

Next Generation Surveillance System

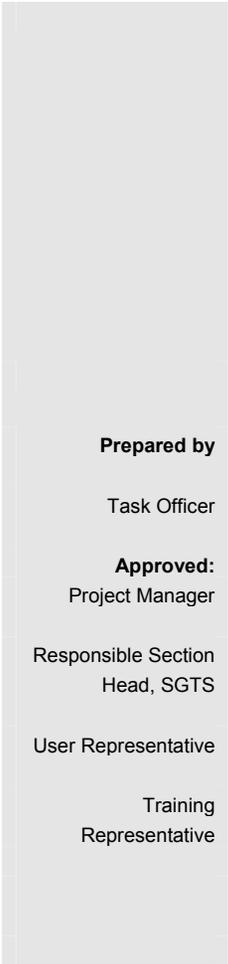
User Requirements Document

Version 0.1
September 28, 2003

Check required approvals and modify as necessary

Prepared by	Date
Task Officer	_____
Approved: Project Manager	_____
Responsible Section Head, SGTS	_____
User Representative	_____
Training Representative	_____

Division of Technical Support
Department of Safeguards
International Atomic Energy Agency



1. Task Summary

Task Name			
Task Code			
Task Officer		Phone	
Bldg/Room		Mail stop	
Customer/User		Phone FAX/e-mail	
Address			
Task Dates	XX/XX/XX→XX/XX/XX		(Start → End)

2. Revision History

Version	Date	Comments
X.X	XX/XX/XX	

3. Table of Contents

1. Task Summary	ii
2. Revision History	ii
3. Table of Contents	iii
1. Purpose of the Intended System	1
1.1 Problem Description	1
1.2 NGSS Intended Purpose	1
1.3 NGSS System Analysis Organization	2
1.4 NGSS Architecture and Construction Overview.....	3
1.5 NGSS Operations Overview.....	6
2. NGSS Requirement	10
Appendix A.....	29
Appendix B.....	34

1. Purpose of the Intended System

This system is being developed for the Section for Installed Equipment, Division of Technical Support in accordance with SGTS policies and procedures for equipment development.

1.1 Problem Description

The IAEA requires a standard surveillance system for a 10-year period starting in 2006. The system addresses the IAEA's need to observe activities that involve declared nuclear materials at facilities of Member States and to record authenticated data upon which safeguards inspectors can draw conclusions of Member States' compliance with international safeguards treaties and protocols.

1.2 NGSS Intended Purpose

The purpose of the Next Generation Surveillance System (NGSS) is to observe ongoing activities involving known quantities of nuclear material at nuclear facilities of Member States and to record those activities so that IAEA inspectors can review the data and draw conclusions regarding a facility's compliance with international safeguards treaties and protocols. The system will operate in unattended and remote modes to: 1) gather relevant safeguards data in a timely manner; 2) minimize the number of inspectors required to verify safeguards and; 3) minimize the time that inspectors must spend working in radiation fields or contaminated areas. The NGSS is expected to operate for a period of 10 years after installation.

The NGSS may be installed in different configurations depending on the complexity of the process being monitored and the size of the facility. In its basic configuration, the NGSS will comprise an image-taking device (ITD), most likely a camera, and a computer processor to generate data. These two components will be housed in a sealable tamper-indicating enclosure (STIE) that can be accessed only by authorized personnel. The NGSS will take images at intervals specified by IAEA safeguards inspectors and will record an authenticated image on electronic media. This media will reside in the image data generator enclosure for a period of up to 396 days before a safeguards inspector retrieves the media. When image data is transferred outside the STIE, it will be encrypted. An IAEA inspector will perform all preventative maintenance on the NGSS unit while he or she is at the facility performing inspection activities.

Depending on the operational requirements, NGSS subsystem components can include radiation hardened cameras, radiation tolerant cameras, gamma cameras, a data consolidator, a tamper-indicating conduit, a data review station, software to assist the inspector with data analysis and with determining the possibility of a diversion of nuclear material, tamper resistant and tamper indicating equipment enclosures, and diagnostic software. The system may operate as a stand-alone system or as a subsystem of a large integrated system comprising radiation monitors, video surveillance, and other sensors, such as balanced magnetic switches or heat sensors, operating over an Ethernet using TCP/IP communications protocol. Networked sensors may trigger NGSS image data generators. NGSS image data generators may be located either inside facilities where they could be subjected to extreme temperatures, humidity, and radiation levels or outdoors where they will be subjected to snow, ice, rain, and fog.

1.3 NGSS System Analysis Organization

To facilitate system analysis, the IAEA divided the NGSS into four subsystems: Image Data Generator subsystem, Data Consolidator and Review subsystem, Structure and Support subsystem, and General Requirements subsystem. The Image Data Generator subsystem addresses the functional requirements of: ITD performance, features, and optics; image processing; data storage; data file management; and data authentication and encryption. The Data Consolidator and Review subsystem addresses the requirements associated with consolidating data from a variety of instruments and sensors and with processing review images and other safeguards data. The Structure and Support subsystem addresses the requirements related to equipment enclosures and connections between subsystems. The General Requirements subsystem addresses those requirements such as safety, security, and standardization that apply to all subsystems. In addition to organizing requirements by subsystem, the IAEA grouped similar requirements into one of 44 different requirement-type categories. Subsystems and requirement types were defined simply to facilitate system analysis. NGSS system designers are free to configure system components to optimize system performance, ease of fabrication, and cost.

1.4 NGSS Architecture and Construction Overview

The NGSS will use a flexible architecture to allow the IAEA to install the system as a single image data generator in an STIE operating in unattended or remote mode, or as a subsystem of a large, integrated network comprising a minimum of 32 image data generators, radiation monitors and other sensors, such as balanced magnetic switches or heat sensors, operating on an Ethernet using a TCP/IP communications protocol. Figures 1 and 2 depict two possible configurations for the NGSS.

The NGSS camera will be a digital, color ITD that uses an industry-standard mounted lens. In all likelihood, there will be two types of ITD electronics: one that is radiation hardened and one that is radiation tolerant. The ITD will work in a low-light environment to accommodate those occasions when facility lighting is poor. Although each facility under safeguards surveillance is responsible for providing lighting for the surveillance system, the IAEA understands that there may be times when the lighting at a facility may be less than optimal due to lighting system malfunctions or operator error

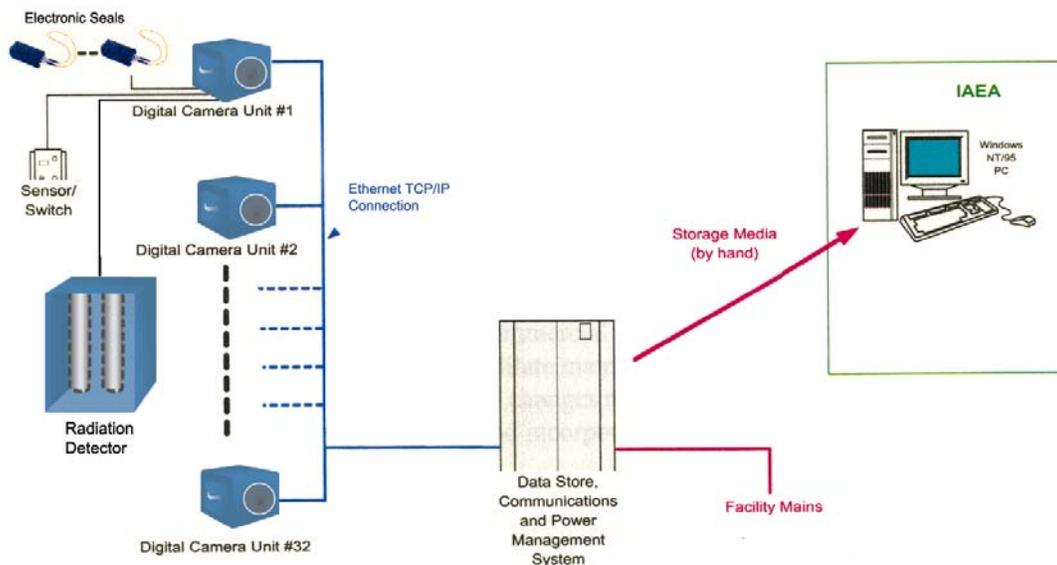


Figure 1 Possible NGSS configuration for Unattended Mode Operation

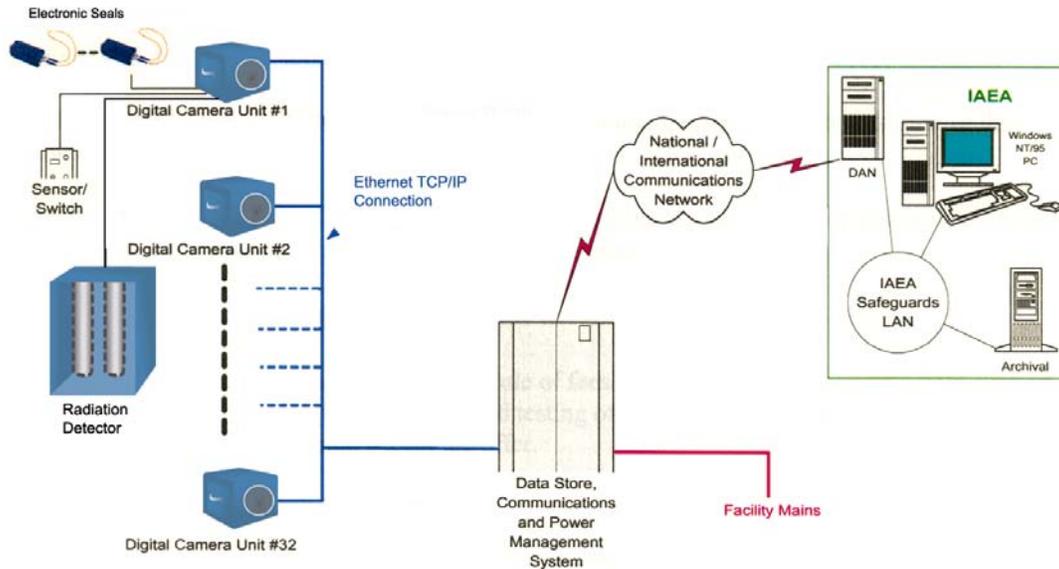


Figure 2 Possible NGSS Configuration for Remote Mode Operation

and it will take some time before the facility can take corrective action to return lighting levels to normal. The NGSS must continue to capture images in these situations so that safeguards inspectors can draw safeguards conclusions. The IAEA requires that the ITD be Ethernet capable. In the event that the ITD is not Ethernet capable, a device should be designed that can attach to the ITD to allow it to transmit data over an Ethernet. The ITD should use an industry standard connector to the data generator. The IAEA understands that no standard connector exists today, but the IAEA must have the ability to change ITDs as a module so that they can reconfigure the NGSS to meet unique installation requirements.

When required, the data generator captures an image from the ITD for processing. The image will be date and time stamped at time of collection and will be authenticated so that it can be proved to be genuine. The image data generator will also encrypt the image. The image and all supplemental information will be stored in non-volatile memory in the image data generator. The image data generator will store the image and supplemental information data in two files. One file will contain the image and all supplemental information. The second file will contain only the supplemental information. This data file configuration is necessary to allow IAEA technicians, who are not authorized to view safeguards information, access to State of Health (SoH) and other critical system setting information. The

image data generator will store up to 13 months of pictures in memory. Assuming that a picture is taken every 5 minutes and each image is approximately 50K in size, the memory required is estimated to be 4 Gigabytes.

