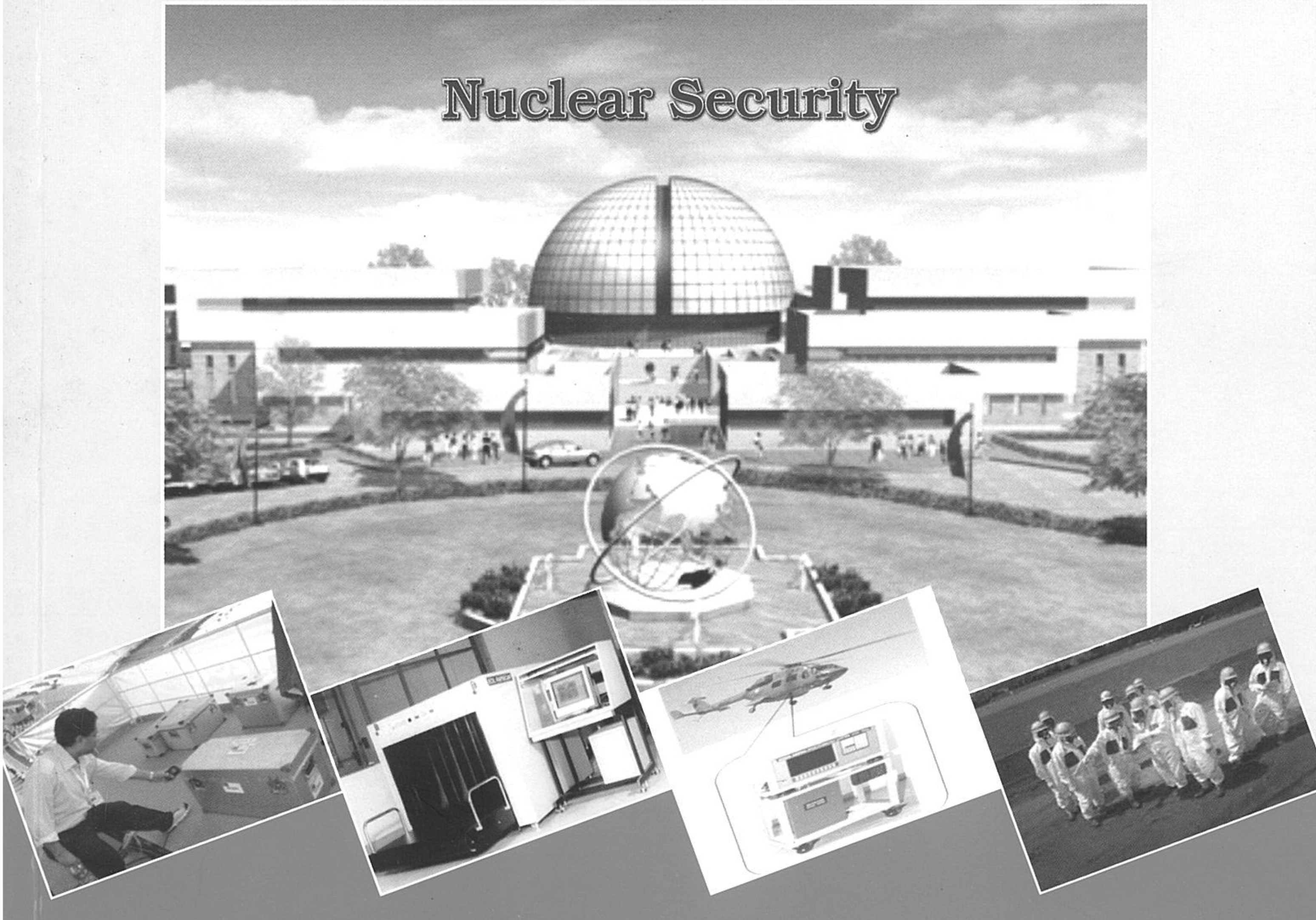
IANCAS Bulletin

INDIAN ASSOCIATION OF NUCLEAR CHEMISTS AND ALLIED SCIENTISTS



www.iancas.org

December 2013 Vol. XI No. 2

Vol. XI. No.2 **Editor : N. Ramamoorthy** **December 2013**

Editorial

The growth of nuclear programmes is one of the important technological advancements sought by a number of countries, predominantly for the societal well-being (leaving aside the defence attributes of the field). The field is being fostered by several entities from both within the Government system and outside, the largest among them being the International Atomic Energy Agency (IAEA). The goal of ensuring security of nuclear materials and facilities has all along been an inherent element in the nuclear programme in every nation adopting nuclear science and technology.

The 9/11 events in USA, and the continuing terrorist activism observed in several other parts of the world, have only enhanced and accelerated the international efforts to further strengthen nuclear security in its entirety. A simple but rather crude analogy, especially in Indian context, could help drive home the point. Gold and similar valuable items are always vulnerable for attack and forced acquisition, but that does not deter any of us from seeking to have/use them (also, building an inventory over time), and, of course, to the best extent possible, taking good care of them with multiple protection mechanisms. The principles of ensuring nuclear security are based on a similar approach with a multi-tier protection system, involving technology aspects, security framework, and standard operating practices, all firmly instituted and scrupulously enforced. The current Issue of IANCAS Bulletin endeavours to cover these aspects through the articles contributed by experts in the field, who are currently dealing with nuclear security matters.

India has always attached a very high degree of importance to nuclear security matters, as has been reiterated by our honourable Prime minister during the Nuclear Security Summit held in Washington DC, USA in 2010, and again in the next Summit held in Seoul, Republic of Korea in 2012. Similar sentiments are evident in the preparations leading to the next Summit scheduled to be held in The Netherlands in March 2014, and that should be reassuring for one and all, that, nuclear security aspects are, and will continue to be, given the highest attention. The final article in the current issue devoted to the Global Centre for Nuclear Energy Partnership (GCNEP) bears testimony to the on-going efforts of the Department of Atomic Energy (DAE) in translating the promise of our honourable PM at the 2010 Summit into reality.

I wish to thank Shri Ranajit Kumar for accepting our request to be the Guest Editor for this thematic issue and coordinating the preparation of the issue. Thanks are due to all the contributing authors for their efforts and cooperation in making timely submission, and in a

CONTENTS

Editorial (Contd.)

few cases, accepting certain editorial interventions sought from them. My special words of thanks go to Shri G.P. Srivastava, for his Focus Column. As the Indian Member of the IAEA's Standing Advisory Committee on Nuclear Security (AdSec), as Former Director of Electronics and Instrumentation Group, BARC, and also as a Former CMD of ECIL, he has been steering the nuclear security matters in various capacities, and the current issue is a beneficiary of the expertise and competencies built by him.

Nuclear Security - Concepts and Misconceptions

Ranajit Kumar

Control Instrumentation Division, Bhabha Atomic Research Centre, Trombay, Mumbai 400 085;
E-mail: ranajitk@barc.gov.in

Introduction

Nuclear Technology is like a double edged sword. It has numerous beneficial applications, which can potentially uplift billions of lives. Application of nuclear technology includes but not limited to power generation, desalination of water, food preservation, radiation therapy to treat diseases, industrial radiography, medical products sterilization, nuclear medicine, agriculture etc. The list is endless. However, when applied maliciously, the same extremely beneficial technology can be potentially dangerous for people, society and environment. Nuclear security aims at preventing, detecting and responding to malicious intents and acts involving nuclear and radioactive material, associated facilities or transport, in order to reduce, if not avoid, any one intentionally causing harmful effect of radiation on public and environment. In other words, nuclear security ensures that nuclear and radioactive materials are used within a defined, regulated framework, whereby scope and risk of their malicious use can be minimized as low as possible. Nuclear security activities span all nuclear fuel cycle facilities and radiation facilities, in their entire life cycle. This article describes some of the fundamental concepts of nuclear security and also aims to dispel some common misconceptions on nuclear security.

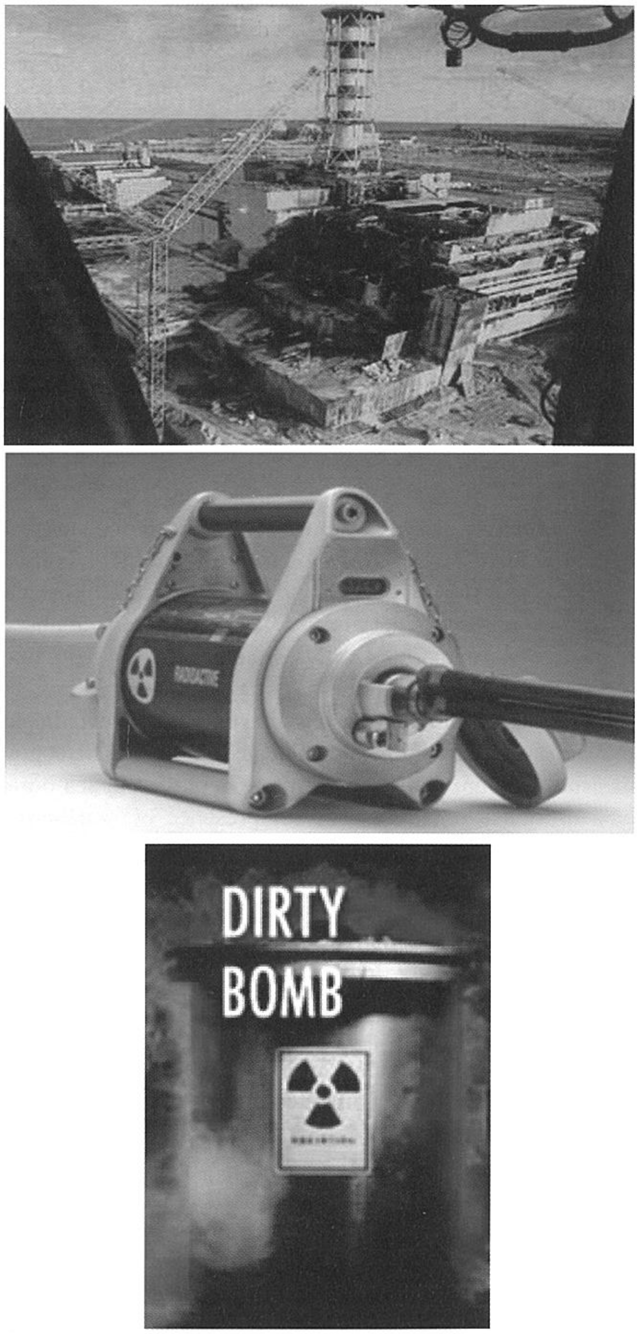


Fig. 1 Nuclear security concerns

Nuclear Security Concerns

The primary concerns of nuclear security are Theft or Diversion of Nuclear and other Radioactive Materials, which could be used to develop improvised nuclear explosive device or to develop radiological dispersal device (RDD) or so called 'dirty bomb'. This issue has the potential of creating an adverse impact beyond the location of occurrence and therefore is not limited to the Facility or the Country specific.

Another concern of nuclear security is Sabotage of a nuclear or radiation facility, or a nuclear or radioactive material transport, which may potentially endanger public and environment by exposure of harmful radiation. This may also have impact on neighboring regions/countries, depending upon the geographical position.

The subject of nuclear security has drawn international attention since the beginning of the nuclear age. However, the terrorist attack of 9/11 has catapulted nuclear security to the top of the international security agenda. Nuclear security is not limited to countries having nuclear power plants/facilities, but also to those using radioactive materials for various applications or involved in transportation of these materials.

Therefore, international platforms such as Global Initiative to Combat Nuclear Terrorism (GCINT), UNSC and the IAEA have stepped up efforts in terms of international initiatives, e.g. Resolutions, Conventions and Guides, for greater awareness on the subject, as well as building the necessary legal/regulatory framework, Man/Machine infrastructure and international platform/network for future updates and sharing of expertise.

Nuclear Security Concepts

Nuclear Security, as defined by IAEA is (1) prevention (2) detection (3) response to theft, sabotage, unauthorized access, illegal transfer and other malicious acts involving nuclear material, other radioactive substances and associated facilities. As can be observed, there are three major areas of nuclear security viz. prevention, detection and response.

Prevention is the first line of defence against malicious use of nuclear and other radioactive material against people and environment during its use in a facility, storage, or transport, by stealing nuclear or other radioactive material, or causing a sabotage of a plant or facility leading to release of radioactivity. It includes measures to protect nuclear and other radioactive materials against theft or other form of diversions, illegal possession, smuggling, and unauthorized use. Other measures include protection of nuclear installations and transport against **sabotage** and other malicious acts that can result in radiation exposure to the general public or the environment. Physical protection (PP) measures in the nuclear power plants or other nuclear fuel cycle facilities, radiation facilities, nuclear or radioactive material transport, are examples of prevention measures.

Detection is the second line of defence against malicious use of nuclear and radioactive materials and refers to the measures to detect and intercept unauthorized movement of these materials outside the protected boundary of a nuclear or radiation facility, at borders of the state, like sea ports, airports and land based border check points, to detect material coming in to, or going out of, a state in illegal manner and also within the State. Examples of detection measures include radiation monitors deployed in sea ports and airports to check cargos for presence of radioactive materials. As detection measure, several airports and sea ports have been equipped with cargo scanning and radiation monitoring equipment, including personnel monitoring portals.

This would necessitate creation of Notification Centre, wherefrom all the concerned departments of security could be communicated for response, recovery and records.

Once any malicious act involving nuclear or radioactive material is detected, the material must be recovered and brought to the safe custody within a limited time. If there is some sabotage caused to a nuclear or radiation facility or transport that may lead to radiation exposure to people and environment, the effect of such malicious act must be contained at the earliest.

Response refers to all such activities which aim at 'reversing' the immediate consequences of harmful uses of nuclear or other radioactive materials. The response may include measures to minimize any potential health hazards and to bring the material under regulatory control. Response measures will depend on the nature and scale of event and may include decontamination of affected people, area and equipment treatment of exposed personnel and also recovery of material which has gone out of regulatory control to safe

Fig. 2 Examples of prevention measures

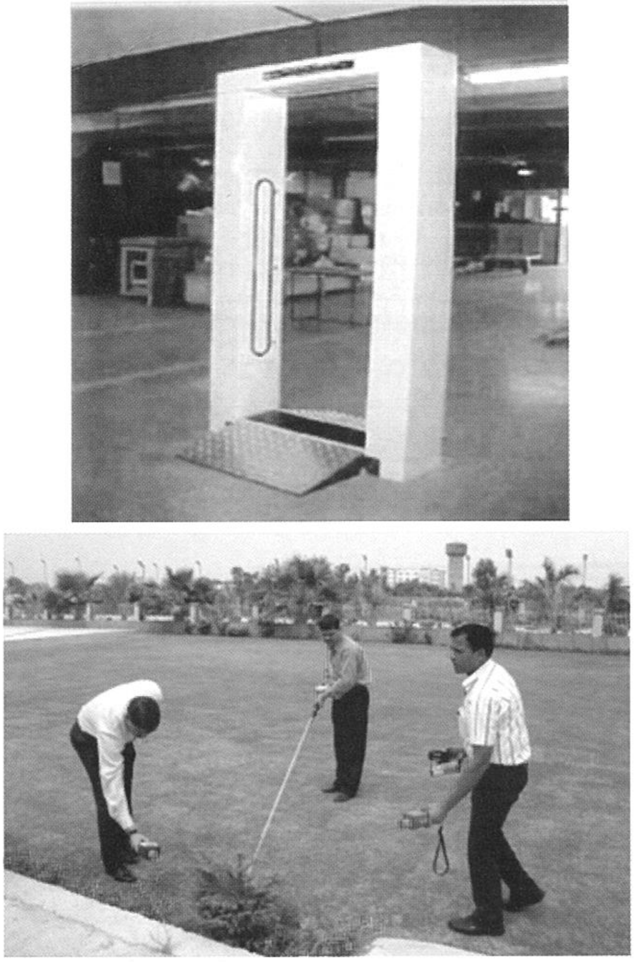


Fig. 3 Examples of detection measures

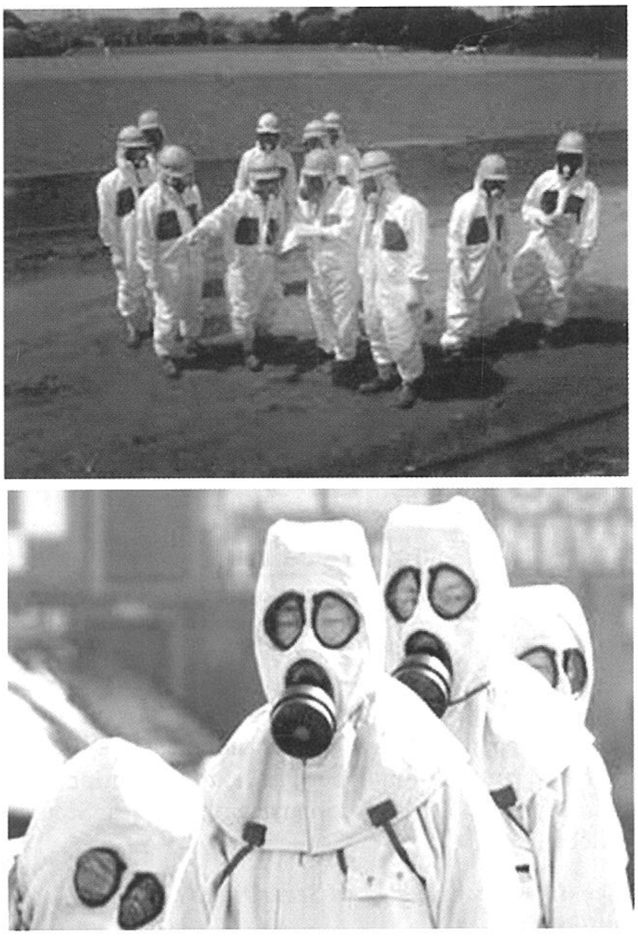


Fig. 4 Examples of response measures

custody. The Notification Centre mentioned above also acts as the nodal response center for the surrounding regions.

