SAND2013-8685C

Containment and Surveillance

An Overview

International Safeguards and Technical Systems Department
Sandia National Laboratories

Sandia National Laboratories is a multi program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000. SAND

Objectives

To see the value of containment and surveillance in supporting international safeguards

To be able to define key containment and surveillance system requirements

Goal of Containment and Surveillance

In traditional International Safeguards, accountancy ensures that nuclear materials are present and used as intended

Containment and Surveillance ensures continuity of knowledge

That is to ensure no changes occur between inspections

- As a class we will identify an item and agree to put it into this box for safe keeping
- When we leave for the day, I will take the box with me

- As a group, identify what methods you can use to ensure the item will be the same item when you come in tomorrow
  - The methods you identify must ensure that attempts to remove or replace the item are detected
  - The methods you identify should also ensure attempts to alter the item are detected

- Put each method on a separate note

From Texas A&M Nuclear Safeguards Education Portal

Containment

structural features of a facility, containers or equipment which are used to establish the physical integrity, and to maintain the continuity of knowledge by preventing undetected access to, or movement of, or interference with the items.

Surveillance

the collection of information through inspector and/or instrumental observation aimed at detecting movements, or tampering with equipment, samples and data.

http://nsspi.tamu.edu/nsep/courses/containment-and-surveillance/introduction/what-is-cs-and-why-do-we-need-it

Advantages and Disadvantages

- **Select one of the methods you identified**
  - **Identify key advantages this method has for supporting either containment or surveillance**
  - **Any disadvantages?**

Advantages and Disadvantages

Advantages

Disadvantages

Ideal requirements for devices

Reliable – functions without failure during inspector's absence (months to years)

- Inspectors are responsible for servicing equipment
- Includes environmental qualifications

Recorded data is authentic – must be able to trust as Safeguards conclusions are drawn from this data!

In situ verification desirable for timeliness reasons

Reduction of inspection effort realized through remote interrogation and verification

Ease of evaluation of results and their conclusiveness are important

Low cost

Ease of use, including additional equipment

- Application and time to apply seal
- Includes possibility of operator use

For optical surveillance, ability to reduce data using external triggering, including scene change detection, versus time-interval triggering alone

Example of IAEA Safeguard Containment Device

- **The Remote Monitored Sealing Array (RMSA)**
  - **The RMSA is an active fiber optic seal**
  - **Features include:**
    - *Ability to send secure RF messages (both state-of health and tamper events such as unauthorized opening of fiber)*
    - *Tamper Indicating Enclosure*
  - **Additionally it is low power and has a low life-cycle cost**

Picture courtesy SNL

Note: Details and examples of containment and surveillance devices are included in your handouts

Conclusions

Based on these short activities can you see how C/S can be used to support international safeguards?

Understanding the key advantages for each method can help you to define your key C/S system requirements

Reference Material

Containment and Surveillance
Systems and Devices

Tamper indicating devices (TIDs)/Seals

- **Attached to a secured asset in such a way that its removal, tampering, or destruction would be both necessary to gain the desired access and record such access**
- **Typically applied to individual items containing nuclear material or unattended IAEA monitoring equipment**
- **TIDs can be passive or active**
  - **Passive: do not require an energy source while attached, or receive energy from seal interrogation**
  - **Active: require power for the seal to operate**
- **Around 2006, IAEA fielded some 30,000 passive seals per year; 2,000 active seals; and 300 – 500 special application seals**

