GUIDELINES
FOR DEVELOPING UNATTENDED AND REMOTE MONITORING AND MEASUREMENT SYSTEMS

prepared by the ESARDA Working Groups on
Containment and Surveillance (C/S)
and
Techniques and Standards for Non Destructive Analysis (NDA)

1. INTRODUCTION

In December 2000, the ESARDA Scientific Council and Co-ordination Board (SCCB) charged the Working Groups on C/S and on NDA to collaborate in promoting technical developments.

The SCCB encouraged the Working Group on C/S to take the lead in preparing a guidelines document on comprehensive and integrated tools (e.g., integrated C/S-NDA systems) to support new safeguards requirements. This activity will meet the Working Group's objective '*To promote the technical evolution of automated and remote monitoring instrumentation needed by large, automated fuel facilities for cost effective operation, concentrating on the safeguards perspective*'. The strategy would be '*to collaborate with other Working Groups to develop guidelines*' and '*to prepare a guidelines document*'.

The Euratom Safeguards Directorate (European Commission, DG TREN-I) and the International Atomic Energy Agency (IAEA), termed the 'Inspectorates', at declared nuclear facilities, pursue the concept of substituting on-site inspection effort by unattended monitoring techniques. This concept had been proposed by the Working Group on C/S in 1992 [1] to the end of improving the cost effectiveness of routine safeguards by reducing inspection time in the field, and reduce the burden to the operators. In addition, nuclear radiation exposure of inspectors and technicians will be reduced. Another objective is improving the data collection and analysis by acquiring safeguards data in a timely manner at random or programmable time intervals.

Recent developments have allowed the Inspectorates to make wider use of NDA sensors in unattended mode, using the radiation signal to extract "quantitative" information, as it was always done for NDA instruments in attended mode: Pu-U mass, isotopic composition. In this document we define this "mode" of use of NDA sensors as measurement mode. Unattended Remote Monitoring and Measurement Systems (URMMS) in this document, therefore, comprise two categories of systems:

- Monitoring systems, whose role is the "classical" C/S monitoring and comprises components for image surveillance, radiation monitoring, electronic sealing and their integration in sensor networks. In these instruments radiation detectors are <u>not</u> used as measuring devices, but mainly as monitors (NDA components used in Surveillance or Monitoring mode), generally with the task to trigger an action (e.g., an alarm, a data acquisition, a camera) when the radiation level is higher than a fixed threshold and/or to count radioactive items (e.g., irradiated fuel assemblies) passing the sensor.
- The second category of URMMS has the same functions as the previous one, but, in addition, the NDA signal is used to provide (also) quantitative data, similar or identical in nature to the data which are produced by transportable, attended NDA systems, as for instance, Pu mass via neutron assay, Pu or U isotopic composition through gamma spectrometry. Several examples of this kind of "quantitative" use of NDA in URMMS, have been implemented in nuclear facilities in Europe for several years. [2,3]

Measurement accuracy and quality control (QC) are important issues for these systems and often the geometry of the measurement head (the sensor) is strongly conditioned by factors like sample geometry, plant requirements and detection efficiency, imposing boundary conditions that require individual design.

To be acceptable for safeguards applications, both kinds of equipment have to comply with agreed standards which are addressed in this document.

In November 2000, the ESARDA Working Group on C/S discussed the IAEA's draft Essential User Requirements for Safeguards Unattended Monitoring Systems [4]. In October 2002, the NDA Working Group started to incorporate in the document the aspects of measurement mode. This paper presents the recommendations of both ESARDA Working Groups.

This document discusses first general aspects:	Chapter 2	General remarks
Then gives an overview of the guidelines:	Chapter 3	Guidelines – overview
Specific considerations follow:	Chapter 4	Guidelines – specific considerations
And finally, detailed guidelines:	Chapter 5	Guidelines – details

2. GENERAL REMARKS

The large variety of nuclear facilities to be safeguarded requires a great flexibility on the part of the Inspectorates in designing facility specific safeguards equipment systems. Secondly, electronic components have short times to obsoleteness requiring short-term replacement. Data carriers are a typical example for rapidly changing technologies. These aspects require the use of digital techniques (hardware, firmware, software) and modular hardware and software solutions for automated on-site instrumentation.

Safeguards equipment systems will be combinations of customised and commercial-off-the-shelf (COTS) components. Safeguards-specific requirements, i.e. high reliability for loss-free data acquisition and high data security, require customised solutions for hardware and firmware to be used in the sensitive parts of a safeguards system, i.e., the sensor heads. In other parts of the safeguards system the use of COTS components helps to reduce procurement costs for both hardware and software as well as costs on training and servicing.