Misconceptions on Nuclear Security

Myth-1: Nuclear Security is just a Guard, Gun and Gate

Nuclear security is an overarching activity to prevent, detect and respond to the malicious use of nuclear and radioactive material during their use, storage and transport, both within nuclear and radiation facilities and beyond the perimeter of such facilities. Nuclear security encompasses many measures which are not restricted to a facility boundary.

Physical protection system (PPS) is the integration of people, equipment and procedures in protection of (nuclear) assets or facilities against theft, sabotage, or other malevolent human attacks. It includes three interrelated functions of detection, delay and response. Guards, guns and gates are part of these three essential functions of physical protection. However, physical protection systems consist of many more systems and gadgets, people and procedures.

Myth-2: Nuclear Security is non-productive

Nuclear security helps to prevent the malicious use of nuclear and radioactive materials and malevolent acts towards nuclear and radiation facilities and their transport. The goal of nuclear security is the same that of nuclear safety - the protection of public and environment from harmful uses of radiation. Some of the measures recommended in nuclear security e.g. physical separation, can also directly aid safety. Also, many measures required for safety directly aid security. Security measures like access control, area surveillance can also add to productivity - for example, by bringing in discipline in work force. In addition, a strong nuclear security culture aids in removing the misconception and fear of radiation in the mindset of public by assuring adequate protection against perceived threat from malicious acts.

Myth-3: No need for Nuclear Security, since nothing has happened in the past

Nuclear security addresses threats towards nuclear and radioactive materials in their use, storage and transport. In order to address these threats, a variety of technical, operational and administrative measures are deployed. These measures scuttle any attempts of malicious acts towards nuclear activities. But it has to be understood that threat exits with some probability at any time. So, it may not be a good idea to live on past laurels that no nuclear security events have occurred in the past and therefore remain complacent. In fact, in order to address dynamic threat

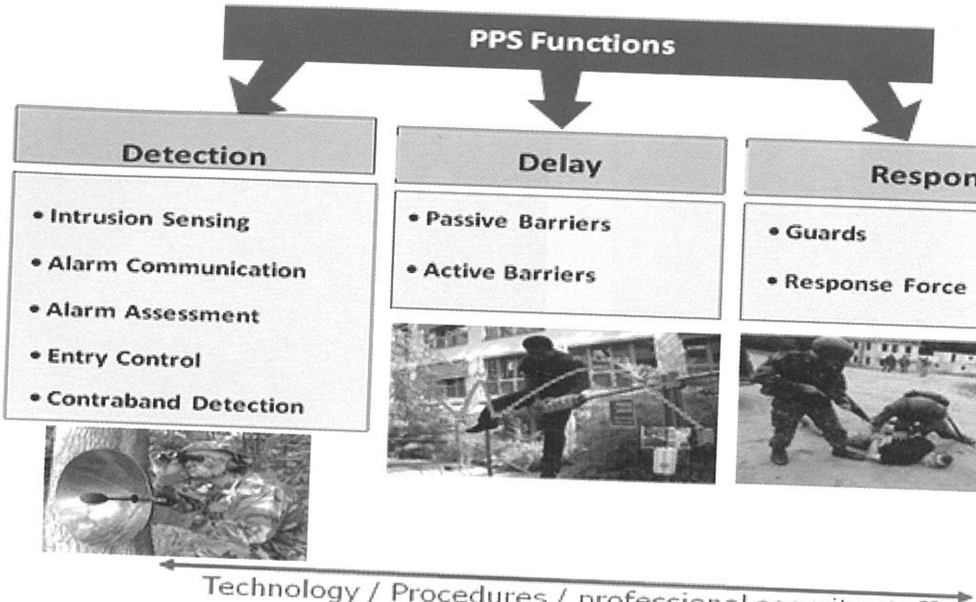


Fig. 5 PPS Functions

scenario in the global geo-politics, nuclear security measures should be appropriately reviewed and updated at regular intervals. International debates and institutions are testimony to the efforts on development of Nuclear Security – Globally.

Myth-4: Nuclear Safety and Security are always conflicting

Nuclear safety and security has a common goal, that of protection of people and the environment against radiation risks. 'Safety' is the achievement of proper operating conditions, prevention of accidents and mitigation of accident consequences, resulting in protection of workers, the public and the environment from undue radiation hazards. Safety concerns both risks under normal circumstances and risks due to abnormal environments such as flood, fire, earthquake or accidents. Security refers to the measures to detect, prevent and respond to malicious acts by adversary that may endanger human life and environment. There are some conflicting requirements in safety and security: for example, conventionally, provision of "Emergency Exit" is a safety requirement for providing an easy path for evacuation of personnel from a plant. This is, however, against security which requires that all entry and exits in a plant should have same the level of protection measures. However, such issues have been identified and adequately sorted out.

However, in many areas of safety and security procedures, there is good scope for synergies and complementary roles. Some examples include, but not limited to, the regulatory infrastructure; engineering provisions in the design and construction of nuclear installations and other facilities considering insider threat; controls on access to nuclear installations and other relevant facilities.

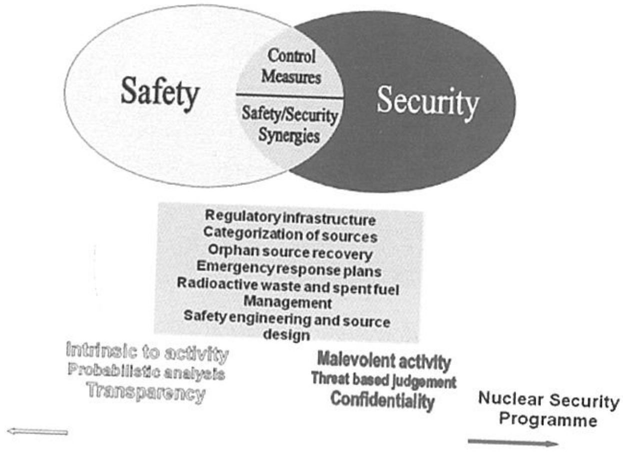


Fig. 6 Safety Security interface

References

[1] http://www.aerb.gov.in

[2] http://www-ns.iaea.org/security/

[3] Nuclear Security of Radioactive Sources in Radiation Facilities, AERB/RF-RS/SG-1, 2011

[4] Nuclear Security Requirement for Nuclear Power Plants, Issued by AERB in 2011

[5] "The Design and Evaluation of Physical Protection Systems" – Mary Lynn Garcia, second edition, BH Publication, 2008.

[6] Nuclear Security Requirement for Nuclear Fuel reprocessing Facilities (NFRF), Issued by AERB in 2013

[7] Nuclear Safeguards, security and Non-Proliferation, Edited by James E. Doyle, BH Publication, 2008

[8] Security of Radioactive Material during Transport, AERB/NRF-TS/SG-10, 2008

[9] IAEA and Nuclear Security: Trends and Prospects - Jack Boureston, Dr. Andrew K. Semmel, December, 2010

[10] Consenting process for Nuclear Power Plant and Research Reactors, AERB/NPP & RR/SG-G1

***Shri Ranajit Kumar**, an Electronics & Tele-Communication Engineering graduate from Calcutta University joined the 28th batch of BARC Training School in 1984. He has been involved in the indigenous development of technologies for electronic security systems for application in nuclear installations and various other non-nuclear industry segments. He has been actively involved in the nuclear security regulatory activities and serves in various nuclear security committees of AERB. He represents the country in the "Nuclear Security Guidance Committee" (NSGC) of IAEA. He serves as faculty for IAEA training activities in nuclear security and takes active participation in development of nuclear security documents and training course material in nuclear security. He is currently heading the Physical Protection System Section of Control Instrumentation Division, BARC and the School of Nuclear Security Studies (SNSS), Global Centre for Nuclear Energy Partnership (GCNEP)*

Integrated Security System for Nuclear Facilities

S.A.V. Satya Murty, G. Prabhakara Rao

Indira Gandhi Centre for Atomic Research, Kalpakkam, Tamil Nadu 603 102; E-mail: satya@igcar.gov.in

Introduction

The purpose of nuclear security is to prevent and neutralize nuclear terrorism, be it espionage, radiological sabotage, damage, theft etc. To carry out a comprehensive security assessment for a nuclear facility, the following needs to be understood thoroughly.

- What it is to be protected and how vulnerable it is.
- Type of threats the facility might face (Design Basis Threat) and what measures are required for prevent or mitigate.
- Understand the principles of Deterrence, Detection, Delay, Response, Recovery and Re-evaluation.
- Implement the most appropriate integrated security system for the facility based on the above inputs.

The Physical Protection System (PPS) include both trained security personnel and electronic security gadgetry, which shall be designed based on "Design Basis Threat" (DBT) of the state / Country. Also it is necessary to revise the DBT on periodic basis and upgrade the PPS accordingly.

This paper details the overview of security systems in nuclear installations and their interfaces in order to achieve maximum protection against the Design Basis Threat.

Design of Physical Protection System

The implementation of an effective Physical Protection System requires systematic approach in the design such that the PPS designed shall exceed or meet the Design Basis Threat. The first principle to be followed in the design of PPS is defense in depth, balanced protection with graded approach.

The principle of defense-in-depth is a layered security mechanism which increases security of the system as a whole. It is based on the fact that the probability of intruder bypassing multiple security measures is far less than bypassing a single security measure. If an attack causes one security mechanism to fail, other mechanisms will still provide the necessary security to protect the system. However, while designing, the various security measures taken have to be divergent. The balance protection concept provides adequate protection against all threats along all possible pathways. In other words, delay through each pathway, probability of detection with each detection element shall be equal and thus response force provides the necessary protection to prevent a successful malicious act.

Graded approach provides the highest security (delay, detection, response), as it moves towards the adversary target.

Thus to incorporate the principles of defense in depth and balanced protection, the facility shall contain several

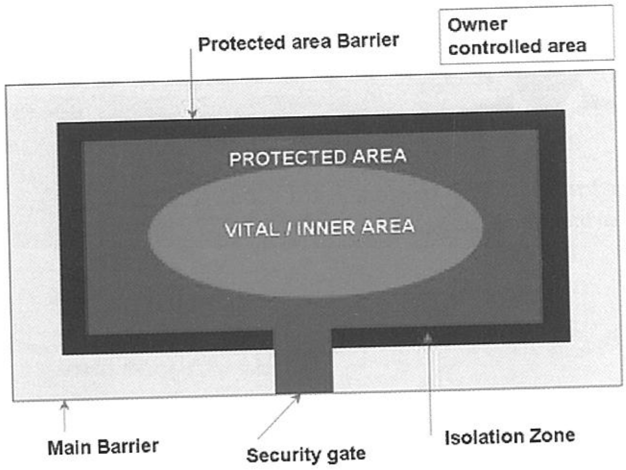


Fig. 1 Security barriers of Nuclear installation

layers of barriers and each barrier shall be equipped with PPS equipment at entrances, and all along the barrier, such that the delay times and detection probability of intrusion of each barrier shall be equal to or more than the minimum specified. Fig.1 shows the typical layout of a nuclear facility with several barriers with the concept of defense in depth, balanced protection and graded approach.

Integrated Electronic Security System design

The integrated electronic security systems facilitate communication of information from all electronic security systems to the central monitoring system in Central Alarm System (CAS) and Secondary Alarm System (SAS). This shall facilitate ease of integration, ease of information processing and ease of decision making by the security personnel. For example, an alarm from intrusion detection with auto homing of CCTV shall facilitate the security personnel to assess whether the alarm is due to intrusion or nuisance or false alarm. Based on alarm assessment, the security personnel can communicate to the response force for neutralizing the adversary.

Figure 2 shows the broad interface diagram connecting all the electronic security systems to Central Alarm Station (CAS) and Secondary Alarm Station (SAS), which in turn are connected via voice communication to the response force, local law enforcement authorities and plant management.

Electronic Protection Systems

Adversary detection, delay and neutralization are the main parameters in the design of Physical Protection System of nuclear facilities. While designing Physical Protection Systems, it is to taken in to account that the total time for detection and response must be less than the time remaining

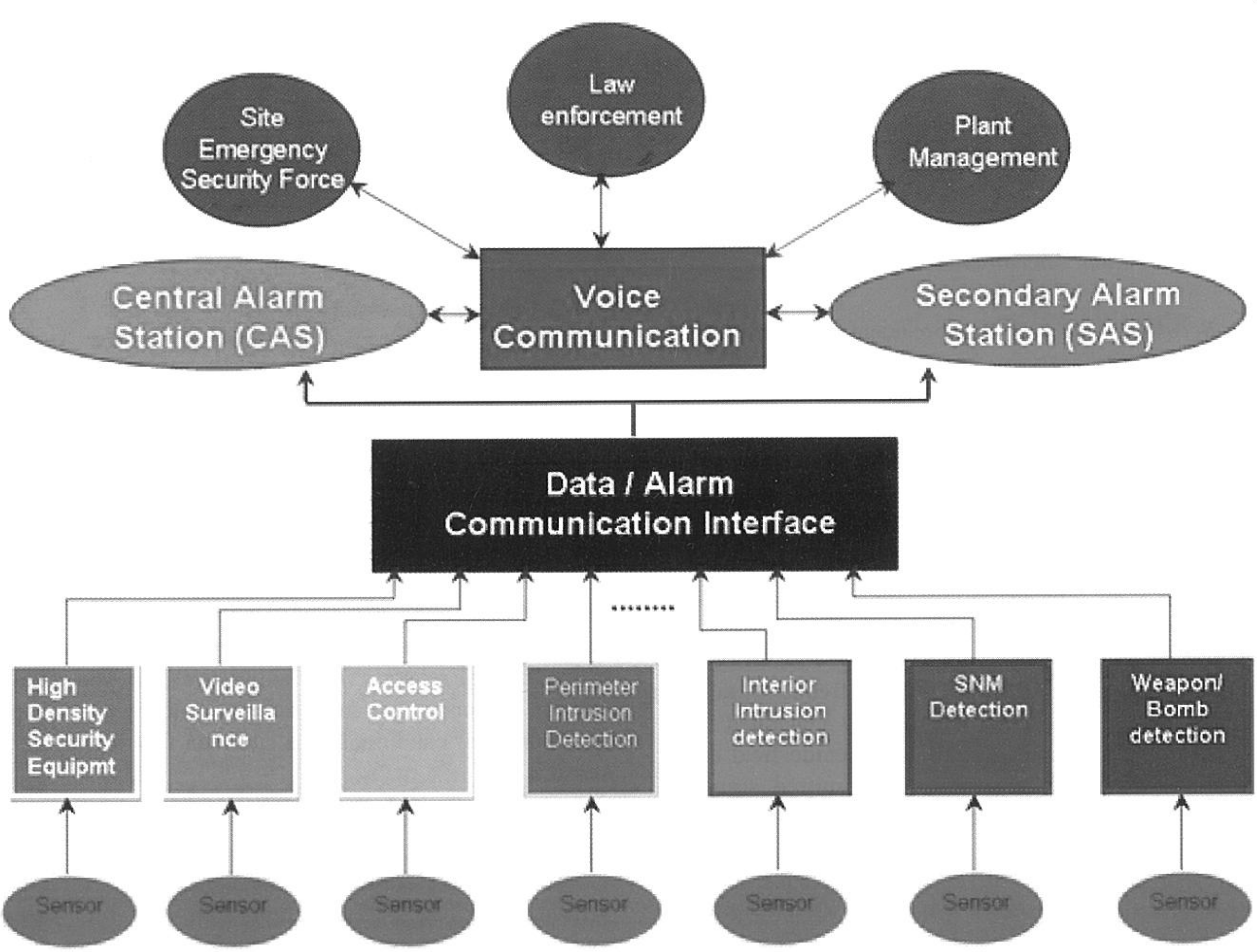


Fig. 2 Security system interface

for the adversary to complete his task after first alarm. Also it is necessary to design PPS having protection-in-depth, and balanced protection. Electronics security systems with interconnectivity among the systems help in neutralizing the adversary within the adversary task time.

The electronic systems shall be designed for the prevention of intrusion of adversary (both exterior and interior) by designing appropriate entry control system (access control), CCTV surveillance, SNM detection, weapon / bomb detection, high density security gadgets for preventing unauthorized vehicles etc.