The image data generator enclosure protects the ITD and data generator from dust, moisture, and corrosion. The enclosure system will be tamper indicating and will be designed to accept standard Agency seals. The Agency requires that the system be able to detect a tamper event, log it in non-volatile memory, and take a picture. The IAEA desires that the camera enclosure be mounted on a platform that can be attached to the facility walls using hardware that supports the existing surveillance equipment. Using existing hardware will obviate the need for drilling new boltholes in facility walls. Obtaining permission to drill holes in facility walls and the work itself is difficult and is best avoided if possible.

When the NGSS is installed in areas where there is a low radiation field, the ITD and data generator may be contained in a single enclosure. For this type of installation, both the ITD and the data generator must be radiation tolerant. For NGSS installations in high radiation fields, the IAEA assumes that the ITD will be radiation hardened and the data generator will be radiation tolerant. For this type of installation, the data generator will need to be located outside the high radiation fields. In this case, the ITD and data generator enclosures may be two structures connected by a secure communications channel. The secure communications channel may be a cable inside a tamper-indicating conduit or a new technology identified by the system designer. The issues of radiation hardening the data generator and securely connecting the camera with the data generator are design issues that will be left to the NGSS system designer, subject to the approval of the IAEA.

It is important to protect safeguards data to ensure that no one tampers with it and that no unauthorized personnel may view the data. To this end, the Agency requires that all images be encrypted. Further, the Agency requires that the system provide protection to mask data transmissions so that unauthorized personnel may not gain knowledge of system settings, such as picture taking intervals, through an analysis of data transmissions between the Data Generator and the Data Consolidator. The Agency must approve all data security schemes.

The NGSS will work in unattended and remote mode. The NGSS may be configured to run as a single system or as a

subsystem of a network of safeguards instruments on an Ethernet using TCP/IP communications protocols. The NGSS will be able to be triggered by other instruments on the network. The date and time of all trigger events will be logged so that they can later be correlated to other system data. When selecting a technology for networking the NGSS, designers must address a variety of technical, political and administrative constraints. Building codes and construction standards vary by facility and by country. What may be accomplished easily in one country may be difficult to accomplish in another. NGSS network designs are subject to facility approval prior to installation and must meet local quality assurance requirements and construction standards. There may be problems obtaining facility approval if the network requires significant conduit runs and wall penetrations. The cost of installing the network in an existing facility will also constrain the solution. The IAEA recently made a significant capital investment for installing cables in some facilities to support DMOS installations. Because of the amount of money invested in the DMOS cable systems, the Agency desires to use these existing DMOS cable systems in any future NGSS network if possible.

1.5 NGSS Operations Overview

IAEA safeguards inspectors are generally satisfied with the DCM-14-based surveillance systems and the GARS review system. When they were asked what features that would like to see in the NGSS, they expressed their thoughts in terms of modifying the present DCM-14-based system rather than starting with an entirely new approach. Designers should not infer from this statement that the IAEA is not open to new approaches. Rather it means that designers should be familiar with the operation of the existing surveillance systems and image review system when considering the design of the NGSS. The following paragraphs provide supplemental information that expands upon or interprets information in Section 2, NGSS Requirements. The IAEA's intent is to communicate to the designer specific surveillance problems that the IAEA is trying to solve, to explain the conditions and constraints that bound the IAEA's problems and needs, and to explain the basis for some of the NGSS requirements.

IAEA inspectors desire operator aids to guide them as they start up, shut down, and service the NGSS system, and as they retrieve images. The operator aids should be simple, straightforward, and based on the English language. IAEA inspectors must operate and service a wide variety of safeguards instruments and equipment, many of which have

multiple models and operating systems and are installed in the field in many different configurations. It is difficult for inspectors to maintain proficiency on all safeguards systems and, by extension, to do their job with a high degree of confidence. The use of operator aids or wizards will help the inspectors do their job better and will increase system reliability. Inspectors would also like the NGSS to assist them with administrative activities that they presently perform manually. The administrative activities that the inspectors identified include completing inspector and facility-specific information on reports and data forms and conducting NGSS subsystem equipment inventories.

Black images and poor image quality due to inadequate lighting in facilities under safeguards is a continuing problem for IAEA inspectors. Facilities are required to provide lighting for IAEA surveillance systems but, for a variety of reasons, adequate lighting is problematic. In some instances, the facility experiences an unexpected power loss. In other instances, facility operators simply turn the lights off to conserve power or to support plant testing. Over the past 6 years, there have been 12 occasions where facility lights were turned off for a period greater than 30 hours. Regardless of the cause, inadequate lighting can defeat an optics-based surveillance system. The IAEA must address the issue of maintaining surveillance under low-light conditions. Although the IAEA intends to work with Member States to reduce lighting outages, the NGSS must be able to capture images in less than optimal lighting conditions. Infrared devices may be considered, but broad use of these devices will be constrained by cost and by the difficulty of tuning the system to the wide spectra of frequencies of interest. Supplemental lighting systems may be considered, but they will be constrained by the size of the backup battery system. Other technologies should be considered to assist the Agency with the problem of maintaining surveillance during periods of little or no light.

The NGSS image review system should include analysis tools to facilitate effective review of facility images. Tools that help an inspector review a greater number of images per unit of time and that assist the inspector in resolving ambiguities in images are most valued. One analysis tool feature proposed by safeguards inspectors is the ability to superimpose facility-design information or a reference image over the ITD image to identify objects in the ITD image. Another feature is the ability to correlate data from other sensors to understand more completely the activities that the inspector is seeing on the screen. Inspectors identified the need to streamline the image documentation process to

allow them to document their observations and conclusions directly on the image as they conduct their reviews. These examples are presented here to illustrate the types of tools that the inspectors desire. It is not a comprehensive list of tools and features.

Windows XP is the IAEA standard operating system for personal computers. The IAEA understands that Microsoft will eventually replace Windows XP with a new operating system. For NGSS planning purposes, the IAEA assumes that when Microsoft replaces Windows XP, the IAEA will upgrade to the new Microsoft operating system, whatever it may be. If the NGSS designer plans to use a personal computer in the NGSS, this computer's operating system must be Microsoft-based and approved by the IAEA. If no personal computer is to be used in the NGSS, the designer is free to choose an operating system providing that the data generated by the NGSS for review can be processed by an inspector's personal computer, which will be running a Microsoft-based operating system.

In order to facilitate maintenance in the field, the IAEA requires that the NGSS use a modular design so that system components and subsystems can be easily replaced in the field. Further, the IAEA requires that system components be plug and play. For the NGSS, this means that the NGSS will recognize when a component is replaced and will automatically configure the new component. It also means that the NGSS will recognize when a new component, such as a new ITD, is installed and will automatically configure that device. When determining component layout and subsystem accessibility, the designer should assume that maintenance and installation in the field must be accomplished by a qualified person, wearing protective clothing and gloves, and working in a radiation field.

The NGSS must be thoroughly tested in accordance with the Common Qualification Test Criteria for New Safeguards Equipment. Safeguards inspectors universally agree that they could not lose safeguards data as the results of instrument failure in the field. With the advent of integrated safeguards, it is possible that some surveillance systems may be operating for 18 months before an inspector or Agency technician will have the opportunity to check or service the system.

The NGSS must co-exist with sensors presently installed in facilities worldwide and be able to retrieve and review data files stored in the present IAEA approved file format. The Agency has more than 800 surveillance systems in use. In some facilities, sensors are located in areas where personnel

access is available only once every few years. It is probable that the circumstance will arise where a facility's surveillance system is upgraded to the NGSS, but not all sensors can be replaced at the same time because some are inaccessible. The NGSS must be able to process the image data from the old sensor so that inspectors can review the images.

Construction of the NGSS must meet TUV Rhineland and CSE standards. The IAEA understands that there are conflicting requirements between these two standards. When conflicts arise, the IAEA will decide on a case-by-case basis which standard will take precedence.

The IAEA requires that image data files use a published or open standard file format. The basis for this requirement is that the IAEA wants to have the flexibility to add new information to the image file and does not want to be constrained by proprietary data file format. Using a file format based on a published standard, such as jpeg, is one way of assuring that the IAEA will have the flexibility that it desires.

The IAEA will be implementing a public key infrastructure (PKI)-based cryptography system using X.509 certificates for the new surveillance system. This will alleviate many of the problems associated with symmetric authentication and encryption by eliminating the need to use the camera's secret authentication keys in computers in the field. Although private encryption keys must still be used in the field, their potential for exposure will be minimized through the use of FIPS 140 certified PKCS #11 cryptographic tokens.

The IAEA recognizes the operational desirability of allowing commands, keys, and even firmware updates to be sent to the cameras over the network, and will be working toward developing secure methods for accomplishing this. However, the security risks associated with this capability are very high and deployment of this capability will be delayed until extensive vulnerability assessments are performed. It is possible that this capability will not be implemented in the initial deployment of the system, but the system must be designed with the functional capacity required to include this functionality without a hardware redesign.

2. NGSS Requirements

This section lists NGSS general requirements and capabilities. There are 37 general requirements. General requirements are identified by a number (2.X) and are **bolded**. Each general requirement has at least one capability statement that clarifies the general requirement or provides additional details. Capability statements are listed under their associate general requirement. NGSS capabilities have been designated as 1) Required, 2) Desired, or 3) Optional.

2.1 Image data generators must support several resolutions in colour. The minimum resolution should allow safeguards inspectors to observe a fuel assembly measuring 20 cm by 20 cm by 8 meters from a distance of 10 meters.