It is expected that remote data retrieval will enhance the technical possibilities of reducing on-site inspection effort. The precondition is, however, that the retrieved data are authenticated and encrypted and can be evaluated at headquarters. Also, there must be an overall cost benefit compared to each current safeguards approach under consideration; i.e., the implementation of remote monitoring systems requires cost-benefit analyses on a case-by-case basis.

It is difficult to assess the investment costs for remote monitoring and measurement systems, as technical progress leads to new concepts and requires periodical replacement of safeguards equipment any way. Reduction of on-site inspection effort results in cost savings, whereas data communication encounters costs. Communication costs may vary significantly from one country to the other; in addition, the Inspectorates may face investment costs for communication infrastructure. Depending on the communication technique and the number of facilities involved, the Inspectorates may not be able to transmit data to the desirable extent. Regarding the use of encryption algorithms for authentication and encryption, the situation may become more favourable, as it is expected that algorithms become available free of charge. Archiving requirements as well as evaluation effort may be identical for systems with and without remote data retrieval.

Even under the provision that only remote monitoring and measurement systems are implemented which meet a certain reliability level, there may be a need for remote system access on the part of the system administrator, i.e., Inspectorates. If the Inspectorates request remote system access, e.g., for software upgrading and trouble shooting, it has to be evaluated whether security concerns can be sufficiently met. In fact, any provision of authorised remote system access incurs a non-negligible security risk, as unauthorised remote system access cannot be excluded. Furthermore, camera access potentially undermines the principle of delayed image transmission, if required by the plant operator.

For reasons of communication costs but also for technical reasons 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. Transmission times may become unacceptably long, archiving capacities extremely large, data management and evaluation very laborious, when considering a whole country. Data reduction is achieved by applying compression algorithms; e.g., image files can be reduced to about 20,000 Bytes per image[1]. In addition, scene change detection can help to reduce the number of relevant images. In a field trial a factor of 7 compared to time-triggered images was achieved. Furthermore, it is possible to correlate different types of data. For instance, images could be acquired only if radiation is detected, or if an electronic seal is opened.

The remote retrieval of state-of-health data will allow to monitor the performance of the safeguards systems and to initiate immediate repair and maintenance. Uninterrupted power, local buffering of data and high reliability of the sensor module provide the assurance of continuity of knowledge, while temporary outages of COTS components can be tolerated if they do not lead to data loss.

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.

3. GUIDELINES – OVERVIEW

3.1 Unattended Integrated Remote Monitoring and Measurement Systems

Unattended integrated remote monitoring and measurement systems consist of sensor heads, associated electronics, data generators, a data collection system, and network interfacing equipment for remote data retrieval. This document discusses requirements related to modern unattended systems that are computer based. Some of the listed requirements may also be valid for systems that are not computer based.

3.2 Sensors and Data Generators

Both sensors with their electronics and data generators are security relevant components, as they are the sources of the safeguards data. Therefore, any unauthorised access to the sensitive parts must be prevented by containing these components in tamper-indicating housings and by restricting their servicing, repair and replacement to the Inspectorates' staff. A sensor which is mounted with its data generator in a single tamper-indicating enclosure constitutes a "smart sensor". The digital surveillance camera consisting of a low power OEM (original equipment manufacturer) CCD (charge-coupled device) camera and the digital camera module DCM 14 [5] mounted in the sealable IAEA standard camera housing has been the first example of a "smart sensor" [6].

It features loss-free data acquisition, and all acquired data are authenticated as closely as possible to the signal source. Loss-free data acquisition is based on the principle of uninterruptable powering (backup battery), sufficient local data storage, and compliance with the highest achievable reliability requirements.

Other sensors such as radiation detectors (in both monitoring and measurement modes) usually need to be physically separated from their data generators; in this case, the principle of tamper-indication

[1] un-compressed B/W image files may have typical sizes of about 300 kBytes per image.

must be maintained for the sensor, the signal line, and the data generator and signals from sensor to analyser and from analyser to data collection system should be authenticated.

The concept of “smart sensor” as defined above, has not been developed so far for radiation sensors: this is an area (authentication for NDA equipment, auto-authentication for radiation sensors) where R&D has to be promoted to fully use the potential of URMMS. The development of the digital unattended multi channel analyser DIUM is one step in this direction [7].

3.3 Data Collection System

The data collection system receives data from the sensors used within the same nuclear facility. It stores the data until retrieved on site by an inspector or remotely transmitted to the safeguards authorities’ headquarters.

