Containment and Surveillance – Status and Perspectives

Bernd Richter

1. Introduction

Containment and surveillance (C/S) measures can only provide indications for possible diversions of nuclear materials or misuse of nuclear facilities, and their rôle is considered complementary to nuclear materials accountancy. However, present generation nuclear facilities such as commercial reprocessing and mixed-oxide fuel fabrication plants, long term intermediate storage and conditioning facilities require highly automated and customized safeguards systems based on C/S techniques thus enhancing the rôle of C/S. This article begins by discussing the rôle of C/S on the basis of the nuclear treaties. Practical experience has led to a list of design and functional requirements for C/S techniques which are basically determined by the necessity for unattended use of the equipment. Then, examples for the application of C/S are given, followed by an outline of the evolution of C/S devices. Furthermore, there is a discussion of techniques which are in current use by the International Atomic Energy Agency (IAEA). Finally, the article discusses development projects of C/S techniques which are currently under way. The article basically draws upon literature which is listed at the end under References.

2. Legal Basis of Containment and Surveillance /1/

The Euratom Treaty of 1957 /2/ requires the European Commission to satisfy itself that, in the territories of the Member States, nuclear material is not diverted from its intended purposes as declared by the users. Euratom Safeguards are applied to all civil nuclear material in all Euratom Member States. Apart from the fact that the Treaty does not discriminate between nuclear weapons states and non-nuclear weapons states, nuclear material is the key objective suggesting inspections and accountancy as the measures of fundamental importance.

The Non-Proliferation Treaty (NPT) of 1968 /3/ requires (only) the non-nuclear weapons states to accept Agency Safeguards on all nuclear material in all peaceful nuclear activities with the view to preventing diversion to any nuclear explosive devices. According to Art. III para. 1 it is assumed that the peaceful activities may be carried out within the territory of a member state, under its jurisdiction, or under its control anywhere. Again, it is the nuclear material that is in the focus.

As the non-nuclear weapons states party to the Euratom Treaty are also member states of the NPT, the Euratom and Agency safeguards systems had to be coordinated in order to avoid unnecessary duplication of safeguards. The Commission, the Agency and the non-nuclear weapons states concluded the Verification Agreement (VA) known as INFCIRC/193 derived from INFCIRC/153. In the VA, C/S measures are mentioned several times. This will be discussed below in detail.

Finally, details of safeguards implementation in all Euratom member states are laid down in Euratom Regulation no. 302/2005. Art. 6, para. 2(e) of this regulation states that the Commission uses Particular Safeguards Provisions to establish, among others, C/S measures according to the arrangements agreed upon with the person or undertaking concerned. According to Art. 6, para. 1 also consultation with the relevant Member State is required.

It is interesting to note that on this basis the Commission is entitled to cooperate directly with the facility operators, whereas the Agency has to cooperate with the governments.

The VA assigns the following functions and relevance to C/S:

- Use shall be made, for example, of containment as a means of defining material balance areas for accounting purposes (VA, Art. 7(b)).
- C/S shall be used to concentrate measurement efforts at key measurement points (VA, Art. 46 (b)(ii)).
- C/S may be applied and used by the IAEA as part of its inspections (VA, Art. 74(d)).
- The IAEA may apply its seals and other identifying and tamper-indicating devices to containments (if so agreed and specified in the Subsidiary Arrangements) (VA, Art. 75 (e)).
- The IAEA may install its own surveillance equipment (if so agreed and specified in the Subsidiary Arrangements) (VA, Art. 75 (d)).
- The actual number, intensity, duration, timing, and mode of routine inspections, among others, are correlated to the criterion 'degree of containment [of nuclear material]' (VA, Art. 81 (c)).

From these provisions it can be interpreted that C/S are not assigned fundamental but rather auxiliary functions. Regarding the integrity of containments, C/S are intended to register anomalies in the absence of inspectors as opposed to diversions of nuclear material. Furthermore, well-applied C/S can provide continuity of knowledge of nuclear material flows and inventories and thus can make a facility more transparent and inspection activities in a facility more cost-effective and possibly less intrusive.

The rôle of C/S was legally spelt out at a time when the impacts of bulk handling facilities with large throughputs and of long term storage facilities with difficult-to-access or even inaccessible material were not really considered. Instead, safeguards focused on reactor facilities, fuel fabrication and enrichment plants where the material is still accessible for item verification, sampling, and measurements. Nowadays, a large part of the nuclear material is enclosed in heavily shielded process piping and emplaced in thick-walled casks which will be stored over long terms with no intent to be opened for periodical physical inventory taking.

The VA constitutes nuclear material accounting as a fundamentally important safeguards measure. Therefore, the IAEA used to aim at a quantitative statement on the detection probability of diversion. However, this is only possible for facilities where nuclear material inventories and flows are periodically measured to the end of determining the material-unaccounted-for. Consequently, no detection probability can be determined for facilities in which only qualitative or no measurements are made. Moreover, as the detection probability decreases with increasing nuclear material inventory and flow, also in large commercial processing facilities the significance of a detection probability must be questioned. Hence, the importance of C/S measures and inspection activities is enhanced.

Based on many years of practical experience, the IAEA in its Glossary tried to arrive at a comprehensive list of functions assigned to C/S /4/. The most important aspects are the monitoring of movement of nuclear material, interference with containment, tampering with (unattended) safeguards equipment and preservation of previously obtained measurement results, thereby reducing the need for re-measurement.

3. Safeguards Requirements

The safeguards inspectorates, developers from a number of countries as well as international advisory and working groups, such as the ESARDA Working Group on C/S, have extensively dealt with the requirements for C/S techniques. Due to the principally unattended use of C/S techniques, the functional requirements are very specific; however, depending on application they may also be facility-specific. In the following the principal criteria are discussed.

The device must be reliable in the sense that it functions without failure during the intended inspection period, e.g., during an inspector's absence of three months. The reliability criterion requires a specified environmental qualification. The recorded data must be authentic, i.e., falsified data must be recognizable. That is why authentication implies tamper-indicating functions. For timeliness reasons in situ verifiability is of great advantage. Inspection effort can be significantly reduced if remote interrogation and verification functions are realized. Regarding seals, this is also true for archival functions, because seal data are archived upon seal application and retrieved for comparison upon re-verification. In general, the ease of evaluation of results and their conclusiveness are important requirements. The ease of use is another factor, as the inspectors have to carry out many different types of activity including the handling of measurement systems, seals, and optical surveillance systems. In addition, ease of use may be relevant in cases where facility operators agree to take over safeguards activities in the absence of the inspector. Two more criteria have gained importance as microprocessor-controlled equipment is deployed: Recording capacity and integration capability. As inspection periods may be extended, the amount of data to be stored will increase, and different C/S devices are being integrated into C/S systems with new capabilities, such as the integration of video surveillance and electronic sealing or radiation monitoring.

Optical surveillance requires consideration of some additional criteria influenced by the recording capacity of the data carrier but ultimately by the inspector's reviewing effort. The application of external triggering, e.g., using scene change detection, restricts both recording and reviewing requirements to only those scenes which show possible movements of nuclear material. Practical experience shows that the reduction factor may be as large as 20 compared to constant time-interval triggered recording. Another method is to use data compression algorithms reducing the recording capacity needed per scene.

As the optical information has to be evaluated by the inspector automatic reviewing and data processing techniques can significantly reduce the inspector's evaluation time to reviewing those scenes which are of safeguards relevance. This requires, of course, that both the optical surveillance system and the automatic review station are designed and operated appropriately. It should be realized that an automatic technical review, i.e., evaluation regarding the system performance, became possible only after deployment of video techniques.

Furthermore, remote transmission and interrogation of safeguards data may also help to reduce inspection effort, especially in large countries where the nuclear material is located at many different places. The implications of remote transmission should also be investigated for highly industrialized small countries with good infrastructures. In this connection, encryption of video data will be important. Standardization and compatibility between devices as well as exploitation of the consumer market could increase the flexibility of integrated C/S system designs and reduce equipment costs when designing facility-specific C/S systems.

4. Application Examples

The following table I shows a list of safeguards relevant features for both operator activities and facility components with respect to most of the commercial stations of the nuclear fuel cycle. These safeguards relevant features do not represent a complete list but have to do with C/S measures, which are indicated in the very right column. However, the question of their application has to be answered on a case-by-case basis taking into account specific sets of criteria. These include above all the timeliness of detection and the assumed diversion strategies. More detailed information will be given in chapter 7 below.

Table I: Potential C/S Instrumentation for Different Facility Types and Activities

Facility Type / **Operator Activity/ Facility Component**	**LWR[1] reactor**	**CANDU[2] reactor**	**Pu fuelled reactor**	**MOX[3] fuel fabrication**	**enrich-ment plant**	**reprocess-ing plant**	**storage facility[4]**	**Potential C&S Instrument**
handling of fresh fuel containers	X	X	X					camera
fresh fuel in store	X	X	X	X				seal, camera
handling of fresh fuel	X	X	X	X				camera, bundle counter
reactor core	X	X	X					camera, seal
handling of spent fuel	X	X	X			X	X	camera, bundle counter
handling of spent fuel containers	X	X	X			X	X	camera
spent fuel in store	X	X	X			X		camera, seal, SCD[5]
shipping containers with spent fuel	X	X	X			X	X	camera, seal
handling of UF6 containers				X	X			seal
UF6 containers in store				X	X			seal
store for SNM[6] in bulk form				X	X	X	X	camera, SCD[5], seal
filling/emptying of SNM[6] containers	X	X	X	X	X	X		seal, camera
SNM[6] process containment						X		camera, SCD[5]
Pu cans				X		X	X	weld seam
fuel assemblies	X	X	X	X		X		seal
process sampling				X	X	X		seal, portal monitor

(1) Light Water Reactor.
(2) Canadian Deuterium Uranium Reactor.
(3) Mixed Plutonium Uranium Oxide.
(4) E.g., dry intermediate storage of spent fuel assemblies.
(5) Scene Change Detection.
(6) Special nuclear material, i.e., fissile nuclear material.

5. Evolution of Containment and Surveillance – The first four decades 1957-1997 /5/

The IAEA was established in 1957 as a functional organization, including the commencement of inspections at nuclear facilities in member states. The first inspections began in the early 1960s at small research reactors, and expanded in 1962 to power reactors. Although there was little C/S equipment available for use, it was in this time frame that the first use of C/S began. Several commercially available seals were placed in use, initially on a trial basis. In the fall of 1966, the IAEA was using the US Internal Revenue Service (IRS) seal. Brookhaven National Laboratory (BNL) in the US later developed solder techniques designed to strengthen the tamper resistance of these seals. When implemented for IAEA Safeguards on a routine basis, the IRS seal became known as the "Type E" seal. Even after 40 years, it is still in use. No optical surveillance or monitors were in use in the first decade of the IAEA.

Starting in the second decade after 1967, a variety of equipment was introduced. In the area of seals, the backbone became the aforementioned Type E metallic seal. Today, after several modifications, it remains the most widely used seal. Adhesive (paper) seals were introduced, principally for short term sealing applications. The first fibre optic seal, termed Fiber Lock, was developed and offered for evaluation by the US Arms Control and Disarmament Agency (ACDA). Also, the development of electronic seals began at Forschungszentrum Jülich in Germany, and Sandia National Laboratories (SNL) in the US.

By early 1976, the IAEA had about 60 optical surveillance systems in use, including several types of single frame 35mm, 16mm, 8mm, Super 8mm cameras, and a few custom made video units. This came about as a result of the rapidly expanding commercial market for industrial and home use of film-based movie photography. These systems included:

Film Systems – One of the first optical surveillance devices used was the 35mm Robot Camera, custom made for the IAEA by a German vendor. This system was mains powered and had an 8,000 frame capacity, with time recorded on each frame from a battery operated 24 hour clock. It produced excellent picture quality, and was evaluated in several nuclear facilities in Europe and South America.