- 2.1.1 With the camera viewing a standard resolution chart and under optimal lighting, the system (camera to review) shall be able to resolve horizontal lines at the following resolution settings for monochrome: High resolution - 400 lines (horizontal) with 256 gray scale levels; Medium resolution - 300 lines (horizontal) with 256 gray scale levels; Low resolution - 200 lines (horizontal) with 256 gray scale levels; With the camera viewing a standard resolution chart and under optimal lighting, the system (camera to review) shall be able to resolve horizontal lines at the following resolution settings for colour: High resolution - 400 lines (horizontal) with 4:2:2 YUV; Medium resolution - 300 lines (horizontal) with 4:2:2 YUV; Low resolution - 200 lines (horizontal) with 4:2:2 YUV {Based on present needs and technology}
- 2.1.2 System shall be able to display a single fuel pin of width ____ cm at a distance of ____ m. {Required}
- 2.1.3 The ITD shall have the following dynamic ranges: Colour: Internal auto gain 6 dB ratio 1,000:1 (with auto iris); Monochrome: Ratio 10,000:1 at 555nm (nominal). {Required}
- 2.1.4 The ITD shall have an auto-iris response time of <0.1 seconds at 555 nm. {Required}
- 2.1.5 The ITD shall have an aperture range (typical) of 10,000:1 at 555nm. {Required}

- 2.1.6 The image data generator shall be capable of accommodating viewing angles in the range of 30 to 100 degrees while accommodating optical filters and a hood. {Required}
- 2.2 Image format must conform to a published or open standard (e.g., jpeg 2000).**
- 2.2.1 Image format must conform to an industry standard. {Required}
- 2.3 The image data generator will be capable of operating independently in a stand-alone mode as a subsystem of a large integrated system comprising multiple cameras, radiation monitors, and balanced magnetic switches while communicating over a sensor network.**
- 2.3.1 The NGSS shall be capable of collecting images and data from a minimum of 32 image data generators without reduction in any image data generator's individual performance. {Required}
- 2.3.2 Instruments shall have the capability to trigger other instruments via a network. {Required}
- 2.3.3 When operating in an integrated system, daily time synchronization and a common time base shall be provided for all subsystem clocks to within +/- .5 seconds. When compared to an international time standard, the drift of the network time base must be less than 1 second/day. {Required}
- 2.3.4 The image data generator will be capable of operating independently in a stand-alone mode as a subsystem of a large integrated system comprising multiple cameras, radiation monitors, and balanced magnetic switches while communicating over a sensor network. The system should operate with a minimum of 32 cameras. {Required}
- 2.4 The NGSS should be plug and play to achieve the replacement of sensors and the addition of new hardware.**
- 2.4.1 The NGSS should be plug and play to achieve the replacement of sensors and the addition of new hardware. {Required}

2.5 Memory shall be expandable via a plug-in module.

2.5.1 The image data generator's memory shall be scaleable in both individual recording sub-unit capacity as well as the number of units which can be combined easily to provide the most cost-effective data storage configuration. {Required}

2.6 The NGSS shall be modular.

2.6.1 The system should be easily serviced in the field by incorporating a modular design. {Required}

2.7 Each image data generator shall have its own accessible, non-volatile, plug-in memory which has a minimum capacity of 4GB and which has the capability of being upgraded to at least 32GB.

2.7.1 The image data generator's non-volatile memory media shall be replaceable without requiring the image data generator to be powered down or requiring any portion of the NGSS to be stopped. {Required}

2.7.2 All image data generators shall have at least 4GB of non-volatile memory. {Required}

2.7.3 Efficient access should be provided to the information stored on removable media in individual components and/or subsystems. {Required}

2.7.4 An image data generator's data storage capacity must be able to store data in an unattended mode without data retrieval for at least 396 days. {Required}

2.7.5 The NGSS data storage shall be scaleable to provide cost-effective capacity for the connection of a minimum of 32 image data generators in various operational modes. {Required}

2.8 Data (images, events, messages) and SoH information shall be stored separately with different access privileges in non-volatile memory accessible to a PC.

2.8.1 State of Health file shall contain the following data: date/time of loss of mains power; date/time of restoration of mains power; date/time of low battery voltage; date/time of battery voltage restoration; watch dog actuated flag; watchdog implemented flag; date/time and value of high and low

temperature and humidity readings; cabinet status (open or closed). {Required}

2.8.2 SoH information regarding the operation and performance of the ITD shall be contained within each image and data file. {Required}

2.8.3 The data file (images, events, messages) and SoH file (performance and critical indicators) shall be stored separately and together, with a different access privilege, in non-volatile memory accessible to a PC. {Required}

2.8.4 SoH data of the monitoring system shall be stored in non-volatile memory at a selectable interval within the range of 1-3600 seconds. {Required}

2.9 Data files shall contain sufficient information to allow safeguards inspectors to draw safeguards conclusions.

2.9.1 The data file shall include the following data types and allow for additional user specified data types: image data (compressed); image number; time; date; storage media identification number; time interval; triggering source; environmental data; tamper events; NGSS camera unit inventory number; camera unit module inventory numbers (if required); number of recordings during the surveillance period; software self-diagnosis results; date/time of temperature and humidity extremes for the entire surveillance period; recording interval; surveillance period start; information security elements; file format; file length; image size (in bytes); software version; firmware version; checksums; ID of the device requesting images or data; video standard; resolution; image compression algorithm; performance monitoring values of critical voltages and currents; performance monitoring values of critical temperature values (present, highest, lowest); information on external power outages (start/end date and time); status of camera battery; camera error events; save error events; and local interface error events. {Required}

2.10 NGSS sensors shall communicate over an Ethernet using the TCP/IP stack.

2.10.1 The system shall be Ethernet-based using the TCP/IP communication protocol. {Required}

2.11 The NGSS shall ensure that all data and commands are genuine and confidential.

- 2.11.1 After the vulnerability assessment and any subsequent security reviews have been completed, the security critical components of the software shall be compiled using a trusted compiler so that the Agency is assured that the executable code comes from the source code that has been reviewed. The Agency shall maintain the master copy of the executable, and no further changes to the security critical executable code can be permitted without another security review and/or another vulnerability assessment. For this reason, it is highly recommended that the security critical components of the software be implemented as completely separate executable programs that can be run independently from any other software that may require changes for operational reasons. {Required}
- 2.11.2 The camera shall store the Certificate Authority's (CA) key in secure storage to prevent substitution of an unauthorized key. {Required}
- 2.11.3 The camera shall support two-key Triple DES, 128 bit AES, and 256 bit AES encryption and decryption. {Required}
- 2.11.4 The camera shall support DSA signatures and 1024 bit and 2048 bit RSA encryption, decryption, and signatures. Encryption will use RSA envelopes. The hash function shall be SHA-1. {Required}
- 2.11.5 All cryptographic functions shall be implemented to allow the corresponding functions that require private or secret keys to be performed on PKCS#11 tokens. {Required}
- 2.11.6 The camera shall include multiple public encryption keys. Timed images will be encrypted using one public key, and triggered images will be encrypted using the public key assigned to that trigger source. This allows the sharing of subsets of the images with the host without compromising the security of the other images. {Required}
- 2.11.7 The ability to upgrade software and issues commands remotely shall be done only if multiple levels of secure communication protocols are used to authenticate the data transmitted to the device. {Desired}
- 2.11.8 The camera shall accept all commands and keys sent over the local command port, which can only be accessed by opening the camera's STIE, but will only accept commands

sent over the network after verifying their authenticity cryptographically. {Required}

- 2.11.9 Images and data shall be encrypted using certified strong encryption methods which provide a target assurance level according to the Common Criteria for Information Technology Security Evaluation or Information Technology Security Evaluation Criteria (ITSEC). The implementation of the encryption methods must be approved by an independent third party analysis. Loss of power shall not cause the loss of an encryption key. {Required}
- 2.11.10 For systems developed for the Agency, the system shall provide the ability to verify the integrity of security critical system firmware using a user-supplied key and the firmware's ROM image to generate a cryptographic message authentication code (MAC). {Required}
- 2.11.11 If authentication cannot be implemented directly on a sensor, a credible physical or electronic system of tamper indication must be used between the sensor and the point at which authentication is applied. {Required}
- 2.11.12 Authentication information shall be embedded into the data record as or before it is emitted from the image data generator enclosure. {Required}
- 2.11.13 All safeguard relevant information, from the item under safeguards through to the inspectorate review station, shall be authenticated by credible means. Authentication information shall be embedded into the data record as or before it is emitted from image data generator enclosure. The authentication method should be capable of withstanding a level of threat comparable to that which could be undertaken by a national authority. Authentication of the system shall assure that genuine information is transmitted by an authorized source or device and has not been altered, removed or substituted. The IAEA will approve the authentication scheme depending on a positive outcome of an independent third party analysis. If commercially available data authentication equipment is used, a third party analysis will not be required if the equipment has been certified as complying with FIPS-140 level 2 (if used inside an Agency approved tamper indicating enclosure) or FIPS-140 level 3 (if an adversary might have access to the equipment at any time) OR a Common Criteria certification to a Protection Profile giving equivalent security functionality. The equipment must be used exactly as specified in the Security Policy under which it was evaluated. {Required}

- 2.11.14 At the time of collection, the data generators shall date and time stamp the data to within +/- 0.5 seconds of time on the local system server. {Required}
- 2.11.15 Data generators shall have a direct Ethernet connection to the Data Collect system. All unused ports and functions must be permanently disabled for security purposes. {Required}
- 2.11.16 All triggers must be authenticated. {Required}
- 2.11.17 In case of remote transmission, data must be encrypted, with a certified encryption method, prior to leaving the facility. A certified encryption method provides the Agency and the State assurance that confidentiality is maintained. Proprietary encryption methods must be specifically approved by the IAEA. Certification of the algorithms and methods must come from either the National Institute of Standards and Technology or the Common Criteria, other certifications may be considered by the IAEA. {Required}
- 2.11.18 Review of images and data shall only be available to authorized users using access control to positively identify the user and encryption keys to secure and authenticate only those images and data to which the user has access. It shall be possible to provide separate access controls key groups. Review of images must be done in the field and the access to those is controlled by private keys. The method of protection of the confidentiality of those keys used in the field must be approved by the IAEA. If the encryption system is appropriately implemented, this decryption can be accomplished using certified PKCS#11 tokens without exposing the private keys in the field. {Required}

2.12 Individual subsystems shall indicate any effort to tamper with the NGSS.

- 2.12.1 System shall employ active intrusion detection with remote reporting for the image data generator enclosure. {Required}
- 2.12.2 Tampering with an image data generator shall be detected and recorded. The detection of a tamper shall trigger an image and data file. Details of that tamper shall be stored securely within the image and data file. {Required}
- 2.12.3 At no point shall it be possible for unauthorized personnel to gain access to those images and data (where encryption is implemented) or to alter, remove, insert or substitute those images or data without detection. {Required}

2.13 The image taking device shall operate under the environmental conditions specified in Common Qualification Test Criteria for New Safeguards Equipment Version 1.0

2.13.1 The image taking device shall operate under the environmental conditions specified in Common Qualification Test Criteria for New Safeguards Equipment Version 1.0 {Required}

2.13.2 The camera units will be capable of operation in radiation fields up to 2 MRad (gamma) integrated over a 10-year lifetime. {Required}

2.13.3 The system must be able to operate in a radiation field of _____ neutron and _____ gamma. {Required}

2.13.4 The image taking device shall operate under the environmental conditions specified in Common Qualification Test Criteria for New Safeguards Equipment Version 1.0 {Required}

2.14 The image taking device will detect and record activity under conditions of low light.

2.14.1 Sensitivity (max): Must be capable of operation at the following lighting levels (10% of initial set-up: Colour: Minimum 5 lux (no filter or only with colour balancing (mired) filters) Recommended 200 lux Maximum: 1000 lux Monochrome: Minimum 0.5 lux (no filter) 5.0 lux (with IR filter) Recommended 200 lux Maximum:1000 lux. {Required}

2.15 An additional image data generator enclosure will be designed to allow the camera to operate underwater to monitor fuel assemblies in the spent fuel pool.