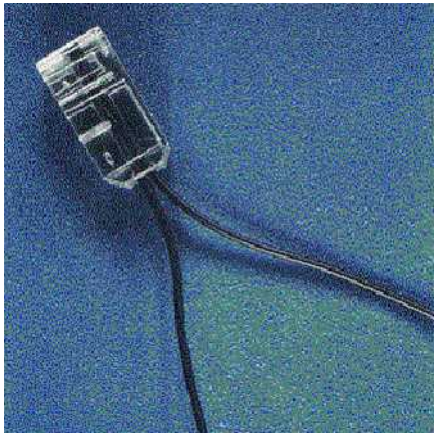
Passive seals

E-Cup/Metal Seal

- **Conventional "loop" seal – used in applications that include hasps or the need to loop wire to ensure continued closure**
  - Wire ends are secured inside seal body
- **IAEA began using in 1966 as a modification of the U.S. Internal Revenue Service (IRS) seal**
- **Simple, passive, single use**
- **Survivable in extreme conditions and physically robust**
- **Small size and lightweight**
- **Verification labor intensive (not in situ)**
  - Done at IAEA HQ
  - Image random scratches on inside surface to verify its unique identity
  - Laser surface authentication (LSA) possible on top surface for identity verification, in situ
  - Investigation into eddy current wire integrity instrument to detect cut and splice attempts on standard IAEA wire
- **Looking to replace**
  - R&D on ceramic and glass seal bodies
- **IAEA uses about 18,000 per year**