Intrusion Detection

Intrusion detection is the detection of a person or vehicle attempting to gain unauthorized entry in to an area that is being protected. The intrusion detection boundary is ideally a sphere enclosing the installation being protected so that all intrusions, whether by surface, air, water, underwater or underground are detected. While designing the intrusion detection systems, it is necessary to consider the performance parameters such that the system has high probability of detection, less false alarm rate, and less vulnerable to defeat with tamper protection.

There are variety of intrusion detection sensors based on classification whether it is covert or visible, line of sight or terrain following, volumetric or line of detection, passive or active. Also it is necessary to interface the intrusion detection system (IDS) with CCTV surveillance. The interface provides IDS alarm signals to the CCTV's video switcher so that the correct CCTV camera will be displayed on the CCTV monitors to allow real-time alarm assessment and video recording as required.

Intrusion Detection Sensors

Intrusion detection consists of both interior intrusion (wall, window, door, ceiling, duct opening etc.) and exterior intrusion detection (crossing the boundary of protected area). Exterior intrusion needs to cover large distances and thus requires many sensors compared to interior intrusion detection.

Interior Intrusion Detection

Structural-Vibration Sensors: Structural-vibration sensors detect low-frequency energy generated in an attempted penetration of a physical barrier (such as a wall or a ceiling) by hammering, drilling, cutting, detonating explosives, or employing other forcible methods of entry.

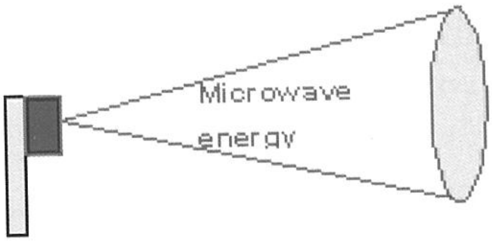


Fig. 3 Mono static Microwave sensor

Glass-Breakage Sensors: Glass-breakage sensors detect the breaking of glass. The noise from breaking glass consists of frequencies in both the audible and ultrasonic range. Glass-breakage sensors use microphone transducers to detect the glass breakage. The sensors are designed to respond to specific frequencies only, thus minimizing such false alarms as may be caused by banging on the glass.

Microwave Motion Sensors: Interior microwave motion sensors (Fig.3) are typically mono static; the transmitter and the receiver are housed in the same enclosure (transceiver). They may each be provided with a separate antenna or they may share a common antenna. The high-frequency signals produced by the transmitter are usually generated by a solid-state device, such as a gallium arsenide field effect transistor. The frequency of the transmitted signal is compared with the frequency of the signal reflected back from objects in the protected area. If there is no movement within the area, the transmitted and received frequencies will be equal and no alarm will be generated. Movement in the area will generate a doppler frequency shift in the reflected signal and will produce an alarm, if the signal satisfies the sensor's alarm criteria. The doppler shift for a human intruder is typically between 20 and 120 hertz.

PIR Motion Sensors: PIR motion sensors detect a change in the thermal energy pattern caused by a moving intruder and initiate an alarm when the change in energy satisfies the detector's alarm criteria. These sensors are passive devices because they do not transmit energy; they monitor the energy radiated by the surrounding environment. All objects with temperatures above absolute zero radiate thermal energy. The wavelengths of the IR energy spectrum lie between 1 and 1,000 microns. Because the human body radiates thermal energy of between 7 and 14 microns, PIR motion sensors are typically designed to operate in the far IR wavelength range of 4 to 20 microns.

Video Motion Sensors: A video motion sensor generates an alarm when an intruder enters a selected portion of a CCTV camera's field of view. The sensor processes and compares successive images between the images against predefined alarm criteria.

There are many sensors available for interior intrusion detection viz. Passive Ultrasonic Sensors, Detection Transducer, Balanced Magnetic Switches, Grid-Wire Sensors, capacitance sensors, pressure mats, pressure switches etc.

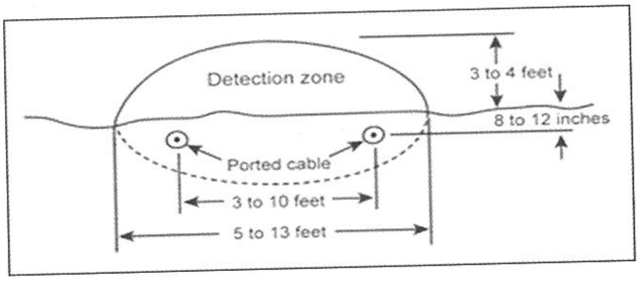


Fig. 4 Buried line sensor

Exterior Intrusion Detection

Exterior intrusion-detection sensors are meant to detect an intruder crossing the boundary of a protected area. Exterior sensors are designed to operate in outdoor environmental conditions. The detection function must be performed with a minimum of nuisance alarms such as those caused by wind, rain, animals, and other sources. Important criteria for selecting an exterior sensor are the probability of detection (PD), the sensor's susceptibility to unwanted alarms, and the sensor's vulnerability to defeat. The PD of an exterior sensor is much more vulnerable to the physical and environmental conditions of a site than that of an interior sensor.

Because of the nature of the outdoor environment, exterior sensors are also more susceptible to nuisance and environmental alarms than interior sensors. Inclement weather conditions (heavy rain, hail, and high wind), vegetation, the natural variation of the temperature of objects in the detection zone, are major sources of nuisance alarms

Several different types of exterior intrusion-detection sensors are available. They can be categorized as

- Fence sensors.
- Buried line sensors.
- LOS (Line of Sight) sensors.
- Video motion sensors.

The type of sensor is to be selected based on the probability of detection, environmental conditions, terrain of the area, wind, annual rain fall, ice, water body nearby, animals and birds etc.

Fence sensors: Fence sensors detect attempts to penetrate a fence around a protected area. Widely used fence sensors are Strain-Sensitive Cable, Taut-Wire Sensor, Fiber-Optic Cable Sensors, Electric-Field Sensors, Capacitance Proximity Sensors etc.

Buried Line sensors: A buried-line sensor system (Fig.4) consists of detection probes or cable buried in the ground, typically between two fences that form an isolation zone. These devices are wired to an electronic processing unit. The processing unit generates an alarm, if an intruder passes through the detection field.

Line of sight (LOS) Sensors: The LOS sensors, which are mounted above ground, can be either active or passive.

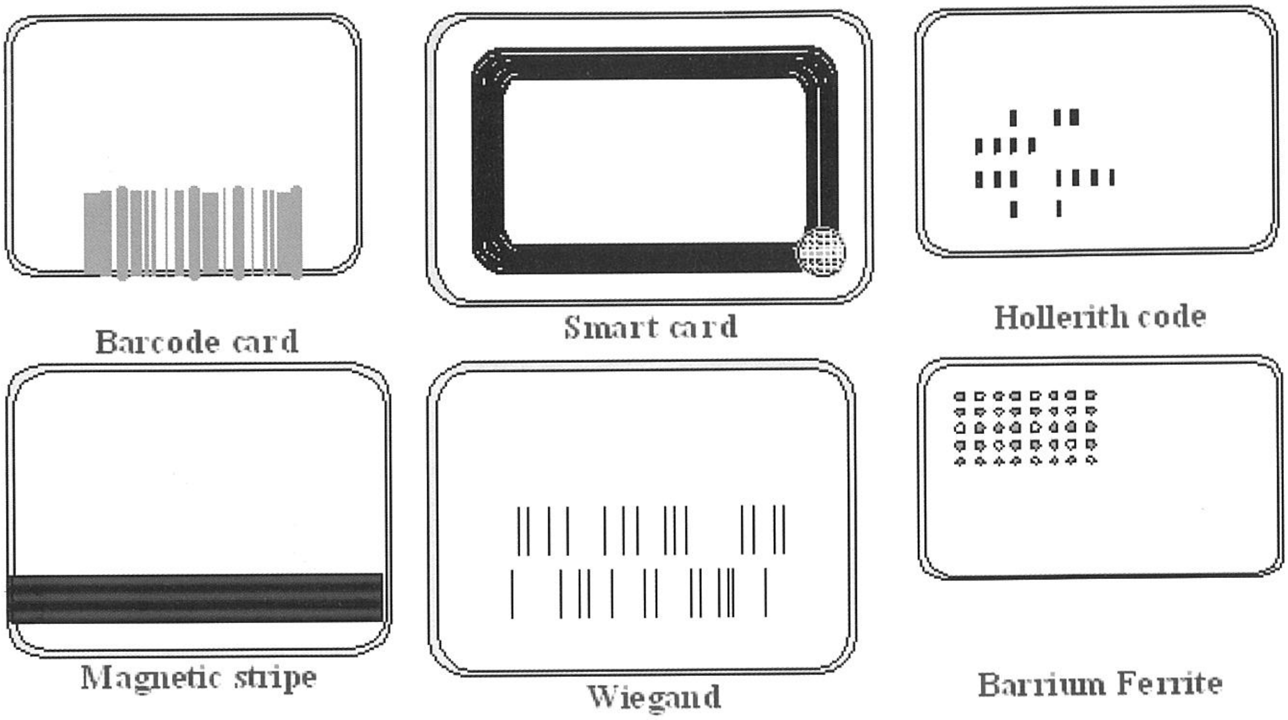


Fig. 5 Credential Devices

Active sensors generate a beam of energy and detect changes in the received energy that an intruder causes by penetrating the beam. Each sensor consists of a transmitter and a receiver and can be in a mono static or bi-static configuration. Passive sensors generate no beam of energy; they simply look for changes in the thermal characteristics of their field of view. For effective detection, the terrain within the detection zone must be flat and free of obstacles and vegetation.

There are many types of LOS sensors, which include bi-static microwave, Mono static microwave, long range exterior PIR, video motion sensors, active IR sensors etc.

Electronic Entry Control

The function of an entry control system is to ensure that only authorized personnel are permitted into or out of a controlled area. Entry can be controlled by locked fence gates, locked doors to a building or rooms within a building, or automatic control by means of coded cards or by biometric authentication systems..

All entry-control systems control passage by using one or more of three basic techniques—something a person knows, something a person has, or something a person is or does. Automated entry-control devices based on these techniques are grouped into three categories—coded, credential, and biometric devices.

Coded Devices Identification

Coded devices operate on the principle that a person has been issued a code (PIN) to enter into an entry-control device. This code will match the code stored in the device and permit entry.

Credential Device Identification

A credential device identifies a person having legitimate authority to enter a controlled area. A coded credential (card) contains a prerecorded, machine-readable code. An electric signal unlocks the door if the prerecorded code matches the code stored in the system when the card is read. Like coded devices, credential devices only authenticate the credential; it assumes a user with an acceptable credential is authorized to enter. Various technologies are used to store the code upon or within a card. Examples are Hollerith, bar coded, magnetic-spot, watermark magnetic, proximity, wiegand, RFID card, Smart card etc. (Fig. 5)

Biometric Device Authentication

The third technique used to control entry is based on the measurement of one or more physical or personal characteristics of an individual. Because most entry-control devices based on this technique rely on measurements of biological characteristics, they are known as biometric devices. (Fig. 6). Characteristics such as fingerprints, hand geometry, voice prints, hand writing, and retinal blood-vessel patterns have been used for controlling entry. Typically, in enrolling individuals, several reference measurements are made of the selected characteristic and then stored in the device's memory or on a card. From then on, when that person attempts entry, a scan of the characteristic is compared with the reference data template. If a match is found, entry is granted. Rather than verifying a code or a credential, biometric devices verify a person's physical characteristic, thus providing a form of identity

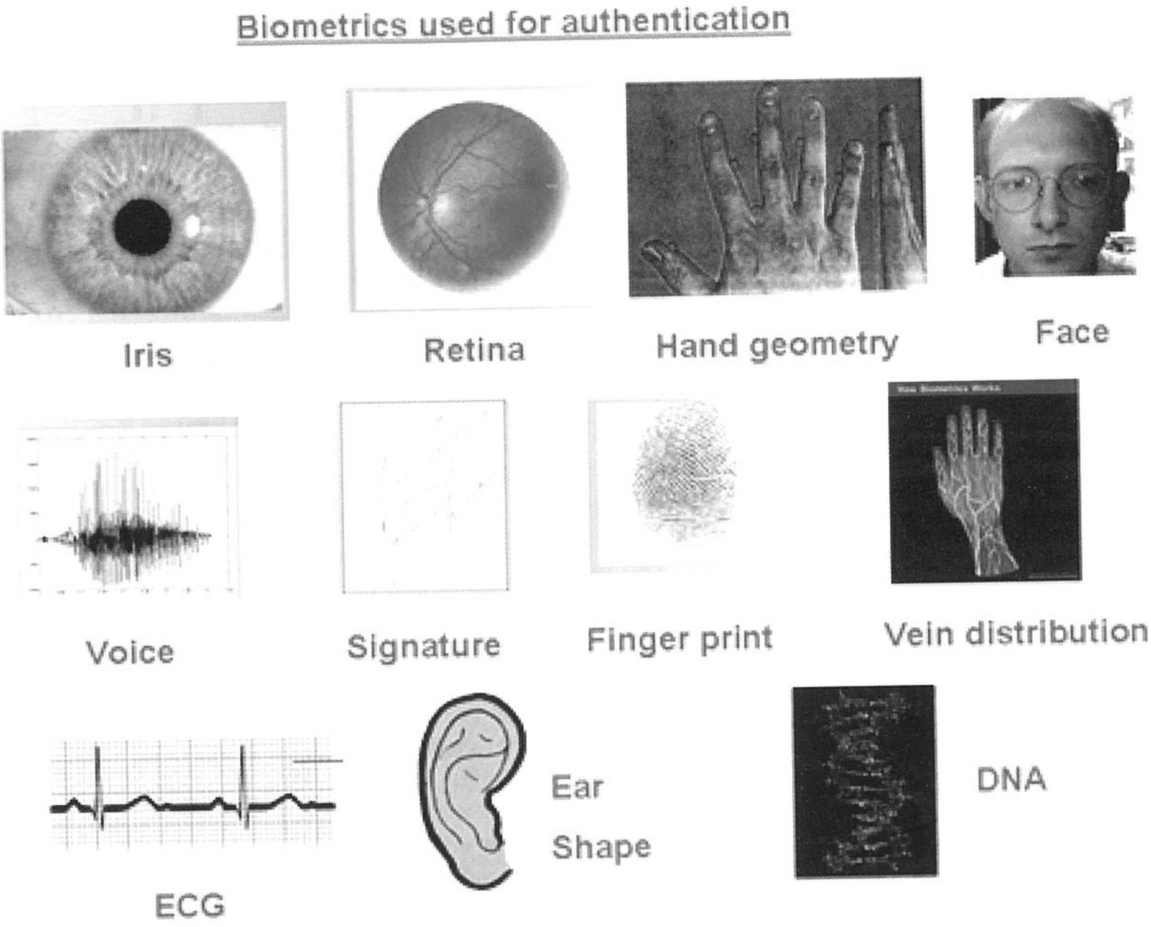


Fig. 6 Biometric based authentication

verification. Because of this, biometric devices are sometimes referred to as personnel identity verification devices. Some of the important automatic biometrics being used in most of the highly secured installations are given below. Multimodal biometrics (authentication of more than one biometric feature) can be explored for extremely high secured areas.

CCTV for Alarm Assessment and Surveillance

An integrated CCTV assessment system provides a rapid and cost-effective method for determining the cause of intrusion alarms. For surveillance, a properly designed CCTV system provides a cost-effective supplement to guard patrols. The alarm-assessment system is designed to respond rapidly, automatically, and predictably to the receipt of all alarms at the security center. Figure 7 shows a typical CCTV system configuration.

Vehicle Access Control System

Automatic Road Blockers (Fig.8) Bollards, Tyre Killers (Fig.9) are an effective means of controlling access to high security areas, stopping vehicles or heavy trucks from entering. These systems can be designed to remain fully operational after the impact and consequently continue to guarantee the full level of security. The blockers, tire killers are available in different dimensions, different impact

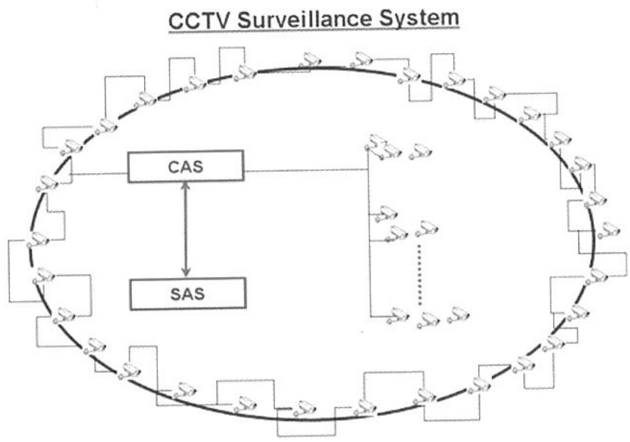


Fig. 7 CCTV Surveillance System

strength, different heights and minimum raise time. The blockers and tire killers can be fitted with vehicle sensing inductive loop on both sides, so that damage of authentic vehicle can be prevented.

