEMPERATURES – -20 °C to +80 °C (-4 °F to 176 °F).
- HUMIDITY – 10% – 90% non condensing.
- Splash waterproof to meet IP54 standard.
- LASER PEAK POWER – <0.4 mW.
- LASER WAVELENGTH – 130 nm.
- Seal Wire –
  - Maximum length up to 1000 meters; maximum recommended length is 50 meters (8 mm diameter required to feed the FO cable).
  - MINIMUM BENDING RADIUS – 30 mm.

ISO 9001 SYSTEM CERTIFIED

CANBERRA