For on-site retrieval the data must be available on an exchangeable storage medium such as a digital linear tape (DLT), magneto-optical (MO) disk, recordable compact disc (CD-R) or 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 the safeguards authorities’ headquarters.

The confidentiality of the collected data must be guaranteed at all times. If the data are retrieved on site, confidentiality is the responsibility of the safeguards staff member, also during transport from the facility to the headquarters. The inspector may want to transport encrypted data only (see below), in order to ensure confidentiality in case of loss of the data carrier.

If the data are remotely transmitted by means of a communication network, the confidentiality of the data must be guaranteed by means of an appropriate encryption mechanism.

The reliability of the data collection system can be guaranteed 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.

3.4 Network Interfacing Equipment

This equipment is used to interface the data collection system to a public communication network (e.g., PSTN, ISDN, ADSL, satellite), with the aim to transmit the collected data and to give the safeguards authorities access to the system.

The following aspects are important: secure remote access to the data collection system; assurance of confidentiality of the transmitted data, if this would not yet be guaranteed by the data collection system; prevention of unauthorised access to the data collection system and integrity of the data.

3.5 Commercial-Off-The-Shelf (COTS) Components

Many system components such as data buses, communication links, microcomputers, 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 all data processed in these components are authenticated, tampering is not possible undetected. The components could be serviced, repaired and replaced by commercial contractors.

3.6 Approval for Routine Inspection Use

Given the safeguards specific requirements outlined above, it is necessary that prior to acceptance as equipment authorised for routine inspection use the systems successfully pass the following evaluations:

- Qualification testing including radiation testing [2],
- Third Party vulnerability analysis of the safety and security (e.g. authentication and encryption) methods (limited for NDA sensors) [3],
- acceptance testing including usability review, and
- field testing.

4. GUIDELINES – SPECIFIC CONSIDERATIONS

4.1 Sensor level

The following aspects should be addressed:

- data authentication;
  Note: If NDA radiation monitoring sensors need to be physically separated from the data generators, then the principle of tamper-indication must be maintained for the sensor, the signal line, and the data generator, with other measures, like incorporating the three components in separate protection boxes and authenticating the signal from the sensor.
- front end data reduction including data compression, data correlation[4], and scene change detection;
- sufficient data storage capacity/data buffer;
- remote retrieval capability of data directly from the data generator; and
- uninterruptable power supply.

4.2 Data collection system level

The following aspects should be addressed:

- compatibility between devices of different origins;
- redundant data storage capacity;
- uninterruptable power supply;
- data encryption;
- remote data transmission capability out of facilities to Inspectorates‘ headquarters;
- integrated data review;
- provision for the plant operators to perform safeguards relevant activities, e.g., replacement of data carrier.

4.3 System Architecture

In April 1999, the Canadian Safeguards Support Programme to the IAEA organised the Workshop on Integration of Safeguards Equipment Systems involving developers [8]. The following design recommendations for unattended monitoring systems with remote data retrieval capability are supported:

- The systems should be built up from modules, as far as possible.
- Smart sensors, components and other instruments should be interconnectable by adequate standard information exchange interfaces and should have a built-in redundancy for data buffering and power supply.
- There should be a wiring topology between the data generators and data collection systems.

[2] For environmental testing the IAEA and Euratom have co-operated under the Euratom Support Programme to the IAEA at the Joint Research Centre at Ispra. For radiation testing the IAEA has co-operated with the Atominstitut in Vienna. The IAEA and Euratom have applied their “Common Qualification Test Criteria for New Safeguards Equipment”, version 2.0, January 2002.

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

[4] i.e. external triggering, e.g., by radiation monitor or electronic seal

- For the data collection system an adequate COTS operating system should be used.

4.4 Handling and Operation

Regarding the handling and operation of integrated safeguards systems, the following recommendations should apply:

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

5. GUIDELINES - DETAILS

The following detailed recommendations are mainly derived from a draft document prepared by the International Atomic Energy Agency [4].

5.1 General Recommendations

(1) The system shall be modular in design.

(2) Meaningful information shall be stored on individual components and/or subsystems and shall be easily retrievable.

(3) The data collection system shall be based on PCs, with adequate operating system, e.g., Windows NT 4.0 or newer Windows versions, communicating over local area network using TCP/IP communication protocol.

(4) Commercial-off-the-shelf hardware and software shall be used to the maximum extent possible. Customised hardware and software shall be used for the security relevant parts, i.e. sensor heads and data generators.

(5) Any facility mains power failure and any restoration of power shall be noted in the state of health information file.

(6) The system must function in an unattended mode without servicing for at least 100 days.