Under Vehicle Surveillance System (UVSS)

UVSS (Fig.10) is designed to scan, monitor, and digitally record, clear digital video images of the entire width of a vehicle's under chassis. This shall enable the security personnel for finding any unauthorized object being carried

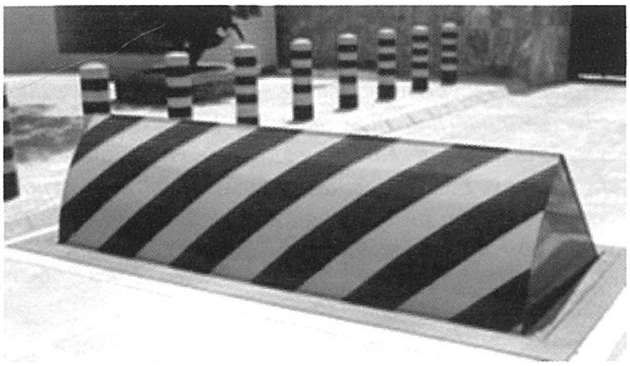


Fig. 8 Road blocker

at the bottom of the vehicle. Also UVSS systems are provided with number plate recognition, which will record all the vehicles entering the premises. Figure 10 shows various constituents of UVSS.

Explosive, Artillery, SNM and Contraband Detection

The detection method shall be non-destructive process to determine whether a container contains explosive material, ammunition, artillery and any contraband. Several types of systems were developed to detect trace signatures for various explosive materials. The most common technology for this application is ion mobility spectrometry (IMS). This method is similar to mass spectrometry (MS), where molecules are ionized and then moved in an electric field in a vacuum, except that IMS operates at atmospheric pressure. The time that it takes for an ion in IMS to move a specified distance in an electric field is indicative of that ion's size to charge ratio: ions with a larger cross section will collide with more gas at atmospheric pressure and will therefore be slower.

Trained dogs can be used to detect explosives. Though they are very effective, their effectiveness comes down as a dog becomes tired or bored.

Various devices based on different techniques are available in the market for detecting Special Nuclear Materials (SNM) such as uranium and plutonium. These systems enable the security guard to detect and identify the adversary carrying any nuclear material out of the premises and take preventive action.

X-ray machines are used to screen objects non-invasively for any Improvised Explosive Detectors, artillery etc. Packages/ bags are examined for possible weapons, including bombs. The main parts of an X-ray baggage inspection system are the generator used to generate X-rays, the detector to detect radiation after passing through the baggage, signal processor unit (usually a personal

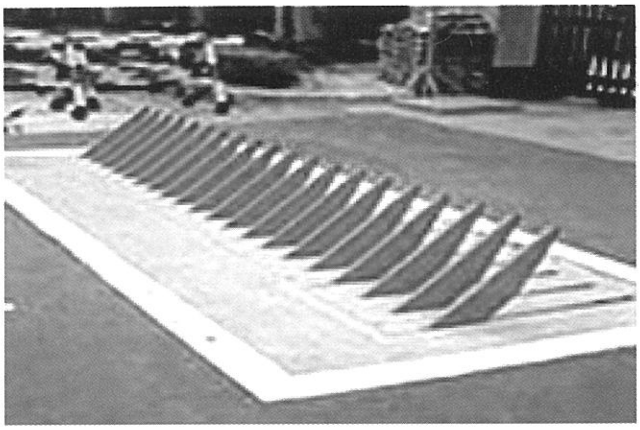


Fig. 9 Tyre killer

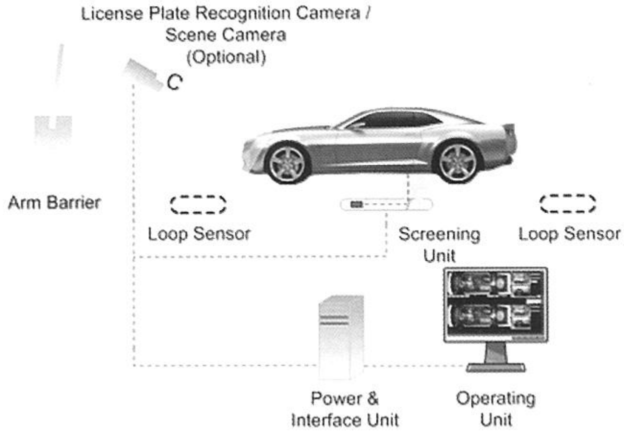


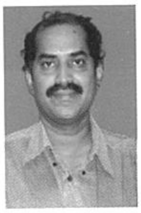
Fig. 10 Under vehicle surveillance system

computer) to process the incoming signal from the detector and a conveyor system for moving baggage into the system.

Summary

For the protection of nuclear facility, it is necessary to design the Physical Protection System consisting of security personnel and integrated security electronic systems which exceeds or meet the Design Basis Threat. Also it is very important to have built-in tamper proof system, so that the adversary cannot bypass the alarm with insider assistance. Also while designing the PPS systems, it is kept in mind that false alarm rate shall be lowest (not more than one per day) with online surveillance facility. For effective security an integrated system with different devices based on divergent principles is essential. Also the security systems have to be upgraded with time in tune with the intrusion methods and developments in technology.

Shri S.A.V.Satya Murty *did his B.Tech. from Jawaharlal Nehru Technological University in 1977. He was a University Gold Medalist in his B.Tech. Later, he joined one year orientation course in Nuclear Science & Engineering (21st Batch) at BARC. He was awarded Homi Bhabha prize for getting 1st rank. He has more than 150 Journal Publications / Conference Papers and edited two International Conference Proceedings. He had written two chapters in important books. He also has more than 50 Internal Design Reports. He is a member of various technical committees of DAE. He had submitted his Ph.D thesis in the area of Wireless sensor networks. Currently, Shri Satya Murty is the Director of Electronics, Instrumentation and Radiological Safety Group of IGCAR and Director, Engineering Services Group of GSO. He was awarded Outstanding Service award 2011 by Indian Nuclear Society and Group Achievement award by DAE in 2011 and 2012.*



Shri G. Prabhakara Rao, *graduated from 29th batch of Babha Atomic Research Centre (BARC) training school, Mumbai 1985. Subsequently he joined Indira Gandhi Centre for Atomic Research (IGCAR), Kalpakkam. Presently he is Head of Security Electronics Section / Electronics, Instrumentation & Radiological Safety Group. His areas of interest are development of Radio Frequency Identification (RFID) systems for multi application. Biometric systems for access control, CCTV systems, Intrusion Detection systems and Development of Embedded systems for security etc. MEMS (Micro Electro Mechanical Systems) based accelerometer data acquisition systems for Reactor structural monitoring. He also developed various systems for Reactor control and monitoring.*

Development of Nuclear Security Regulations by AERB

Fredric Lall

Atomic Energy Regulatory Board, Niyamak Bhavan, Anushaktinagar, Mumbai 400 094; E-mail: flall@aerg.gov.in

Introduction

Atomic Energy Regulatory Board (AERB) was formed in the year 1983 with the powers to lay down rules and regulations for enforcing regulatory and safety requirements. AERB carries out review and assessment through its Committees to ensure that nuclear facilities are built and operated in a safe and secure manner and they do not cause unacceptable radiological risk and/or toxic chemical exposure to plant & site personnel, the public and the environment.

Nuclear Security Objective

It has been decided that aspects related to Nuclear Security would also be reviewed and assessed, for different types of nuclear facilities, by AERB.

- To minimize the risk of unauthorized removal of nuclear & radioactive material
- To minimize the risk of sabotage on nuclear & radiation facilities
- To minimize the risk of adverse impact during the above acts

Nuclear Security under AERB's Purview

Aspects of Security having Bearing on Nuclear Safety (Main Plant Boundary (MPB) and area inside MPB) are regulated by AERB.

- Engineering Aspects of Physical Protection System (PPS) within MPB.
- Nuclear Security of:
  - Nuclear Power Plants/Projects (NPPs), H_2S based Heavy water plants, interim Fuel Storage facilities, FRFCF.
  - Radiation Facilities
  - Radioactive materials during transportation

Reviews

- The regulatory review for this purpose covers the design, operation and maintenance of nuclear security systems within MPB including Operating Island, Vital/ Inner Areas and Central Alarm Station
- Regulatory review based on the provisions brought out in the documents prepared by AERB & relevant IAEA documents on security of NPPs
- Review observations/recommendations considered while granting clearance for particular stage of NPP

Committees to review Security Aspects:

AERB has three tiers of review on nuclear security aspects:

- First Tier Review:
  - Committee for Reviewing Security aspects of Nuclear Facility (CRSANF)
  - Committee for review of Nuclear Security aspects of radiation facilities and for transport of Radioactive Materials (CRSARF & T)
- Second Tier Review
  - Safety Security Interface maintained at AERB level by review of reports of first tier by Safety Review Committee for Operating Plants (SARCOP) for Plants and respective Advisory Committee for Project Safety Review (ACPSR) for Projects, Safety Review Committee for Application of Radiation (SARCAR) for Radioactive Material.
- Third Tier Review
  - Atomic Energy Regulatory Board
- Advisory Committee on Security (ACS)- Advises on all nuclear security aspects

Documents Prepared

- Nuclear security requirements for NPPs, H_2S based HWP, ISFS, FRFCF
- Guide lines for reporting of nuclear security events
- Checklist for Regulatory Inspection (RI) of NPPs, H_2S based HWP
- Procedure for identification of Vital Areas
- Security of radioactive sources in Radiation Facilities (RF)
- Security of Radioactive Material (RAM) during Transport
- *Other documents under preparations*
  - *Check list for RI of ISFS & FRFCF*
  - *Check list for RI of RF, RAM during transport*

Preparations of Preliminary Document

Design and operational provisions for the security of nuclear material and facilities in India have been significantly upgraded since 2002. A manual on security for NPPs was prepared by the Atomic Energy Regulatory Board (AERB) covering aspects such as physical protection systems, training & certification of personnel, documentation and reporting. Since implementation of all the provisions of the manual would have taken considerable time, 'Minimum Requirements of Physical Protection System (PPS)" was specified for all NPPs. These requirements include; checking credentials of personnel, establishment of exclusion boundary, main plant boundary and operating island and incorporation of delay elements, physical barriers, Central Alarm Station (CAS), configuration management etc. using a graded approach. Such documents were prepared taking inputs from IAEA documents related to security. All sites were asked to be compliant with these requirements, followed by regulatory inspections.

Updating Minimum Requirements of PPS

Based on the review of regulatory inspection and response from site, the minimum requirements for PPS for NPPs upgraded to include aspects such as,

- Upgraded to include based on experience: Auxiliary CAS, Inclusion of distress alarm system to other important locations, Secured back-up power supply, Cable layout for PPS through diverse routes, Water Body, Fail safe / secure feature, Security Organization, Safety - Security Interface
- Upgraded to include policy/procedures: Maintenance policy, dedicated maintenance group for PPS equipment, Standard Operating Procedures (SOP), exercises and improvements based on feedback, Quality Assurance & Quality Control, Training of personnel, Licensing of security system operator, plant operator & response force, Security event reporting system, documentation and record keeping, confidentiality requirements, Modification/ upgradation proposals of PPS.

Utility's comments were considered during document development

Requirements for Projects

Consideration of Design Basis Threat (DBT) for PPS design

Details of physical protection system design should address site specific DBTs to show that, suitable technical and administrative precaution will be taken in order to prevent persons from carrying out unauthorized actions, which could jeopardize safety, willfully or otherwise.

PPS Requirements for Projects

The AERB guide on Consenting Process for NPPs and Research Reactors lays down the requirements of safety and security for different stages of a project and all the projects under construction will have to comply with these requirements. This also includes the security requirements for new fuel storage area before arrival of fuel at the site.

Procedure exists for review of PPS for grant of authorization for different stages of the Projects. Reviewing authorities for different stages of projects are identified based on the importance of the stages. The major stages of AERB's consenting process are as follows:

- Siting
- Construction
- Commissioning
- Operation

Based on the experience, these requirements were updated and additional requirement for projects coming up near operating NPP was specified. Access control procedures for contractor's personnel, vehicles and materials have been specified for projects being constructed near an operating plant.

Some of the additional requirements such as; Identification of critical area during different stages of the projects and provision for monitoring and control, Commissioning of PPS for New Fuel Storage Building before arrival of fuel, commissioning of all PPS before Initial Fuel Loading (IFL).

It was recommended that the nuclear security aspects review of projects, for which construction clearance granted up to January 2008 should be done at the stage of Fuel Loading, and for Projects for which construction clearance was granted after January 2008, it will be reviewed from siting onwards.

PPS requirements at different stages considered for the project with single units coming up at new place, project with multiple units at new sites, and projects coming up at sites with already existing operating nuclear power plants.

Difference in requirements for single and multiple units is, that for multiple unit projects, as soon as the first unit is ready for Initial fuel loading, it needs to be segregated from the unit under construction and commissioning. Similarly, if the projects are coming near already existing operating plant, the operating nuclear power plant should be segregated from the upcoming project to avoid any unauthorized access by personnel, unauthorized movement of material or vehicle.

All PPS requirement are to be commissioned before the stage of initial fuel loading to the plant. These should also include: Establishment of PPS, Training and licensing, Quality Assurance, Surveillance requirements on PPS, Record Maintenance and Documentation Control, Maintenance of Security Culture, Establishment of Security Organization, Audit and Inspections, Security Emergency Plan, identification of Hazardous Material and its control and monitoring during storage and handling.

Regulatory Inspection

Basic philosophy of nuclear security RI is the same as that of safety RI of NPPs. It may be planned/ unplanned/surprise inspections. It is being done once in a year for Operating Plants, and for Projects, depending on the stage of the project. Approval is taken for yearly inspection schedule for plants along with authorisation of Team Leader/ Lead Inspector/Inspectors. The Member of the Inspection Team are trained and experienced in the nuclear security aspects. Mostly the members are from CRSANF. Intimation to sent site for planned inspection. Approximately 4 members are there in Inspection team. Inspection is carried out for 2-3 days depending upon number of Operating Islands to be inspected.

Inspections based on checklist for RI, AERB documents, recommendations made by AERB, follow-up of previous RI, Security Events reported earlier, Modifications/ Upgradation done in PPS systems

Introductory meeting held with only those connected with nuclear security aspects. Initial briefing is by Team Leader followed by presentation by site on present physical protection systems & status of previous RI observations. Finally, the plan for the inspection is decided

RI are carried out by field checks, documents verification and interviews/ competency checks.

During Field visits checks are done at different layers; Main Plant Boundary (MPB), Operating Island (OI) and Vital Area (VA) /Inner Area (IA) for: Detection, Delays, Assessment, Access control for personnel, Vehicle and Materials, Functioning of various gadgets, Power supplies, Communication, Alarms, Central Alarm Station/Alternate Alarm Station, Illumination, physical protections on Water body side. Also during field visits, the checks are done for impact of new projects under construction near operating plants such as; Segregation between project and operating plant, Access control for construction personnel, vehicle and materials to project, Location of Construction labour camp, Location of contractors work shop,.

Document verified are list of Vital Areas/ Inner Areas, Access controls procedures for; personnel (Visitors & Contractors), Vehicle & Material Movements. Records of; Surveillance & Audit (Internal & external), PPS gadgets maintenance, Exercises done and deficiencies and corrective actions taken, Modifications & Up-gradation of PPS, Non availability of gadgets and alternate measures adopted, Security committees constitution orders their minutes of meeting along with follow-up actions, Training Syllabus, Configuration Control, Internal Audit, Security Organization. Procedures for; standard operation, Reporting and Evaluation, Contingency. Interfaces between: Safety and Security, Plant Management and Security organization, Site security organisation with external agencies

Interviews/ competency checks for : Plant Management, Central Alarm Station (CAS) operators, Main Guard House (MGH) Security Personnel, Operational & Maintenance staff.

Exit Meeting held for briefing of observations & deficiencies and immediate corrective actions. While according major clearances by AERB satisfactory resolution on security issues are ensured.

Nuclear Security Event (NSE) Reporting System:

NSE is to monitor the nuclear security status of nuclear facilities. It may be associated with the system, structure, component of the facility, physical protection system (PPS) or administrative procedures for security. Graded approach is followed for the events reportable to the Regulatory Body (RB): Nuclear Security Event (NSE) and Significant Nuclear Security Event (SNSE).

NSE

Events related to the outer most barrier and other administrative controls: These are reported to RB in specified format within specified time by facility management after review by security review committee along with the comments of their apex committee on security.

SNSE

Any casualty related to security in any area within Exclusion Boundary, nuclear security events related to operating island, inner area, vital area & CAS has to be reported to RB in three stages within specified time i.e. Prompt Notification (first stage) - within short time, SNSE report (2nd stage) – within specified time. Should include sufficient technical details and human factor data, Root Cause Analysis (RCA), Corrective actions (taken or/and planned), Lesson learned. Final Report (3rd stage)

The reports are stored with confidentiality preferably in electronic form, which are to be analyzed on a trial basis before fixing the actual review frequency. It is also used to strengthen the PPS, security related administrative procedures and identification of new field of security concern

Vital Area Identification

Vital Area Identification is a structured approach based on logic diagrams to identify location of critical components, sabotage to which may cause unacceptable radioactive release.

General guidelines have been prepared for identification of vital areas. Utility should carry out Vital Area Identification methodically. Based on operating experience gained, utility should be able to justify why a particular area is designated as vital area. Once the area is declared as vital area, all the PPS requirements for Vital Area should be fulfilled.