2.15.1 An image data generator enclosure will be designed to allow the camera to operate underwater to monitor fuel assemblies in the spent fuel pool. {Required}

2.16 The NGSS should operate on power systems worldwide without the need for manual intervention.

2.16.1 Automatic start and restart shall occur after interruption of normal operation due to power failure without inspector loading or reloading software. {Required}

- 2.16.2 The power system must comply with international standards and meet TUV Rhineland standards. {Required}
 - 2.16.3 There should be only power conversion stage from the mains to 24 VDC. {Required}
 - 2.16.4 The IDT should function on all lighting systems based on DC and on 45 Hz - 75 Hz AC. {Required}
 - 2.16.5 The NGSS must be capable of operating from mains power supplies, over the range of 85Vac – 250Vac and frequency ranges of 45 Hz to 70 Hz, without having to change the internal power supply and without requiring a manual voltage select switch. {Required}
 - 2.16.6 Over-voltage protection and over-current protection shall be provided where the image data generator is connected directly to the local mains. {Required}
- 2.17 The NGSS should have a backup power source to maintain operation in the event of the loss of mains power.**
- 2.17.1 Each ITD should be able to operate for a minimum period of 48 hours from a fully charged battery. The size and weight of the batteries should not exceed ___ and ___. {Required}
- 2.18 The NGSS shall generate specific SoH information and shall provide analysis tools for interpreting the information.**
- 2.18.1 The system shall generate a single SoH summary report that includes status of the seal, SOH, failed critical indicators, picture count, and file size. {Required}
 - 2.18.2 During the operation, the system image data generator shall record the following SoH information: tamper events*, power events, temperature, humidity. The asterisk denotes a critical indicator. For critical indicators, the data shall be recorded within ___ msec of event occurrence. Otherwise, the recording interval shall be once per day. {Required}
 - 2.18.3 SoH reporting shall be possible through a communication connection in the remote monitoring mode or stored to the storage media for unattended operation. Remote SoH information shall be included as part of the detailed data configured for remote monitoring. {Required}
 - 2.18.4 While operating, the system shall produce a SoH summary file, the contents of which can be easily viewed on the

monitor screen during inspector data retrieval or technician service. The summary file shall be created automatically at a preset interval (e.g. daily), on demand when requested by authorized personnel, and before servicing the equipment. {Required}

2.18.5 For an ITD operating in a radiation area, the system shall provide a means for alerting the inspector when a sensor located in a high-radiation area needs to be replaced. For a camera, no more than 5% of the picture elements may be faulted. For memory, ... {Required}

2.19 The system shall be designed for a 10-year minimum lifetime with a planned maintenance cycle of no less than 18 months.

2.19.1 Routine maintenance shall have a periodicity no less than 18 months. {Required}

2.19.2 The system shall be designed such that the maximum repair time by a trained technician is ___ hours (assembly replacement) from the time of the technician's arrival at the equipment's location. {Required}

2.20 The vendor must provide a plan to provide parts for the entire production run and for projected spare parts for the lifetime of the system. This strategy will ensure the Agency's ability to use the system for a ten year minimum lifecycle.

2.20.1 The vendor shall guarantee to support the system with spare parts for a period of 10 years following initial procurement. {Required}

2.21 The NGSS shall allow a single non-technician wearing protective double-cotton gloves while standing on a plastic or rubber coated ladder to easily install, replace, configure, or troubleshoot a subsystem without tools with the exception of the sealing method.

2.21.1 All controls shall be arranged to minimize the risk of accidental movement or inadvertent operation. Markings or calibrations (clearly labeled in the English language) shall be provided so that correct settings of the controls can be easily and quickly restored. {Desired}

2.21.2 The image data generator unit shall be less than 8Kg in weight. {Required}

2.21.3 A trained inspector should be able to perform routine maintenance on the system during regularly scheduled

inspections without the need for any tools. Specifically, no tools shall be required to remove and replace system modules and batteries. The entire self-contained system shall be less than 8Kg in weight. {Required}

2.21.4 The system shall be modular, easy to assemble, configure and operate on-site by trained but non-technical personnel who will perform installation and maintenance while wearing protective clothing and gloves. {Desired}

2.22 The NGSS will meet all safety requirements specific TUV Rhineland and CSE. Where conflicts between these two standards exist, the IAEA will resolve those conflicts on a case by case basis.

2.22.1 NGSS cables shall meet the requirements of IEC 332-3 cat. C for flame propagation. {Required}

2.22.2 NGSS cables shall meet IEC 754 for halogen content. {Required}

2.22.3 Warning labels shall be affixed to the equipment and the equipment's cover plates to indicate where hazardous voltages may exist. {Required}

2.22.4 The NGSS shall meet TUV Rhineland or CSE requirements for the class of equipment. {Required}

2.23 The NGSS shall have the ability to operate in the unattended or remote mode. The NGSS shall support local and remote data transfer.

2.23.1 While setting up for remote transfer, the system shall employ a transfer manager that shall retransmit failed transmissions at a user-specified periodicity until a retransmission is successful or a user-specified transmission period expires. If the transmission period expires, the transmission failure shall be logged. {Required}

2.23.2 The surveillance system will have the capability to transmit XX and data, upon request, to an authorized recipient. {Required}

2.23.3 A technician should be able to make global changes to the system, such as key changes or motion detection threshold. {Desired}

- 2.23.4 During remote data transfer, the data manager of the system shall track the following download statistics: download start time, download duration, and downloaded file size. {Desired}
 - 2.23.5 The system should be able to set the following parameters remotely: For the camera: 1) PTI, 2) key encryption/auth, 3) zoom setting, 4) equipment attached to the camera over a network, and 5) ping features. For the seals: 1) key, and 2) ping features. {Desired}
 - 2.23.6 The NGSS's start delay shall be selectable to up to 999 hours with visual prompt. {Required}
 - 2.23.7 The system shall allow local data removal that is accessible only by authorized personnel. {Required}
 - 2.23.8 The system shall allow data to be externally accessible on a daily basis via a TCP/IP connection. {Required}
- 2.24 The NGSS shall include a review application that correlates data from various sensors, performs automated analysis, provides search filters, provides image enhancement tools, and produces reports.**
- 2.24.1 The review software shall provide a range of temporary image enhancement tools. The minimum image enhancement tool set shall include the following: image brightness control, image contrast control, image gamma correction control, image colour saturation control (for use with colour images only). {Required}
 - 2.24.2 Inspectors shall have the ability to make comments on the data files directly in the field. {Required}
 - 2.24.3 The review software shall coordinate data obtained from all sensors. {Required}
 - 2.24.4 The image data generator shall provide automatic data entry capability to complete standard information blocks on inspections forms. Information blocks include inspector name, ... {Desired}
 - 2.24.5 The system shall automatically perform a system equipment inventory and report the results to the inspector for inclusion with this inspection report. {Required}
 - 2.24.6 The review portion of the system shall have the capability to store overlays of facility design information and it shall allow

- the use of overlays to assist the inspectors in drawing safeguards conclusions. {Desired}
- 2.24.7 If front end scene change detection is used, the scene change detection capability shall be immune to general lighting changes in the field of view which result from normal facility lighting fluctuations (up to 6 dB @ 10 Hz), seasonal lighting changes and differences in day and night lighting conditions. {Required}
- 2.24.8 During a review, the review software shall provide graphical displays (e.g., histograms) for the following data: (1) image record status vs. date/time, (2) SoH parameters vs. date/time. {Required}
- 2.24.9 Time drift shall be insufficient to cause event correlation errors. {Required}
- 2.24.10 The review software shall be capable of filtering images and data based on user-specified parameters. User-specified parameters include: 1) channel ID; 2) specific period of specifying a start date and start time and an end date and end time; 3) scene numbers; 4) events. {Required}
- 2.24.11 As part of its initialization at start-up, the review application shall test the system by comparing a specific set of stored reference images for change and no change in defined areas on interest. In the event that the system fails the test, the user shall be alerted to a possible hardware or software error. {Required}
- 2.24.12 The system shall have the capability to store up to 1000 review session set-up parameter sets for individual reviews using unique identifiers for each. {Desired}
- 2.24.13 The safeguards review software shall produce summary reports in a tab-delimited text format. The data shall include: number of images recorded between the specified start date and time and end date and time; technical events: total and specific date/time(s); SoH information from the NCDP and each connected camera unit; safeguards relevant events: total and specific date(s) and time(s); relevant safeguards data: date(s) and time(s); tamper events: total specific date(s) and time(s); errors: total and specific date(s) and time(s); missing scenes: total and consecutive with date(s) and time(s); equipment management and performance data; inspector comments from the review; environmental data; configuration data (component IDs, firmware, and software versions). {Required}

- 2.24.14 The system GUI should allow for real time viewing of data with the ability to easily go back into the data base to view stored data. {Required}
 - 2.24.15 The review software will allow the user to modify the displayed image size. {Desired}
 - 2.24.16 The review application should allow the user to specify at least __ regions of interest. {Required}
 - 2.24.17 The review system shall automatically identify scenes of uniform contrast (including black scenes), missing scenes, and scene changes. {Required}
 - 2.24.18 The software user interface will have the following controls: scroll bars, VCR emulation buttons (e.g., fast forward and reverse, pause, step forward and reverse, and stop), a toggle control to display images with and without supplementary data (SoH, technical events, etc.). {Desired}
- 2.25 The NGSS must co-exist with installed sensors and be able to retrieve and review data files stored in the present format.**
- 2.25.1 The operation of the NGSS must be compatible with the Agency's existing Remote Monitoring System data acquisition and archival. {Required}
- 2.26 The NGSS shall have the ability to automatically change parameter settings on receipt of specified events.**
- 2.26.1 For applications when there is normally low or no activity in the area, it should be possible for the system to take pictures at a higher PTI when there is activity in the room and then take pictures at a lower PTI when there is no activity. {Required}
 - 2.26.2 The camera should have scene-change detection capability. {Required}
 - 2.26.3 The system should track equipment inventory automatically. For example, equipment numbers should be automatically detected from each equipped instrument and reported in the SoH log. {Required}

2.27 The NGSS shall perform self-diagnostic checks during new equipment installation (for example, the use of wizards), periodically throughout an inspection period, and after equipment servicing.