(7) The sensor heads and data generators must produce authenticated data.

(8) In case of remote data retrieval the authenticated data must be encrypted.

(9) The system shall be able to continually monitor all its critical components and subsystems for operability and record all the equipment performance related events in the state of health information file.

(10) Data filtering and/or data compression shall not cause the loss of a safeguards relevant event.

(11) In an integrated system, daily time synchronisation and a common time base shall be provided for all subsystem clocks to within +/- 1s maximum drift/day.

(12) After a loss of power or other interruptions, the system shall perform an immediate synchronisation of all subsystem clocks upon return of mains power.

(13) The resolution of the system time stamp clock shall be better than the shortest data collection period or data gate.

(14) The system shall be designed to minimise power consumption.

5.2 Hardware Recommendations

(1) The measuring equipment and sensors shall be enclosed in sealable and tamper indicating housings.

(2) The surfaces of the equipment and sensor enclosures, internal and external, shall provide conclusive evidence of any tamper attempt.

(3) Measures shall be included to record securely tamper events in the state of health information file.

(4) The housings shall also be equipped to enable the application of safeguards seals.

(5) The enclosure shall be designed to protect against accidental damage of seal and seal wire (metal wire or fiber).

(6) The AC connection, the sensor input connections, and the DC external connection shall be tamper indicating.

(7) An uninterruptable power supply (UPS) shall be provided, capable of running the entire security system in the event of mains power failure for at least four hours without any performance degradation.

(8) For mains power failures longer than 4 hours and up to fourteen days the system shall be able to operate in a reduced performance mode with the following minimum features:

- all sensors including data generators are operating;
- all triggering signals are maintained;
- all collected data are locally stored in the sensor data generators;
- all non-essential functions are switched off to save power.

(9) After UPS power is depleted and upon return of mains power, the system shall restart in its normal operating configuration and data collection shall resume.

(10) The sensor head and data generator shall meet the requirements of the Euratom-IAEA document [9]for “High Class”.

(11) A removable mass storage device shall be provided so that system data, such as raw data, system and components identification data, event tables, and performance data, can be easily retrieved. The removable mass storage device shall be light, rugged and easily transportable.

(12) TCP/IP connectivity shall be the standard for connections between data acquisition systems.

(13) Data generators shall have a direct LAN (local area network) connection to the data collection system. For long distance and small data volume transfer a RS485 connection may be a potential alternative to the LAN.

(14) In case of failure of the data collection system or of the connection between the data collection system and data generators, data shall be stored locally in the data generators having a storage capacity of 100 days.
NDA sensors (when used in Measurement mode) generate usually large amounts of data (pulse trains, gamma spectra). For secure use in unattended measurement mode, to fulfill this condition (14) and other requirements, like Hardware Requirements 1,2,3,4, NDA data generators must be designed to incorporate the adequate data storage capacity.

(15) As far as feasible, the unattended monitoring system shall use the following standardized components:

- system enclosures
- uninterruptible power supply
- data collection computers
- external and internal cabling
- connectors
- cable entries
- patch panels
- breakers
- power terminators
- accessible controls
- junction boxes
- battery and battery enclosures
- detector assembly enclosures.

Details regarding these standardized components are to be provided by the Inspectorates to the Developer.

5.3 Software Recommendations

(1) The user software shall be designed to provide for easy operation and use by the safeguards inspector carrying out inspections in nuclear facilities.

(2) Software shall be implemented so that the system shall automatically start/restart after interruption of normal operations, such as power failures, without a need for the inspector to load/reload the operating software.

(3) Data shall be protected from loss during such interruptions.

(4) The software must have built-in diagnostics for both the software and hardware parameters. It must also include a self-monitoring feature to check the correctness of its setup.

(5) For NDA systems in measurement mode, the system shall provide all QC information (from calibration, re-calibration, long term follow-up) which were incorporated in the procedures of use of the system.

(6) The system shall provide visual indicators that can be clearly seen at the time of servicing by the inspector as to whether an error has occurred during the unattended monitoring interval.

(7) The system shall produce a performance summary file, the contents of which can be easily viewed on the monitor screen during service. The summary file shall be created regularly (e.g. daily), and any time when requested.

(8) After the inspector has completed servicing, the system shall provide a visual indication of correct setup to indicate that the system is fully operational. If the system is not operational, an indication of the fault shall be provided.

(9) An easy method of software verification, following repair or maintenance, shall be provided.

5.4 Data Recommendations

(1) Data must be date and time stamped by the data generators at the time of collection.

(2) Data must be retrievable on site upon demand of authorised personnel.

