DEVELOPMENT AND EVALUATION OF NEW ELECTRONIC SEALS AT THE IAEA

Roumen Tzolov, Michael Goldfarb, Laurent Pénot
Department of Safeguards,
Division of Technical Support
International Atomic Energy Agency – Vienna,
Austria

Abstract

During the recent 5 years a wide program for evaluation of existing and development of new tamper-indicating devices was started at the IAEA. The purpose of this program is to assess functionality, usability and possible vulnerabilities of seals already in use, to define the requirements and enhanced features of new devices and systems and to test them appropriately. Emphasis was given to the development and assessment of electronic seals, which represent the family of multiple use, multiple verification tamper-indicating devices with the capability to store internally substantial information about the history of their handling. This information can be retrieved, transferred, processed and evaluated later allowing to establish conclusions about possible tampering of the protected object as well as assurance about the "state of health" of the tamper-indicating device and its components. The present paper describes the main features of the currently used VACOSS-S seal as well as the needs for its replacement, and the most important Agency's requirements for the newly developed electronic seals. The implementation of these requirements is being shown on the examples of new developments mainly supported by the Member States Support Programmes for the IAEA Safeguards. The main technical data of the presented electronic seals are compared. Short description of the necessary steps for the IAEA acceptance testing and authorization procedure for new electronic seals including lab functional tests, usability check, environmental and EMC qualification tests, radiation tests, safety and vulnerability assessments as well as field tests completes the presentation.

1. Introduction

The International Atomic Energy Agency, Vienna, is using world-wide a variety of seals to attain its safeguards objective in the area of Nuclear Non-Proliferation. Seals are used to protect containers with nuclear material and special tools, machines, and instruments, access doors, hatches and other objects in nuclear facilities.

But what is a seal? A seal is a tamper-indicating device designed to leave non-erasable, unambiguous evidence of entry or tampering. Unlike locks, seals are not meant to necessarily delay unauthorized access, just record that it took place. [1]

The seals can be characterized according to their main properties: single or multiple use, single verification (post-mortem or on-site) or multiple on-site verification. Table 1 shows the different types of seals used or under evaluation for future use by the IAEA. The electronic seals belong to the group of multiple use, multiple on-site verification seals and represent the most sophisticated and user-friendly type of security seals, which can be easily integrated in small or large unattended automated data acquisition systems for Containment/Surveillance including also Remote Monitoring Systems at nuclear facilities and elsewhere.

Table 1. Seal types

	Single verification (post-mortem)	**Single verification (on-site)**	**Multiple verification (on-site)**
Single use	Metallic seals (CAPS)	Adhesive seals (VOID)	COBRA seal IRUSS seal
Multiple use	-	-	***Electronic seals (VACOSS, EOSS, IRES, TRFS)***

2. Generic Electronic Seal Design

The generic electronic seal design is shown on Figure 1.