- 2.27.1 The system will perform self-diagnostic checks. Error indicators shall be provided by the image data generator to alert the inspector should an error have occurred in the NGSS's operation during the surveillance period. Reports of NGSS's malfunctions or errors shall be communicated to and stored as a separate log file for subsequent retrieval by the inspector. {Required}
- 2.27.2 Self-diagnosis shall be performed periodically on the operating system, after equipment servicing, and after the installation of new hardware. {Required}
- 2.27.3 Self-diagnosis shall be possible for the operating system, application and on-site network communication, and for the image data generator hardware components. {Required}
- 2.27.4 As part of its initialization at start-up and at pre-selected intervals, the ITD shall perform a self test. A false result shall result in an alert to the user of a possible hardware or software fault. {Required}
- 2.27.5 The ITD should conduct self-checks to verify that no data has been lost. {Required}
- 2.27.6 After the inspector has completed data retrieval, 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. {Required}

2.28 The NGSS shall have the ability to change settings locally or remotely.

- 2.28.1 Software shall be provided to set up all the available ITD functions. That software shall be capable of running on the notebook computer with a Microsoft-based operating system. {Required}
- 2.28.2 Software must be provided which will allow the image data generator to be set up, configured and maintained, locally with a portable PC or remotely via the data consolidator in a secure manner. {Required}

- 2.28.3 The PTI shall allow for a random PTI capability with selectable maximum and minimum recording intervals. {Required}
- 2.28.4 It shall be possible to enable/disable each of the triggers using the set-up software. Trigger options, scene change detection, external timers, contact switches, gamma detect, neutron detector, electronic seals [similar to the VACOSS-type seal but final type to be decided], 5xTTL (TTL= Transistor-Transistor Logic (simple electronic switch)), and network message trigger. {Required}
- 2.28.5 For fixed-time PTI under normal operation, the picture taking interval shall be: 1 second to 4:59 minutes, selectable in 1 second intervals; 5 minutes to 60 minutes, selectable in 1 minutes steps. {Required}

2.29 The image data generator will have the ability to take an image when triggered.

- 2.29.1 Image recording lock-out: Upon the detection and recording of a trigger event or image, it shall be possible for the camera unit to ignore the next trigger signal for a selectable time interval of 0 minutes (no lock-out) up to 60 minutes in steps of 1 minute. {Required}
- 2.29.2 Upon the detection and recording of a trigger event or image, it shall be possible to store at least 2 pre- and at least 2 post-images at selectable time intervals. {Required}
- 2.29.3 Periodic alarm and trigger message generation shall cease when a valid response is received from the intended recipient of the message. {Required}
- 2.29.4 The system shall generate triggers that will cause an image to be recorded by one or more of the following: scene change detection; external timers; contact switches; gamma detectors; neutron detectors; electronic seals [similar to the VACOSS-type seal but final type to be decided]; 5xTTL (TTL= Transistor-Transistor Logic (simple electronic switch)). {Required}

2.30 The vendor will test the NGSS prior to delivery using a test plan developed by the vendor and approved by the IAEA.

- 2.30.1 The supplier will perform a reliability test on the pre-production NGSS, demonstrating that it will meet the agreed

- specifications with a minimum MTBF of 1000 months in all Agency field installations. {Required}
- 2.30.2 The image data generator shall meet the “High Class” tests specified in the Agency’s Qualification Testing of New Safeguards Equipment – Test Procedure, for countries with nominal mains supplied between 90 VAC and 250 VAC at 50 Hz and 60 Hz. {Required}
- 2.30.3 Critical components shall be subjected to accelerated life testing equivalent to a 10-year operating cycle and shall successfully pass the accelerated life testing. The 10-year operating cycle is the minimum standard. {Required}
- 2.30.4 The Supplier shall provide documentation to prove that the system is fully certified and tested prior to delivery to the IAEA. {Required}
- 2.30.5 The NGSS equipment shall successfully pass a usability assessment by an independent laboratory prior to final approval. {Required}
- 2.31 The NGSS shall be fault tolerant and have a MTBF of at least 1000 months.**
- 2.31.1 The system shall tolerate a failure of a low-level module without resulting in complete system failure. The MTBF is 1000 months. {Required}
- 2.32 The IAEA must be able to develop the NGSS and maintain it with the resources presently available in their budget for surveillance systems.**
- 2.32.1 The IAEA must be able to develop the system and maintain it with the resources presently available in their budget for surveillance systems. The development costs should not exceed X and the annual maintenance spare parts budget should not exceed Y. {Required}
- 2.33 If a personal computer is incorporated in the design, an appropriate Microsoft operating system should be used.**
- 2.33.1 If the system uses a personnel in its design, it will use a Microsoft operating system. {Required}

2.34 NGSS construction will meet Agency standards and practice when applicable and will be based on best engineering practices.

- 2.34.1 The system shall be designed to work with 4X1.5mm+1X2X0.25MM/Radox 125 cables and 7C+1Koax/8/G042+RXL+PAIR/1/7-01 cables. {Required}
- 2.34.2 The image data generator used for underwater applications should have dimensions such that the total volume of space taken does not exceed 200 cc. {Required}
- 2.34.3 All electrical external connections shall be resistant to accidental disconnection. {Required}
- 2.34.4 Cables shall have at least 80% copper braiding coverage around each data-carrying wire set and shall not have signal leakage as detected by ... {Required}
- 2.34.5 All hardware components shall be based on the metric system. {Required}

2.35 The image data generator shall be enclosed in a sealable, tamper indicating enclosure (STIE) that will protect it from the environment. All the enclosures are defined to be part of the NGSS.

- 2.35.1 During operation, all equipment shall block the intrusion of dust and other particles greater than ___ microns. {Required}
- 2.35.2 During normal decontamination wash-down, the housing of the image data generator enclosure shall be leak-proof. {Required}
- 2.35.3 The image data generator enclosure will provide protection against corrosion as a result of condensation. {Required}
- 2.35.4 The image data generator shall have the capability to utilize existing wall mountings and bolts that are presently installed at State facilities. {Desired}
- 2.35.5 It shall be possible to seal the unit with IAEA metal E-type seals or IAEA fiber optic seals. Protection shall be provided against accidental damage of the seal wire or fiber on the recording console. {Required}
- 2.35.6 The enclosure shall be made of, or coated with, materials which shall provide positive indication of physical tampering. {Required}

- 2.35.7 An Error indicator shall be provided within the image data generator enclosure to alert the inspector in the event that an error has occurred during the surveillance interval. {Desired}
 - 2.35.8 If rack-mounted electronics are used, the equipment will be mounted in 19" racks. {Required}
 - 2.35.9 The enclosures shall be equipped to accommodate a standard IAEA metal E-type or fiber optic seal. Attempts to open the sealed portion of the cabinet must result in complete severing of the seal wire. {Required}
 - 2.35.10 All cameras shall use an industry standard lens mount. {Desired}
 - 2.35.11 The enclosure shall be designed to protect against accidental damage of seal and seal wire (metal wire or fiber). {Required}
- 2.36 The NGSS shall use internationally recognized indicators, symbols, and colour codes.**
- 2.36.1 All instrument indicators, instructions and symbols used, printed, etched on the hardware, or displayed by the software shall conform to one or more ISO metric standards or shall be recognized internationally. {Required}
- 2.37 The vendor will provide all required documentation in English to the IAEA including: 1) technical specifications, 2) design drawings, 3) operating procedures, 4) image and data security procedures, 5) system test plan, 6) maintenance manuals, 7) inspector training materials, 8) spare parts management plan.**
- 2.37.1 All documentation shall be in the English language: technical and design specifications (including drawings), in draft form; operating manual, in draft form; image and data security procedures, in draft form; detailed test plan for acceptance testing, in draft form. {Required}
 - 2.37.2 As part of any procurement contract, training shall be provided to IAEA personnel on the maintenance and operation of the system. Training materials shall be performance-based and shall include learning objectives, student workbooks, and instructor aids where applicable. {Required}

Appendix A

Definitions, Acronyms, and Abbreviations

1. Definitions

component: One of the parts that make up a *system*. A component may be hardware or software and may be subdivided into other units or components [IEEE Std 610.12-1900]. Note: For the purpose of this specification, the term component will be used in preference to the terms module and unit.

critical component: Those components whose failure may result in the loss of safeguards significant data.

critical indicator: State of health information from a critical component.

data generator: Any device that receives data directly from a sensor, stores, and manipulates it as required for the purpose of data retention and/or transmission.

embedded operating system: A software platform that is hidden from a user on top of which application programs run.

extendibility: The ease with which a system or component can be modified to increase its storage or functional capacity [IEEE Std 610.12-1990] (synonyms: extensibility; expandability).

functional requirement: A requirement that specifies a function that a system or system component must be able to perform [IEEE Std 610.12-1990]. In this User Requirements Document, functional requirements specify how the inputs to the equipment should be transformed into outputs [IEEE Std 830-1984].

interface requirement: A requirement that specifies an external item with which a system or system component must interact, or that sets forth constraints on formats, timing, or other factors caused by such an interaction [IEEE Std 610.12-1990].

maintainability: The ease with which a system or component can be modified to correct faults, improve performance or other attributes, or adapt to a changed environment [IEEE Std 610.12-1990] (contrast with *extendibility*).

mean time between failure (MTBF): $= -t (\text{specified}) / \ln R$ (specified where t is 3 months and R is the specified reliability).

module: See *component*.

performance: The degree to which a system or component accomplishes its designated functions within given constraints, such as speed, accuracy, or memory usage [IEEE Std 610.12-1990] (contrast with *reliability*).

performance requirement: A requirement that imposes conditions on a functional requirement; for example, a requirement that specifies the speed, accuracy, or memory usage with which a given function must be performed [IEEE Std 610.12-1990] or a static numerical requirement such as the number of simultaneous users to be supported or the number of files and records to be handled [IEEE Std 830-1984].

ping functions: A utility to determine whether a specific IP address is accessible. PING is used primarily to troubleshoot internet connections.

portability: The ease with which a system or component can be transferred from one hardware or software environment to another [IEEE Std 610.12-1990] (synonym: transportability).

product: (For this document) a system or component—along with any necessary data and documentation—for which requirements are specified in a *requirements specification*.

reliability: The ability of a system or component to perform its required functions under stated conditions for a specified period of time [IEEE Std 610.12-1990] (contrast with *performance*).

requirement: (1) A condition or capability needed by a customer to solve a problem or achieve an objective; (2) a condition or capability that must be met or possessed by a *system* or *component* to satisfy a contract, standard, *specification*, or other formally imposed document; (3) a documented representation of a condition or capability as in (1) or (2) [adapted from IEEE Std 610.12-1990].

security critical component: Any component of hardware or software that, if compromised, would result in a compromise of the security of the system. Security critical components include, but are not limited to, any component that generates, stores, or accesses secret or private cryptographic keys, and software that verifies authentication signatures on data.

sensor: Any device that responds to physical stimulus (such as light, heat, radiation, pressure, motion) and transmits a resulting impulse.

specification: A document that prescribes, in a complete, precise, verifiable manner, the *requirements*, design behavior, or other

characteristics of a *component* or system and often, the procedures for determining whether these provisions have been satisfied [IEEE Std 610.12-1990].

state of health (SOH): Any data relating to the condition of any hardware or software.

system: A collection of *components* related in such a way as to produce a result greater than what their parts, separately, could produce.

Transmission Control Protocol/Internet Protocol (TCP/IP): TCP is one of the main protocols in TCP/IP networks. IP specifies the format of packets, also called datagrams, and the addressing scheme. TCP enables two hosts to establish a connection and exchange streams of data. TCP guarantees delivery of data and also guarantees that packets will be delivered in the same order in which they were sent.

unit: See *component*.

usability: The ease with which a user can learn to operate, prepare inputs for, and interpret outputs of a system or component [IEEE Std 610.12-1990].