Interfaces

In order to ensure effective PPS without interfering with safety, interfacing between security & safety, and between plant management and security organisation should be established. The detailed work on these aspects will be taken up in near future, while some guidelines have already been established as described below;

Security & Safety Interface

All recommendations of safety and security committees are communicate to each other in order to ensure recommendations of either committee does not jeopardise the safety or security.

Interface between Plant Management and Security Organization

The senior most persons of the plant management and security organization present at the site should be in communication with each other. However there is need to prepare guidelines on this topic for proper co-ordination between the two organization to cope with the security related emergencies in an effective and efficient safe manner.

Interface between Site Security and External Site Security Agencies

Procedures should be prepared for interface between site security and external security agencies for additional response requirements. The procedure should be checked at routine intervals to check the functions of gadgets and verify the implementation of procedure.

Security of Radioactive Sources in Radiation Facilities & during Transport

To address the issues of security of radioactive source in the radiation facilities, the AERB Safety Guide on "Security of Radioactive Sources in Radiation Facilities" (AERB/RF-RS/SG-1) and AERB Safety Guide on "Security of Radioactive Material During Transport" (AERB/NRF-TS/SG-10) have been issued.

Checklist for RI has been prepared which will be sent to the radiation facilities and compliance will be obtained followed by conduct of RI.

Awareness program for law enforcing authorities and radiation facility owners and RSO have started. Initially done at Mumbai region, it will cover all the four zones by the end of 2014. The awareness program is to sensitise the law enforcing agencies and the facility owners regarding requirement of registration of security plan by the local law enforcing agencies for Category I radioactive materials and verification of antecedents of owner and handlers of category I &II radioactive materials.

Conclusion

- Adequate security coverage exists for operating plant and projects concerning Physical Protection.
- Regulatory reviews of RAMs on nuclear security aspects will start shortly as per published document.
- Continuous improvements based on experience and new developments are underway.
- Further Guidelines will be developed based on experience / requirement.

References

[1] Nuclear Security Requirement for Nuclear Power Plants, Issued by Atomic Energy Regulatory Board (AERB) in 2011

[2] Nuclear Security of Radioactive Sources in Radiation Facilities, AERB / RF-RS / SG-1, 2011

[3] Nuclear Security Requirement for Nuclear Fuel reprocessing Facilities (NFRF), Issued by AERB in 2013

[4] Reporting System for Events related to Nuclear Security for Nuclear Power Plants, Issued by AERB in 2011

[5] Guidelines for reporting of Nuclear Security Events (NSEs) and Significant Nuclear Security Events (SNSEs).

[6] Issued by AERB in 2011

[7] Minimum Requirement for PPS at all NPPs, Issued by AERB in 2010

[8] Security of Radioactive Material during Transport, AERB / NRF-TS / SG-10, 2008

[9] Consenting process for Nuclear Power Plant and Research Reactors, AERB / NPP & RR / SG-G1

[10] AERB manual on Security for Nuclear Power Plants, Issued by AERB in 2003

[11] Security Requirement for H_2S Based Heavy Water Plants, Issued by AERB in 2013

***Shri Fredric Lall**, Electrical Engineer, joined 21st batch of BARC Training School in August 1977 and after completion of training, he was working as qualified operations engineer in CIRUS and Dhruva reactors, in Reactor Group BARC until January 2001, when he was transferred to Nuclear Projects Safety Division of Atomic Energy Regulatory Board. He was involved in Design safety review of KGS 3&4 and RAPP 5&6 from siting to operational stage. He is also involved in design safety review and commissioning of Kudankulam units 1&2. He is Chairman of committees for review of nuclear security aspects of Nuclear & Radiation Facilities and during transport of radioactive materials. He is also member secretary of Advisory committee for Security, AERB. Many regulatory documents on nuclear security aspects for Nuclear and Radiation facilities have been prepared and issued under his guidance.*

Security in Transport of Radioactive Material

A.N. Nandakumar

Formerly Head, Radiological Safety Division, Atomic Energy Regulatory Board, Mumbai, E-mail: a.n.nandakumar@gmail.com

Safety and Security

Transport of radioactive material has an impressive safety record globally. This is due to the safety standards and the associated safety requirements which have been enshrined in national and international regulations for the safe transport of radioactive material. Approach to safety has two components, viz., design standards for packages and radioactive material and control measures for transport. The design standards are so devised that the package can withstand severe accident conditions that may be encountered during transport and storage in transit. Recently, however, the scenario is showing signs of change. There are security threats lurking on the road, as it were. The types of challenges that a shipment under security threat may face are widely varied. A package containing radioactive material, during transport, is in public domain. It is manifestly impossible to provide security escort to every radioactive consignment. In India, more than one hundred thousand radioactive consignments are transported every year and the number is increasing.

International regulations for the safe transport of radioactive material require that measures be taken to ensure that radioactive material is kept secure in transport so as to prevent theft or damage and to ensure that control of the material is not relinquished inappropriately [1]. In India, the Atomic Energy Regulatory Board has published a guidance document on the security of transport of radioactive material [2].

Need for Transporting Radioactive Material

Production of nuclear power and the many uses of radioisotopes in medicine, industry and research require carriage of radioactive materials. In connection with the production of nuclear power uranium ore concentrates should be moved from the mines for fuel fabrication. Fabricated fuel has to be sent to nuclear power plants. Spent fuel and radioactive wastes from nuclear power plants have to be transported to appropriate repositories.

Radioisotopes are used in hospitals for the diagnosis of a large number of diseases and to study the function of various organs. They are used in the treatment of cancer. There are nearly 500 medical facilities where diagnostic and therapeutic procedures are carried out in India using these sources of radiation. The sources should be transported from the supplier's end to the user institution. Radioactive sources are increasingly used for sterilization of food grains, spices and healthcare products. Industrial radiography for non-destructive testing of welding and casting is a common application of radioactive material. A large number of industrial institutions in India use sealed sources in process control systems such as ensuring uniform thickness of paper, plastic films and metal plates, measurement of density in construction industry, coal mining, oil exploration, determining fluid level in columns, filling levels of beverage cans, etc.

All these applications necessitate transport of (a) new sources from the supplier to the user and (b) decayed sealed sources from the users to the disposal facility.

Security in Transport of Radioactive Material

The unique feature of the transport scenario is that a mishap may occur anywhere during transport. Whereas in a facility, expertise and equipment are available locally, such help in general will not be readily available locally during transport. Hence certain precautions should be observed to ensure that the radioactive material is not diverted, lost or stolen during transport. Control over the radioactive material should be maintained at all times during transport. Thus appropriate security measures should be in place during transport of radioactive material.

Security Threat Scenarios

While the design of the standard packages used for transport of radioactive material will ensure that there would be no significant radiological concern arising from an accident scenario, there could be safety concerns arising due to a breach in the security of such material. This breach in security could occur due to weakness in administrative procedures, which could result in a source getting lost or due to deliberate acts of theft to take control of the source for use in criminal activities like making a radiological dispersal device (RDD) or due to the possibility of sabotage during transport. Consequently, security measures would have to address all these scenarios. Though high radioactivity sources pose a greater threat under such scenarios, they could be considered as an unattractive option by the adversary, except under extreme circumstances, because of the high fatality risk to the person committing the theft. Further, the heavy shielding provided for such sources is a physical deterrent for stealing. Therefore, lightweight packages carrying significant quantities of radioactive material are the ones that have greatest potential for being misused and hence require adequate security provisions.

Security Threat Perception

Security measures are implemented on the basis of perceived threats. Threat may vary from place to place and in a given location threat may vary from time to time. Hence security measures should take into account the threat level at the time of the proposed transport. Transport is potentially the most vulnerable phase in the life cycle of a radioactive material. If a conveyance is seized, it could be used to quickly move the material to high consequence locations for dispersion or coercion.

Threat has two components, viz., intent and capability of the potential perpetrators. Capability includes obtaining suitable material, as well as utilizing it effectively. Security must directly address limiting the capability.

Graded Approach to Security

The extent of security control provided for a radioactive shipment should be commensurate with the potential risk associate with the loss of control over the shipment. Risk may be defined as the product of the probability of occurrence of a security event and the consequence. The consequences of a security threat may have many dimensions including loss of life, damage to property, social disruption and psychological effects. The radiological consequence can be related to the nature and quantity of the radioactive material being transported. Hence security measures should have direct bearing on the risk associated with the shipment. This graded approach has resulted in identifying four levels of security, namely, prudent management practices, basic, enhanced and additional levels of security.

The International Atomic Energy Agency has published recommendations specific to security in the transport of radioactive material and nuclear material [3-5].

Security Levels

Three levels of security are envisaged during the transport of radioactive material. These are detailed in the following paragraphs.

Level 1 - Prudent Management Practices

This is the minimum level of security, which is expected to be available with the adoption of prudent management practices that would be put in place by any responsible operator. For a material which has very low quantities of radioactivity and therefore poses relatively low risk of radiological hazard to the public, this level of security is considered adequate during its transport. Consignments of excepted packages (e.g. packages containing smoke detectors and luminous compounds), low specific activity material (e.g. uranium ore concentrates) and surface contaminated objects (e.g. contaminated metal parts of a decommissioned nuclear facility) pose limited potential consequence. Hence common Prudential Management Practices (PMP) would provide the required level of security.

In order to implement PMP, consignor should have formal systems for

Accounting radioactive material: quantity produced, dispatched and balance in stock

- Proper selection of carrier
- Keeping track of shipment
- Prompt notification to consignee regarding dispatch
- Confirmation of receipt by consignee

This level of security would be applicable to radioactive material transported in 'Excepted Packages' and 'Industrial Packages (Types IP-1, IP-2 and IP-3)'.

Level 2 - Basic Security

This is the basic security level which would be available with the adoption of specific procedures / measures, over and above the prudent management practices.

Basic security measures include

- prudent management practices
- general security provisions
- provision of security locks
- Security related information exchange
- Training of personnel on security
- verification of –
  - ♦ security of conveyances
  - ♦ identity & trustworthiness of personnel

The consignor should

- Confirm carrier's credentials for transporting radioactive material
- Establish consignee's credentials by confirmation with national regulatory authority
- Consider all threat information
- Posses information on position of shipment
- Alert if packages are not delivered to consignee in time
- Initiate actions to recover package, if package lost or stolen
- Provide security during storage in transit
- Provide training to personnel on security awareness
- All transport workers should be trained prior to employment to be supplemented by periodic retraining
- Only accredited institutions may conduct training programmes.
- Training to include:
  - ♦ nature of security threats
  - ♦ recognising security threats
  - ♦ security concerns
  - ♦ methods of addressing such concerns
  - ♦ actions to be taken if breach of security occurs
  - ♦ awareness of security plans

Examples of the type of radioactive materials, which would require this level of security would be sources used in nucleonic gauges, nuclear medicine, low dose rate (LDR) brachytherapy sources, etc. This level of security would be applicable to all radioactive material, except fissile material, transported in Type A packages.

Level 3 - Enhanced Security

This security level includes enhanced security procedures/ measures, over and above the basic security level. This level of security would be applicable to all radioactive material (except irradiated nuclear fuel and fissile material) transported in Type B (U)/(M) packages. The IAEA system of security in the transport of radioactive material envisages enhanced security in the case of packages containing radioactive material of activity in excess of a specified limit.

The security measures include

- basic security measures
- availability of formal security plans with the operators
- installation of hardware for tracking shipments
- provision of communication links

Security plans should include:

- Allocation of responsibilities for security
- Records of radioactive material transported
- Assessment of vulnerability of operations
- Policies regarding
  - training
  - response to higher threat conditions
  - new employee verification, etc.
- Operating details; e.g.,
  - choice of routes
  - use of guards, if needed
  - controlling access to packages in storage
- Resources required to implement security plans
- Procedure for carrier identification
- Procedure for dealing with security threats
- Procedure for testing security plans
- Procedure for review / update of plans
- Measures to track shipment
- Measures to control sensitive information

An important component of this security level is installation of hardware for tracking shipments which includes

- System to track any change in authorised route
- System to locate shipment at any given time.
- Provisions to track shipments through GPS such that any attempt to detach GPS device should set off alarm in control room or in the driver cabin of vehicle
- Back-up system for tracking shipment in case GPS fails

Examples of the type of radioactive materials, which would require this level of security would be sources used in teletherapy, irradiator, high dose rate (HDR) brachytherapy sources, industrial radiography sources, etc.

Transport Requiring Special Security Measure

Over and above the commonly transported radioactive materials, there would be certain types of shipment for which, elaborate measures/procedures would need to be put in place to ensure security. These measures would include amongst others prior approval for the shipment, special vehicle, additional security personnel and escort, secure communication support and on line tracking system, etc.

Some shipments may need elaborate measures to ensure a high level of security. Measures include –

- Competent authority approval prior to shipment
- Special vehicle
- Additional security personnel and escort
- Secure communication support

Consignor should submit to competent authority, a security plan that should give details of

- route
- conveyance
- security escort
- communication facilities
- tracking mechanisms, etc.

Security plan should include:

- Administrative Controls
- Advance Notifications
- Control of Information
- Design of Package/ Conveyance
- Physical Security Measures
- Contingency Response Plans
- Special Training

This level of security would be applicable to fissile material as well as irradiated nuclear fuel packages and very high activity sources.

Safety vs Security

The provisions for the safety of radioactive material including shielding, containment, tamper-proofing and control measures contribute significantly to the security of the radioactive material. However, certain safety requirements such as conspicuous labelling, notification to persons about the shipment run counter to the security requirement of restricting information. These apparent differences in requirements may result in avoidable contradictions. Overall control measures should be implemented depending on the material being transported and considering its attractiveness and the potential consequences of a breach of safety and security.

Conclusion

The need for providing adequate security during transport of radioactive material cannot be overemphasized. Security arrangements should be commensurate with the potential consequences of breach of security. Coordination among transport operators, the regulatory authorities and the enforcement authorities is vital for security to be achieved. Promotion of security culture among all stakeholders is important.

References

[1] INTERNATIONAL ATOMIC ENERGY AGENCY, Regulations for the Safe Transport of Radioactive Material, Specific Safety Requirements, SSR-6, IAEA, Vienna, 2012.

[2] ATOMIC ENERGY REGULATORY BOARD, Security of Radioactive Material during Transport, Safety Guide No. AERB/NRF-TS/SG-10, AERB, Mumbai, 2008.

[3] INTERNATIONAL ATOMIC ENERGY AGENCY, Security in the Transport of Radioactive Material, IAEA Nuclear Security Series No.9, Implementing Guide, IAEA, Vienna, 2008.

[4] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5), IAEA Nuclear Security Series No. 13, Recommendations, IAEA, Vienna, 2011.

[5] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Recommendations on Radioactive Material and Associated Facilities, IAEA Nuclear Security Series No. 14, Recommendations, IAEA, Vienna, 2011.

Dr. A.N. Nandakumar *has done Ph.D. in Physics from Mumbai University. He worked in Bhabha Atomic Research Centre from 1968 to 2001. He has worked on safe transport of radioactive material and shielding requirements for transport containers and radiation facilities. He joined the Atomic Energy Regulatory Board in 2001 and served as Head, Radiological Safety Division. He worked in the Transport Safety Unit of IAEA from 2004 to 2006 and again during 2008 -09. He is presently serving as member of some of the safety committees of AERB.*

Role of Nuclear Material Accounting & Control in Nuclear Security

L.R. Sawant, B.S. Tomar and K.L. Ramakumar

Radioanalytical Chemistry Division, Radiochemistry and Isotope Group, Bhabha Atomic Research Centre, Mumbai 400085;
E-mail: lrsawant@barc.gov.in

There is an increasing interest in nuclear power around the globe which can be attributed to the need for sustainable low carbon emission energy source. Nuclear energy plays an important role in the society. Special nuclear materials (SNMs) which are required to get this energy are not only valuable but are of strategic significance in the nuclear programmes. While these materials have the potential to contribute to health and prosperity, the security aspect associated with them is of perennial concern. Nuclear security today has become considerably more complex than it was during the Cold War. After the events of 11 September 2001 and recent deadly terrorist attacks in the UnitedKingdom, Spain, Indonesia and elsewhere, theinternational community has recognized that newer and strongermeasures need to be taken to protect against and preparefor a broad range of terrorist scenarios including nuclear terrorism. Situations may arise where terrorists may attempt to steal or acquire nuclear weapons/ nuclear materials necessary for a nucleardevice. They could also try to sabotage nuclear power stations, research reactors, storage facilities or transport operations with the aim of spreading radioactive contamination. Such possibilities appear more probable because today's suicide terrorists hold no fears concerning their own safety. Nuclear materials are the essential raw materials for nuclear explosive devices or radiological weapons. However they present public health and environmental hazards which make the safety and security a big challenge. All states possessing nuclear materials are therefore required to have an accurate estimate of all the nuclear material owned by them. The knowledge of nuclear material locations, its form and adequate security measures from theft or loss is currently the responsibility of states possessing them. These states gather this knowledge in various ways, though there are no legal binding requirements to maintain high levels of security standards.