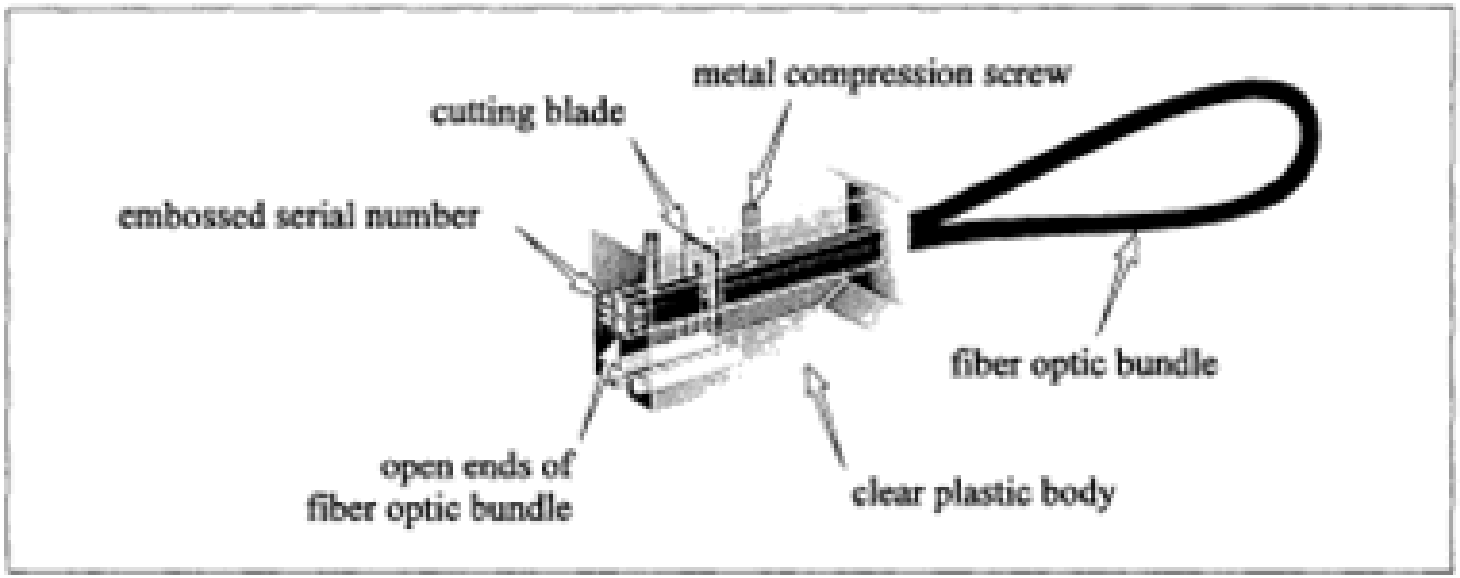
Picture courtesy SNL

Cobra seal



Picture courtesy SNL

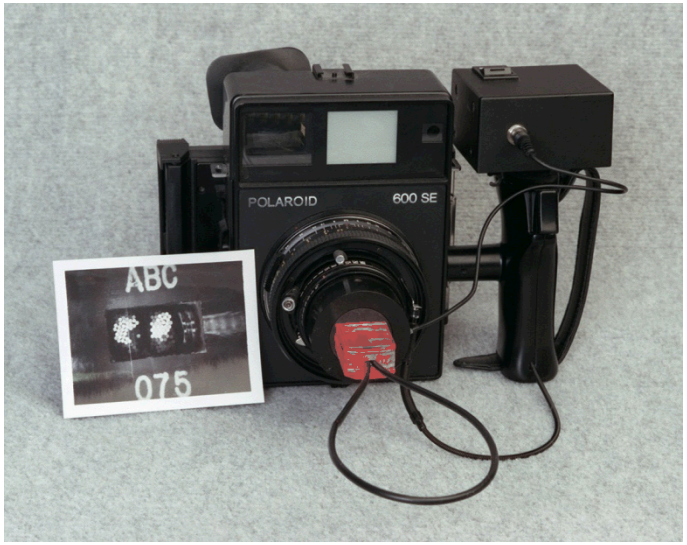
- **Fiber optic loop seal**
  - More expensive than conventional loop seals
  - More time intensive to operate/install than conventional loop seals
- **Insertion of a blade into fiber optic bundle cuts into and impedes light flow through arbitrary strands**



Picture courtesy SNL
SAND93-1726/2

Cobra seal

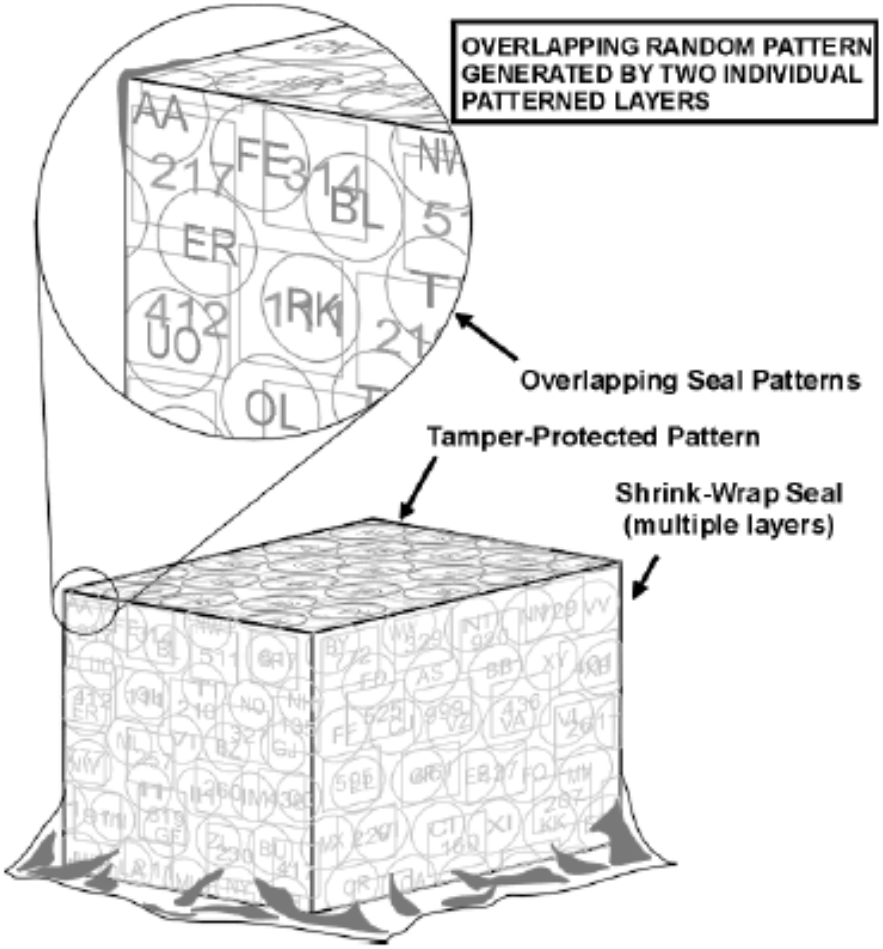
- Digital images are used to record and verify distinctive characteristics of light through cut fiber strands
- Performs well against most environmental factors
  - Radiation sensitivity
- Durable and easy to use
- Verification of seal identity and integrity in situ
- Small and lightweight
- Improvements currently being investigated, including reflective particles in seal body for increased tamper indication, and new seal reader (image is old reader)
- IAEA uses about 1,200 per year