Throughout this decade, numerous commercial film cameras were developed and appeared on the market. A number of these systems were evaluated by the IAEA, and to a limited degree, used in field applications. These systems included:

- Zeiss 35mm Contarex camera
- Flight Research 35mm camera
- Bolex 16mm camera
- 8mm Minolta D-4 camera (first 8mm system)
- Minolta D-6 camera
- Minolta D-10 camera
- KodakAnalyst Super 8mm camera
- Minolta XL-400 and XL-401 Super 8mm cameras

The first models of the Minolta XL-400 camera system used a French mechanical timer, were battery operated, with constant or random picture taking time-intervals, and had a 3,600 frame capacity. Later models had an electronic built-in timer, a 7,200 frame capacity, and used Kodak MFX film. By 1978, the Twin Minolta XL-401 camera system, after a number of timer modifications, became the primary IAEA optical surveillance system, and was in worldwide use for well over two decades, until it was replaced by video systems.

In some cases, inspectors had to develop the film in the bathtubs/sinks of their hotel rooms, producing a variety of inconveniences and results. The inspectors later used the Porto-PAC dry process Kodak developer for processing the film. Use of this developer eliminated the hotel room-bathtub-film developing routine.

Video Systems – As video emerged on the market, the IAEA was quick to realize the potential benefits that could be derived, most notably of which were vastly increased scene capacity, and, with an appropriate monitor, rapid scene review. On an Agency contract, Psychotronic Elektronische Geräte, an Austrian vendor, produced the first IAEA video system, the Psychotronic System. This system used a time lapse recorder operating in pulse mode. It was designed in the early years of video technology, and used a reel-to-reel recorder having a capacity of 180,000 frames. Ultimately, some 30 systems were purchased, many of which were placed in safeguards use. The maintenance level was quite high. In time, the system was modified to use tape cartridge recorders.

Review of Optical Surveillance Data – The purpose of optical surveillance is to record the events that occur during the inspector's absence. This results in the need to review the collected data. Even with the use of film cameras, this is recognized as a very laborious job. The review process was performed with rather basic equipment which could be set to run the film at a relatively slow speed, or, if the inspector chose, a particular frame could be stopped for more detailed viewing. While this was very useful, it was found that, with some review equipment, leaving the film stopped for a period of time resulted in burning the particular frame being examined. The Recordak Motormatic Reader was one of the systems used at IAEA Headquarters.

Monitors and Other Devices – In the second decade of the IAEA (1967-1976), the use of monitors and sensors was introduced, albeit not on a wide-scale basis. While it is debated whether such devices can be categorized C/S equipment, it is interesting to take notice of them. Some of these devices are briefly described below:

Reactor Thermal Power Monitor – This unit, developed in South Africa, was donated to the IAEA in 1969. The second power monitor, developed in Denmark, was installed in the Danish DR-2 reactor. Its first use was in the 1968-1969 time frame.

Reactor Electrical Power Monitor – This system was developed in the former Czechoslovakian Socialist Republic.

Track Etch Monitor – This unit was sponsored by the US-ACDA and developed by the General Electric firm. It provided a means of monitoring neutron flux level related to power level, and was used in a number of facilities.

Bundle Counter – This system, sponsored by the US-ACDA and developed by SNL, was designed for application in on-load fuelled power reactors. It provided a count of the number of irradiated bundles moved from reactor core to the storage pond and vice versa. It was installed in a Canadian Deuterium Uranium (CANDU) reactor in 1975 and operated for years without failure. A second bundle counter system, designed to perform a similar function as the one above, was developed in Canada, by Atomic Energy of Canada, Ltd. (AECL).

Glass Dosimeters – Radio Photo Luminescence (RPL) dosimeters of fluoro-glass were introduced as yes/no monitors to measure exposure to radiation. They were used to detect flow of irradiated material through unauthorized routes. They easily fit inside the Type E Seal, and were used in several facilities such as on-load fuelled power reactors.

In the third decade of the IAEA (1977-1986), there were many technology advances, and the level of C/S equipment activities increased. Equally important, a number of IAEA member states established R&D programmes in support of the IAEA, and several of these programmes had significant activities in the area of C/S. In this decade, as in the previous one, to many, C/S meant "cameras" and "seals". Considerable effort was devoted to the development of film camera systems with increased film capacity, video systems utilizing video cassettes and discs, electronic seals, and a variety of other C/S equipment. Some of these systems are listed below.

In Canada, AECL developed the first multiplexed video system for use in CANDU power reactors. This system used video discs as the storage medium. It was configured to store data from multiple cameras, eliminating the need for a storage device for each camera. The maintenance required for this system was found to be excessive, and it was ultimately replaced.

Also the IAEA developed a multiplexed video system. In addition, the IAEA pursued the development of the Laser Scanning System (LASSY) for use principally at spent fuel storage pools to detect objects being retrieved from the storage pool. LASSY was designed to scan a layer immediately above the water level.

Within the Commission of the European Communities (CEC), the Joint Research Centre at Ispra (JRC Ispra) developed an ultrasonic sealing system for Boiling Water Reactor (BWR) fuel assemblies. Concurrently, in the US, SNL developed the Fuel Assembly Identification Device (FAID)/Seal Pattern Reader (SPAR) ultrasonic sealing system, also for BWR fuel assemblies. These two systems were simultaneously tested at the Kahl experimental power reactor in Germany, with successful results. The EURATOM Safeguards Office developed a dual recorder video system.

In Germany, several types of systems were developed. Forschungszentrum Karlsruhe developed an 8mm film camera system using the ELMO camera, which had a film capacity of twice the one of the Minolta System. The Inaccessible Inventory Instrumentation System (IIIS) was developed which was an integrated C/S system designed for monitoring the handling of the fuel at the Kalkar sodium-cooled fast breeder reactor. This system and the SNL Integrated Monitoring System mentioned below, were among the first integrated C/S systems. Forschungszentrum Jülich developed the Variable Coding Sealing System (VACOSS), an electronic seal which was implemented by the IAEA and EURATOM after 1990. This seal provided the capability of in situ verification, recording of multiple opening and closing, and a high level of tamper indication. The IAEA started to take it out of service in 2006.

In Hungary, underwater optical instruments were developed to enable underwater reading of nuclear fuel assembly serial numbers. Similar efforts were conducted in the US.

In Japan, the Japan Atomic Energy Research Institute (JAERI) developed a large capacity 8mm film camera system, a semi-automatic verifier for the Cobra Seal System, and a portal and penetration monitoring system for the Fast Critical Assembly (FCA) Facility. The Power Reactor and Nuclear Fuel Development Corporation (PNC) developed a spent fuel monitoring system for use at the Tokai Reprocessing Facility. In addition, the Nuclear Material Control Center (NMCC) and others developed an electronic seal and a remote monitoring system.

In the US, ACDA developed the RECOVER System, designed to remotely, via commercial telephone lines, monitor the operational status of C/S devices. This system was extensively tested, on a worldwide scale, and served to demonstrate the basic feasibility of remote monitoring. Concurrent with the RECOVER activities, in Germany, Forschungszentrum Jülich developed and tested the LOVER (Local Verification) System intended for use within facilities in the same local area. Following the tests of the RECOVER and LOVER systems, in Japan, JAERI continued development of remote monitoring equipment. Los Alamos National Laboratory (LANL) developed the Reactor Power Monitor which was implemented in several facilities. SNL developed the Surveillance Television And Recording (STAR) System, the MINISTAR System, the Passive Environmental Monitor (PASEM), and the

Cobra Seal System (fibre optic). Also, the Integrated Monitoring System was developed, which combined radiation detectors, crane monitors, and a data collection module, and provided a trigger for optical surveillance devices.

In a cooperative effort between AECL and SNL, the AECL Random Coil (ARC) Seal/SNL SPAR System was developed, tested, and approved for routine safeguards use. This ultrasonic seal system is used to seal spent fuel storage racks in CANDU on-load fuelled reactors.

In a cooperative effort between JRC Ispra and SNL, development of the MOX Fuel Assembly Ultrasonic Seal System was commenced. This project was an extension of the earlier mentioned JRC Ispra/SNL ultrasonic seal systems for BWR fuel assemblies.

The first attempt at easing the film review process came in about 1981, with the development of a film scanner. This equipment, developed by SNL, was based on early scene change detection technology. The film was projected, and with a change of the scene, the scene was transferred to a video disc. This technique proved to be useful when there was hardly any operational activity the area under surveillance. In the cases where there was activity, many scenes were stored – in fact, so many, that frequently the disc was filled to capacity, stopping the review process.

In the late 1980s, it became evident that the film camera technology would be replaced by video technology, and that steps were necessary to insure that, when that time came, the IAEA would be prepared to replace some 200 Twin Minolta Film Camera Systems that were deployed. Both Japan and the US addressed this problem – JAERI with the Compact Surveillance Monitoring System (COSMOS), and SNL with the Modular Integrated Video System (MIVS) which was placed in routine safeguards use in early 1991.

The age of video surveillance was bringing with it a tremendous increase in the amount of recorded data. While the increased amount of surveillance was very desirable from the standpoint of determining what has occurred in the inspector's absence, it also brought along a burden to inspectors who had to review all the data. A drawback, however, was the loss of colour as compared to film cameras. In recognition of the large amount of data that resulted from the transition from (colour) film camera to (black and white) video systems, EURATOM and the US commenced development of video review systems: at JRC/Ispra, the Polyline System; at SNL, the MIVS Image Processing System (MIPS); and at a commercial firm in the US, Aquila Technologies Group (ATG), the Mk V Review Station. In the early 1990s, the Multi-system Optical Review Station MORE was developed under the German Support Programme by Dr. Neumann Consultants (DNC). MORE was designed to select images with scene changes and, thus, increased the efficiency of the inspector's image review process. This semi-automated optical surveillance review process of "back end data reduction" was implemented for routine use by IAEA and EURATOM, and has proven to be extremely effective.

In another approach to review aids, the European Commission, France, and Germany pursued development of video "front end" processing of surveillance data, i.e., scene change detection at the camera level. This and other optical surveillance developments are described below:

- In Canada,the AECL Improved Multiplex System using time lapse video recorders.
- At EURATOM, a video system coupled with video motion detection circuitry, and a fully digital video system (EMOS) with multiple storage modes.
- At JRC Ispra and EURATOM,the Computer Aided Video Surveillance System (CAVIS).
- In France,at CEA, digital video systems.
- In Germany,at DNC, the Multi-Camera Optical Surveillance System (MOS).
- In the US,the SNL Portable Surveillance Unit (PSU).