Adequate nuclear security requires rigorous internal controls and accounting to protect nuclear materials against external threats such as terrorists and also against insider threats like individual or group of individuals who are either authorized to have access to the facility or have special knowledge of procedures and security measures that allow them to provide key aid to an adversarial plot to steal, divert, or sabotage nuclear material. Proper materials control limits the handling of nuclear materials to only authorized areas and properly identified personnel and ensures that two people are present during nuclear materials transactions. It helps track nuclear materials from one site to another, from facility to facility, and from room to room. It ensures that there are a limited number of entries to and exits from the locations where nuclear materials are stored, and it alerts authorities to potential theft or diversion. It identifies nuclear materials for tracking purposes.

Consequent to the signing of the treaty on the Non-Proliferation of Nuclear weapons (NPT) by a state, it becomes imperative that the state will have a system of accounting and control (SSAC) under which the inventory of nuclear materials in its declared nuclear facilities will be reported to IAEA on a regular basis. The IAEA document INFCIRC/153 contains the detailed procedures for implementation of the IAEA safeguards under the NPT.

Modern materials accounting employs statistical and computer-based measures to maintain knowledge of quantities of nuclear materials present in each area of a facility. The accounting system relies on inventories and material balances to verify the presence of material or to detect a loss. It tracks all transactions, including domestic and foreign transfers, operating losses, and inventory differences. Nuclear materials accounting records of all nuclear materials on inventory and inventory changes are maintained by operators for each facility under safeguards. This information should be identical to that which exists in each state's "domestic" system of accounting and control. This inventory information is transmitted through the state authorities to the IAEA. (International Body) These state declarations on the nuclear materials present at facilities and the facility operations provide a baseline for the IAEA's verification activities. The overall objective is to provide credible assurance of both the non diversion of nuclear material from declared activities and of the absence of undeclared nuclear material and activities in the state as a whole.

"Nuclear security"means measures designed to address the risks associated with theft and trafficking in nuclear and radiological materials (including for the benefit of would-be proliferators), sabotage of nuclear facilities, and the danger of terrorists acquiring and using a nuclear weapon. Globally, nuclear security is less well developed than nuclear safeguards and nuclear safety. The three main elements of the nuclear security regime are national laws and regulations; international agreements, instruments and institutions; and ad hoc and voluntary cooperative measures. The accurate measurements of nuclear materials contribute to nuclear security and nonproliferation besides the detection of illicit trafficking of nuclear materials.

Nuclear material accounting comprises of activities carried out to (1) establish the quantities of nuclear material present in defined environments and (2) the changes in those quantities taking place within defined periods of time. The areas or facilities where nuclear material balances are established are called material balance areas (MBAs) and the intervals at which they are drawn from these facilities are called material balance periods (MBPs). The concept of nuclear material accountancy rests on the closed material balance or MUF equation.

MUF= BI+R –S-MD-EI

In order to have a meaningful material balance closing all the terms of the above equation must be physically measured rather than by difference estimates. Essential elements of nuclear material accounting are material measurements, records keeping, preparation and submission of accounting reports, verification and analysis of these accounting data to determine correctness, accuracy of material unaccounted for (MUF) and the evaluation of the causes of MUF.

MUF can result from any or all of the following:

- Imprecise and/or inaccurate measurement techniques
- SNM stuck in plant process equipment, ventilation ducts
- Higher than expected SNM in hard-to-measure waste streams
- Diversion for weapons

When the nuclear material is kept in item form and the integrity of the items remain unaltered the value of MUF is zero but the situation becomes more complex in bulk-handling facilities which as the name implies hold nuclear material in bulk form, such as powder, metal, alloy, oxide, carbide,aqueous, organic liquids or it may be present as feed awaiting processing, material in process, product, scrap in recovery process, waste awaiting discard. Here the quantities of nuclear material can only be determined with uncertainties that depend on the characteristics of the process, the nature of the material and the quality of the plant operator measurement systems. So the MUF in BHF is associated with an uncertainty. Here the statistical analysis is carried out to decide whether it is indicative of diversion.The measurements of nuclear materials are critical when i) material arrives at the facility ii) material is being inventoried and iii) material is being removed from one facility to another (inter or intra facility transfers).

Types of MBAs –Item vs Bulk

MBA	Characteristics
Items	identifiable “pieces”
	No change in chemical composition
	Verification/confirmation
Bulk	“loose”
	Changes in chemical composition and/or physical form
	Accountability through material balance

The basic aim of NMA is to know how much nuclear material you hold, in what form, where it is located and how it is contained. A material account is in many respects like a money account. In financial accounts all transactions are resolved into money terms similarly in NMA all transactions are resolved in nuclear masses. They both have physical protection (guards, guns and surveillance cameras) and various levels of accounting. The important difference is that money does not have a measurement uncertainty whereas measurements of nuclear materials have.

Accounting and control are essential to detecting and preventing theft of nuclear material. For those of us in the nuclear field, it has become obvious that ourwork to strengthen nuclear security is both vital and urgent and that we must not wait for a ′watershed′ nuclear security event to provide the needed security upgrades. Four potential nuclear security risks are: (1) the theft of a nuclear weapon (2) theacquisition of nuclear materials for the construction of nuclear explosive devices (3) the malicious use of radioactive sources including in so-called “dirty bombs” (4) and the radiological hazards causedby an attack on, or sabotage of a facility or a transport vehicle.These risks are real and current, but they are not all the same.While the probability of a nuclear explosive device being acquired and used by terrorists is relatively small, it cannot be dismissed,and the consequences would be devastating.

While nuclear safetyand nuclear security are national responsibilities, IAEA the most prominent body plays the key role in the development of safety standards, nuclear security guidance and relevant conventions based on best practice.

Since 1993, theIAEA′sown database on illicit trafficking has recorded, over 650 confirmed incidents oftrafficking in nuclear or other radioactive material. Last year alone, nearly 100 such incidentsoccurred, 11 of which involved nuclear material. While the majority of trafficking incidents do notinvolve nuclear material, the number of incidents shows that the measures to control and securenuclear materials need to be improved.Hence strong State Systems of Accounting for and Control of Nuclear Material are essential to assist States in preventing any illicit or non-peaceful use of nuclear materials.

Methods for Measurements of SNM

NMA&C depends on the measurement of nuclear material.Material balance requires accurate determinationof quantity of nuclear material. These include both (DA) destructive analysis and (NDA) non destructive analysis/assay.

Destructive Methods

Destructive analysis refers to analytical chemistry and mass spectrometry. However they require fixed laboratory to receive and analyze nuclear material samples. Sample transport and analysis usually involve a significant time before results are available. They usually provide most accurate results.

Non-destructive Methods

Usually measure the entire item rather than a small part of it and provides immediate results. It is less accurate than DA. These techniques are applied for process control, criticality safety, waste and hold up assay, safeguards inspections and customs inspections. They are gamma ray spectroscopy, neutron counting and calorimetry.

Nuclear security is more effective when accounting and control is established as the accounting system provides a complete audit trail for all nuclear materials from receipt through disposition. If the responsibilities likematerial control, material accountancy, safeguards, physical protection, operationsand safetywork together nuclear security will be more strengthened.

References

[1] Nuclear Safeguards, Security and Nonproliferation, Editor, J. E. Doyle, Butterworth-Heinemann, Elsevier, USA, 2008

[2] Nuclear Safeguards and Nonproliferation, Editor, G. Janssens-Maenhout http:bookshop.europa.eu, December 2008

[3] Course material for two day Workshop cum Training Course on "Nuclear material accounting and control: current practices and future perspectives" (NUMAC-PP-2013) organized by School of Nuclear Material Characterization Studies (SNMCS), Global Center for Nuclear Energy Partnership (GCNEP) during October 3-4, 2013 at Homi Bhabha National Institute, Anushaktinagar, Mumbai 400 094, India.

[4] Analytical methods for nuclear material accounting, K.L. Ramakumar and V. Venugopal, BARC Report (2010).

Smt. L. R. Sawant *joined BARC in 1981 after serving as a Lecturer in Mumbai University for the period of four years. She has been associated with the Nuclear Materials Accounting & Control (NUMAC) for more than twenty years. She is well versed with the chemical analysis methods for the measurement of nuclear materials and database of computer storage & retrieval systems, for accounting data of DAE facilities with respect to plutonium, uranium and thorium.*

Dr. B.S.Tomar *is currently Head, Radioanalytical Chemistry Division, BARC and Dean Academic (Chemical Sciences), Homi Bhabha National Institute, DAE. His areas of expertise include, Nuclear Chemistry, Ion beam analysis, perturbed angular correlation and actinide speciation. His current areas of research include speciation and radio-analytical chemistry of actinides. He is a Ph.D guide of Mumbai University and Homi Bhabha National Institute in Chemistry and so far 10 students have completed their PhD under his supervision. He has 145 publications in international journals.*

Dr. K.L. Ramakumar *is Director, Radiochemistry & Isotope Group, BARC. He is a specialist in Analytical Chemistry, Trace Elements Analysis employing Mass Spectrometry, Differential Scanning Calorimetry, Chromatography and Optical Spectrometry. He has been a peer reviewer for International Science Foundation, USA for financial grant to Russian Scientists. Dr. Ramakumar was also on expert assignment to the IAEA for mass spectrometry measurements. Dr. Ramakumar is a recognized Ph.D. Guide for Mumbai University and Homi Bhabha National Institute (HBNI) for Chemistry and also for Strategic Studies.*

Development of National Level Preparedness for Response to Radiological Emergencies / Threats

K.S. Pradeepkumar

Radiation Safety Systems Division, Bhabha Atomic Research Centre, Mumbai 400 085, INDIA; E-mail: pradeep@barc.gov.in

Introduction

Mankind has been exposed to natural radiation since time immemorial. However, possible exposure to manmade radiation, either due to normal operation of nuclear facilities or due to incidents leading to release of radioactivity into the environment may generate concern or panic in public mind even though the levels of possible exposure are much less than exposure due to natural radiation, and negligible in comparison to High Background natural Radiation Area (HBRA). Nuclear emergencies at TMI, Chernobyl, Fukushima and radiological emergencies at Goiania, Mayapuri etc have demonstrated that psychological impact due to fear of ionization radiation is many folds larger compared to the actual health effect they could have created.

During the design and operation of the nuclear facilities and development of emergency preparedness for response to any accidental situations including those caused by malicious intent / act, safety and protection of the public from all possible routes of exposure to radiation is taken into account. Emergency preparedness system ensures minimum risk to the public even under worst accidental situations. Taking into account the challenges of the illegal trafficking / smuggling of radioactive sources as well as the threat from Radiological Dispersal Devices (RDD – also known as Dirty bomb), state of the art monitoring systems and methodologies have been developed and kept in readiness for quick assessment of radiological impact and to mitigate its consequences during any radiological threats / emergencies.

Any unauthorized use of sources or, in situations where sources are lost/stolen, or if the sources are not handled properly, there is a potential risk of causing acute radiation exposures, which can cause severe health effects.

The safety logics applied for all ncuear reactors follow three basic principles;

- Reduce the probability of any major accidents
- Reduce the release of radioactivity to the environment
- Reduce the radiological consequences even if release occurs breaching the containment

The radiological impact of any nuclear/radiological accident depends on:

- Source term of the accident (quantity of radioactive release)
- Height of release for the effluents
- Topography (of the area to which it is released)
- Characteristic of the releases: (a) Isotopic composition (b) Physicochemical form (c) Delay in release and duration of release
- Meteorological conditions during the release (a) Wind direction (b) Wind speed (c) stability class
- Population density / distribution with respect to direction and distance from release point
- Level of radioactive deposition / contamination on ground
- Implementation of countermeasures (if carried out in time)

Radiological consequences can be prevented or significantly reduced if countermeasures can be implemented effectively. This requires preparedness for emergency response documented for all nuclear facilities. The fundamental logic for all emergency preparedness is that: money to be spent for response with 'preparedness for emergency response' will be very small compared to the money required for responding to an emergency without having 'preparedness for response'. Since radiation cannot be seen or smelt, rumours / hearsay can create panic unless radiation monitoring is carried out to assess the radiological status and remove the fear factor. An early symptom of acute high level radiation exposure can be nausea and vomiting, but this can be initiated even by other reasons, anxiety (who have not got exposed) among who are not affected but believe to have got affected can become many folds, this is commonly reported during all radiation emergencies.

'Orphan Sources' and the Challenges

Adequate security through approval of secured installations and storage of sources, regulatory, engineered safety features and additional administrative controls ensure 'cradle-to-grave' control of them. A source becomes 'orphan' i.e., goes out of regulatory control due to:

(a) Lack of or breach of the provisions

(b) Import of sources without licence deliberately or out of ignorance

(c) Loss or misplacement

(d) Theft

(e) Unauthorised disposal

(f) Mishandling of source consignments at entry and exit ports of the country

(g) Lack of awareness in the public and the officials

Such sources may also enter into public domain through illegal trafficking. These orphaned sources may be malevolently used by unlawful elements in the society leading to radiological emergency in public domain. Though

Table – 1: Summary of lost or stolen radioactive source/emergencies (IAEA)

Radiological Emergencies			
Country	Source	Strength in TBq	Health consequences
Istanbul	^{60}Co	23.5	Severe injury–life threatening
Samut Prakarn	^{60}Co	15	3 deaths
Tammiku	^{137}Cs	7.4	1 death
Goiania	^{137}Cs	50	4 deaths
Lilo	^{137}Cs	0.164	Severe injury
Lilo	^{137}Cs	0.126	Severe injury
Yanango	^{192}Ir	1.37	Severe injury–life threatening
Gilan	^{192}Ir	0.185	Severe injury
Morocco	^{192}Ir	1.2	8 deaths
Georgia (RTGs)	^{90}Sr	1000	Severe injury–life threatening
Mayapuri, Delhi	^{60}Co	1	1 Death

accidents during transportation of radioactive sources may result into a radiological emergency situation, the probability of such an event is small.

Radiological Emergency situations due to orphan sources are reported from many counties (Table 1). The sources involved were mainly ^{60}Co, ^{137}Cs and ^{192}Ir. The situations resulted in fatalities or severe injuries to a few people who got exposed. In India, in medical institutions, there were a few cases of lost brachy-therapy sources, as well as loss of industrial radiography sources and nucleonic gauges, while there was no fatality reported in such incidents.

Radiological Dispersal Device (RDD) and Response to Radiological Emergencies

Radiological Dispersal Device (RDD) is defined as 'any device, including any weapon or equipment (other than a nuclear explosive device), designed to disperse radioactive material by disseminating it to cause destruction and damage and additional injury due to the radiation emitted by the material'. It is feared that many radioactive materials, including fission products, spent fuel from nuclear reactors, medical, industrial and research waste may be integrated with conventional explosives to make a RDD.

In case of a RDD explosion, blast and thermal effects of fire due to chemical explosives will be the only cause for immediate deaths, since lethal levels of radiation exposure from the dispersed materials requires extremely large quantity of radioactive material to be integrated with the RDD. Such an eventuality can easily be detected due to radiation monitoring units, suspicion on heavy mass / shield during its transport, persons associated with fabrication of the RDD may receive leading to radiation injuries thereby giving clues for security / safety personnel to locate the RDD prior to its explosion. Panic caused by fear of radiation can result into large disruption and the required cleanup of the radioactive material / contamination and any consequent avoidance of the location (if not cleared of contamination

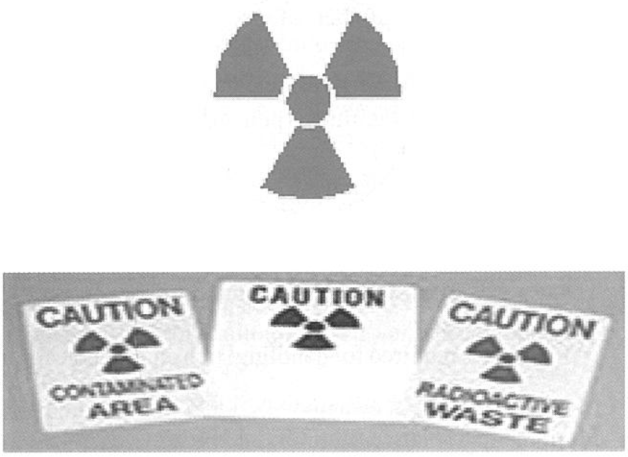


Fig. 1a Radiation symbols

even after many attempts of cleanup) may cause huge economic losses.

Requirements for Responding to Radiological Emergencies

Since a source having dispersed by dirty bomb may lead to spread of contamination, may affect many buildings / area lead to generation of large volume of radioactive waste. Thereby, strengthening control over the radioactive sources, preventing illegal transport of sources and developing quick response capability are very much essential. Locating radiation symbols (Fig. 1a) have helped in identifying and addressing some of the radiological emergency situation developing in public domain and prevention of further inadvertent exposure.