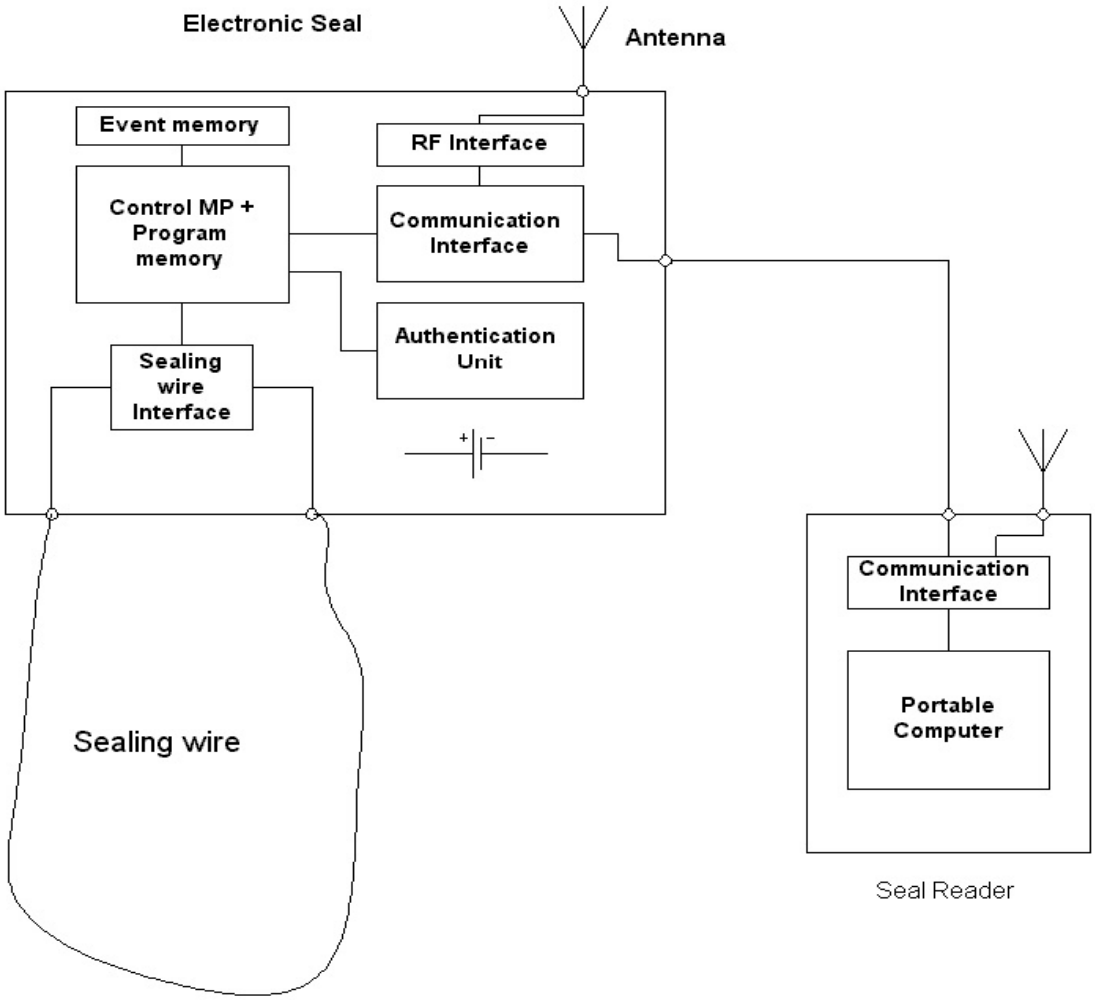

FIG. 1. Block Diagram of a generic electronic sealing system

The sealing system contains two main components: the electronic seal and the seal reader. The sealing wire, which can be an electric wire or a fiber-optic cable, secures mechanically the object under seal (container, equipment, etc.). In the shown simple configuration both

components, seal and seal reader are stand-alone, autonomous functioning active devices powered by internal batteries.

2.1. Main modules of an electronic seal:

- Control microprocessor and program memory, which contains the internal firmware and perform the control and communication between the remaining modules;
- Sealing wire interface – it checks periodically the integrity of the sealing wire and communicates the results to the main microprocessor;
- Event memory, where all events are stored and later retrieved by the seal reader. The events include time stamped information about the status of the sealing wire and the seal enclosure, as well as information about the so-called "state of health" (SOH) of the internal modules of the seal like functional diagnostic, battery level, temperature etc. The event memory is often non-volatile and retains its content even without power. This helps to reconstruct later the complete history of events before the power failure and not to loose essential information.
- Communication interface, which enables the proper communication with the seal reader;
- An RF interface may be included as an alternative for wireless communication using a small external or internal antenna;
- The authentication unit, which may be realized also in the main processor, ensures that all information provided by the seal is genuine, originates from the particular seal and has not been altered, replaced or withhold. The process includes generation of a specific signature for each event inside the seal and its subsequent check after reading the information by the seal reader. Figure 2 and 3 show the principle of event data authentication [2].