(3) If remote monitoring is provided, temporary storage of data in the case of transmission failure on a non-volatile, highly reliable medium is necessary. These data must be transmitted automatically to an authorised requester when communications are restored.

(4) State of health data of the monitoring system shall be stored in a non-volatile memory at selectable intervals.

(5) In case of remote monitoring, the performance summary shall be transmitted on request to an authorised requester at Headquarters.

(6) For ease of use, the reports shall be concise and unambiguous. The use of graphical methods to display information is encouraged.

(7) The data retrieved by the data collection computer shall be complete and not have any missing records.

(8)

(9) State of health data showing system status and safeguards data shall be stored simultaneously.

(10) Authentication information shall be embedded into the data record as or before it is emitted from the data generator.

5.5 Information Security Recommendations

(1) The information (messages, data, images, etc.) from which safeguards conclusions are drawn shall be independent and genuine.

(2) All safeguards relevant information, transmitted from the item under safeguards to the Inspectorate‘s review station, shall be authenticated by an approved method. Authentication of the data shall assure that genuine information is transmitted by an authorised source or device and has not been altered, removed or substituted.

(3) All software triggering signals shall be authenticated.

(4) When authentication cannot be implemented directly on a sensor, an approved physical system of tamper indication must be used between the sensor and the point at which authentication is applied.

(5) All information shall be handled in accordance with the Inspectorates‘ procedures for protection of safeguarded and other sensitive data.

(6) In case of remote transmission, data must be encrypted, with an approved encryption method, prior to leaving the facility to provide the Inspectorate and the State assurance that confidentiality is maintained. Proprietary encryption methods shall be specifically approved by the Inspectorates.

(7) Data authentication shall pass a third party vulnerability assessment.

5.6 Reliability Recommendations

(1) To the extent possible no single point failure shall cause loss of safeguards information.

(2) The point estimate MTBF shall be at least 150 months.

5.7 Documentation Recommendations

(1) Engineering drawings shall be supplied by developers to show how the equipment in a system is interconnected.

(2) Component lists must be provided showing the manufacturer and model of all components and recommended maintenance spares required by the Inspectorates.

(3) The following documentation shall be prepared by the responsible party/parties, then reviewed and approved by the Inspectorates:

- User Requirements/Specifications (prepared by Inspectorates)
- Functional Specifications
- Design Specifications
- Quality Assurance Plan
- Safety Analysis and Evaluation
- Manufacturing test programme, procedure and results
- Operating Manual including troubleshooting
- Maintenance Manual
- Software Code and Documentation
- Calibration Procedures
- Acceptance Test Plan and Procedure
- Training Manual for Inspector
- Training Manual for Technician

6. REFERENCES

[1] ESARDA Working Group on C/S, Report of the Workshop on C/S Safeguards Techniques Applicable to the Intermediate and Long-Term Storage of Irradiated Fuel, 14th Annual ESARDA Meeting, ESARDA 25, 1992, p. 75-89.

[2]. P. Schwalbach, M.T. Swinhoe, P. Chare, W. Kloeckner
A Survey of Integrated Unattended NDA Instrumentation used routinely by Euratom Safeguards Directorate Proceedings INMM Phoenix, USA, 1997

[3] P. Schwalbach, P. Chare, T. Girard, L. Holzleitner, S. Jung, W. Kloeckner, E. Roesgen, A. Smejkal, M. Swinhoe:
"RADAR" : The Standard Euratom Unattended Data Acquisition System,
Proceedings Symposium on International Safeguards, Wien, 2001.

[4] DRAFT Essential User Requirements for Safeguards Unattended Monitoring Systems, International Atomic Energy Agency, Vienna, 21 February 2000.

[5] K.J. Gaertner et al.; The Design and Testing of a Digital Video Data Authentication and Encryption Device, Proc. 37th INMM Annual Meeting, 1996.

[6] G. Neumann et al.; The Use of Smart Sensors and its Implications on Safeguards Procedures, Proc. 38th INMM Annual Meeting, 1997.

[7] J. Stein, A. Guerguiev, H. Brands, A. Kreuels, B. Richter, M. Aparo, R. Arlt, P. Schwalbach
Design Concept of the Digital Unattended Multi-Channel Analyzer, Proc. 43rd INMM Annual Meeting, 2002.

[8] Workshop on Integration of Safeguards Equipment Systems, Minutes, Niagara Falls, 7-9 April 1999, Release 1, IAEA, Vienna, April 1999.

[9] IAEA-Euratom “Common Qualification Test Criteria for New Safeguards Equipment”, version 2.0, January 2002.