Taking into account the likelihood of large number of people / area getting contaminated following a radiological accident or RDD explosion, the following are identified as the requirements for an effective response:

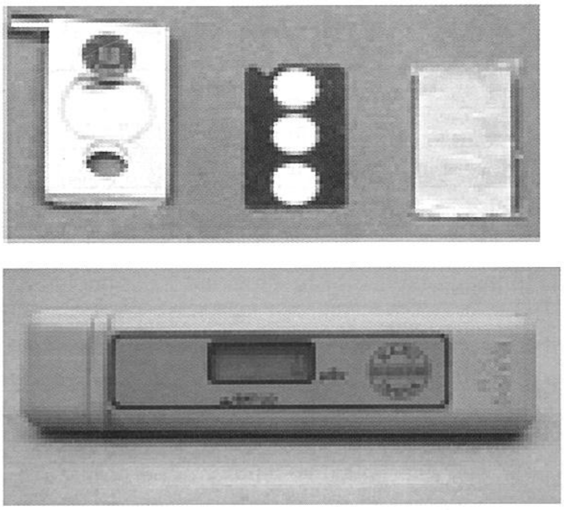


Fig. 1b Thermo Luminescent Dosimeters (TLDs) and Digital Pocket Radiation Dosimeter used for exposure Dose assessment to responders

- Monitoring large number of people (suspected to be contaminated)
- Radiation Survey of large affected area
- Decontamination facilities (personnel, houses, public places, vehicles, etc.)
- Medical triage and treatment
- Isolation and confinement of contaminated areas
- Removal and disposal of contaminated soil
- Teams ready to work in complex conditions and territories

Resources required for handling such emergencies are:

- Manpower trained on Radiation Safety
- Equipment, Radiation Monitors and Protective equipment for large number of personnel
- Medical facilities with decontamination agents, trained staff to attend to severely injured/exposed to radiation

Response organization for such radiological emergencies should comprise of:

- First Responder
- Response Initiator (duty officer, emergency service dispatcher, facility radiation safety officer)
- Emergency Manager
- On-Scene Controller
- Radiological Assessor (example: Member of DAE's Emergency Response Team)

Following any radiological emergency in public domain, protective actions for inner cordoned area inside safety perimeter (Table 2) should be carried out. First Responders shall establish and supervise an access and contamination control point as near as possible to the safety perimeter, up wind, inside the security perimeter, where ambient dose rate is close to background.

If for some reason, the radiation level at the contamination control point increases to more than 10 μSv/h (1 mR/h), the contamination control point needs to be moved to another upwind location within the security perimeter where the level is close to the prevailing background or at least sufficiently low to allow suitable detection limits. Persons working in the contaminated area i.e. the first responders, have to wear personal monitoring/ equipment, such as TLD badges and pocket dosimeters, respirators and other protective clothing (Fig. 2).

Preparedness for response and mitigation of the consequences of radiation emergency requires the following:

- Appropriate monitoring systems for detecting, locating and identifying sources
- Effective training and awareness programme for all concerned
- A well coordinated and effective response at National level

Table – 2: Radius of inner cordoned area (safe distances) for Radiological Emergencies (suggested by International Atomic Energy Agency [IAEA])

Situation	Initial Distance of Inner Cordoned Area (Safe Distance)
Unshielded or unknown source (damaged or undamaged)	30 m radius or at: - Ambient dose readings of 100 μSv/h - 1.0E+07 Bq/m^2 (gamma/beta deposition) - 1.0E+06 Bq/m^2 (alpha deposition)
Fire, suspected RDD, explosion or fumes, spent fuel plutonium spill	400 m radius (or more to protect against effects of an explosion) or at - Ambient dose readings of 100 μSv/h - 1.0E+07 Bq/m^2 gamma/beta deposition - 1.0E+06 Bq/m^2 alpha deposition

Note: Dose rate of 100 μSv/h = 10 mR/h

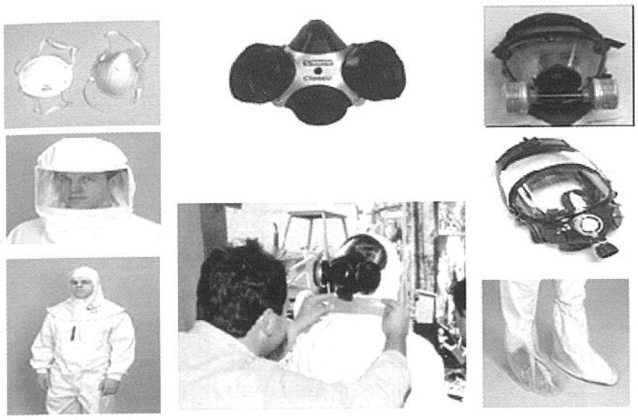


Fig. 2 Different types of respirators and protective wears - for responders working in a contaminated area

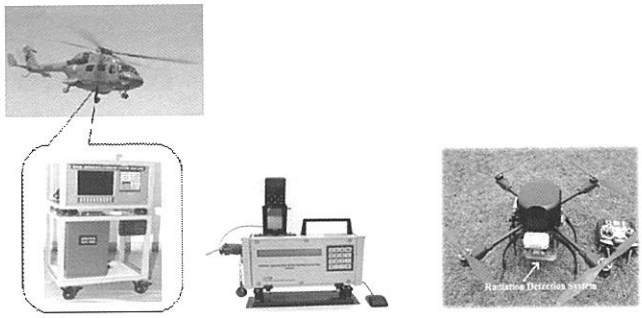


Fig. 3 Aerial Gamma Spectrometry system (AGSS), Compact Aerial Radiation Monitoring System (CARMS) and Quad-rotor based Aerial radiation monitoring System (QARMS)

A number of sensitive systems and monitoring procedures have been developed by BARC for use at installations handling and storing sources, and to detect illegal movement of sources and locate in public domain, identify and search lost sources. Some of the important systems developed in BARC are:

1. Aerial Gamma Spectrometry system (AGSS) (Fig. 3)
2. Compact Aerial Radiation Monitoring System (CARMS) (Fig. 3)
3. Quad-rotor based Aerial radiation monitoring System (QARMS)(Fig. 3)
4. Portal Monitor and Limb Monitor (Fig. 4)
5. Vehicle monitor (for monitoring goods/scrap in vehicles)

Portal, Limb and Vehicle monitors are deployed as installed / stationary monitors to detect unauthorised movement of radioactive material either by suspected persons or in vehicles in public domain as well as from nuclear facilities

Aerial Gamma spectrometry survey methodology is developed with optimised flight path, altitude of flying and flight routes for various purposes. Many aerial survey exercises (Figs. 5, 6) and mobile radiation monitoring surveys were carried out to demonstrate the capability of AGSS, CARMS etc. These systems, though developed for usage by installing in helicopters and Unmanned Aerial Vehicles [UAV] based aerial surveys for quick assessment of the radiological impact following release of radioactivity into the atmosphere or large area contamination(Fig. 7), they were also used for mobile environmental monitoring by installing in in train, car, van, boat etc . These systems can be useful for a) searching orphan sources/dirty bombs and qualitative and quantitative estimation of radioactive contamination over large area on ground and search of Orphan Sources. QARMS can be used for search of orphan sources, RDD and Impact assessment after any 'Dirty bomb explosion' and for Radiological surveillance of inaccessible areas (scrap yard, Cargos).

Development of DAE Emergency Response Centres (DAE-ERCs) for National Level Emergency Preparedness

DAE is the nodal agency for providing technical support during any radiological emergency anywhere in the country. The Crisis Management Group of DAE (CMG) is identified as the overall coordinator among various agencies

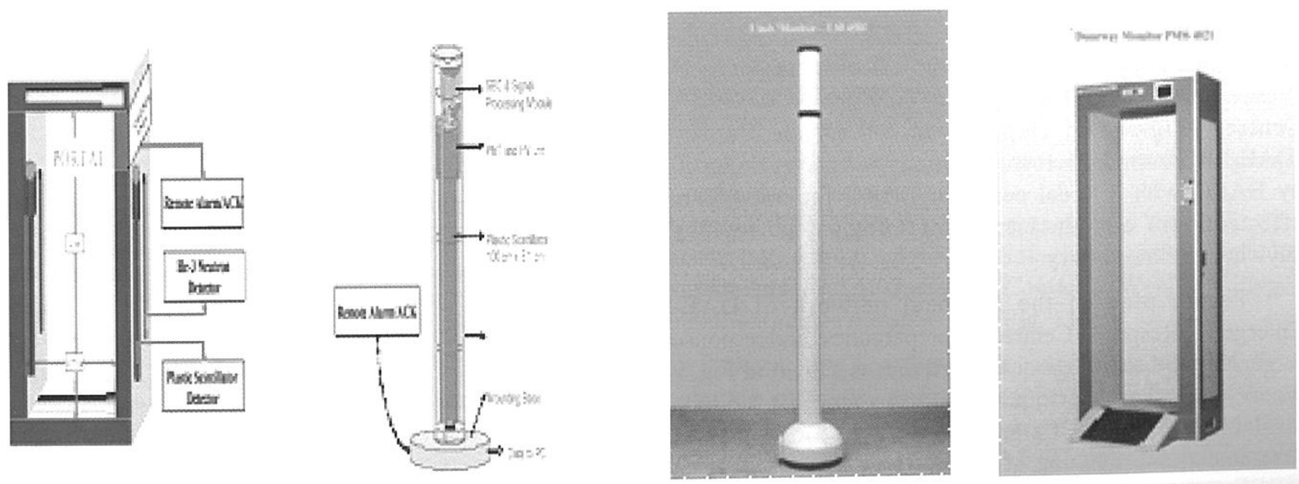
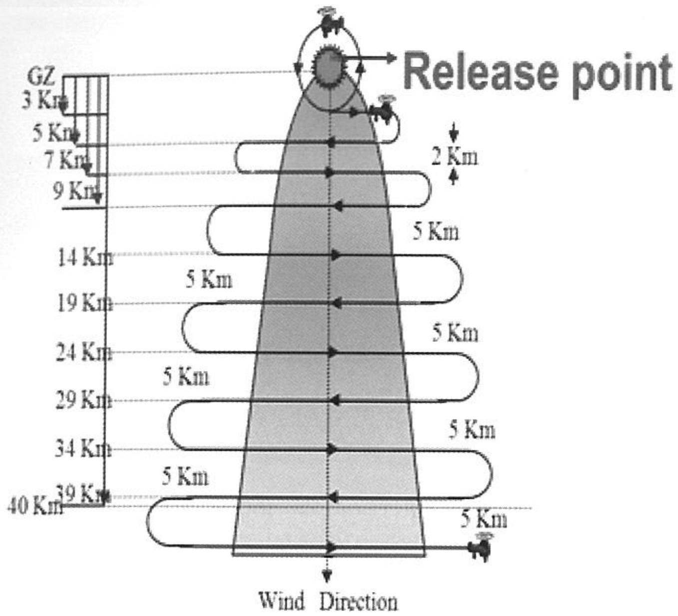


Fig. 4 Portal Monitor and Limb Monitor for detection and prevention of illegal transport of radioactive material



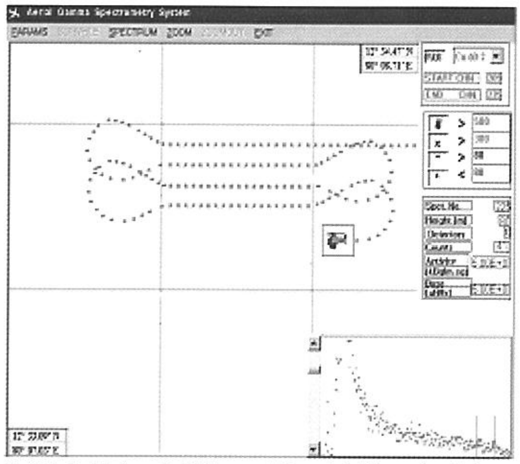


Fig-2 : Typical display on the AGSS screen during an Aerial 'Source Search' Survey

Fig. 5 Aerial survey methodology for quick assessment of radiological impact in case of any radioactivity release to the environment

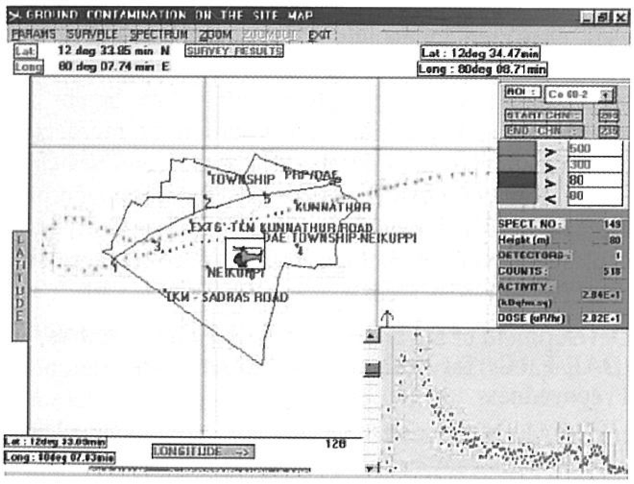


Fig. 6 Display on the AGSS screen showing the flight path and spectrum during a 'Orphan Source search' exercise

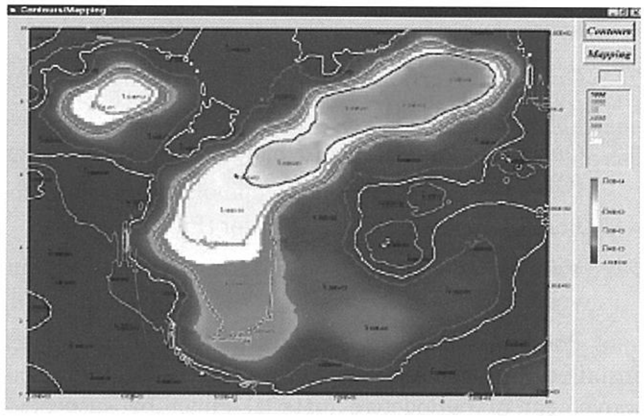


Fig. 7 Iso-dose mapping of a simulated 'affected area' based on Aerial survey. Area colour coded identify 'safe' and 'unsafe' area requiring 'interventions'

to facilitate a well-coordinated and effective response to such emergencies. Twenty two Emergency Response Centres (Fig. 8) of Department of Atomic Energy (DAE-ERCs) spread across the country has been developed by BARC with a nodal centre at BARC for responding effectively to any nuclear or radiological emergency anywhere in the country.

Future plan of the National network of DAE-Emergency Response Centres for preparedness and response to nuclear and radiological emergencies is shown in Fig. 9 where data from various monitoring systems will be available online at ERCs and will be used for the impact assessment and planning of response by First Responders NDRF teams, under the technical guidance from DAE's ERTs. In addition to developing 8 NDRF-ERCs, NDMA will be equipping ~1000 police stations and their patrolling vehicles selected from major cities with radiation detection systems, with BARC support. This is also aimed at response to radiological emergencies, and act as deterrent against radiological threats.

On receipt of relevant message at centralised Emergency Communication Room (ECR) situated at (CMG) of Department of Atomic Energy, Mumbai, depending on the severity of emergency, ERC closest to the site of incident, or more DAE-ERCs, will be activated by the Emergency Response Director (Director, HS&E Group, BARC). DAE's Emergency Response team under the leadership of BARC-ERC responded to radiological emergency at Mayapuri, Delhi (Fig. 10) by carrying our source search, identification, recovery and decontamination of affected area avoiding further spread of contamination and inadvertent exposure to public. During the Commonwealth

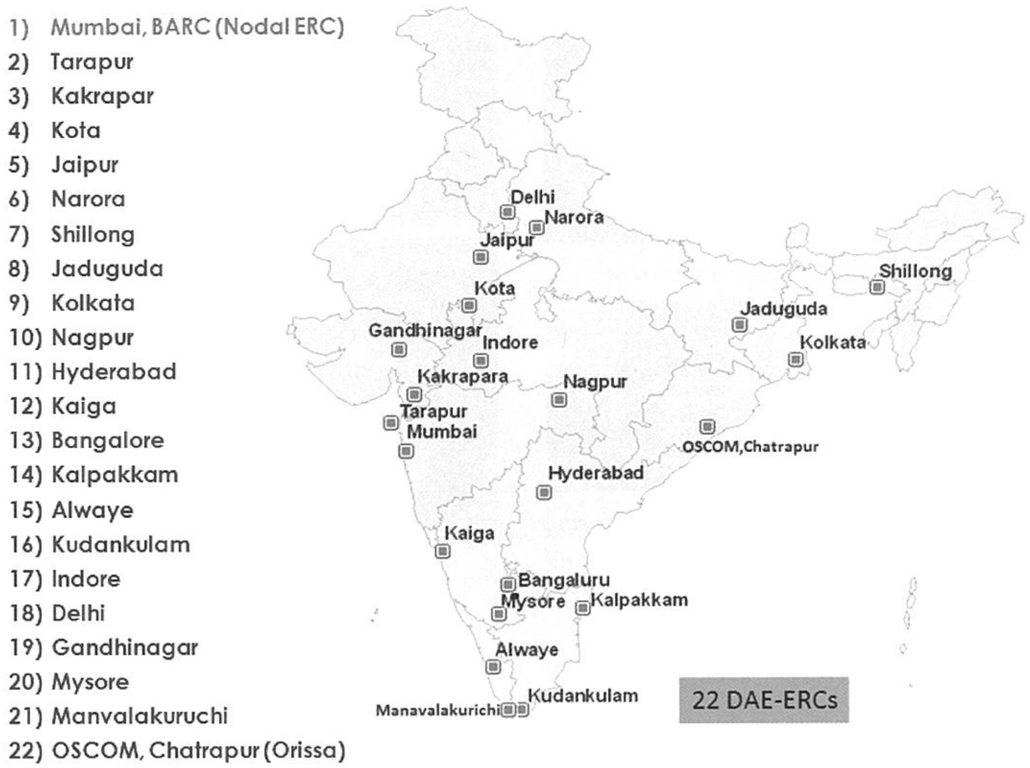
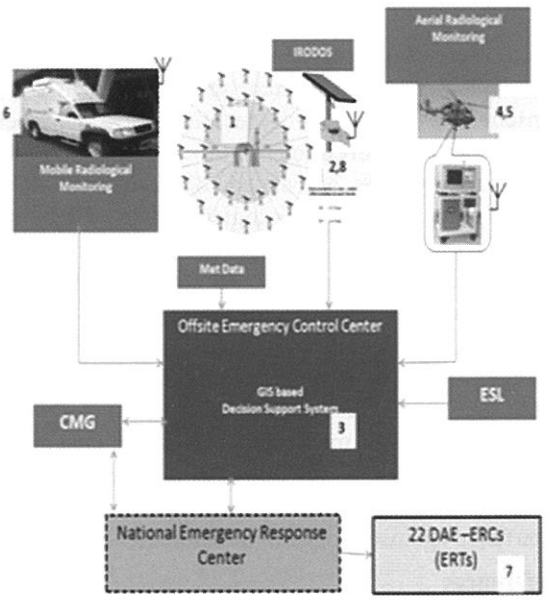