Other significant C/S development activities included:

- In Australia,a remote monitoring system capable of transmitting video data over commercial telephone networks.
- At JRC Ispra, a semi-automatic verification system for Type E seals, and an improved Laser Scanning System (LASSY).
- In France, the CEA Spent Fuel Transfer Monitoring System (CONSULHA), and the CLTO Fibre Optic Seal System.
- In Germany, at Dornier company an improved VACOSS Seal, and at DNC a Tamper Resistant Video Link.
- In Japan, an improved JAERI FCA Portal/Penetration Monitoring System, the PNC Plutonium Fuel Production Facility (PFPF) Advanced C/S System, the PNC video systems at the Tokai Reprocessing Plant, and the Fuel Number Reader activities at Japan Nuclear Fuel Services, Hitachi, and Toshiba.
- In the US, the SNL Modified Cobra Seal System, video and data link authentication systems, the Authenticated Item Monitoring System (AIMS), the Item Identification System, the Re-usable In-situ Verifiable Authenticated (RIVA) Seal System, Valve Monitors, a Secure Container for Glove Boxes, and Sample Vial Containment. In addition, ATG manufactured a lightweight version of the Modified Cobra Seal.
- In a cooperative effort between AECL, LANL, and the IAEA, a Core Discharge Monitoring System for use in CANDU stations.
- In a cooperative effort between EURATOM, British Nuclear Fuels Ltd. (BNFL), LANL and SNL, the Thermal Oxide Reprocessing Plant (THORP) Skip Monitoring System, integrating radiation detectors and video surveillance.
- In a cooperative effort between Canada, JRC Ispra, and the US, the In situ Readable Ultrasonic Seal System (IRUSS) for ARC, VAK, and other ultrasonic seals.
- In a cooperative effort between France and EURATOM, a small general purpose ultrasonic seal/transducer combination system (TITUS), and associated equipment for remote transmission of the TITUS data.
- In a cooperative effort between JRC Ispra and BNFL, the Advanced Sealing and Item Identification Multi Element Bottle (MEB) Bolt Seals, ultrasonic seals for spent fuel casks. In the early stages of this effort, a similar cooperative effort between BNFL and SNL was conducted.
- In a cooperative effort between Forschungszentrum Jülich, Dornier company and SNL, the VACOSS/MIVS Interface System.

6. Introduction of Digital Systems /6/

For more than 25 years the nuclear safeguards system had been based on states' declarations and IAEA's ([7]) verification /7/. The world community, in response to the violation of the Treaty on the Non-proliferation of Nuclear Weapons (NPT), strengthened the safeguards system, i.e., NPT compliance verification system, by establishing the Additional Protocol (AP) /8/. Under the AP, the IAEA's mission is not only to verify the correctness and completeness of states' declarations but also to detect undeclared nuclear facilities, materials and activities,. While continuing to use material accountancy to detect diversion of nuclear material, the IAEA has to execute extended access rights within the nuclear facilities as well as on the states' territories. Furthermore, the IAEA has to handle more comprehensive information to be provided by the states as well as information acquired by the IAEA from

([7]) IAEA = International Atomic Energy Agency, Vienna, Austria.

open sources about states' nuclear activities. To this end, the IAEA has acquired new competence in open source information analysis including satellite imagery analysis and is re-engineering its safeguards information system. In Eastern Europe and Asia new states have come under safeguards, and nuclear programmes in Asia and elsewhere are being expanded. Finally, in the course of nuclear disarmament in nuclear weapons states the IAEA will have to safeguard excess fissile materials transferred from former military use.

In order to cope with these challenges, the IAEA, in cooperation with member states, is developing approaches to increase its efficiency and effectiveness in using its resources. The IAEA will focus more on qualitative safeguards measures concerning the nuclear fuel cycle in a state as a whole and on key activities like enrichment and reprocessing. Inspection effort related to routine activities at declared nuclear sites that are less sensitive will be reduced enabling the IAEA to re-allocate its staff. In 1992, the ESARDA ([8]) Working Group on Containment & Surveillance had proposed the concept of substituting on-site inspection effort by unattended and remote monitoring techniques with data evaluation at IAEA headquarters, as this may not only improve the cost effectiveness of routine safeguards but also reduce the interference with plant operations. In addition, nuclear radiation exposure of IAEA inspectors and technicians as well as of plant operators' staff will be reduced. Also, the European Commission, especially in designing new safeguards approaches in a regional union of, now, 27 member states, has started to consider this concept. Another aspect of unattended and remote monitoring is improving the data collection and analysis by acquiring safeguards data in a timely manner at random or programmable time intervals. Given the ever increasing amount of safeguards data it is also important to develop appropriate data review methods.

The whole concept requires the use of state-of-the-art technologies. In autumn 2004, after in-depth discussions, the two ESARDA Working Groups on C/S and on Techniques and Standards for Non Destructive Analysis (NDA) issued guidelines for developing unattended and remote monitoring and measurement systems /9/. In this context, the ESARDA Working Group on C/S has also started to revisit the issue of how to determine the performance and assurance of containment & surveillance equipment, an issue which the working group already addressed in the late 1980's.

This chapter highlights trends in the area of image surveillance, radiation monitoring, and electronic sealing. The example techniques presented will meet the requirement of system integration into sensor networks which will become more and more important in nuclear safeguards. Also, it should not be overseen that, in the future, some activities up till now carried out by the safeguards inspectors may be carried out by the nuclear facility operators provided the performance and assurance of the safeguards equipment will find the operators' acceptance.

The large variety of nuclear facilities to be safeguarded requires a great flexibility on the part of the IAEA in designing facility-specific safeguards instrumentation. The use of digital techniques (hardware, firmware, software) and modular hardware and software solutions for automated on-site instrumentation enables to design equipment systems integrating different sensor techniques such as cameras, radiation monitors, and seals. It has to be taken into account though, that electronic components have short times to obsoleteness requiring short-term replacement. Examples for rapidly changing technologies are microprocessors and data carriers. Also, technical progress leads to new concepts and requires periodical replacement of safeguards equipment.

For cost reasons (procurement, training, repair and servicing) it is desirable to use commercial-off-the-shelf (COTS) components to the greatest extent possible. However, it is necessary and expensive to adapt COTS components to nuclear safeguards applications. From the IAEA's point of view the critical component of a safeguards system is the sensor head with digital data generator module. Here,

([8]) ESARDA = European Safeguards Research & Development Association.

loss-free data acquisition and local storage as well as a high data security including authentication are required. Normally, this is realised with customised solutions for hardware and firmware, which, by nature, are expensive, as the nuclear safeguards market is very small, and these requirements are not requested in other verification systems. Therefore, IAEA member states support the IAEA in developing customised equipment, in order to keep the IAEA's procurement costs free from the development costs.

In a remote monitoring scheme the IAEA must be able to evaluate the safeguards data at IAEA headquarters. For the reason of safeguards confidentiality only encrypted safeguards data will be transmitted. The implementation of remote monitoring systems requires cost-benefit analyses on a case-by-case basis. Costs depend on country-specific factors such as the number of facilities involved, availability and quality of a communication infrastructure, and communication tariff, and on other factors such as licensing of encryption algorithms and archiving requirements.

For software upgrading and trouble shooting, the IAEA may wish to have remote system access to its remote monitoring systems. This will only be granted under the provision that the plant operator's security concerns can be sufficiently met, as there is always a non-negligible security risk of unauthorised access. Furthermore, the plant operator may be concerned about the unaltered status of the data transmission scheme, if, for instance, delayed transmission of surveillance data has been implemented.

The amount of data to be handled must be kept as low as possible, i.e., only relevant data should be transmitted, archived and evaluated. Otherwise, transmission times may become unacceptably long, archiving capacities extremely large, and data management and evaluation very laborious, when considering a whole country. For example, the remote transmission of optical surveillance data involves large data files. Applicable data reduction methods are: (1) mathematical compression to reduce the file size; and (2) front end scene change detection to transmit only relevant images. To further reduce the amount of transmitted data, it is possible to correlate different types of data, e.g., images are relevant only if radiation is detected.

The remote retrieval of state-of-health data allows to monitor the performance of the safeguards systems and to initiate timely repair and maintenance. While highly reliable sensor head/data module units with uninterrupted power and loss-free data storage provide the assurance of continuity of knowledge, temporary outages of COTS components can be tolerated.

In some types of facilities inspection effort can be reduced by the facility operator performing safeguards relevant activities. For instance, transport and storage casks with spent fuel are sealed under camera surveillance using electronic seals with seal-video interfacing approved for safeguards use.

6.1 Digital Safeguards Instrumentation

Unattended integrated remote monitoring and measurement systems will play a major rôle. They consist of sensor heads, associated electronics, digital data generators, a data collection system, and network interfacing equipment for remote data retrieval. The majority of such systems is computer-based, as compared to customized solutions.

Sensors with their signal processing electronics as well as digital data generators are security relevant components, as they are the sources of the safeguards data. Any unauthorised physical access must be inhibited. Data authentication takes place in the data generator. Ideally, the components are mounted in a common tamper-indicating enclosure (TIE). Servicing, repair and replacement must be restricted to the IAEA's staff.

This concept is realised in two equipment categories used by the IAEA: (1) Digital image surveillance and (2) electronic sealing. The IAEA's standard digital camera unit has a low power OEM ([9]) CCD ([10]) camera and the digital data module DCM 14 mounted in the sealable IAEA standard camera housing. Also, the VACOSS electronic seal has many features of the concept.

In contrast, for radiation sensors development efforts have to be directed towards authentication of NDA data and tamper protection. The development of the digital unattended multi channel analyser DIUM is a first step in this direction (see below). It is worth mentioning that radiation detectors usually need to be physically separated from their data generators. In this case, the principle of tamper-indication must be separately maintained for (1) the sensor, (2) the signal line, and (3) the data generator module.

Within a nuclear facility the data collection system receives data from the sensors used. It stores the data until retrieved on site by an inspector or remotely transmitted to IAEA headquarters.

For on-site retrieval the data must be available on an exchangeable storage medium. Contemporary standards are digital linear tape (DLT), magneto-optical (MO) disk, recordable compact disc (CD-R), and DVD. In addition to the exchangeable storage medium, data collection systems may have other internal storage devices.

If a data collection system is interfaced to a public communication network, the data can be directly transmitted over the network to IAEA's headquarters. In this case, the confidentiality of the data must be guaranteed at all times by means of an appropriate encryption scheme. If the data are retrieved on site, confidentiality is the responsibility of the IAEA staff all the way from the facility to the headquarters. The inspector may want to transport encrypted data only, in order to ensure confidentiality in case of loss of the data carrier.

The reliability of the data collection system can be ensured by a range of measures including one or more of the following: Uninterruptable power supply, sufficient local storage to store the data from the different sensors over a longer period of time, redundancy of the system's vital components, auto-monitoring of different state-of-health parameters, transmission of state-of-health alarms. Networked data collection systems must offer a sufficient level of security against unauthorised access.

Network interfacing equipment is used to interface the data collection system to a public communication network, with the aim to transmit the collected data and, if agreed, to give the IAEA remote access to the system. The following aspects are important: Confidentiality of the transmitted data; prevention of unauthorised access to the safeguards system and safeguards data; IAEA's secure remote access to the data collection system.

Due to the concept of loss-free data acquisition and storage in sensor head/data generator modules, other components such as data buses, communication links, microcomputers, and data collection system are not security relevant and, therefore, may be COTS products. Failures and mains power outages do not result in a loss of data. As only authenticated data are processed in these components, tampering is not possible undetected. The components can be serviced, repaired and replaced by commercial contractors. This will further reduce the IAEA's interference with plant operation.

([9]) Original equipment manufacturer.
([10]) Charge-coupled device.

Prior to authorising equipment for routine inspection use the IAEA requires the systems to successfully pass different evaluations:

- Qualification testing including radiation testing ([11]);
- Third Party vulnerability analysis of the hardware and firmware as regards safety and security including data authentication and encryption methods ([12]);
- acceptance testing including usability review;and
- field testing.

Unattended and remote monitoring techniques for safeguards should have the following features:

- Data authentication at the sensor level
- front end data reduction including data compression and data correlation
- sufficient data storage capacity at the sensor level
- data encryption
- remote data transmission out offacilities to IAEA headquarters
- compatibility between devices ofdifferent origins
- integrated data review
- option for plant operator's performance ofsafeguards activities.

A widely accepted compliance with these features may help to reduce procurement costs and training effort for inspectors and technicians, solve data security issues, and match development efforts spent under different member states programmes in support of the IAEA.

When handling and operating unattended integrated remote monitoring and measurement systems the IAEA should:

- Perform strong configuration controls for data security,
- perform system access controls,
- use approved encryption algorithms,
- apply standardised vulnerability assessments,
- apply vulnerability assessment to entire system,not just to the security algorithm,
- use certified copies ofcommercial-off-the-shelf software,
- provide implementation guidelines for TCP/IP connectivity ofEthernet standard, and
- apply appropriate procedures for key management related to authentication and encryption.