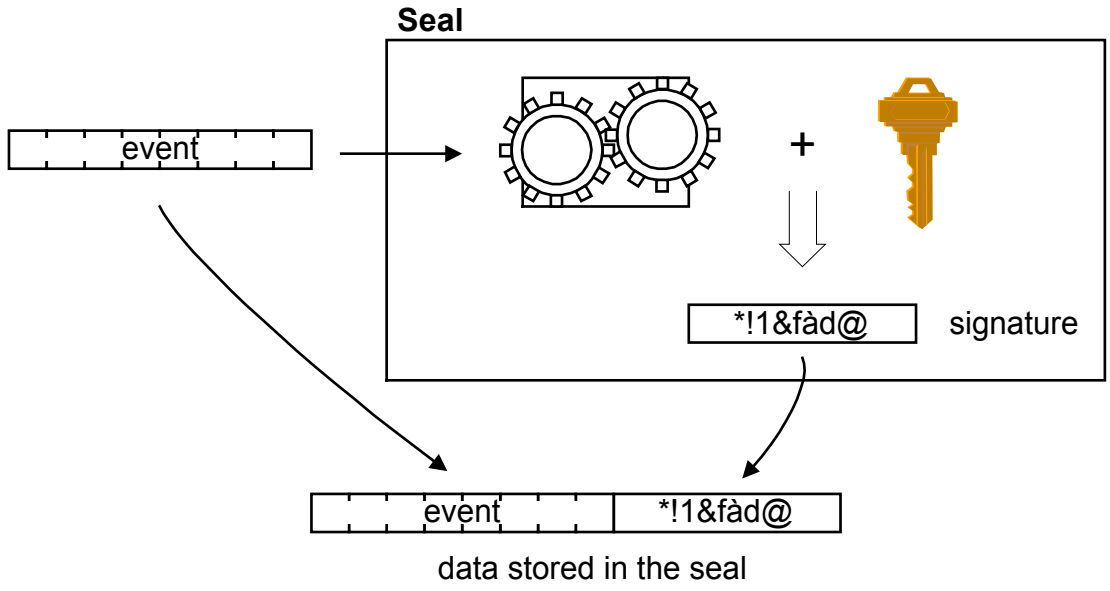

FIG. 2. Generation of the authentication signature in an electronic seal

Standard but also proprietary algorithms are being used for accomplishing of the authentication feature. Depending on the type of authentication used (symmetrical or asymmetrical) the verification of the signature utilizes either the secret private key or a non-secret public key, which can be used only for checking the signature but not for creation of a new one. This is an important advantage of the asymmetrical authentication methods.

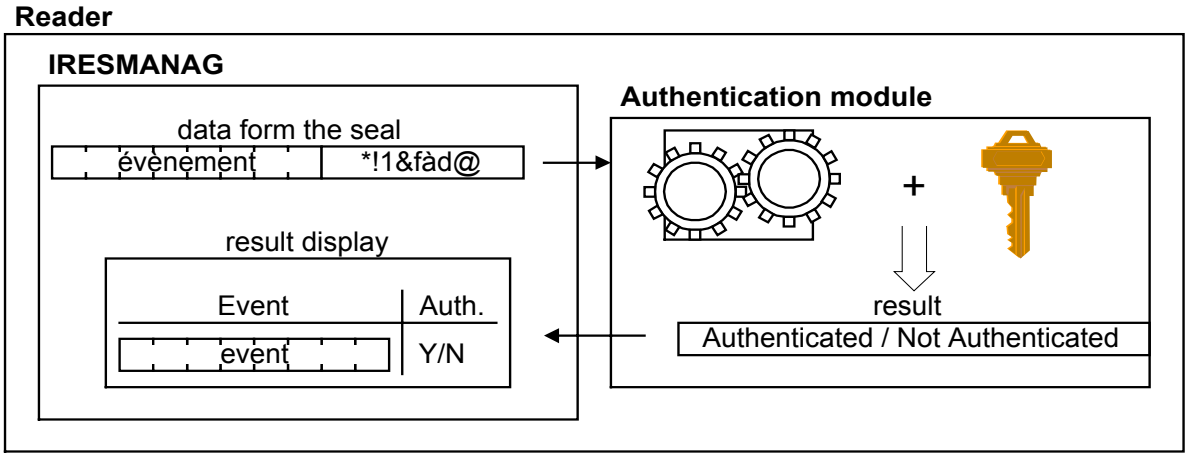

FIG. 3. Verification of the authentication signature in the seal reader.