Picture courtesy SNL

Shrink-wrap laminar

- Sheets of film printed with differing ink patterns
- Article of interest is enclosed with multiple continuous layers and a heat source is applied
- Reference photograph is taken for authentication during subsequent inspections
- Advantages – ease of use in field, easy to install, few tools are required, no surface preparation
- Disadvantages – not very durable
- Best use is for odd geometric shapes; otherwise use as a compliment to other seals



Picture courtesy SNL
SAND99-2455

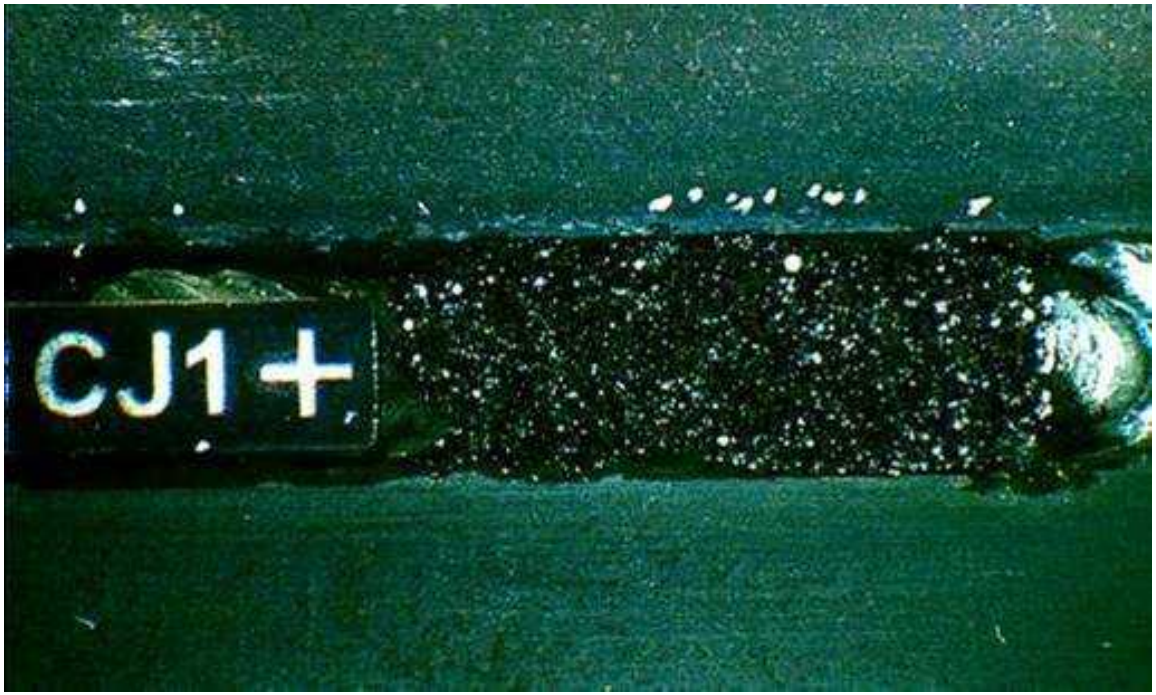
Sandia National Laboratories

Adhesive (paper) seal

- Short term sealing application (24 hours or less)
- Made of special material which cannot be removed without leaving evidence of seal damage
- Cannot be reattached
- Advantages
  - Ease of use
  - Low unit price
  - Low operations, maintenance, and logistics train
- Research into use of one-way chromatic (color changing) inks to identify tamper attempts using temperature extremes or solvents
- IAEA uses about 12,000 per year