([11]) The IAEA applies the IAEA/Euratom "Common Qualification Test Criteria for New Safeguards Equipment", Version 2.0, January 2002. For environmental testing the IAEA co-operates with the Joint Research Centre at Ispra under the Euratom Support Programme to the IAEA. For radiation testing the IAEA co-operates with the Atominstitut in Vienna. The procedure for irradiation testing is currently being revised under the German Programme in Support of the IAEA.

([12]) The DCM 14 digital camera module was evaluated by an Australian Expert Team in the frame of a joint Australian-German Support Programmes task.

6.2 Technical Approaches

Three examples are given for existing or upcoming digital systems complying with the requirements of unattended operation, remote data transmission, and system integration. The given examples cover the major monitoring principles, i.e., image surveillance, radiation monitoring, and electronic sealing. The equipment is designed for integration into systems with new functionality, including the correlation of image data with radiation data and electronic sealing. For example, an image or sequence of images will only be registered, if a certain radiation level or radiation characteristics is present, or if an electronic seal is attached to or detached from a spent fuel cask.

Optical Surveillance System

Optical surveillance systems are designed to run in unattended mode. Their advantage is that they do not interfere with plant operations when registering safeguards relevant image information on operator's activities. The safeguards inspector matches this information with the operator's declarations, without the need for his physical presence. The IAEA uses optical surveillance in the following safeguards applications, worldwide:

- Single-camera surveillance at locations that are easily accessible for inspectors,
- single-camera surveillance at locations that are difficult to access including underwater applications,
- multi-camera surveillance for all location types,and
- hort-term and portable surveillance.

The IAEA's current systems are based on the DCM 14 digital camera module and the associated family of single- and multi-camera surveillance systems which were developed between 1993 and 2001 and authorised for inspection use between 1999 and 2002. The IAEA generally requires an equipment lifecycle of up to 10 years. In 2008, the design and most of the technology will be between 10 and 15 years old. Assuming a minimum period of 4-5 years to be necessary to design, develop, evaluate, test, and approve (for inspection use) custom-designed safeguards equipment, the IAEA, adhering to the concept of a digital camera module as the core component, has recently initiated the development of a "next generation surveillance system". This will be addressed in a separate section.

The DCM 14 (see Figure 1) provides the following functions and capabilities: Image acquisition, analogue-to-digital conversion, data compression, data authentication, data encryption, internal and external triggering, maintenance capabilities, power management, battery backup, and local data storage on PC-card. The module including camera can operate on battery power for 10 days at a 10-minutes picture taking interval (or 1 day at a 1-minute interval). In addition to various single-camera configurations there is also the DCM 14-based Digital Multi-camera Optical Surveillance (DMOS) System.

The collected data can be reviewed locally at nuclear facilities and/or at IAEA field offices and headquarters. Furthermore, the system is designed for remote data transmission out of facilities with the transmitted data remotely to be reviewed when received at IAEA field offices and headquarters.

The DMOS system permits the connection of up to 32 cameras. Each camera and DCM 14 is mounted in a tamper indicating enclosure (TIE), i.e., the sealable blue IAEA standard camera housing. The control and recording unit is installed in a 19-inch cabinet. The camera units are connected via RS-485 cables to a custom-designed interface providing the camera data via RS-232 cable to the computer.

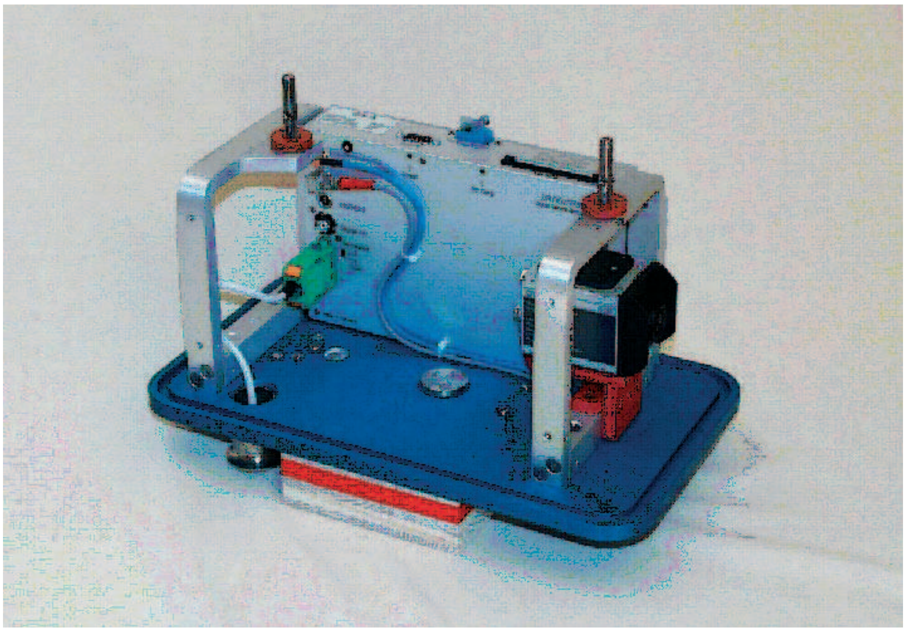

Figure 1: Base plate of IAEA camera housing with DCM 14 module and CCD camera (courtesy: Dr. Neumann Consultants)

The DMOS system uses compact low power CCD cameras (OEM products) with auto iris lenses. For facilities with 50 Hz and 60 Hz mains power supply two video standards, CCIR and EIA, are available. The following COTS-components were initially implemented: (1) hardware: industrial PC with TFT ([13]) display and membrane keyboard, SCSI ([14]) array, and digital linear tape drive; (2) operating system: Windows NT 4.0 Server. The DMOS system allows remote image transmission with the option of delayed image retrieval ([15]). Status data are associated with each image file, such as the status of the housing switch of the camera and the temperature in the camera housing. These data should be retrievable at any time without delay, as they can help to monitor and enhance the performance of the unattended system by triggering servicing.

Field experience has resulted in new design requirements (see below) and the requirement of mitigating the general hardware and software (operating systems) obsolescence problem. To facilitate a future replacement programme, the IAEA wants the next generation digital camera module to be compatible with the existing DCM 14-based surveillance technology.

Unattended Radiation Monitoring

Unattended radiation monitoring systems developed for the IAEA have so far not been standardised. The objective of the digital unattended multi-channel analyser (DIUM) project is to use as many standardised components as possible. These components are the system enclosure rack with an uninterruptible power supply, external cabling to radiation detectors, and eventually detector assemblies and enclosures.

The DIUM (see Figure 2) will use high frequency sampling and patented digital signal processing. Furthermore, it will be designed for unattended operation in nuclear facilities with the data collected to be retrieved and reviewed locally, in IAEA field offices and/or at IAEA headquarters, or with the data transmitted remotely and reviewed when received there.

([13]) Thin Film Transistor.
([14]) Small Computer System Interface.
([15]) Delayed data retrieval means that each data file is released only after a preset time interval.

Figure 2: Digital Unattended Multi-channel Analyser prototype (courtesy: ICx Radiation GmbH)

The functionality of the DIUM will be comparable with the DCM 14 camera module: local data storage, uninterruptable power supply, data compression, time stamping, authentication, encryption, remote data transmission, trigger capabilities. The data storage capacity will cover 5 days, if mains power or the data collection computer will not be available. In addition, it will provide high voltage to the detector and power to the preamplifier.

The DIUM will be capable of operating with different types of detector heads, e.g., sodium iodide, germanium, and cadmium-zinc-telluride, and it will be designed for installation and integration with other data acquisition modules, such as the DCM 14 digital image surveillance technology, and other digital signal sources. To capture fast processes, e.g., in bulk handling facilities and storage facilities, the measurement time may be short. Therefore, the DIUM will have a high data acquisition rate.

Although universal multi-channel analysers are being widely used in attended and unattended modes, there is no product commercially available, which would perform this task satisfactorily. While capturing fast processes in real time, the instrument is very much comparable to a surveillance camera system taking a picture every second. The difference to optical systems lies in the character of the data. The DIUM is storing radiation spectra and counting rates rather than pictures. In contrast to a digital camera unit, the radiation sensor may be separated from its data acquisition module.

Measurement times are in the range of 100ms to a few minutes. The measurements are similar to those performed in radioactive decay studies after neutron activation with the unattended data acquisition constantly going on and, thus, producing an enormous amount of data. The DIUM system is able to handle very high input counting rates from the radiation detector. This feature will minimise the effect of being overloaded and thereby blinded for important data. A high throughput is desirable, in order to minimise the statistical error for the data analysis.

It is very important to have no dead time periods between two consecutively measured spectra. A continuous stream of spectra with no missing code is stored on a flash memory disk.

The DIUM has an extra large memory to store many short time spectra on the board level. A safeguards-specific feature is embedded authentication and encryption of spectrum data. Together with an accurate time stamping, the authentication record added to each individual spectrum ensures that the data are not tampered with. In addition to the spectrometric input for detectors, trigger inputs and outputs are required for synchronisation purposes and electronic seals. Among the various radiation detectors that may be connected, there are also plastic scintillators and GM-tubes for gamma counting.

The main task of an unattended multi-channel analyser is to acquire repeatedly spectra from the same location, i.e., to detect changes in the radiation field. The interesting information is the difference between consecutive measurements rather than the analysis of a single measurement itself. If not explicitly stopped, the unattended multi-channel analyser will continue to collect spectra and deliver them to a remote computer. Loss-free data acquisition is ensured by storing all data locally in the data module on a removable storage medium. When the local data storage device is full, the oldest data are overwritten. This procedure works rather like a ring buffer, until the storage medium is removed for evaluation and replaced in the data acquisition module.

Local data storage capacity has been designed for up to five days operation until a potential problem may be fixed. When taking a spectrum every second, nearly 500,000 spectra must be stored without loss. Even with the ever-growing capacities of memory cards data compression is mandatory.

Together with the spectrum data a state-of-health record is stored. It contains information like ambient temperatures, detector high voltage and bias current, and preamplifier power. Tampering with the detector and detector failures will cause a change in one or more of such parameters.

The temperature is recorded as one parameter of physical stress. Another stress factor in nuclear facilities is often an elevated level of neutron radiation. Ongoing electronic circuit miniaturisation causes an increased sensitivity to neutrons inducing malfunctions and system crashes. The problem is moderated by using selected memory chips which are not prone to such neutron-induced effects. A software technique using checksums and error correction with watchdog functions ensures safe operation in the standard instrument cabinet.

For reasons of data integrity and authenticity an authentication method similar to the one implemented in the DCM 14 camera module will be used to authenticate individual spectra. The DIUM signal sampling, while taking a spectrum, also acquires true statistical noise in the form of random zeroes and ones as a natural base for all encryption algorithms and hash function. When using the natural noise generator for the encryption all publicly known attacks to falsify the authentication are doomed to fail. The authentication method will be subject to a Third Party Vulnerability Assessment. For remote data retrieval also encryption will be required and approved by the state.

Electronic Sealing System

The IAEA started to use electronic sealing on a routine basis in the early 1990's. The sealing method is based on the measurement of light transmitted through a fibre optical cable that is connected to a secure box with electronic circuitry. While the concept has proven highly successful, the seal technology is not state of the art. The IAEA defined the following requirements for a future electronic safeguards seal:

- High detection probability ofbypassing or short-circuiting of the sealing function;
- tamper-indicating housing which, however, can be opened non-destructively for maintenance, upgrade and/or repair;
- up to 3 years operation on battery, while battery replacement information should be highly reliable;

- high-capacity event-log with support for back-end authentication verification;
- secure communication protocol based on a standardised cryptosystem and state-of-the-art cryptography;
- support for network applications, i.e., network of seals as well as seals in a network of different device types including computers, digital cameras, radiation monitors;
- radiation tolerance through software means such as strict watchdog regime and majority vote variables.