2.2. Main modules of an electronic seal reader:

- Communication interface, which allows the seal reader to communicate with the seal and supplies additional power to the seal during the reading process if the communication uses a cable. Alternatively a wireless communication path can be utilized for distant reading.
- Portable computer, realizing the interrogation of the seal information, the verification of the authentication, the storage, review and transfer of the seal information.

The seal reader can be used for subsequent reading by connecting to individual seals or the seals may be connected in a daisy chain configuration and handled more convenient as a group. This arrangement is particularly useful for storage facilities with higher number of electronic seals as well as for unattended monitoring systems.

3. The VACOSS electronic seal

More than 15 years ago the need of an electronic seal for multiple usage was recognized at the IAEA and the VACOSS sealing system was developed under the German Support Programme. The device was later accepted and produced by Aquila Technologies Group Inc., USA for Agency use [3]. Currently more than 1500 VACOSS seals are in use by the IAEA world-wide. The VACOSS sealing system is presented on Fig. 4.

The VACOSS sealing system has following main features:

- Active electronic seal for multiple application and verification on-site
- Uses fiber-optic sealing wire with outer diameter of 3mm and length up to 50m
- Autonomous operation for 18 months on 2 internal Li-batteries
- Memory for 10 time stamped fiber-optic events plus initialization data
- Monitoring of the seal case and battery status
- Possibility for providing of encrypted seal data
- Seal reader using an HP palmtop computer and a small interface box, fully portable
- Small size and weight
- Password protection for identity check
- Party-line connection of multiple seals possible
- Simple and reliable DOS reader software for palmtop and desktop PC.

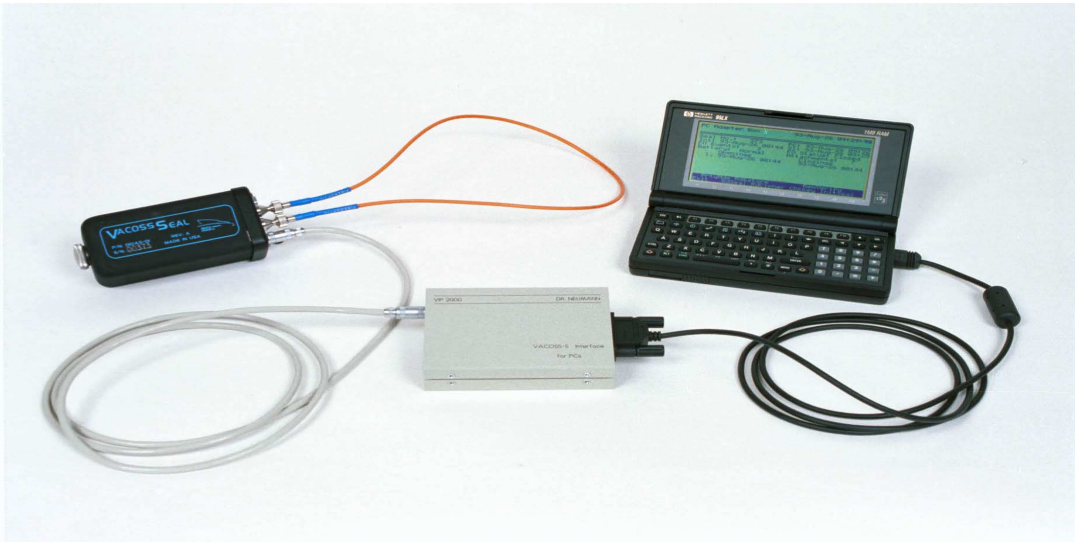

FIG. 4. The VACOSS-S sealing system

During the time the heavy usage of the VACOSS sealing system provided a lot of experience but showed also some weaknesses and deficiencies especially related to the introduction of remote monitoring systems involving electronic seals. Therefore based on this experience, the IAEA decided to establish a set of user requirements considering the most important features of a new electronic seal suitable for the future Agency's safeguards use [4]. The development of the system was proposed to the Member States Support Programmes.