Reflective Particle Tags (RPT)

- Hematite particles embedded in acrylic matrix
- Speckle pattern is unique and extremely difficult to duplicate
- Application is relatively simple and field verifiable
- Disadvantage is difficult alignment of reader



Picture courtesy SNL

Ultrasonic Sealing Bolt (USSB)

- Designed for closing and securing shipment and storage containers of Light Water Reactor (LWR) spent fuel assemblies in underwater applications
- Verified by transmitting ultrasonic pulses through the bolt with a suitable transducer and observing unique pattern of reflections
- Compare pattern obtained when installed with that obtained during subsequent in situ checks

Active seals

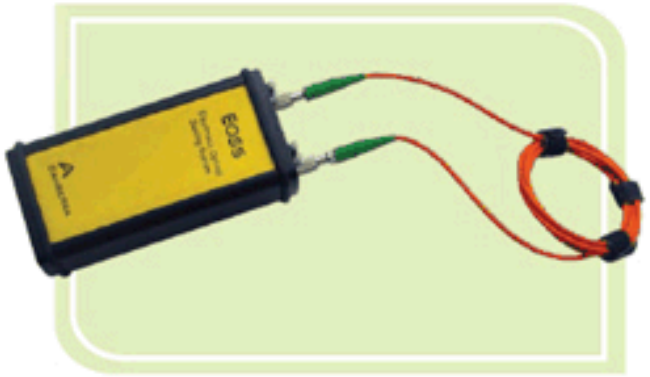
VACOSS fiber optic

- Active electronic seal for applications requiring periodic access (reusable) and verification on-site
- Records time, date, and duration of loop opening and closing
- 18 month operation time on 2 internal Li-batteries
- Local memory of up to 10 time-stamped fiber-optic events
- Case and battery monitoring
- Could provide encrypted seal data
- Party-line connection for multiple seals is possible
- Remote monitoring capability
- IAEA uses about 1,500 per year

Picture courtesy Canberra

Electro-Optical Sealing System (EOSS)

- **Fiber optic seal**
- **Viewed as replacement for VACOSS seal in 2006**
- **Battery life of 3 years**
- **Registering of sealing wire events, case events and SoH in non-volatile memory**
- **Data authentication based on 3-DES with 128 bit keys**
- **Tamper-indicating composite seal enclosure**
  - **Two compartments – inner part contains all security-sensitive components, outer part houses the batteries as well as electrical and fiber optic connectors to facilitate repair**



Picture courtesy Canberra

T-1 Radio Frequency Seal

- **Active fiber optic loop seal with two-way RF communication**
  - **Other fiber optic seals are read with handheld readers**
- **Digital sensors in T-1 include fiber optic seal, motion, high-low temp tamper indicator, case tamper, three unassigned digital input/output ports, two digital switch closure ports**
- **Analog sensors – temp, battery voltage, two unassigned**
- **IAEA accepted for specific facility (KAMS)**

Picture courtesy SRS/KAMS

Remotely Monitored Sealing Array (RMSA)

- **The RMSA is an active fiber loop seal for IAEA Safeguards application**
  - Seal integrity and status is reported via authenticated and encrypted wireless transmission to a central "translator"
  - Seals units are optimized for low power consumption and last 4-5 years on a battery without replacement
  - Incorporates advanced tamper indication and communications capabilities
  - Low life-cycle cost