2. Acronyms and Abbreviations

AC:	alternating current
CCITT:	International Telegraph and Telephone Consultative Committee
CCD:	charge-coupled device
CD-ROM:	compact disk read-only memory
DC:	direct current
FIPS-140:	Federal Information Processing Standard Number 140, “Security Requirements for Cryptographic Modules”, published by the National Institute of Standards and Technology.
FTP:	File Transfer Protocol, the protocol used on the internet for sending files.
EIA:	Electronic Industries Association
EMC:	Electromagnetic Compliance
INMARSAT:	International Maritime Satellite Network
IAEA:	International Atomic Energy Agency
IEC:	International Electrotechnical Commission
IEEE:	Institute of Electrical and Electronics Engineers
ID:	identification
ISDN:	integrated services digital network
ISO:	International Standards Organization
LAN:	local area network
MIVS:	Modular Integrated Video System
MTBF:	Mean Time Between Failure— = t (specified)/ $\ln R$ (specified where t is 3 months and R is the specified reliability).
MTTR:	mean time to repair
NCDP:	Network Communications, Data Store and Power Management Unit

NGSS	Next Generation Surveillance System
PC:	personal computer
PDF:	Portable Document Format
PSTN:	public switched telephone network
PTI:	picture-taking interval
RM:	remote monitoring
SCSI	Small Computer System Interface
SOH:	State of Health—Any data relating to the condition of any hardware or software
STIE:	sealable tamper indicating enclosure
TBD:	to be decided
TCP/IP:	Transmission Control Protocol/Internet Protocol—TCP is one of the main protocols in TCP/IP networks. IP specifies the format of packets, also called datagrams, and the addressing scheme. TCP enables two hosts to establish a connection and exchange streams of data. TCP guarantees delivery of data and also guarantees that packets will be delivered in the same order in which they were sent.
TTL:	transistor-transistor logic
TÜV:	Technisches Überwachungs-Verien
VACOSS:	Variable Coding Seal System
VSAT:	very small aperture terminal satellite network

Appendix B

Light Water Reactors (LWR)

There are a number of different LWR facility configurations under safeguards. The Agency categorizes them for safeguards purposes as Type 1 and Type 2. Different containment and surveillance (C&S) measures are applied at these two LWR types. A further distinction that the Agency makes in LWRs is reactors that burn Mixed Oxide Fuel (MOX) and those that do not burn MOX. Since this User Requirement relates only to optical-based surveillance systems, the following treatment of safeguards at LWRs will emphasize the optical-based component of surveillance.

In a Type 1 LWR, the reactor pressure vessel and the spent fuel pool are in a single containment building. It is therefore possible for a single surveillance camera to survey both the spent fuel pool and the reactor vessel. An important subclass of Type 1 is the dual-unit VVER reactors, where two reactors and two spent fuel pools are in one building. In this Type 1 subclass, several surveillance cameras are installed which survey both reactor units and the fuel operations areas between the units. Figure 3 depicts a model layout of a Type 1 LWR. Typical camera locations are shown on the diagram.

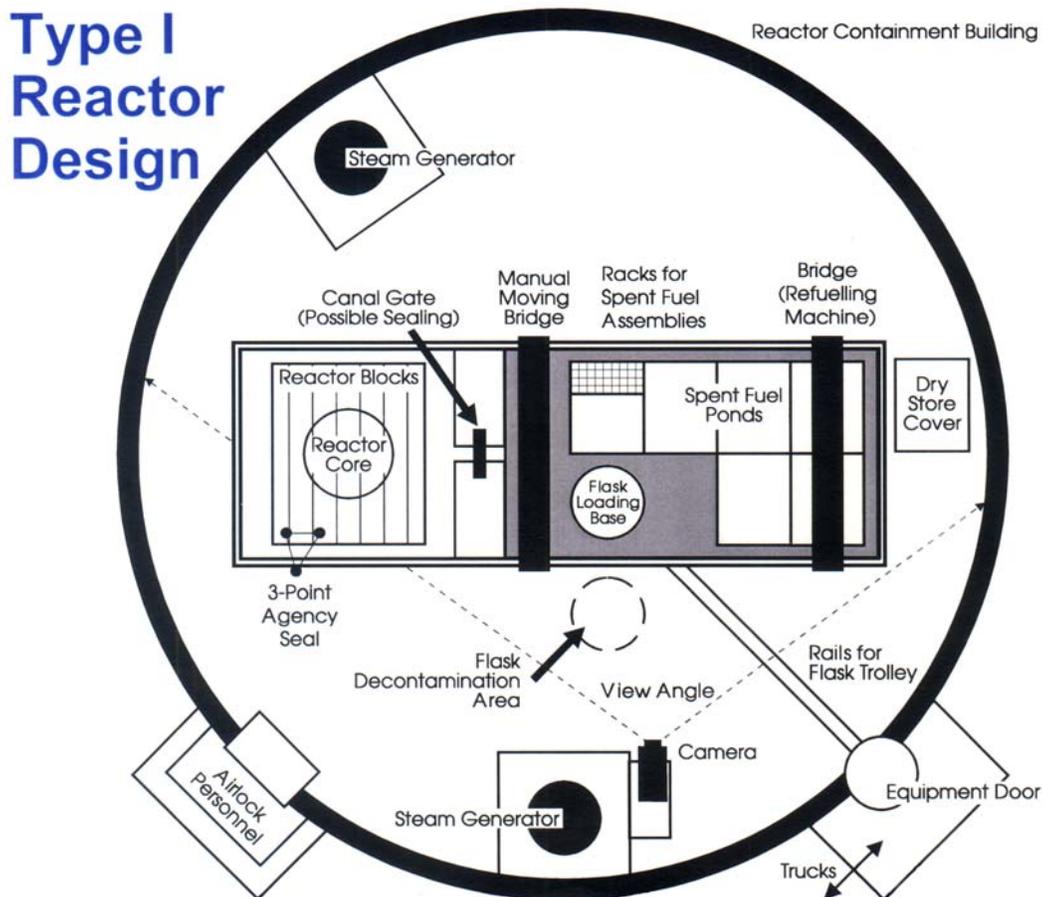


Figure 3 Type I LWR Reactor Design

In a Type 2 LWR, the reactor pressure vessel is in a containment building and the spent fuel pool is in an adjacent auxiliary building. Surveillance is installed in the auxiliary building. During power operation, access is not permitted in the reactor building and a camera, where installed, is not accessible. A fuel transfer channel connects the two buildings. There is a large equipment hatch in the reactor building, which is opened during refueling. Figure 4 depicts a model layout of a Type 2 LWR.

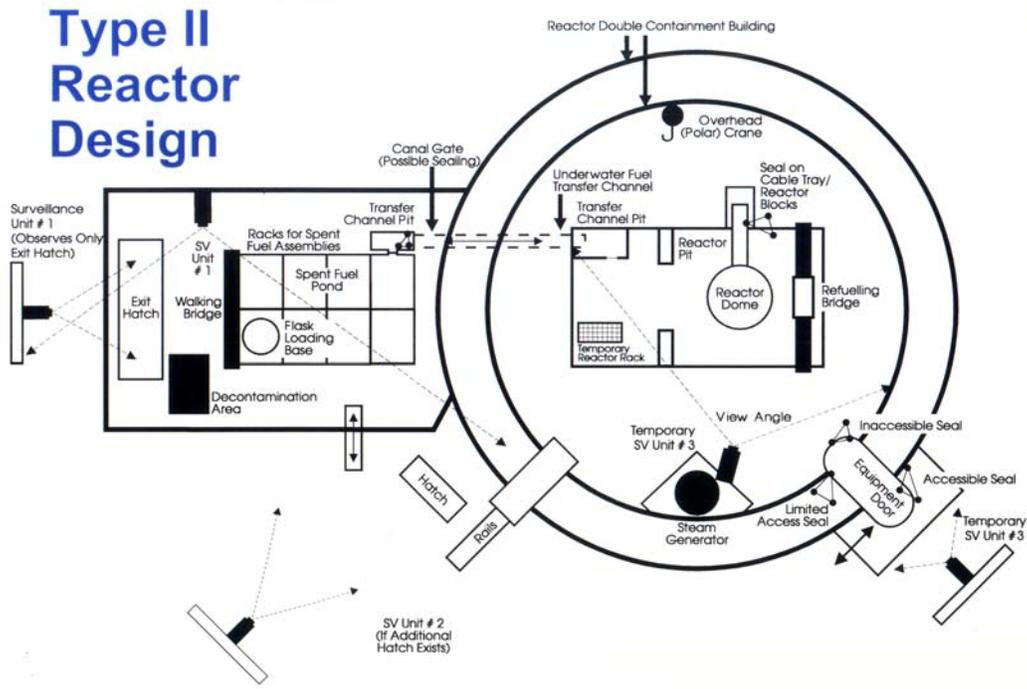


Figure 4 Type II LWR Reactor Design

In Type 1 reactors without MOX fuel, a single camera with a wide-angle lens is used to monitor movement in and around the spent fuel pool and to monitor activity when the reactor core is open. In a Type 2 reactor, temporary cameras are mounted in the containment building to monitor the reactor core (when it is open), a camera permanently mounted to monitor the exit hatch, and one camera permanently mounted to monitor the spent fuel pool.

C/S Equipment Installed at LWR with MOX

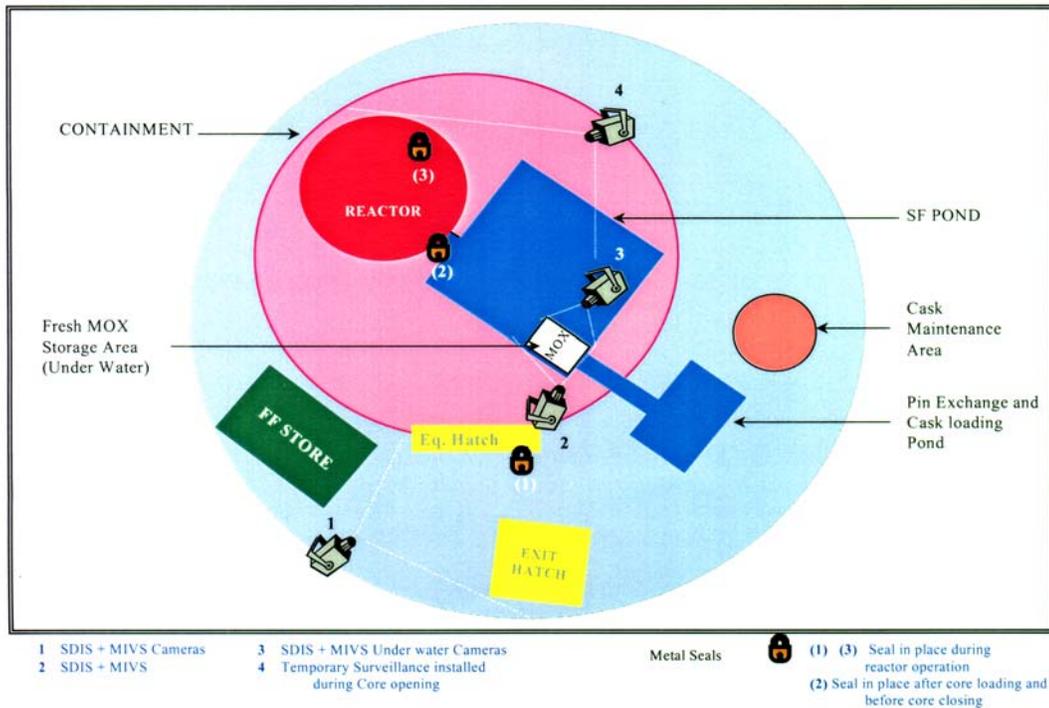


Figure 5 C&S Equipment Layout in a MOX Facility

How Surveillance Is Currently Implemented at LWRs

Open core surveillance: Currently coverage through surveillance is required of possible unreported fuel transfers to and from the open core at LWRs during refueling. This requirement was established to address possible unrecorded production (assurance regarding misuse). It was introduced to provide continuity of knowledge of the core, in recognition that in the period after the PIV of the core until the closure of the reactor vessel, fuel assembly transfers could be made by the operator without Agency knowledge (e.g., unreported replacement of an irradiated assembly by a fresh fuel assembly). It also provides assurance that there is no direct removal of a core fuel assembly (or of target material) from the reactor vessel during the whole period that the core is open. These diversion scenarios are of particular importance when MOX fuel is used.