A new seal is the electronic optical sealing system EOSS (see Figure 3) which started to be implemented for inspection use in 2006. The sealing function is realised by using a fibre-optic cable (FOC). The sealing security is based on the fact that fibre-optic cables are generally more difficult to tap or bypass and to repair than electrical wires.

Figure 3: Electronic Optical Sealing System prototype
(courtesy: Dr. Neumann Consultants)

The seal has a light source and a light sensor with the light being transmitted through an external FOC. The FOC is designed for multiple connection and disconnection. It can be manually "opened", i.e., disconnected, and "closed", i.e., connected, without using any tool. Every opening and closing is registered by the internal micro-controller with annotation of date and time. The open/closed status of the FOC is monitored by transmitting and receiving short light pulses at certain time intervals. If the FOC is closed, every light pulse is immediately detected by the receiver. If no signal is detected, then the FOC is considered to have been opened. Moreover, the seal checks for the tamper-indicating event of light being received with the optical transmitter being switched off.

EOSS uses a single-mode cable that has to be operated with laser light. In contrast, the multi-mode technology uses considerably larger core diameters as well as normal light, typically from light emitting diodes. The higher requirements regarding precision, make single-mode systems more difficult to tamper with.

The EOSS housing consists of two compartments. Whereas the inner part contains all security-sensitive components, the outer part houses the batteries as well as the electrical and fibre-optical connectors, in order to facilitate repair.

The battery pack consists of two lithium AA-cells for redundancy and dedicated electronics for monitoring the battery lifetime. The lithium technology provides a high energy capacity as well as a wide temperature range from –20 to +85°C. A single battery will power the seal for more than years.

At very low temperatures, certain memory cells tend to keep their information for a long time even without power supply. Theoretically, this would allow to retrieve the authentication keys by deep freezing the seal and short-cutting the battery. Therefore, the temperature is monitored and, at very low values, the keys are erased.

The EOSS registers different categories of events. The Seal Log contains openings and closings of the fibre-optic cable. The User Log contains activities like user log on/off and key-set generation. Moreover, the User Log registers potential or real tamper attacks (e.g., denied requests from the network). The third part of the log contains State-of-Health information (e.g., battery usage, min. and max. temperature).

Data authentication implemented in the seal uses the Triple Data Encryption Standard (TDES).

The EOSS seal has a RS-485 interface. The hardware allows cable lengths of up to 1,000 m. Up to 32 seals can be connected to one twisted pair cable (party-line). The seal reader is a standard notebook or personal computer. A compact size RS-485/RS-232 converter is available to connect the party-line to the PC's serial port.

In the future, it will be desirable to have available an appropriate generic review capability for integrated safeguards systems. Development efforts are going on at LANL and, in connection with the next generation surveillance system, at Canberra Albuquerque, Inc.

7. Currently Used Containment and Surveillance Techniques /10/

Containment and surveillance techniques are extensively used by the IAEA, because they are flexible and cost effective. The two main C/S categories are optical surveillance and sealing systems.

Optical surveillance is most effective in storage areas, such as spent fuel storage ponds, with relatively few plant operator's activities that could be interpreted as the removal of nuclear material. A typical application would consist of two or more cameras positioned to completely cover the storage area. The field of view of the cameras is such that any movement of items that could be the removal of nuclear material is easily identified. This means that items have to be sufficiently large within the field of view to be identified and that, preferably, at least two images have to be recorded during the movement of material. The image recording may be set at a periodic frequency (to be significantly shorter than the fastest possible removal time) or the motion (i.e. scene change) may trigger the recording. Optical surveillance is intrinsically an unattended operation that may be enhanced by the remote transmission of image data or system operation data (i.e. the operational status of the surveillance system).

Seals are typically applied to individual items containing nuclear material. A seal can help to indicate that material was neither introduced into or removed from a container. At the same time, sealing provides a unique identity for the sealed container. Unattended IAEA monitoring equipment is also sealed. Most IAEA seals are applied for extended periods of time, typically several months to years. Seals may be single use seals that have to be replaced when the sealed item has to be opened. Other types of seals are verifiable in situ, i.e. they can be checked for integrity and identity in the field without removal. If the seals are verifiable in situ, then the verification activity must be efficient (to limit radiation exposure to the inspector) and extremely reliable. The in situ verification activity must consist of checking the item containment, the seal integrity, and the method of the seal's attachment to the item.

Containment is a very complex issue which still lacks sufficient attention. While some solutions are available, it has only been a few years ago that containment verification began to be addressed more in depth.

7.1 Surveillance

Surveillance includes both human and instrument observation. As it is prohibitively expensive to arrange for permanent inspector presence, the IAEA has acquired a range of optical surveillance systems that can provide effective, ongoing surveillance when an inspector is not physically present on site. Unattended optical surveillance techniques are used widely by the IAEA to support and complement nuclear material accountancy and to provide continuity of knowledge about nuclear materials and other items of safeguards significance between on-site inspection visits.

Effective surveillance is achieved when a camera's field of view covers the entire area of safeguards interest to capture the movement of safeguarded items. Additionally, the picture taking interval is set to record at least two images, should the item be moved, so that its direction of movement can be determined. The image recording frequency may be set at a fixed time interval, which is significantly shorter that the fastest removal time, or may be triggered by scene change detection or other external triggers, such as radiation monitoring or electronic sealing.

Optical surveillance is intrinsically an unattended technique that can be used to record images only, or it may be integrated with other unattended monitoring equipment to provide nuclear measurement, containment history and other data. The IAEA's surveillance systems can also automatically transfer data to IAEA Headquarters or to an IAEA regional office.

Surveillance equipment is designed for the following basic applications:

(a) Single camera systems for easy to access locations,

(b) Single camera system for difficult to access locations,

(c) Multi-camera systems for larger and more complex facilities,

(d) Short term surveillance system for activities that include open core monitoring,

(e) Surveillance systems for remote monitoring,

(f) Underwater closed circuit TV system for attended applications in fuel storage ponds.

IAEA surveillance equipment has evolved from film cameras, through systems based on videotape technology, to today's digital image surveillance (DIS) systems. The evolution of IAEA surveillance equipment has been mandated mostly by strong commercial trends that dictate the availability of applicable technologies on the market. With a significant reduction in the number of moving parts, DIS is inherently more reliable than previous film and videotape technologies. Other benefits include enhanced digital data evaluation, assisted review capabilities, improved authentication and encryption and its facilitation of remote monitoring.

In 1995, the IAEA embarked upon a replacement programme to phase out old and obsolete surveillance equipment. In 1998, the Department of Safeguards decided that surveillance systems based on the custom designed DCM 14 digital camera module (Figure 4) met the essential user requirements for the IAEA surveillance systems and that they were the most suitable equipment for the replacement of the existing film and videotape based systems. While very compact, the DCM 14 performs many tasks required for a safeguards surveillance system, including:

(1) Digitization of a standard video camera image;

(2) Image and data authentication, ensuring genuineness;

(3) Image and data encryption, ensuring confidentiality;

(4) Image compression to reduce image and data storage requirements;

(5) Local storage to ensure redundancy when data are transmitted out of the camera housing;

(6) Detection of changes in the camera's field of view (scene change detection);

(7) Power management to ensure maximum possible operation should the local facility's power fail;

(8) Secure remote surveillance when connected to a communications server.

Safeguards surveillance systems are relatively unique in that the equipment must operate unattended for extended periods in harsh conditions and with a high degree of security and reliability. Commercial off-the-shelf equivalents are not available. Systems that nearly meet the requirements invariably require some degree of modification, if technically possible.

Because of its inherent flexibility, the introduction of the DCM 14 also provided a means to consolidate and standardize future surveillance systems. Using the DCM 14 in different configurations it became possible to assemble single and multiple camera systems for easy and difficult to access locations from a standard array of basic building blocks. Since 1998, the DCM 14 has been used to construct 5 basic digital surveillance systems, meeting the full range of safeguards applications, often in difficult environments. Table II demonstrates the transition from systems implemented in the fourth decade of IAEA safeguards to the DCM 14 based systems implemented in the fifth decade.

Figure 4: DCM 14 with video CCD camera (CCD: Charge Coupled Device)
(courtesy: IAEA, Vienna)

Table II: Replacement and Consolidation Plan for Surveillance Systems

Application	Film, videotape and early digital systems phased out between 1995 and 2002	Current Digital Image Surveillance and other systems
Installed Single-Camera Systems – *for easy to access locations*	Compact Surveillance and Monitoring System COSMOS	ALIS All in one surveillance, mains operated
	Photo Surveillance Unit (Twin Minolta System)	ALIP All in one surveillance portable, battery operated
Installed Single-Camera Systems – *for difficult to access locations*	Gemini Digital Video System GDTV	DSOS Digital single-camera optical surveillance
	Modular Integrated Video System MIVS	
Installed Multi-Camera Systems	Multiplex TV Surveillance System	SDIS Server digital image surveillance Up to 6 cameras
	Multi-Camera Optical Surveillance System MOSS	DMOS Digital Multi- Camera Optical Surveillance Between 6 and 16 cameras
	Upgraded Euratom Multi-Camera Optical Surveillance System EMOSS	FAST FAST company surveillance system *Developed by Euratom for joint inspection use*
	DigiQuad Multiplex Video System	
Short Term Surveillance System	Short Term TV System	ALIP
Surveillance for Remote Monitoring		SDIS
		DMOS
Underwater TV Systems – *for attended applications*	UWTV Underwater TV	UWTV Underwater TV
	UWVD Underwater Viewing Device	UWVD Underwater Viewing Device
Surveillance Review – *hardware and software*	General Advanced Review Station GARS Version 6.3	General Advanced Review Station GARS Version 6.4
	MIVS Advanced Review Station MARS	
	Multi-system Optical Review Station MORE	

Surveillance continues to play an important rôle in safeguards. There has been a steady increase in the number of camera units deployed in safeguarded facilities.

In 2003, the IAEA maintained about 800 cameras connected to 400 surveillance systems in 170 safeguarded sites worldwide. Until about 2005, old and new systems continued to coexist. Table III provides an overview of the IAEA's main systems after 2005.

Equipment has also been developed to provide an increasingly sophisticated review capability for surveillance. Following the same technology trends, review stations have evolved from film review tables, through videotape systems (some with advanced features such as scene change detection) to the IAEA's most recent GARS review software that can be run on a personal computer equipped with the appropriate digital media peripherals. Further details of the IAEA's most widely used digital surveillance systems follow.

Table III: Optical Surveillance Systems

Code	Equipment name	Description and applications
Videotape: single camera surveillance systems		
SIDS	Sample Identification System	Facility specific surveillance system integrated with a high-level neutron coincidence counter and triggered by neutrons above a pre-set threshold, allowing MOX sample identification in a fuel fabrication facility.
UWTV	Underwater TV	Commercial underwater closed circuit TV system (CCTV) for inspector attended fuel identity verification in storage ponds.
Digital: single camera surveillance systems		
ALIP	All In One Surveillance Portable	Battery powered, single camera for easy to access locations or for portable surveillance applications.
ALIS	All In One Surveillance	Mains powered, single camera for installation in easy to access locations.
DSOS	Digital Single-Camera Optical Surveillance	Single camera for installation in difficult to access locations.
Videotape: Multi-camera surveillance systems		
FTPV	Fuel Transfer Video	Facility specific CCTV system used at fuel transfer ponds.
MOSS	Multi-Camera Optical Surveillance System	Videotape based, multiple camera surveillance system for up to 16 cameras. Phasing out.
VSPC	Video system	Facility specific CCTV system for up to 4 cameras on a split display screen.
Digital: Multi-camera surveillance systems		
DMOS	Digital Multi-Camera Optical Surveillance	Multiple camera surveillance system for up to 16 cameras with remote monitoring capability.
SDIS	Server Digital Image Surveillance	Multiple camera surveillance system for up to 6 cameras with remote monitoring capability.
Surveillance review systems		
GARS	General Advanced Review Station Software	For the review of ALIS,ALIP, DMOS, DSOS, GDTV, SDIS surveillance.
MORE	Multi-system Optical Review Station	For COSMOS, MIVS, MXTV, MOSS, DigiQuad. Phasing out.