Picture courtesy SNL

Hi-G-Tek data seal

- Commercial RF seal
- Inexpensive
- In situ verifiable
- Battery is 5 year life but cannot be replaced
- Uncertain of current status

Tamper indicating enclosures/container verification

- **Containment is as important as the seal that closes it**
- **Complex issue and still lacking sufficient attention**
- **Instrument cabinets**
  - One approved design for IAEA
  - Coatings, surface finishes, welds and seals
- **Nuclear Material Storage Containers**
  - Specified by user facilities, not IAEA, and includes storage containers, shipping containers, casks, spent fuel ponds, vaults, etc. (many different types)
  - How do you verify a container you don't own?
  - Variety of solutions required for variety of types
- **Tamper indicating conduit required in some circumstances where data is not authenticated at the data generator**
  - Metal conduit is used currently and inspector visually inspects
  - Need a better method

Some container verification methods

- **T-1a/RMSA blue swirl patterned enclosures**
- **Sample Vial Secure Container (SVSC)**
  - Small plastic container used to seal liquid samples of nuclear materials
  - Small cylindrical body and cover
  - Small metal plate with an engraved serial number is inserted inside cover and cylinder's bottom
  - SVSC is unique identified by swirl patterns injected into the mould during fabrication
  - Advantages: small size, ease of use, low price, and ability to contain highly radioactive materials (for a limited period of time)
- **Eddy-current**
  - Focused on containers that are used to store nuclear material
  - Each container has a unique signature that can be determined from variations due to magnetic permeability and material conductivity in the container, and more specifically at the welds on the container
  - Any cutting, drilling, plugging or re-welding will change these properties
- **Flash thermography**
- **Laser surface authentication**
- **Application of elemental X-ray fluorescence (XRF) compounds onto surfaces and subsequent reading of those XRF signatures**

Surveillance

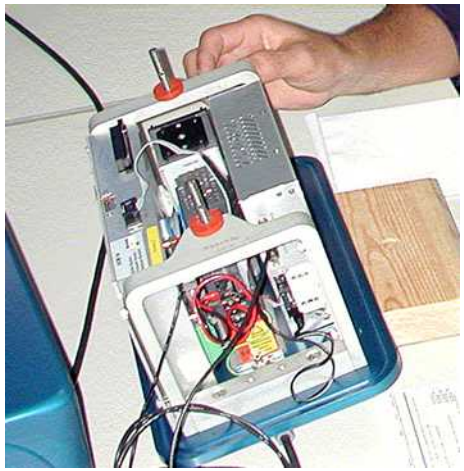
- Purpose of optical surveillance is to record events that occur during an inspector's absence
- Most effective in storage areas, with relatively few plant operator's activities that could be interpreted as removal of nuclear material
- Picture-taking-interval (PTI) must be set to shorter than fastest possible removal time of material, or camera can be triggered by scene change detection or external triggers such as radiation monitoring or electronic seals
- Two images required so that if item is moved, direction can be determined
- Most legacy surveillance systems are based on the DCM-14 (digital camera module)
- Systems are built based on need for single/multiple cameras, access to camera, and remote monitoring capability

Picture courtesy Canberra

Family of surveillance systems

- **Easy to access location, single camera system:**
  - All In One Surveillance (ALIS) – mains operated
  - All In One Surveillance Portable (ALIP) – battery operated, short term surveillance
- **Difficult to access location, single camera system:**
  - Digital Single-Camera Optical Surveillance (DSOS) – digital camera connected to recording unit by special composite cable
- **Multi-camera systems with remote monitoring capabilities:**
  - Server Digital Image Surveillance (SDIS) – up to 6 cameras; also direct interrogation of VACOSS seals
  - Digital Multi-Camera Optical Surveillance System (DMOS) – up to 16 cameras; control and recording unit installed in a 19-inch cabinet
- **Underwater, single camera system:**
  - UWTV (underwater TV) – videotape system, CCTV for inspector attended fuel identity verification in storage ponds
- **GARS – General Advanced Review Station Software, for review of DCM-14 based systems**