4. IAEA Requirements for the new Electronic Seal

These requirements can be summarized as follows:

- Autonomous tamper-indicating device for multiple use and verification on-site;
- Sealing wire with high tamper sensitivity and maximum length of 100m;
- Internal non-volatile memory for 1000 real-time stamped events, unique serial numbers;
- Events shall include wire and case tamper, SOH and inspector actions;
- Reliable authentication of all seal data using certified algorithms and key lengths of 128 bits or more, private/public key system preferred;
- Seal data encryption as an option;
- Communication to the seal reader by standard RS485 with a range of 1200m or wireless with a range up to 20m;
- Battery life longer than 2 years at average interrogation rate 1 per day;
- Possibility to connect multiple seals in party-lines and to interrogate them automatically in unattended or remote monitoring systems;
- Operating temperature range -35^0C to $+75^0$C, humidity 10-90%, splash-waterproof design, protection class IP65;
- High radiation resistance for gamma rays and neutrons;
- High reliability, small dimensions and weight;
- Seal reader based on commercial portable computer or desktop PC, Windows OS;
- Seal reader data base including auxiliary inspection information and review possibility;
- Easy data transfer and evaluation etc.

The requirements were conveyed to the potential developers and 3 MSSPs accepted the proposal and started SP Tasks for the development of a new electronic seal for the IAEA. The following paragraphs will show these projects as examples.

5. The modified enhanced VACOSS 5E electronic seal

This development was started by Aquila Technology Group, USA based on the design of the current VACOSS seal. The new system is presented on Fig. 5.

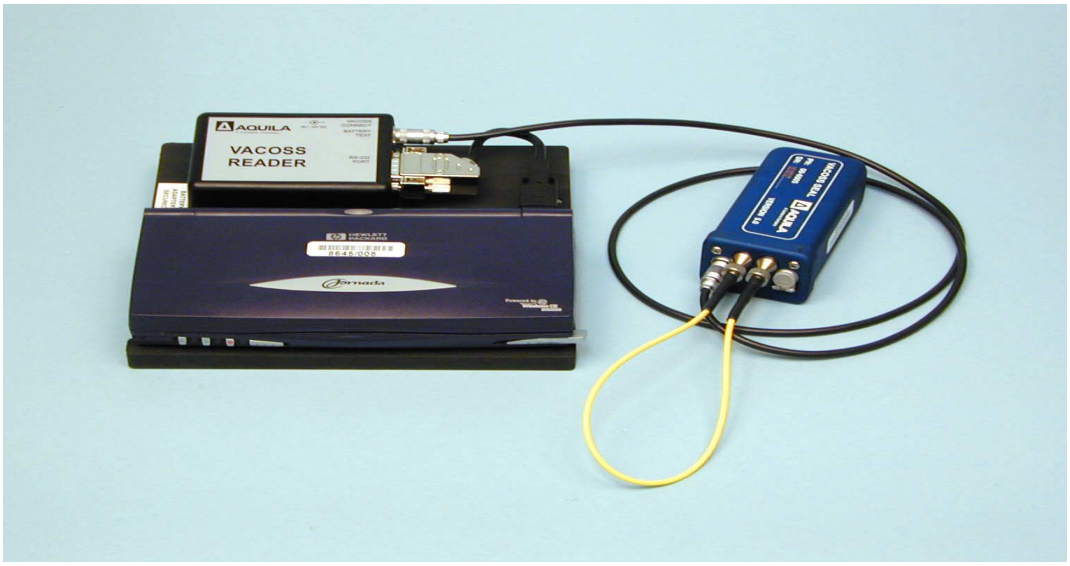

FIG. 5. The enhanced VACOSS 5E sealing system

The main advantages of the system are following:

- Fiber-optic sealing wire, maximum length 500m;
- More reliable operation, capable for fast interrogation;
- Non-volatile memory capacity for 256 events;
- Proprietary authentication of seal data;
- Reader as palmtop Windows CE computer (HP Jornada 690);
- Automatic cyclic interrogation of group of seals;
- Backward compatibility to previous VACOSS seal versions and connections;
- Optional RS485 communication link.