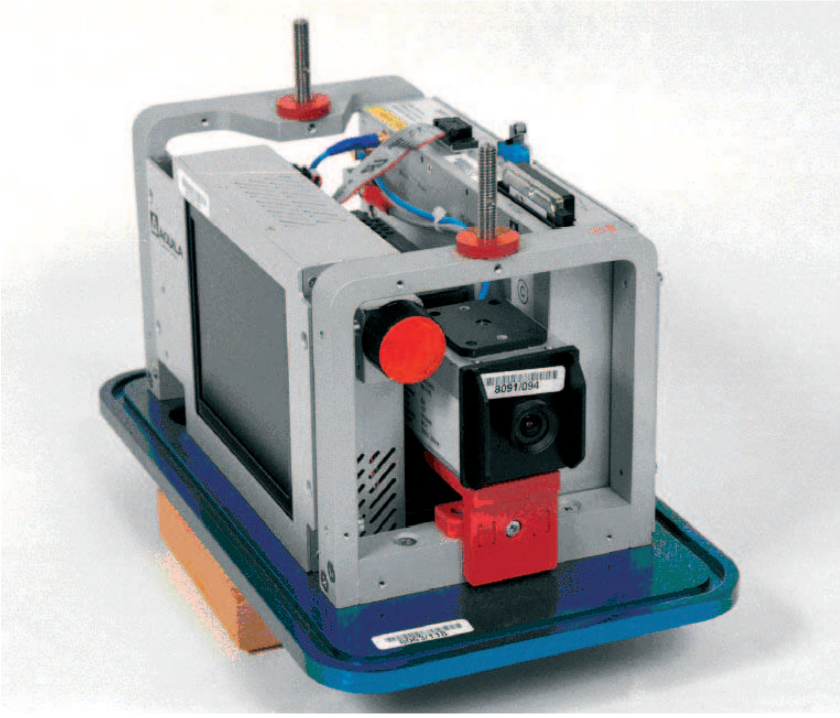

Figure 5: ALIS: All In One Surveillance Unit
(courtesy: IAEA, Vienna)

Figure 6: DSOS: Digital Single Camera Optical Surveillance System
(courtesy: IAEA, Vienna)

Installed single camera for easy to access locations

ALIS. The All In One Surveillance Unit (Figure 5) is a mains operated, fully self-contained digital surveillance system based on the DCM 14 digital camera module. All the components fit within a blue standard IAEA camera enclosure with all the functionality of the DCM 14 plus an integrated inspector interface terminal. Images and associated log files are stored on PCMCIA flashcards. With a 660 MByte flashcard installed, ALIS can record between 40,000 and 50,000 images, depending on the compression used.

Installed single camera for difficult to access locations

DSOS. The Digital Single Camera Optical Surveillance System (Figure 6) is based on DCM 14 technology and is designed for applications where the camera must be placed in a difficult to access location. DSOS consists of a DCM 14 based digital camera connected to a recording unit by a special composite cable. The recording unit, which is also based on DCM 14 technology, allows an inspector to service the system at a more convenient and safe location using procedures similar to those used when servicing an ALIS.

Installed multi-camera

SDIS. The Server based Digital Surveillance System (Figure 7) was initially developed for remote monitoring applications. Its primary function is the collection of images and data from up to 6 DCM 14 surveillance cameras. It may also be used for the direct interrogation of VACOSS seals. The SDIS server sorts and classifies image and other data and can securely transfer images and data to IAEA offices. An uninterrupted power supply unit is an integral part of SDIS and has been designed to keep the system in full operation for about 48 hours without an external mains power supply. Figure 8 shows the internal parts of SDIS. Two modes of operation are available:

(1) Unattended: The data are stored on a removable Jaz-type disk and are physically carried to the GARS equipped review station.

(2) Remote monitoring: The data are transferred to an IAEA office by telephone line (PSTN), ISDN, ADSL, frame relay or satellite link and subsequently reviewed on a GARS equipped review station.

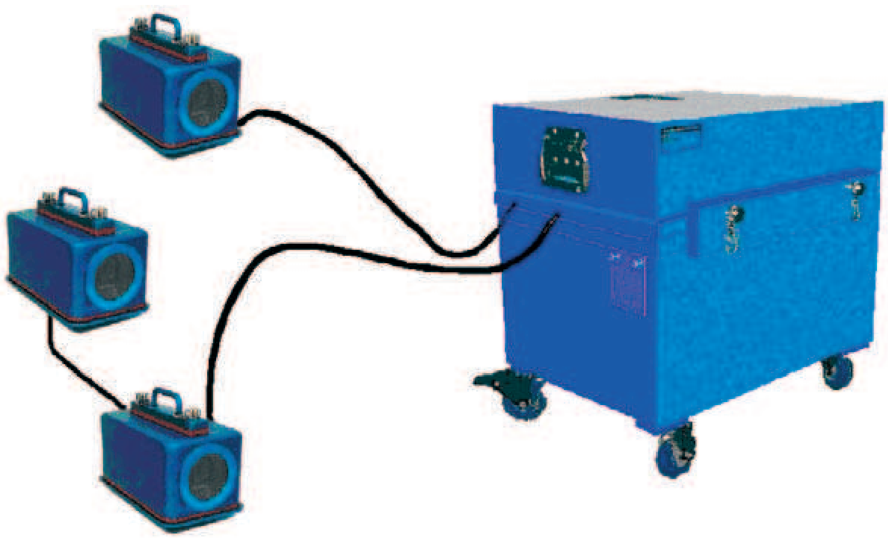

Figure 7: SDIS: Server based Digital Surveillance System
(courtesy: IAEA, Vienna)

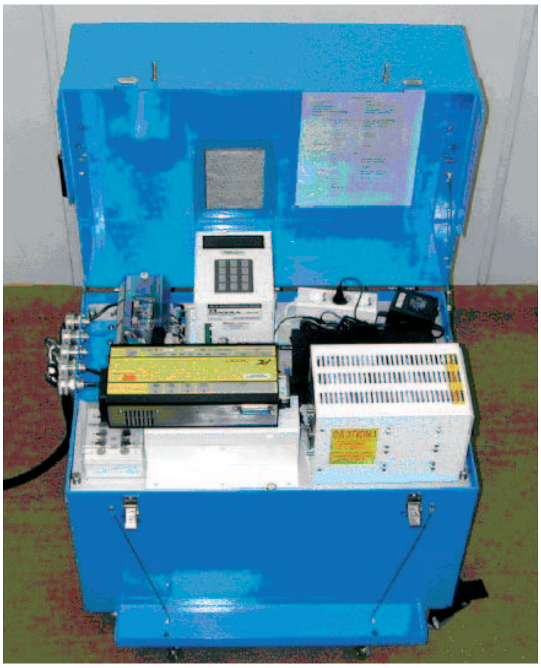

Figure 8: SDIS server ('blue box' – lid open) (courtesy: IAEA, Vienna)

DMOS. The Digital Multi-Camera Optical Surveillance (Figure 9) is designed for unattended and remote monitoring applications. DMOS is used for applications requiring between 6 and 16 cameras connected to a central recording and communications console. DMOS is based on DCM 14 technology and each camera is interrogated by a server computer. Images and data from each camera are initially stored on a large RAID array prior to final storage on a removable digital linear tape (DLT).

Figure 9: DMOS: Digital Multi-Camera Optical Surveillance (courtesy: IAEA, Vienna)

:Short term surveillance

ALIP. The All In One Surveillance Portable unit (Figure 10) is a battery operated, fully self-contained digital surveillance system based on the DCM 14 digital camera module. It consists of a camera, a video terminal, the DCM 14 digital camera module, a mains operated power supply and a set of batteries, all of which are enclosed in a camera housing that has the same footprint as the standard IAEA camera housing but has been extended vertically to accommodate the batteries. With fully charged batteries, the system can perform surveillance duties for up to 100 days with no external power. Images and associated log files are stored on PC cards. With a 660 MByte flashcard installed, ALIP can record between 40,000 and 50,000 images, depending on the compression used.

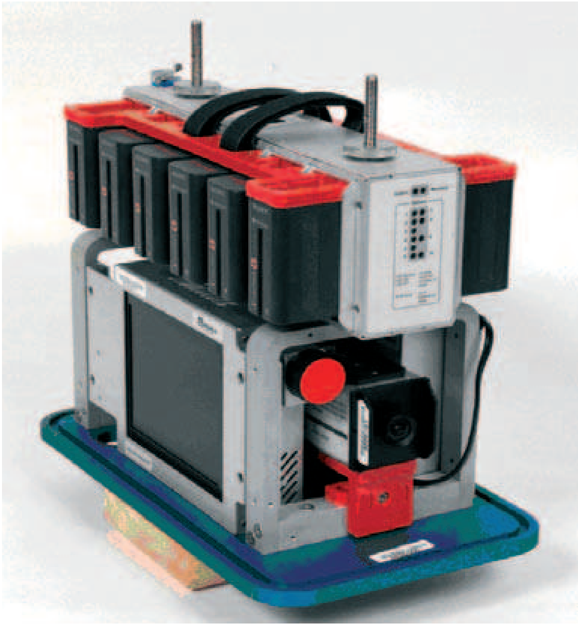

Figure 10: ALIP: All In One Surveillance Portable Battery Unit (courtesy: IAEA, Vienna)

Underwater TV for attended applications

The portable UWTV system (Figure 11) is mainly used for verifying bundles in spent fuel ponds of CANDU type reactors. It can also be used for all other kinds of underwater inspections. A complete system consists of a radiation hardened camera, a camera control unit (CCU) and various accessories such as a motorized 90 degree rotating head and a light system. Light accessories are available for long and short distance verification activities. For bundle identity verifications, the camera must be capable of reading small letters under limited light conditions and withstand a very high level of radiation, still remaining watertight down to a depth of 15 metres in water. The CCU has a built-in monochrome monitor for on-site review. The video can also be recorded on an external videocassette recorder.

Figure 11: UWTV system (courtesy: IAEA, Vienna)

Surveillance review software

MORE. The Multi-System Optical Review Station (Figure 12) was designed to assist inspector review of COSMOS, MIVS, MXTV and MOSS videotapes. Each MORE system comprises an IBM compatible computer running MORE software (with a built-in DAT drive to archive digitized images), a display unit for the computer, a monochrome video monitor with automatic CCIR/EIA-170 video standard detection, three videotape recorders to replay surveillance tapes and a printer for reports. To utilize the scene change detection option it is first necessary to create set-up files. Regions of interest are defined within the recorded image captured by the camera in the field. Regions of interest are defined in the field of view as areas of safeguards significance (e.g. possible paths for the removal of safeguarded material).

Figure 12: MORE: Multi-System Optical Review Station
(courtesy: IAEA, Vienna)

GARS. The General Advanced Review Station software (Figure 13) was developed to run on a personal computer with the appropriate media drives to review the recorded images from ALIP, ALIS, DSOS, DMOS, GDTV and SDIS. The basic GARS version provides a flexible and user friendly inspector interface (similar to popular commercial media players) for the review of images and data from flashcards, Jaz-type disks, removable hard drives, CD-ROMS and DLTs. GARS also has advanced features that can be used to reduce an inspector's review effort. Those features include image and data authentication verification, image and data decryption, scene change detection of recorded images, digital image enhancement and multiple camera display options.