Pictures of surveillance systems



ALIS

ALIP*

DSOS*

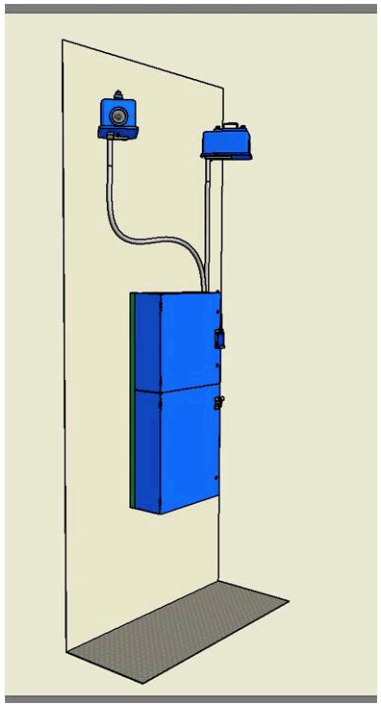
SDIS*

DMOS*

* Pictures courtesy Canberra

Secure Video Surveillance System (SVSS)

- **System built specifically by SNL/ABACC for ABACC to support unannounced inspections**
  - Up to two hours may elapse between the notification of inspection and when inspectors reach a facility location of interest
  - Video surveillance with a fast picture-taking interval covers this delay time
  - The surveillance technology presently in use by ABACC is obsolete and unreliable
  - SVSS employs commercial, off the shelf components



Sandia National Laboratories

Next Generation Surveillance System (NGSS)

- **Will eventually replace all DCM-14 based systems**
- **Improvements include: color imagery; enhanced tamper indication; pan/tilt/zoom; 4 separate channels, each having different triggers and picture taking intervals (allows exclusive ownership of data set for multiple partners)**

Pictures courtesy Canberra

Unattended and remote monitoring (URM)

- **Allows IAEA to reallocate staff to more qualitative safeguards measures**
- **Advantages:**
  - **Less intrusive to operator (reduce interference with plant operations)**
  - **Less radiation exposure to inspectors and technicians as well as plant operator staff**
  - **Improve cost-effectiveness of routine safeguards**
    - *Requires cost-benefit analyses on a case-by-case basis*
    - *Country specific – number of facilities involved, availability and quality of communications infrastructure, communications tariff, licensing of encryption*
  - **Provides for continuous monitoring of high-interest items**
- **Disadvantages:**
  - **Operator concerns about the unaltered access of data transmission scheme, for instance, not altering delayed transmission of surveillance data if implemented**
  - **Amount of data to be transmitted may be high**

General URM instrumentation guidelines

- Digital techniques are implemented to the extent possible
- Modular hardware and software solutions are desirable
- Integration of different sensors
- Electronic components have short times to obsoleteness requiring short term replacement
- Technical progress leads to new concepts and requires periodic replacement of safeguards equipment
- COTS equipment to greatest extent possible, then adapt components to Safeguards applications

URM system specifics

- **Systems include the following:**
  - **Sensor heads, associated electronics, digital data generators**
    - *These are security relevant and should be inside a tamper indicating enclosure*
    - *Data authentication should take place in the data generator*
    - *Not just seals and cameras now, but scope broadens to other sensors*
  - **Data collection system and network interfacing equipment for remote data retrieval**
    - *These can be COTS, since data should be authenticated at the data generator*
- **Data collection system must be reliable, and might include:**
  - **UPS**
  - **Storage**
  - **Redundancy**
  - **Auto-monitoring of state-of-health**
- **For unattended monitoring only, data collection system receives data from sensors, and stores data on-site until retrieved by an inspector**