6. The Electro-Optical Sealing System

The Electro-Optical Sealing System (EOSS) is under development by the German Support Programme [5]. Developer is Dr. Neumann Elektronik GmbH, Germany. A sample of the EOSS is presented on Fig. 6. The main features include:

- High sensitive fiber-optic sealing wire, maximum length 2000m;
- Battery life 3 years;
- Registering of sealing wire events, case events and SOH in non-volatile memory;
- Data authentication based on Triple DES with 128 bit keys;
- RS485 communication on twisted pair bus up-to 32 devices;
- Tamper-indicating composite seal enclosure;

- Windows reader software, Ethernet connection possible.

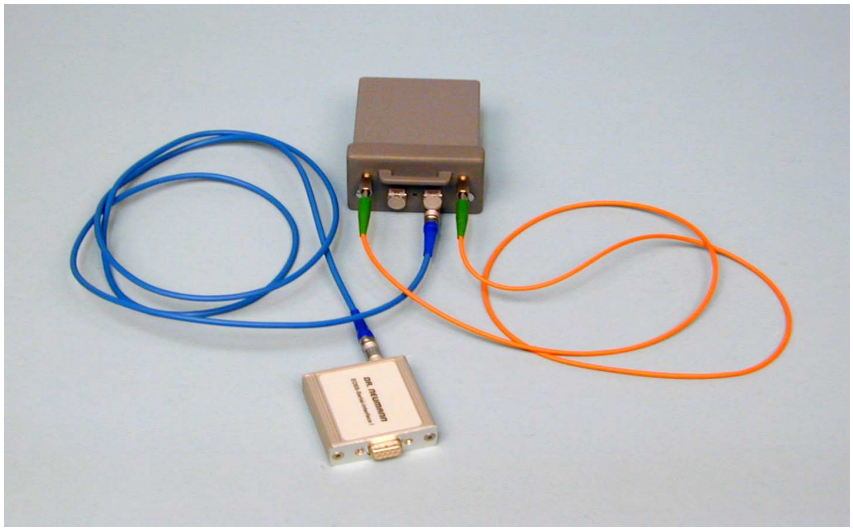

FIG. 6. The EOSS with reader interface box.

7. The IRES sealing system

The Integrable Reusable Electronic Seal (IRES) is under development by the French Support Programme [6]. The developer is the company Saphymo, Massy, France. The sealing system is shown on Figure 7.