Use of surveillance in dual C&S systems: A number of dual C&S systems applied to spent fuel in storage at LWRs include surveillance as one component, with seals as the second component. This is done for cases of multi-layer storage of WWER spent fuel, where the lower layer is designated as difficult-to-access; surveillance is provided by the same cameras as used for covering the spent fuel pools.

Equipment hatch surveillance. Surveillance of the open equipment hatch during refueling is used at some Type 2 LWRs. The Agency installs these cameras permanently outdoors and uses the data only at the time of the PIV.

MOX Surveillance In LWRs

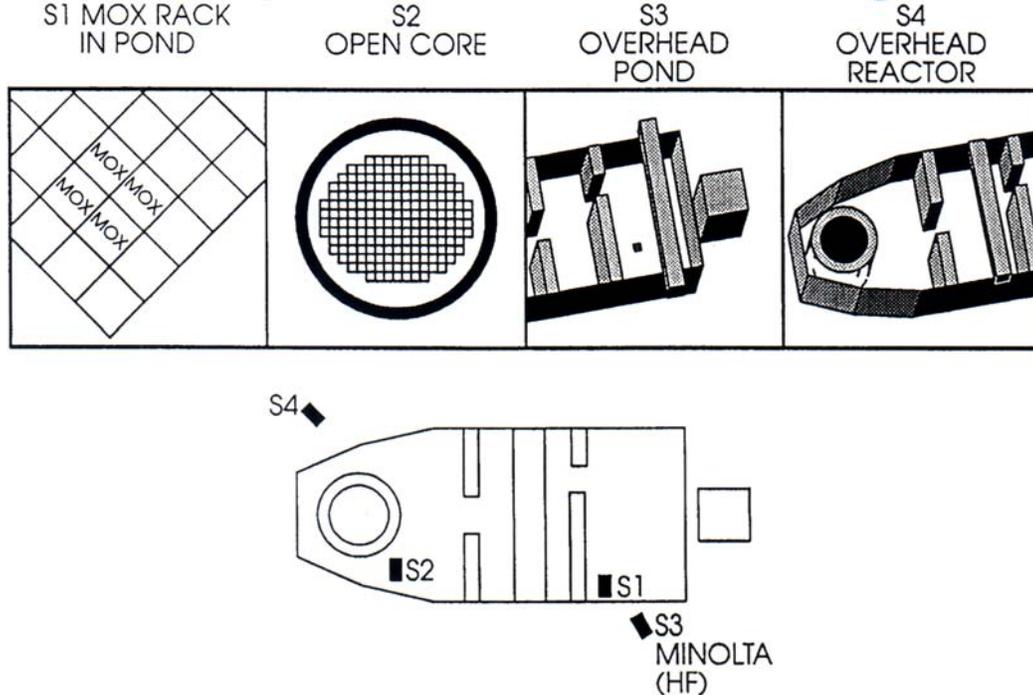


Figure 6 MOX Surveillance in LWRs

How Surveillance Will Be Implemented at LWRs In Integrated Safeguards

The plan is to reduce the frequency of inspections and the degree of intrusiveness of safeguards in those countries that do not have the entire fuel cycle or which have demonstrated that safeguards has been successfully institutionalized. The integrated safeguards approach for LWRs will include an annual physical inventory verification (PIV), a small number of random interim inspections and randomized selection of facilities for inspection. Random unannounced interim inspections will be performed when they can be carried out effectively and efficiently. Where unannounced inspections cannot be used, announced interim inspections supported by surveillance will be used to meet the same objectives. For unannounced inspections, a camera will monitor activity in and around the spent fuel pool for a period of approximately 7 days prior to the inspection. A permanently mounted camera that can be turned on remotely with an adjustable PTI may do this. At LWRs at which MOX fuel is used, the fresh MOX fuel assemblies are to be kept under C&S from receipt at the reactor until loading into the core for maximum efficiency in meeting the timeliness goal. Fresh MOX fuel assemblies are typically stored in a designated part of the spent fuel pool where a dedicated underwater camera has a good view of the assemblies. The timeliness goals for the fresh MOX fuel assemblies can then be achieved either by announced quarterly interim inspections or by quarterly evaluation of remotely transmitted C&S data. To maintain continuity of knowledge of the nuclear fuel in the core of LWRs, surveillance is to be used during refueling. The reactor vessel is to be sealed between refueling.

On-Load-Reactors (CANDU Type)

CANDU reactors represent the majority of OLRs under safeguards. There are two principal CANDU configurations: single unit stations (600 MWe stations, operating in Canada, Argentina, Republic of Korea and Romania; and smaller units operating in India and Pakistan) and large multi-unit stations (operating only in Canada).

Safeguards verification at OLRs is based primarily on item accountancy for spent fuel bundles/assemblies. Complementary C&S measures are used to reduce reverification requirements by maintaining continuity of knowledge of declared nuclear material, including providing timely detection of diversion, and to ensure the absence of misuse of the reactor for unreported plutonium production. Specifically, the core fuel at an OLR is only verifiable during the initial core loading. After operation starts, core fuel is not available for verification. A characteristic of OLRs is that regularly (e.g., every day or 4 to 5 days a week) fresh fuel bundles are loaded into the reactor core and spent fuel bundles are discharged from the core to the spent fuel storage pool. Therefore the measures applied are:

- C&S and other verification of fuel discharges (e.g., bundle counter) ensure that the irradiated fuel bundles discharged from the core have gone into the spent fuel bay; or
- The record of irradiated fuel discharges (e.g., obtained from a core discharge monitor) and other verification of irradiated fuel discharges (e.g., bundle counter) confirm the operator's records of fuel.

For spent fuel in spent fuel bays (pools), item accountancy verification is performed by verifying fuel bundles (item counting plus gross defects) as they enter the spent fuel bays upon discharge from the core, and maintaining continuity of knowledge of the fuel in the spent fuel pools, primarily by surveillance. (In several of the multi-unit OLRs, spent fuel bundles are transferred from one storage-bay to another. These interbay transfers are discussed later.) The current requirement is to maintain spent fuel pools under continuous surveillance (i.e., to continuously survey the surfaces of the bays to confirm that spent fuel has not been removed without being reported). The surveillance record is evaluated for timeliness purposes and at the PIV. When surveillance has been successful throughout the material balance period, only item counting is performed at the PIV. In some OLRs, part of the spent fuel in the bays is placed under dual C&S to avoid remeasurement/reverification (see below). Spent fuel is transferred at most OLRs to on-site dry storage, where it becomes difficult-to-access and is placed under dual C&S (see below).

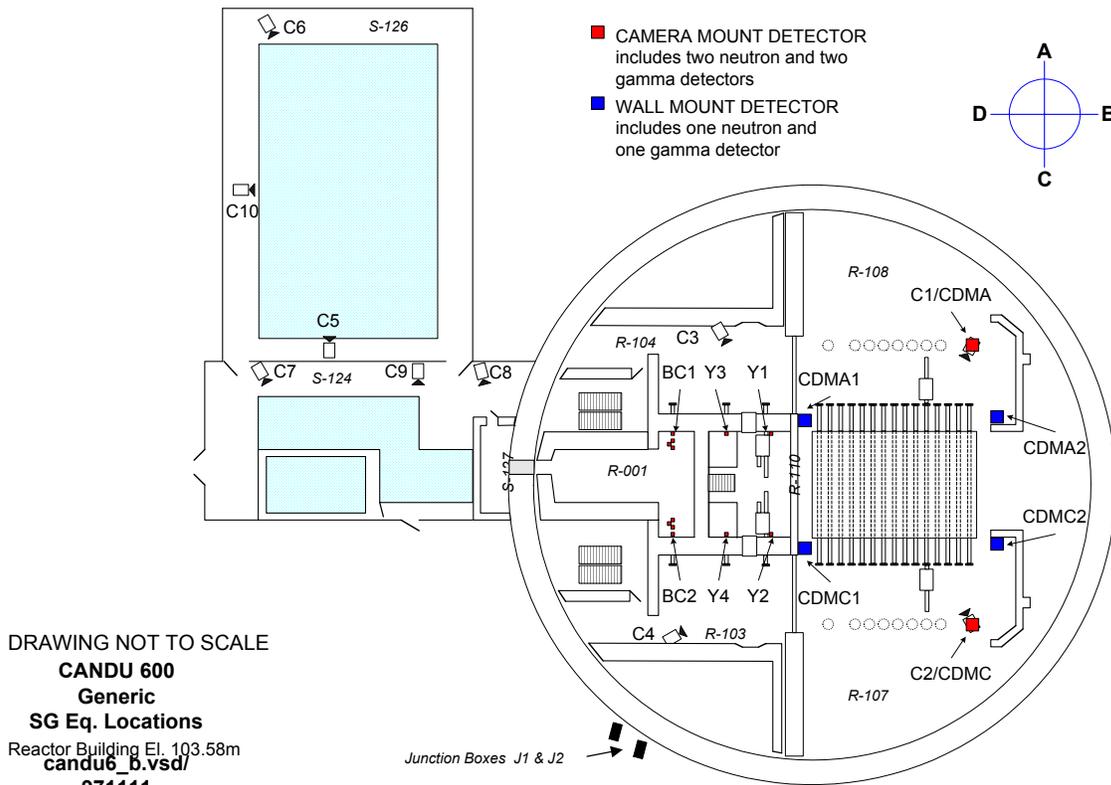


Figure 7 Camera Equipment Layout in a CANDU Reactor

Spent fuel bay arrangement at 600 MWe CANDU reactors: At a single unit 600 MWe CANDU-type OLR, there is a single spent-fuel bay, divided typically into four interconnected sections, of which one serves for routine spent fuel storage. An automated fuel handling system moves spent fuel discharged from the reactor core through bundle counters into underwater storage. In a reception bay, the spent fuel is loaded automatically into storage trays, each of which holds 24 bundles. Storage trays are welded, stainless steel structures, which hold two parallel rows of 12 bundles. Filled trays are moved automatically through a transfer port (in the wall separating the reception and main bays) into the main bay. The trays are placed in stacks, each typically 19 trays high, in close proximity to each other.

Spent fuel bay arrangements at multi-unit CANDU reactors

At the multi-unit stations, the bay arrangements are as follows:

- At the Bruce A and Bruce B facilities, the arrangements are: 24-bundle trays, stacked up to 15 high without stacking frames in Primary Bays; and 24-bundle trays, stacked up to 37 high in 2x2 stacking frames in Secondary Bays. Loaded trays are automatically transferred between the primary and secondary bays through a long tunnel (100 m) filled with water. This is called “interbay transfer”.

- At Pickering the arrangements are: 32-bundle baskets, in stacks up to 6, in the Irradiated Fuel Bay, side A; 96-bundle modules, in stacks up to 7, in the Auxiliary Irradiated Fuel Bay; and mostly stacked modules, with some stacked baskets, in the Irradiated Fuel Bay, side B. Loaded baskets from the Pickering A Irradiated Fuel Bay are transferred in a large flask to the Auxiliary Irradiated Fuel Bay by a truck that travels through an internal tunnel. This is called “interbay transfer”.
- At Darlington, the 4 units have a common spent fuel handling system which discharges spent fuel into either of two spent fuel bays, one at each end of the station. A bay consists of a reception bay and a main bay. Bundles are stored in modules, which are stacked with high density. There are no interbay transfers.