Remote monitoring details

- **If interfaced to a communication system, data can be transmitted to IAEA headquarters**
  - **Safeguards-relevant data must be encrypted (protected from unauthorized disclosure)**
    - *Virtual Private Networks (VPNs) are accepted technology for transmission over Internet*
  - **Amount of data to be transmitted should be kept as low as possible, and methods include:**
    - *Mathematical compression*
    - *Front end scene change detection*
    - *Correlation of different data types (i.e., only record an image if radiation is detected)*
- **For software upgrading and troubleshooting, IAEA may wish to have remote system access to its systems**
  - **Plant operator may have security concerns such as unauthorized access to other systems**
  - **Remote retrieval of SoH data allows monitoring of systems to initiate timely repair and maintenance**

Technical approaches

- **Broadly speaking, URM sensors include electronic seals, optical surveillance, and radiation monitors, but may include other "triggers" or devices as agreed upon**
- **Seals – as previously discussed, with remote monitoring capability**
- **Optical surveillance system**
  - **Record Safeguards relevant information**
  - **Inspector correlates images with operator's declared activities**
  - **Current systems based on DCM-14 and associated family or DCM-C5**
  - **To reduce number of images, triggered by scene change, electronic seals, radiation detectors, or other devices**
- **Unattended Radiation Monitoring**
  - **Not yet standardized at IAEA**
  - **Digital unattended multi-channel analyzer (DIUM) project wishes to standardize as many components as possible**
    - *Will function similarly to DCM-14, except for sensor heads (detectors include sodium iodide, germanium, cadmium-zinc-telluride)*
    - *Authentication*
    - *Encryption*
    - *Time stamping*
    - *Local data storage*

IAEA seal requirements 1998

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

Information security

- International Safeguards relies on making timely and accurate assessments from enormous amounts of collected information, much of which is provided to Safeguards authorities in confidence
- Safeguards authorities must be able to trust the information they receive (authentication) as well as ensure that the information is suitably protected from unauthorized disclosure (encryption)
- Applies to physical phenomena being sensed (e.g. picture in front of camera), sensor (camera), any piece of equipment through which data passes (collection computer), and communication link (Internet)
  - Authentication ideally applied at sensor level

Elements of information security

- **Encryption**
  - Converts data from a readable format to cipher text that only the intended recipient can decipher
  - Chosen algorithm depends on security needs
  - Private key (Secret) versus Public key
- **Equipment Authentication**
  - Verifies device identity
  - Equipment functions according to its design and cannot be tampered with without detection
  - Sealed Tamper Indicating Enclosures (STIEs)
    - *Any attempt to tamper with the equipment inside will leave easily detected evidence on the surface of enclosure*
  - Tamper Indicating Devices (TIDs)
    - *Seals*
- **Data Authentication**
  - Authenticity: received message comes from the alleged source (not an impostor)
  - Integrity: received message has not been altered ("Launch the torpedo" vs. "Do not launch the torpedo")
  - Techniques are available to guard against packet insertion, deletion, delay, and replay (have you seen "Ocean's Eleven"?)
  - Preferred approach is digital signature (public key algorithm)
    - *Requires more computing resources than symmetric key approaches*

VPNs (for public network security)

- **VPNs add security to Internet communications**
  - IAEA previously used costly dial-up, satellites, and frame relay (some sites cost $10k/month)
  - VPNs save money, add flexibility and scalability
- **SNL has trained multiple international partners on the appropriate use of VPNs**
- **SNL has installed multiple VPNs at international partner locations**
- **To date we have teamed with Finland, Japan, Brazil, Argentina, EURATOM, Joint Research Center (JRC) in this area**

Wireless networking

- **If infrastructure doesn't exist…**
  - **Lower cost than buried cable**
  - **Relatively easy installation**
  - **Can be less intrusive to operations**
- **Ease of maintenance**
- **Ease of inspection since cabling can be difficult to locate and access**
- **SNL has been testing wireless systems worldwide (mostly Bluetooth and Wi-Fi)**
- **Currently not fully accepted by IAEA**