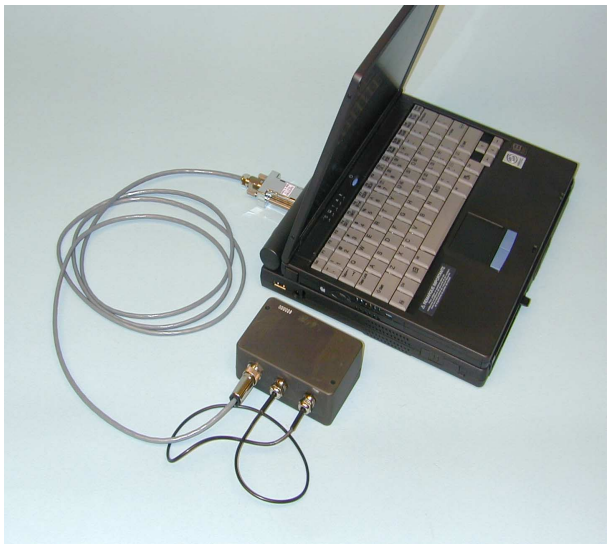

FIG. 7a. IRES seal with cable connection

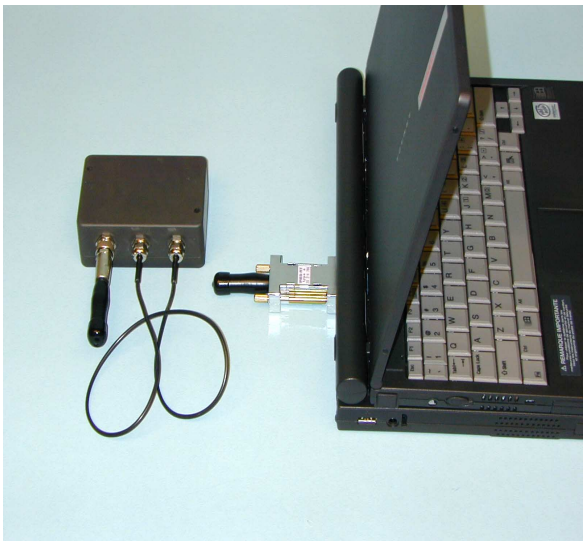

FIG. 7b. IRES seal with RF connection

Main advantages of the IRES sealing system:

- Uses special resistive sealing wire;
- Can support cable communication for 1200m or wireless communication range of 15m;
- Stores up to 1800 events in non-volartile memory: sealing wire events, case events, SOH;
- All data is authenticated using high security elliptic algorithm with 128 bit keys;
- Supports party-line configuration and automatic reading of multiple seals;
- Convenient configuration for up to 3 users with different rights;

- Separate maintenance version for set-up operations;
- Windows NT reader software supports internal data base and additional information;

The seal will be presented in a separate paper at the symposium [7].

8. The TRFS sealing system

Sandia National Lab developed the Two-way Radio Frequency Sealing System with wireless information transfer (TRFS/T-1). The IAEA is currently evaluating the system for potential safeguards use at storage facilities [8]. The system will be also presented at the IAEA SG Symposium. [9] As a short summary it can be characterized as follows:

- Uses low cost fiber-optic sealing wire for easy handling, max. length 30m;
- Sturdy design with long range RF communication for large number of sealed items;
- Battery life up to 4 years, polling and alarm modes;
- Stores internally 100 events, sealing wire, case tampering, SOH;
- Interrogation by a multi-level DAS with high redundancy and storage capacity;
- Flexible configuration for different applications;
- Uses modified TEA algorithm for data authentication;
- Data Review Station for IAEA use under development;

9. Conclusions

All mentioned above new electronic seals are currently under comparative evaluation at the IAEA. The program includes functional tests, environmental and EMC qualification tests, radiation tests, usability evaluation, vulnerability assessment, field tests. After completing of all tests, which are at different stages now, the IAEA will perform based on the results a comparison of the proposed new electronic seals and choose the most appropriate one for immediate future safeguards use. We hope to solve on this way successfully the increasing needs for reliable and affordable electronic sealing systems for the IAEA.

REFERENCES

[1] Roger G. Johnston, Los Alamos National Laboratory, Task 230, Final Report, February 2000.

[2] Jean-Claude Martin, SAPHYMO, Presentation of the IRES Electronic Seal at the IAEA-Vienna, December 2000.

[3] Bundesministerium für Forschung und Technologie, Joint Programme on the Technical Development and Further Improvement of IAEA Safeguards, Task D.15, Development of the VACOSS-S sealing system, KFA Jülich GmbH, 1988.

[4] Roumen Tzolov, IAEA, User Requirements for the New Electronic Seal (Electro-Optical Sealing System), Vienna, 1998.

[5] BMWi/IAEA Joint Programme, Task E.27/E 994, Electro Optical Sealing System.

[6] French Support Programme, Task E 1229, IRES sealing system Development.

[7] D. Brochard, B. Autrusson, J.F. Moreau, J.C. Martin, The IRES Electronic Seal, IAEA Safeguards Symposium 2001, Poster session B, IAEA-SM-367/B/14/01/P.

[8] US SP Task USA E 1205, Evaluation of the Two-way Radio Frequency sealing system for IAEA routine use.

[9] J.C. Matter, R. Tzolov et al., The Two-way Radio-Frequency Seal (TRFS) and its Application for Joint Operator-IAEA Use, IAEA Safeguards Symposium 2001, Poster session A, IAEA-SM-367/A/7/01/P.