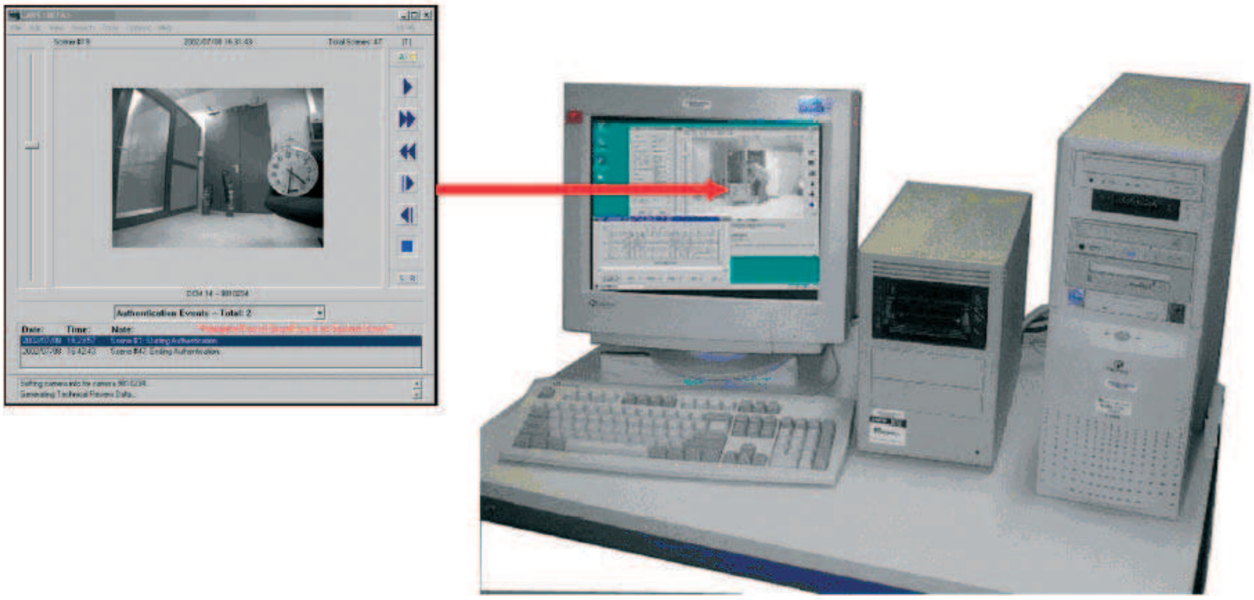

Figure 13: GARS software (courtesy: IAEA, Vienna)

Miscellaneous surveillance systems and options

In addition to the systems described above, other surveillance systems and equipment to enhance the capabilities of existing surveillance equipment are to be mentioned. Table IV summarizes those systems.

Table IV: Optical Surveillance Systems

Code	Equipment name	Description and applications
FAST	FAST company surveillance system	Multiple camera digital surveillance system, developed by Euratom for joint use applications. Under evaluation in 2003.
LRFO	Laser Range Finder Option	Option for the attachment of DCM 14 based cameras to counter in-front-of-lens tampering. Under development.
VMOS	VACOSS-S/MOSS System	Option that allows the integration of the MOSS multi-camera surveillance system with a remotely verifiable VACOSS seal. Phasing out with MOSS.
WCSS	Wall Containment Sensor System	Wall penetration detection for triggering surveillance images. Under evaluation in 2003.

7.2 Seals

Seals, sometimes referred to as tamper indicating devices, are used to secure materials, documents or any other important items in a tamper-proof containment. The purpose of the seals is to provide evidence of any unauthorized attempt to gain access to the secured material. The seals also provide a means of uniquely identifying the secured containers. It must, however, be pointed out that the seals do not provide any kind of physical protection, nor were they designed to provide such protection.

In 2006, the Agency was using eight types of safeguards authorized sealing devices with a number of other systems under development and not yet authorized for use. We have organized the sealing systems discussion by the categories of passive, active, and special applications. This is not a priority ranking, but it is an ordinal one. That is, the Agency currently fields some 30,000 passive seals a year, the order of 2,000 active seals, and the order of 300 – 500 special application seals.

Passive sealing systems

Passive sealing systems do not require an energy source while the seal remains in place, although in some cases a powered reader is required for seal interrogation. Some of these seals are examined in situ, and some are returned to Agency Headquarters for examination. Passive sealing systems represent by far the most common form of Agency seal.

Metal Seal

The Metal Seal is extensively used for sealing material containers, material cabinets and IAEA safeguards equipment. It is the Agency's most popular single-use passive seal with some 18,000 used annually. The seal has 2 metallic parts which, when engaged, cannot be separated without leaving evidence due to damage. A metal wire is used as a sealing wire and a knot is tied inside the seal body to close the loop. With the knot inside the seal, the loop cannot be opened without cutting. The main advantages of the seal are its simplicity, physical robustness, and its small size and weight. Attachment and detachment efficiency is important to limit the radiation exposure of the inspector. The main disadvantage is that verification must be performed at the IAEA's headquarters. To this end, the seal is detached in the field by cutting its wire and brought to IAEA Headquarters for identification. Unique identification of each seal is obtained by imaging random scratches on the inside surface of the metal cap and by comparing the images before installation and after removal (Figure 14).

Figure 14: Comparison of metal cap seal images for seal validation (courtesy: IAEA, Vienna)

Adhesive Seal

The Improved Adhesive Seal is made of special material which cannot be removed without leaving evidence of seal damage. Re-attachment of the seal is not possible. As for all adhesive seals, the seal is intended only for temporary applications (24 hours or less). Its main advantages include ease of use, low unit price, and low operations, maintenance, and logistics (OM&L) train. The seal is intended for use in a wire wrap application and on different surfaces (metal, plastic) and is available in two sizes. The Agency uses about 12,000 of these seals per year.

COBRA Seal

The COBRA seal consists of a plastic body and a fibre-optic loop. The seal wire is a multi-strand plastic fibre-optic loop with its ends enclosed in the seal in such a way that a unique random pattern of fibres is formed. This can be verified by shining light into the ends of the loop and observing the pattern of the fibre ends by means of digital image recording. Immediately after the seal is installed, a reference image of the seal signature pattern is taken. Upon subsequent inspections, follow-up images are taken. The COBRA seal verifier stores digital images and is able to compare the patterns. This procedure enables the inspector to automatically verify the seal identity and integrity in situ and to conveniently store the pattern in a computer. The main advantages of the seal are that it is small, light and inexpensive. This is an in-situ verifiable passive seal (other than the ARC seal, a special applications seal) where multiple verifications on site are possible, a wide temperature range is acceptable, and no electrical power is required. It can stay attached for long periods of time, in some cases, years. The Agency is using about 1,200 such seals per year.

Sample Vial Secure Container

The Sample Vial Secure Container (SVSC) is a small plastic container used to seal liquid samples of nuclear materials. It consists of a small cylindrical body and a cover. A small metal plate with an engraved serial number is inserted inside the cover and the cylinder's bottom. The SVSC is uniquely identified by a pattern (swirls) injected into the mould during fabrication. The main advantages of the SVSC are its small size, ease of use, ability to contain highly radioactive materials (for a limited period of time) and low price. The Agency is currently using about 1,500 SVSCs per year.

Active Sealing Systems

Active Sealing Systems require power for the seal to operate. This is usually supplied by a long life on-board battery. In every case, active sealing systems, either fielded or under development, are either fibre optic or electromagnetic loop monitoring devices.

VACOSS 5.0 Electronic Seal

Electronic seals are being used with increasing frequency in IAEA applications as remote monitoring becomes more universally applied. The first IAEA electronic seal, originally conceived in the 1970s, was the Variable Coding Seal System (VACOSS-S), shown in Figure 15. This seal uses electronic encoding methods in conjunction with a fibre optic loop. The VACOSS-S Electronic Seal is intended for high reliability, long duration surveillance in applications that require periodic access. The time, date and duration of openings and closings of the loop are recorded internally for later retrieval. The fibre optic loop is monitored with a light pulse every 250 ms for continuity of the light path. The internal batteries have an operational lifetime of 18 months. For installations with multiple seals in proximity, the seals may be connected in series. All seals connected in this fashion can be read in sequence without changing the connection. The seal electronics are potted, in order to prevent intentional manipulations. A tamper switch detects any opening of the seal housing. The seal housing is opened only to replace the internal batteries and openings are recorded as tamper events. An interface box enables communication between the seal and the reader. The seal is reusable and in situ verifiable. It is mainly used for applications where multiple openings and closings are expected or when the seal is combined with a remote monitoring system. The Agency currently uses about 1,500 such seals in attended and remote monitoring applications. The VACOSS system is being replaced by the EOSS system beginning in 2006/2007. However, VACOSS systems will continue to be used until the full inventory of EOSS systems has been established. This will take several years to accomplish.

Figure 15: VACOSS 5.0 Electronic Seal with fibre optic loop, interface box and palmtop computer (courtesy: IAEA, Vienna)

Special Application Seals

Special Application Seals may be passive or active, but are typically designed for special applications, perhaps in just a few facilities. They are usually approved for safeguards use in these limited applications only.

Atomic Energy of Canada Ltd. (AECL) Random Coil (ARC) Seal

The ARC seal was developed for underwater applications such as for sealing stacks of spent fuel bundles stored in bays of CANDU reactors. The seal body is mounted on a stud used to fix the fuel in the bay. A reading device is used to obtain the seal's signature, store it and provide verification results. The ARC seal is a single use seal. Multiple in-situ verifications are possible. About 200 such seals are in use, but the seal is rapidly approaching the end of its useful life and a replacement is under development. The seal is constructed to contain a randomly oriented coil of wire. Verification is accomplished by transmitting ultrasonic pulses through the seal with a suitable transducer and observing the unique pattern of reflections. Verification consists of comparing the pattern obtained when installed with that obtained during subsequent in situ checks.

Ultrasonic Sealing Bolt (USSB)

The sealing bolt has been designed for closing and securing shipment and storage containers of LWR spent fuel assemblies in underwater applications. Verification is accomplished by transmitting ultrasonic pulses through the bolt with a suitable transducer and observing the unique pattern of reflections. Verification consists of comparing the pattern obtained when installed with that obtained during subsequent in situ checks.

T-1 Radio Frequency Seal (TRFS)

The first-generation TRFS seal technology is in use at the Savannah River K-Area Material Storage Facility. It is a battery-powered, in-situ verifiable, electronic seal that communicates through an RF link to an interrogator/transceiver. Multiple seal units can communicate with a single interrogator/transceiver up to 250 feet away. The RF transmission is authenticated but not encrypted.

7.3 Containment Systems

In the process of selecting a safeguards approach, all aspects of containment systems must be considered. The containment is as important as the seal that closes it. The severity of the potential loss of containment integrity should drive the choice of the sealing method and its sophistication. However, even if the perfect seal could be developed and deployed, continuity of knowledge cannot be maintained without also knowing that the containment is intact. Currently, this is left to the inspector to visually check for tampering. However, there could be more effective methods to detect possible tampering. Current containment systems include the following.

<u>Instrument Cabinets</u>

Instrument cabinets house radiation detector, computer network, data storage and video surveillance equipment. The IAEA specifies and owns the instrument cabinets and conduits, so that it has control over design and built-in tamper indicating features. Tamper indication is added to the cabinets in the form of coatings, surface finishes, welds, and seals. Presently, there is only one approved design for instrument cabinets.