Safeguards verification and C&S measures currently used at CANDU-type OLRs

In the safeguards approaches at OLRs, strict C&S envelopes have been arranged around the flow path of the spent fuel from its discharge from the reactor core up to its placement in dry storage, in order to attain the safeguards goals for core and spent fuel. There is a chain of C&S systems whose function is to ensure the completeness of flow measurements at strategic points. Such flow measurements are made:

- when bundles are discharged from the reactor pressure tubes into the fuelling machine, by core discharge monitors (CDMs), if installed;
- when bundles are discharged through the discharge port into the spent fuel storage bay area (there are different arrangements at different reactors) by bundle counters;
- upon “interbay transfer” from a primary storage bay to a secondary (auxiliary) bay (where this occurs) by inspector visual observation; and
- upon transfer to dry storage.

The C&S systems at OLR stations differ primarily on whether CDMs are installed. At 600 MWe single unit stations, the C&S systems are based on camera surveillance and bundle counters. The C&S measures installed in a 600 MWe OLR are typically 12 CCTV cameras, several spent-fuel bundle counters, and 6 Yes/No monitors; 2 CDMs are also installed at some units. For the multi-unit reactor stations, operated in Canada, camera surveillance on the core would be unlikely to give conclusive results regarding unreported production because of the larger number of containment penetrations, and CDMs are necessary.

Surveillance systems

Surveillance systems are used for two functions:

- To supplement the bundle counters in covering possible unreported core discharges at 600Mwe units, and
- To cover the spent fuel bays and facility-specific operations that might be used in the diversion of irradiated fuel bundles at all CANDU facilities.

At 600Mwe units, surveillance is used to cover possible unreported discharges from the reactor. Surveillance is applied in the reactor vault, fueling-machine maintenance lock (where there are ports for fresh fuel, irradiated fuel and auxiliary operations) and fresh-fuel loading area (typically 4 cameras are used).

For the spent-fuel bays, several cameras (2 to 5) cover the reception bay and several other cameras cover the main bay (4 to 5). These cameras are used to confirm that no undeclared removals of spent-fuel casks take place through the water surface. They also provide information about plant operations taking place in and above the bays, such as the placement and removal of a shielded cask into the bay and the activities associated with transfers of spent fuel to dry storage. Surveillance is also used to cover other operations, in particular, surveillance is applied to the transfer route for interbay spent fuel transfers (at Bruce and Pickering multi-unit stations).

Verification of spent fuel in wet storage

The multi-layer, close packing of the large number of spent-fuel bundles makes full verification, and even item counting, difficult or impracticable without moving fuel. This fundamental characteristic forces a reliance on C&S measures to maintain continuity of knowledge with limited direct verification, rather than periodic full verification of the spent-fuel inventory in wet storage. Very reliable single and dual C&S systems have been employed based on the MUX CCTV systems. Successful results from these C&S systems reduce the requirements for spent fuel verification for timeliness purposes to C&S evaluation, and for the PIV to C&S evaluation and item counting (for single C&S).

How Surveillance Will Be Implemented at OLRs of CANDU Type In Integrated Safeguards

The model integrated safeguards approach for on-load refueled reactors of the CANDU type includes an annual PIV; the continued use, for cost effectiveness reason, of unattended flow monitors for verifying fuel discharges from the core and C&S measures applied on the spent fuel bays; and a small number of random interim inspections. To verify efficiently the substantial number of transfers of spent fuel to dry storage, new approaches are being developed. These foresee broader involvement of the SSAS/facility operator to assist the Agency in verifying the transfer, together with the use of a “mailbox” system, for the provision of information on such transfers, and

unannounced inspections. SAGSI has advised the Secretariat that, in principle, the integrated safeguards approach for OLRs of the CANDU type provides a reasonable basis for achieving the integrated safeguards sim of optimizing effectiveness and efficiency. However, SAGSI further advised that important practical details of the approach concerning transfers of irradiate fuel to dry storage need to be further defined and demonstrated.

On-Load-Reactors (RBMK)

These are based on Russian technology. One very large two-unit RBMK station is in operation under safeguards in Lithuania. A large RBMK reactor is in operation and two are shutdown in the Ukraine. Several RBMKs are in operation in the Russian Federation

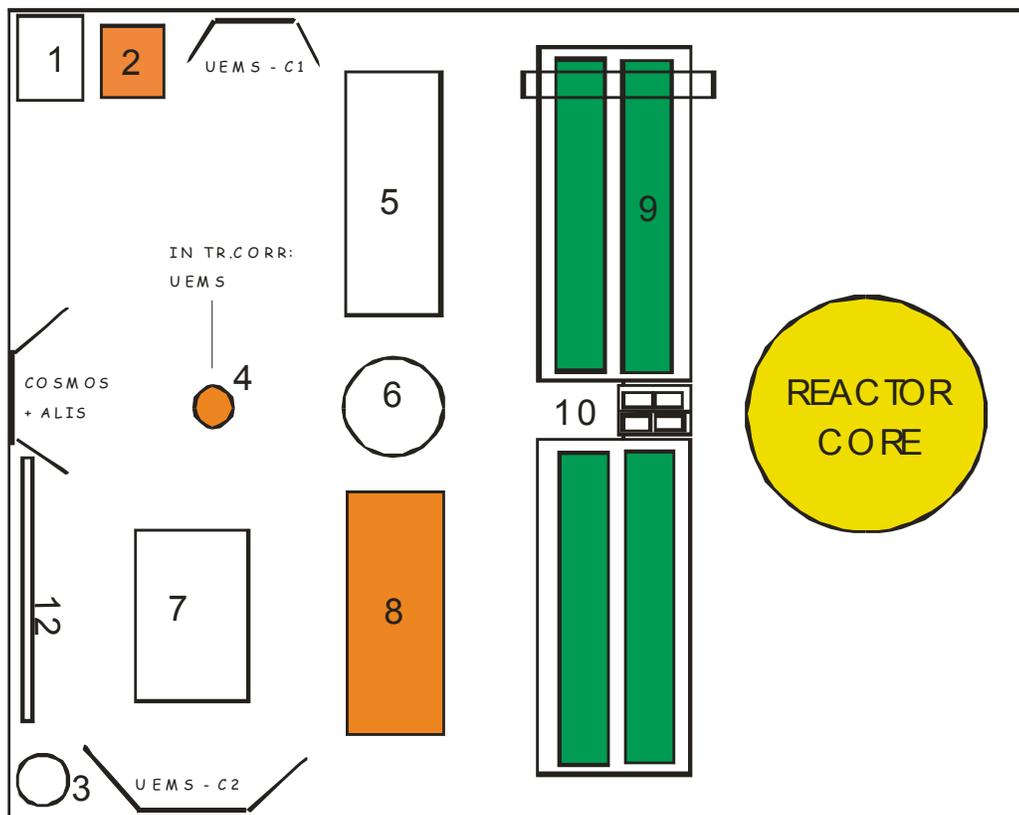


Figure 8 RBMK Reactor Building Layout

- | | |
|---|---------------------------|
| 1 DOOR | 6 REFUELLING MACHINE |
| 2 FRESH FUEL HATCH | 7 SF TRANSFER VEHICLE |
| 3 SMALL CRANE | 8 EQUIPMENT HATCH |
| 4 SPENT FUEL HATCH | 9 INTERIM CF STORAGE |
| 5 LOW LEVEL
CONTAMINATION
STORAGE | 10 FUEL TESTING POSITIONS |
| | 11 INTERIM CF STORAGE |
| | 12 FF RACK |

RBMK reactors are designed to allow the reactor to be refueled without needing to shut down the reactor. These reactors are a source of direct use material and therefore are of great interest to the IAEA. Figure 8 represents a plan view of a typical RBMK reactor building. The reactor building houses the reactor core, an interim spent fuel storage bay, a large equipment hatch, a fresh fuel hatch and a spent fuel hatch, and cranes for moving the fuel assemblies.

Storage Facilities

There are two general types of spent fuel storages: wet storage in pools, and so-called "dry storage". Spent fuel goes into "wet storage" upon discharge from an LWR, OLR or water-cooled research reactor. Spent fuel is also stored underwater in the receipt pools of reprocessing plants. In some cases, spent fuel is transferred from the reactor pools to wet storage in separate storage facilities. Safeguards measures for such wet storages are similar to those applied at reactor spent fuel pools, as has been addressed in the section for LWRs. Therefore, separate wet storages of spent fuel will not be addressed further here.

After a multi-year cooling time to allow the decay heat production to fall to an acceptable value, some spent fuel is prepared for longer term "dry storage". This course is being taken in particular where a decision to reprocess has been deferred or the spent fuel is awaiting long-term disposal; e.g., in a geological repository. Such storages are generally designed for 30-50 years; i.e., for a long time.

The design of a dry storage is selected on economic and State- or facility-specific grounds. Therefore, a wide range of dry storage designs have come under safeguards, involving separate storage containers, separate storage modules and large storage vaults either in-ground or above ground. Some storage facilities, such as those at Ignalina or Chernobyl NPPs, are located outdoors and are subject to snow, ice, and sleet. In order to perform their function, these outdoor cameras must operate in fog and darkness.

Dry spent fuel storages have the common characteristic that the spent fuel containers or containments are not intended to be opened. Therefore, dry storages of spent fuel are a classic situation for the use of C&S in safeguards to maintain continuity of knowledge of a verified inventory. Since these storage facilities are intended for long-term storage, the Agency expects very little activity to take place in and around the storage areas.

Verification of the spent fuel and maintaining of continuity of knowledge until it is placed into dry storage is an important and often inspector-intensive safeguards activity. The verification often takes place at a reactor, after which the spent fuel is placed under Agency seal in a shipping container. However, there are cases where, after the spent fuel is transferred from a reactor to a separate storage in transport containers, it is then removed and transferred into its final storage location. In such cases, continuity of knowledge must be maintained through all the transfer stages, and some level of reverification

may be required at the storage facility, if more than a timeliness goal period is involved.

The IAEA maintains surveillance on static storage areas where continuity of knowledge during spent-fuel transfers must be maintained. The surveillance cameras mounted in storage facilities are permanently installed in the room where irradiated material is stored. The rooms where the nuclear material is stored typically have low radiation levels, but the neutron flux can still be substantial enough to damage electronics due to single event upsets. A typical C&S configuration is a camera or cameras trained on the storage casks and a seal on the door to the room. Radiation monitors can also be employed at storage facilities to monitor the movement of radioactive material into and out of the entrances.

Some facilities are used to store direct use, or "fresh", plutonium and HEU in a bank vault type configuration. For this application, the surveillance system must be capable of taking picture at a very high PTI (< 1 min) in order to see diversions.

How Surveillance Will Be Implemented at Storage Facilities In Integrated Safeguards

The model integrated safeguards approach for spent fuel storage facilities provides for an annual PIV and a small number of random interim inspections. Because most of the nuclear material inventory at such facilities is in static conditions under Agency seal, the random interim inspections do not need to be unannounced. The use of unattended monitors for verification of fuel receipts provides additional savings of Agency inspection effort. The Agency expects to continue to use optical surveillance as part of the safeguards system.