IAEA-SM-367/B/14/01/P

THE IRES ELECTRONIC SEAL

B. AUTRUSSON, D. BROCHARD
Institut de Protection et de Sureté Nucléaire IPSN/DSMR/SATE, France

J.F. MOREAU, J.C. MARTIN
SAPHYMO, France

In the framework of the French Support Program for the IAEA Safeguards, the "Institut de Protection et de Sureté Nucléaire" (IPSN), developed an electronic seal called Integrated and Reusable Electronic Seal (IRES) that enables independent verification by different inspectorates (IAEA, Euratom, and National Inspectorate)

The seal can be remotely interrogated by radio frequency and integrated to other Containment/surveillance systems by serial line RS 485. Data are authenticated and the IRESMAG software manages in the seal reader all functionalities of the seal and records inspection data compatible with the IAEA's Seal Database. To perform this development, IPSN relies on industrial partners: SAPHYMO for the general architecture of the seal and the electronics, THALES for the authentication of data and the security of transmission.

I – THE MAIN FEATURES OF IRES

The main features of the IRES seal are the following

- Interrogation by different inspectorate, allowing independent conclusions.
- Recording of events, including tampering, in a non-volatile memory.
- Authentication of data and enhanced security of the communication between the seal and the seal reader.
- Remote interrogation by an inspector or/and automatic for unattended systems or remote monitoring.
- Reusable after erasing the seal memory and replacement of the batteries (these operations must be performed in a secure maintenance site).

In the light of the results of the feasibility study, prototypes, developed by the SAPHYMO Company, have been demonstrated, in France, between July and September 1999, with data remote transmission to Vienna.

II – SEAL TECHNICAL DESCRIPTION

The seal is manufactured as far as possible with existing industrial components, as following:

Seal enclosure which is a commercially available aluminum enclosure (size 64*98*36 mm), contains all components of the seal except the seal wire.

Sensor element "Sealing wire" : enables to fit through the containment parts for sealing and also to attach to the seal enclosure and electronics. It is a special electrical cable containing a sensitive element able to detect any unauthorized attempt of tampering and which resistivity varies very slightly in the temperature range of the seal operation. Continuous measurement of the resistivity corrected by the temperature insures the tamper indication to detect any unauthorized attempt. This cable was selected to be easy to fit and resistant, with a diameter of 2.5 mm (connectors diameter: 4 mm).

The connection to the electronics is performed through a dedicated watertight connector embedded into the seal enclosure. This connector allows easy connection even with gloves.

Electronics, records any change in the status of the sealing wire connected and other tampering events and produces an internal data base containing a list of date and time stamped events which can be retrieved upon request (by the inspector during inspection or automated in remote monitoring applications). The database includes also state of health messages confirming the proper performance of the seal components (self-diagnostics).

The main micro controller manages all the seal functions. It is designed to minimize the power consumption.

The authentication micro controller hosts the main security functionalities of the seal:

- the authentication software DSA elliptic and the private key. The length of the key is 192 bits.
- the software in charge of the security of the data exchange between the reader and the seal in order to avoid any replay of a command by a malevolent actor. This software is based on an exchange of a question (containing a random aspect) and response to this question, between the seal and the reader which share a common secret.

The non volatile memory installed in the seal (EEPROM) has a capacity of 160 Ko which is sufficient to record more than 1800 events and parameters. Furthermore, the memory stores parameters such as ID and specific code introduced at the factory and at a maintenance site of the inspectorate.

The link between the seal and the seal reader: two kinds of link may be used.

- ***The RF Communication link*** enables the data transfer between seal and the seal reader. This is performed by radio frequency communication with a frequency of 433 MHz. This frequency may be customized according to countries regulations in which the seal will be used. The advantage of this communication mode is to permit the verification of a seal placed into a glove box. It utilizes a standard protocol. The power consumption is some mA in communication and less 1 µA in sleeping mode. The information transferred to the interrogating device is always authenticated between the seal and the seal reader in using a private/public key system. Moreover, specific software has been implemented to avoid any replay of a command.
- ***The serial link*** is a RS 485 standard one and allows to connect up to 32 seals gathered in a daisy chain. This connector hosts also the external power supply. The connector is watertight and easy to connect even with gloves. This link uses the same communication protocol, the same authentication and security systems as the RF link

Practically, there is only one plug devoted to the communication on the seal enclosure; it can be used for both RF and serial link.

The temperature sensor, located close to the enclosure, detects any sudden variation of temperature and records those variations. In addition it corrects automatically the measure of the cable resistivity. The detection of abnormal variation of the temperature will be recorded before that the other components should be affected.

Batteries, are 3 AA lithium type, in case of stand-alone mode. Batteries are exchangeable only during the maintenance of the seal. An additional back up battery ensures recording of events in case of main batteries failure (excepted all other functions).

The seal reader enables the inspector to attach, detach and collect the seal authenticated data (status and performance) by remote data acquisition. The seal reader consists of a commercially available laptop computer running a standard operating system Windows NT 4. A specific customized interface device, which is plugged in the serial port, is needed to establish the RF link to the seal.

The management software, called IRESMANAG, is implemented in the seal reader. Seal data are stored, authenticated, evaluated by the management software, displayed on the screen with a possibility to print out tables for on-site inspections. Data are stored in a database compatible with the MS-ACCESS format allowing their easy transfer to IAEA seals database.

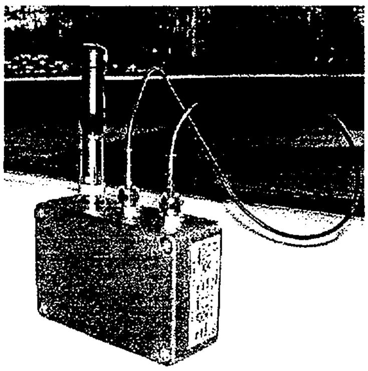

Figure 1: IRES

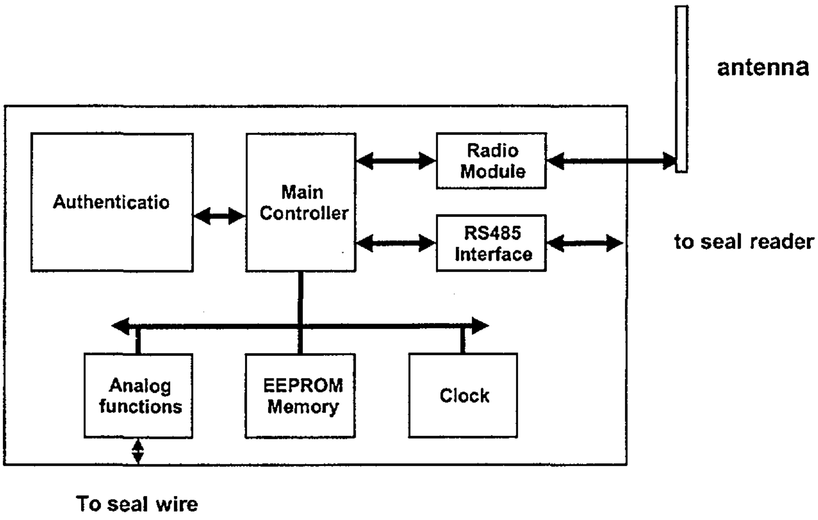

Table 1: Synoptic of electronic board