<u>Nuclear Material Storage Containers</u>

Containers are generally specified by the user facilities, not the IAEA. The problem also lies in the number of different types of containers that have been designed for specific applications. Containment can indicate storage containers, shipping containers, casks, spent fuel ponds, vaults, and many others.

The obvious question that needs to be resolved is how to verify the many different types of containers with minimum impact on the inspection process and minimum intrusion to the operator. Periodically, the Agency re-measures a small randomly selected percentage of material under C/S to add confidence that containment has not been breached and no diversion has taken place.

<u>Conduits</u>

In most cases, data are authenticated and encrypted at the instrument level and a tamper indicating conduit is not necessary. However, in cases where authentication is not possible, conduit is used to provide power and data transmission between radiation exposed equipment (sensors and their monitors) that may be located in potentially damaging high-radiation environments. Metal conduit is the only type of conduit used in these applications. Conduits must be physically inspected to verify that tampering has not occurred. A means to effectively inspect the conduit needs to be identified.

8. Research and Development Projects /11/

8.1 Optical Surveillance

The Next Generation Surveillance System (NGSS) is an important IAEA development project in cooperation with the German and United States Support Programmes which was initiated in March 2005. The first phase of the NGSS project focused on the conceptual design of the system, especially on the development of the Surveillance Core Component (SCC) comprising design of candidate hardware architectures, selection and irradiation testing of crucial components, prototype design, and performance evaluation. In phases I and II an appropriate digital signal processor was selected, firmware prototypes were designed for performance evaluation and a functional design prototype of the SCC was demonstrated. Furthermore, review application prototyping and designing of review database and data consolidator were performed.

For the new technology the following features are deemed crucial:

- Cameraunit: Mid- and high-level radiation tolerance, colour imagery, enhanced tamper indication, picture taking at higher frequencies over extended intervals, Ethernet connection with TCP/IP ([16]) protocol, and hardware mostly based on Field Programmable Gate Arrays (FPGA).
- Storagemedia of the digital camera module: It is anticipated that due to obsolescence of the PC-cards the transition to another commercial-off-the-shelf technology will be necessary. At a certain development stage the most appropriate solution has to be found.
- Batterybackup: While for the DCM 14 a Li-Ion battery proved to be the best choice, during the development of the next generation digital camera module this has to be re-evaluated.
- Colour display for portable single-channel system:ruggedness.
- Operating system for multi-channel system:not necessarily mainstream OS such as Microsoft.

8.2 Seals

Metal Seal

New developments aim at in-situ verification. Since 2004, work is underway to augment or replace the internal optical signature ("scratch 'n solder" pattern) with an intrinsic surface signature. The laser surface authentication (LSA) method uses a captured laser speckle pattern to create a unique and highly counterfeit resistant physical signature of the top and bottom halves of the metal seal. The top signature can be read in-situ as many times as desired. The bottom signature can be verified upon removal of the seal. In either case, a verification result is available in the field as opposed to a forensic examination at Agency headquarters. A second significant effort is the development of an eddy current wire integrity instrument to detect cut and splice attempts on standard Agency wire. This instrument, if successfully deployed, is the first Agency instrument available to quantitatively check for cut and splice attempts on simple wire.

Figure 16: Metal Cap Seal (courtesy: IAEA, Vienna)

([16]) Transmission Control Protocol/Internet Protocol.

Adhesive Seal

Since 2004, the Agency has embarked on the design of a new adhesive seal, using an iterative process between a seals design contractor and a vulnerability assessment team. This approach is maximizing the robustness of the product prior to fielding the next Agency adhesive seal, hopefully in the mid 2007 time period.

Several variants are being considered for special use applications of the adhesive seal:

- Use of one-way chromatic (colour changing) inks or other materials to identify tamper attempts using temperature extremes or solvents.
- Use of optically stimulated luminescent (OSL) materials to produce a dosimetric adhesive seal with a dynamic range of 1 μSv (.1 mR) to 10 kSv (1 MR), compared to current commercial label products with detection sensitivities limited to a minimum threshold of about 50 mSv (5 R).

COBRA Seal

A project to enhance the COBRA seal has been authorized by the Agency and is in Phase III of four phases of development. These enhancements are so extensive that the IAEA considers this project as a new development rather than an evolutionary change to the existing Cobra seal. The following design changes will decrease vulnerability while reducing inspector workload.

- Design changes to the seal and seal verifier to ensure that light is transmitted bi-directionally through the fibre-optic loop during verification.
- Development of a new seal verifier that automatically compares reference and verification data providing a metric that quantifies this comparison.
- Development of a system that allows transmission of encrypted and authenticated seal data to Headquarters electronically.
- Design changes to the seal and seal verifier to automatically identify the seal using a 2-dimensional bar code.

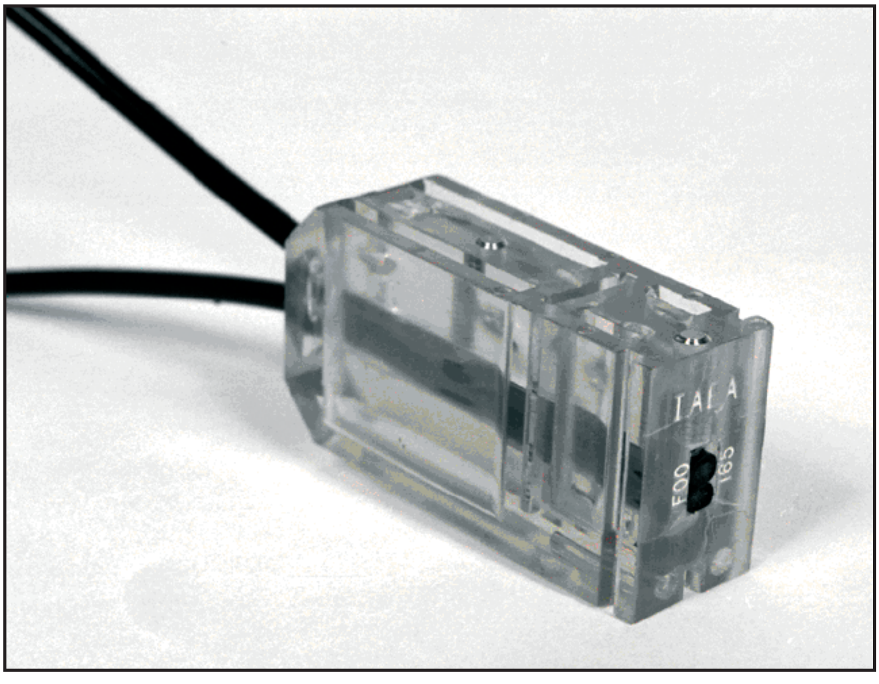

Figure 17: COBRA Seal (courtesy: IAEA, Vienna)

Sample Vial Secure Container (SVSC)

Although there is currently a large stock of SVSCs, the manufacturing tools to produce the SVSC have been "mothballed" and it is unknown whether this capability can be restarted. If not, a replacement for the SVSC will have to be developed.

EOSS Electronic Seal

The Electronic Optical Sealing System (EOSS) is the newest active seal system to become a Category A device, being approved for use in 2005. In time, it will replace the current inventory of VACOSS seals, although a phase-in period will certainly be required. Like the VACOSS, it is an active fibre optic loop system, but with enhanced operability in radiation environments and improved tamper resistance characteristics. Also, the EOSS is fully capable of supporting remote monitoring (RM) applications.

Figure 18: EOSS Seal (courtesy: IAEA, Vienna)

Hi-G-Tek DataSeal

The Agency is currently testing a new inexpensive commercially available RF seal. This new seal was designed for use in the transportation industry by the Hi-G-Tek company. This seal is a battery-powered, in-situ verifiable, electronic seal that communicates through an RF link to an interrogator/transceiver. An internal battery, providing a 5-year expected life, powers the seal. However, the battery cannot be replaced. The seal must be discarded at the end of its battery life. The IAEA has obtained preliminary test results, including an early vulnerability assessment, which are very promising. In addition to the great interest that safeguards inspectors have indicated in such a seal, it is operationally attractive from an operations, maintenance, and logistics standpoint.

JRC CANDU Seal (JCS)

The European Commission Joint Research Centre CANDU Seal (JCS) is currently under development as a replacement for the ARC seal. The JCS is a derivative of the Ultrasonic Sealing Bolt (USSB). The USSB and JCS are products of the Joint Research Centre, Ispra. Both versions require an ultrasonic reading device, which interrogates both the identity and integrity of the sealing bolts used to contain spent fuel. The seal is also much cheaper than the ARC seal with the reader using Windows as opposed to DOS based software.

T-1 Radio Frequency Seal (TRFS)

Since 2004, the T-1 seal became the first seal capable of remote monitoring from the Headquarters in Vienna and data is monitored routinely.

8.3 Containment Systems

Instrument Cabinets

Since 2004, the Agency is pursuing the potential use of x-ray fluorescence (XRF) authentication methods. The system provides an authentication technique for surface areas through the application of elemental XRF compounds, and subsequent reading of those XRF signatures. A feasibility study is envisaged to determine if the method can be used to examine removal and replacement of cabinet panels.

Nuclear Material Storage Containers

The Agency has engaged the Joint Research Centre, Ispra, to determine the feasibility of containment verification with laser surface mapping techniques. In this approach, an entire surface area of a container is scanned with a laser and a reflected amplitude image obtained. Subsequent images generate a matching signature whereas surface penetrations or the wrong container altogether generate a non-matching signature.

Conduits

Since 2004, a bench scale prototype for a conduit monitoring technique has been developed at Oak Ridge National Laboratory in the United States. The technique is able to detect malicious penetrations to the conduit, and distinguish those penetrations from common events such as vibrations and inadvertent cable movements using a proprietary electronic signal analysis method.

ACKNOWLEDGEMENT

Gotthard Stein's invaluable advice during compilation of this article is greatly acknowledged.

9. References

/1/ B. Richter, The Evolution and Rôle of Containment and Surveillance Techniques in International Safeguards, Proc. 15th ESARDA Annual Meeting, Rome, 1993, 743-748.

/2/ Treaty Establishing the European Atomic Energy Community of 17 April, 1957.

/3/ Treaty on the Non-proliferation of Nuclear Weapons of 1 July, 1968.

/4/ IAEA Safeguards Glossary, 2001 Edition, IAEA/NVS/3, 2002.

/5/ C.S. Sonnier, Containment and Surveillance in International Safeguards, The Past – The Present – The Future; Proc. 32nd INMM Annual Meeting, New Orleans, JNMM XX, 1991, 132-138.

/6/ B. Richter, Digital Verification Techniques in the Nuclear Safeguards System: Status and Perspectives, in: Verifying Treaty Compliance, by R. Avenhaus, N. Kyriakopoulos, M. Richard, G. Stein (eds.), Springer Berlin Heidelberg, 2006, ISBN-10 3-540-33853-5, ISBN-13 978-3-540-33853-6, 531-546.

/7/ INFCIRC/153 (corrected) = The Structure and Content of Agreements between the Agency and States Required in Connection with the Treaty on the Non-proliferation of Nuclear Weapons, Vienna, Austria, reprinted in June 1972.

/8/ INFCIRC/540 (corrected) = Model Protocol Additional to the Agreement(s) between State(s) and the IAEA for the Application of Safeguards, Vienna, September 1997, reprinted in December 1998.

/9/ Guidelines for Developing Unattended and Remote Monitoring and Measurement Systems, ESARDA Bulletin 33, February 2006, 45-52.

/10/ IAEA, Safeguards Techniques and Equipment, 2003 Ed., International Nuclear Verification Series No. 1 (revised), chapter 4.

/11/ H. Undem, G. Weeks, M. Zendel, Sealing Systems and Containment Verification Methods, Technology Annex, 2nd Technical Meeting on Sealing Systems and Containment Verification Methods, February 2007.