Fig. 8 22 DAE-ERCs established by BARC for technical support to respond to any Nuclear /Radiological Emergency anywhere in the county



1. Exhaust Monitoring System
2. Indian Real Time Online Decision Support System (IRODOS)
3. GIS Supported Impact Assessment
4. Aerial Gamma Spectrometry System (AGSS), Software & Methodology for Assessment of Large Area Contamination
5. Compact Aerial Radiation Monitoring System (CARMS) for remote aerial surveys using UAVs
6. Mobile Radiological Impact Assessment Lab (M-RIAL)
7. Twenty-two DAE Emergency Response Centers (ERCs)
8. Indian Environmental Radiation Monitoring Network (IERMON)

Fig. 9 Ideal network of DAE-Emergency Response Centres for preparedness and response to nuclear and radiological Emergencies

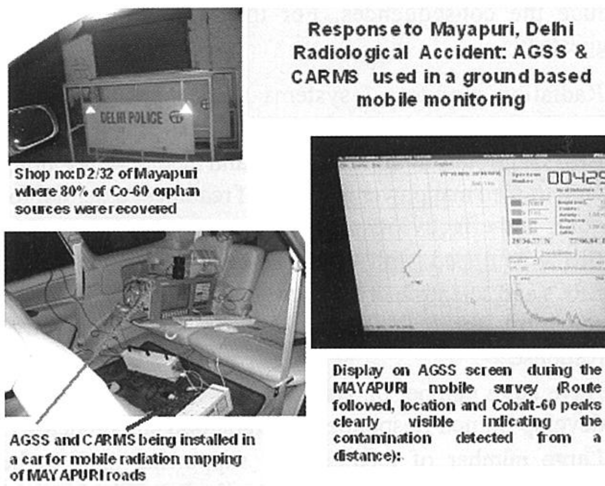


Fig. 10 BARC's ERC team's response for source search, identification which was followed by source recovery during Mayapuri radiological emergency

Games (CWG-2010) the ERCs also ensured the prevention and response to any possible radiological threats in Delhi by monitoring of CWG stadia, Common Wealth Village, important routes transport etc. (Fig. 11).

During the last few years, public functionaries like customs officials, police, fire brigade personnel and paramilitary forces are being trained in handling such radiological emergencies as first responders. Expert Emergency Response Teams (ERTs) are being raised and trained at each DAE-ERC for developing an effective

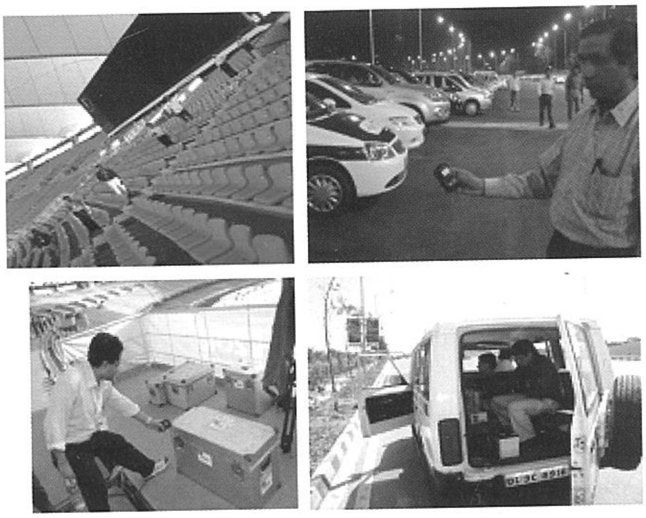


Fig. 11 DAE-Emergency Response Team ensuring prevention and response to 'malicious usage of radioactive material(Radiological threatsZ) during CWG-2010

response to address any mechanism such emergencies (Fig. 12).

Suggestions for Strengthening National Level Emergency Preparedness

Preparedness for quick response capability to meet any nuclear/radiological emergency situation is very essential to reduce the consequences. For this, the following are suggested:

- Radiation monitors / systems to be kept at various locations with various agencies spread over the country
- ERCs with state of the art systems and methodology along with trained manpower in a state of readiness essential for quick and effective response
- ERCs equipped with data transfer facility with other ERCs and scientific organizations which can improve the capability for quick impact assessment and effective response
- Have large number of Trainers with various agencies to develop trained Responders for radiation emergencies.
- Large number of medical and supporting staff to be trained for management of radiation injuries and contaminated victims.
- Include 'Disaster Management and knowledge on response to radiation emergencies' in the syllabus of NDA, IAS etc.
- Fire stations and Police stations to have radiation monitors with knowledge on radiation monitoring
- Create adequate 'Deterrence for smuggling of radioactive sources'.
- Media to play an active role in removing the fear of low level radiation exposure
- At national level, radiation monitors/monitoring systems to be increased significantly to ensure adequate preparedness for 'Large Scale Nuclear disaster/ Radiological emergencies'

Fig. 12 Training of First Responders, Quick Response Teams by BARC's Emergency Response Teams

- Public awareness programme and periodic exercises with participation of all responsible agencies to strengthen the emergency preparedness programme.

Conclusions

Preparedness for quick detection, assessment and response capability to respond to any nuclear / radiological emergency situation is very essential to reduce the consequences. Identification of various nuclear and radiological emergency/threat scenario and their possible consequences are used for deciding the requirements for emergency preparedness. State of the art radiation monitoring systems, associated software, methodology for quick assessment of radiological status, GIS supported impact assessment programs for the decision makers and 22 DAE-Emergency Response Centres are developed by BARC to strengthen national level preparedness for response to nuclear disaster and nuclear and radiological emergencies. Coordinated efforts by defence, medical, paramilitary, administrators and various security agencies, with the support of media and NGOs, can ensure effective response to challenges of any nuclear / radiological emergency anywhere in the country, and can create deterrence against nuclear and radiological threats.

References

[1] IAEA, Method for Developing Arrangements for Response to a Nuclear or Radiological Emergency, Emergency Preparedness and Response Series EPR-METHOD,IAEA, Vienna, 2003.

[2] IAEA, Arrangements for preparedness for Nuclear or Radiological Emergency, IAEA Safety Standards Series No. GS-G-2.1 (2007)

[3] Gonzalez, Lost and found dangers - Orphan Radiation Sources Raise Global Concerns, 1999, Timely action, Strengthening Radiation Safety And Security,2-17,IAEA Bulletin, Vol 41, No.3.

[4] ICRP, Protecting People against Radiation Exposure in the Event of a Radiological Attack, ICRP Publication 96, (2005)

[5] IAEA, Radiological accident in Goiania, IAEA report, February 1989.

[6] IAEA, Lessons learned from the response to radiation emergencies (1945 – 2010), IAEA, 2012

[7] Pradeepkumar, K.S., Krishnamachari, G., Kale, M.S., Probal Chaudhury, Rajvir Singh and Sharma, D.N. Gamma Spectrometric Survey Techniques for Search and Detection of Orphan Sources and Assessment of Environmental Radioactive Deposition in a Post Nuclear Accident Scenario International Congress of the International Radiation Protection Association (IRPA-11),Madrid, Spain, 23-28 May, 2004.

[8] Pradeepkumar K.S., Exposure to the public following atmospheric releases of radioactivity, Radiation Protection and Environment, Vol.22, No.2, 1999.

[9] Nuclear Security Systems and Measures for Major Public Event, Nuclear Security Series No. 18, IAEA, (2012).

[10] Pradeepkumar K.S. and Probal Chaudhury, Development of Radiation Emergency Response System (RERS) for National Level Preparedness, BARC Founder's day special issue, 2012.

[11] Pradeepkumar K.S., Nuclear and Radiological Threats and Emergency Preparedness at National Level, Bulletin of Radiation Protection and Environment, journal of IARP, pp48-53, Vol.31, No: 1-4, (2008).

[12] Probal Chaudhury and Pradeepkumar K.S., State-of-the-art Monitoring Systems and Software for Assessment Radiological Impact, BARC Founder's day special issue, (2012)

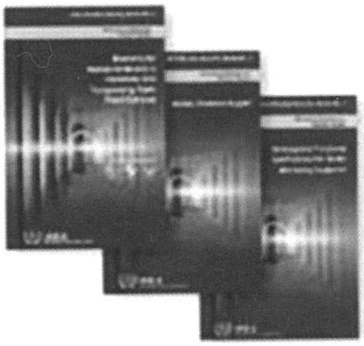
***Dr. Pradeepkumar. K.S.**, a senior scientistof BARC, had taken his M.Sc in Nuclear Physics and PhD on 'Nuclear Reactors and Radiological Safety' and as the Head of Radiation Safety Systems Division, BARC he is responsible for ensuring radiological safety in all nuclear facilities at BARC, Mumbai. He has developed, 22 DAE-Emergency Response Centres(ERCs) with Emergency Response Teams, various state of the art radiation detection systems including Aerial Gamma Spectrometry System (AGSS), monitoring methodologies and software for ensuring radiological safety in nuclear facilities and in the environment and 'Impact Assessment Software' for Nuclear Disaster management. His expertise is utilized by NDMA, MHA, MOD and international bodies like UNSCEAR (United Nations Scientific Committee on the Effects of Atomic Radiation), IAEA for radiological safety and prevention and preparedness for response to nuclear and radiological emergencies. As an Emergency Response Manger, he with his team effectively responded to the 'Mayapuri Radiological Emergency' caused by a Co60 source from Delhi university.*

The IAEA Nuclear Security Series[1]

Anil Upreti

Control Instrumentation Division, Bhabha Atomic Research Centre, Trombay, Mumbai 400 085
E-mail: aupreti@barc.gov.in

Nuclear security issues relating to the prevention and detection of, and response to, theft, sabotage, unauthorized access and illegal transfer or other malicious acts involving nuclear material and other radioactive substances and their associated facilities are addressed in the IAEA Nuclear Security Series of publications. These publications are consistent with, and complement, international nuclear security instruments, such as the amended Convention on the Physical Protection of Nuclear Material, the Code of Conduct on the Safety and Security of Radioactive Sources, United Nations Security Council Resolutions 1373 and 1540, and the International Convention for the Suppression of Acts of Nuclear Terrorism.



Categories in the IAEA Nuclear Security Series

Publications in the IAEA Nuclear Security Series are issued in the following categories:

1. *Nuclear Security Fundamentals*

It contains objectives, concepts and principles of nuclear security and provides the basis for security recommendations.

2. *Recommendations*

It presents best practices that should be adopted by Member States in the application of the Nuclear Security Fundamentals.

3. *Implementing Guides*

It provides further elaboration of the Recommendations in broad areas and suggests measures for their implementation.

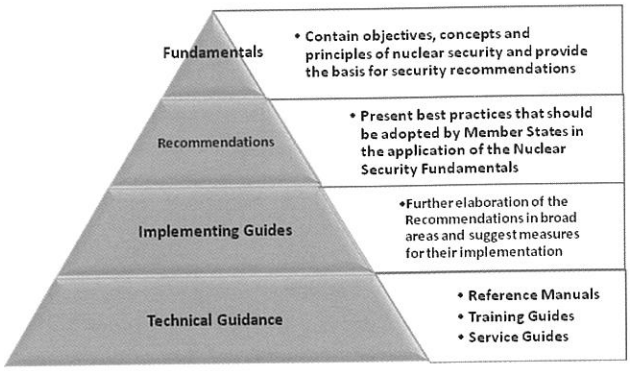


Fig. 1 Categories Nuclear Security Series (NSS) documents

4. *Technical Guidance publications*

It includes reference manuals, with detailed measures and/or guidance on how to apply the Implementing Guides in specific fields or activities; Training Guides, covering the syllabus and/or manuals for IAEA training courses in the area of nuclear security; and Service Guides, which provide guidance on the conduct and scope of IAEA nuclear security advisory missions.

Following is a brief description of published IAEA Nuclear Security Series documents:

NSS 1: Technical and functional specifications for border monitoring equipment – 2006

This publication provides a set of technical specifications that can be used in design testing, qualifying and purchasing border radiation monitoring equipment. Due to advances continually being made in the field of border radiation monitoring equipment they represent a consensus on the minimum specifications presently achievable.

NSS 2: Nuclear Forensics Support, 2006

Nuclear scientists have recognized that much can be learned from the analysis of reported cases of illicit trafficking of nuclear and other radioactive material, specifically, what the material has been used for, where it was obtained from (stock, scrap or waste) and whether the amount seized was only a sample of a much more significant quantity. These and many other questions can be answered through detailed technical characterization of seized material samples.

[1]This article is based on the information available in the IAEA website under the Department of Nuclear Security : http://www.-ns.iaea.org/security/ and is included with due acknowledgement to IAEA.

NSS 3: Monitoring for Radioactive Material in International Mail Transported by Public Postal Operators, 2006

The illegal transport of conventional explosives and biological material has been observed in public mail and could lead to serious health hazards. In response to Member State requests to establish guidance on detecting the movement of radioactive material in international mail, the IAEA and the Universal Postal Union (UPU) undertook a joint effort to prepare this publication. It considers how radioactive materials in international mail might be detected, how best to monitor for these materials in mail facilities and how to respond appropriately.

NSS 4: Engineering Safety Aspects of the Protection of Nuclear Power Plants against Sabotage, 2007

This report provides guidelines for evaluating the engineering safety aspects of the protection of nuclear power plants against sabotage. The guidance, which is the result of extensive dialogue among safety and security specialists, takes into account the existing robustness of structures, systems and components and emphasizes those aspects of sabotage protection that work synergistically with the protection against extreme external occurrences of accidental origin, such as earthquakes, tornadoes and human induced events.

NSS 5: Identification of Radioactive Sources and Devices, 2007

This manual is intended to: assist in the recognition and identification of objects thought to be radioactive devices, sources and transport packages; provide instruction on what to do and how to obtain further help; enhance awareness of the existence of radioactive devices, sources and transport packages; and provide information on the International Catalogue of Sealed Radioactive Sources and Devices through regulatory authorities in IAEA Member States.

NSS 6: Combating Illicit Trafficking in Nuclear and Other Radioactive Material, 2008

This publication is intended for individuals and organizations that may be called upon to deal with the detection of and response to criminal or unauthorized acts involving nuclear or other radioactive material. It will also be useful for legislators, law enforcement agencies, government officials, technical experts, lawyers, diplomats and users of nuclear technology. In addition, the manual emphasizes the international initiatives for improving the security of nuclear and other radioactive material, and considers a variety of elements that are recognized as being essential for dealing with incidents of criminal or unauthorized acts involving such material.

NSS 7: Nuclear Security Culture, 2008

This publication defines the basic concepts and elements of nuclear security culture, with the aim of providing Member States with international consensus guidance on planning and implementing a programme to improve nuclear security culture. Particular emphasis is placed on areas such as regulation, government institutions and general public awareness.

NSS 8: Preventive and Protective Measures against Insider Threats, 2008

This implementing guide presents a comprehensive methodology for the development of preventive and protective measures against insider threats to nuclear facilities and nuclear material transport operations of all types. Institutional insiders who are privy to the inner workings of security systems present a unique challenge to the establishment of effective control systems for nuclear material.

NSS 9: Security in the Transport of Radioactive Material, 2008

This publication addresses the vulnerability of radioactive material during transport. Given the international concern over acts of nuclear terrorism, it is imperative to have a well-defined plan for the security of sensitive materials during transport. This publication provides guidance on implementing, maintaining or enhancing a State's nuclear security regime to protect radioactive material in transport against theft, sabotage or other malicious acts.

NSS 10: Development, Use and Maintenance of the Design Basis Threat, 2009

This publication provides guidance on how to develop, use and maintain a design basis threat (DBT). It is intended for decision makers from organizations with roles and responsibilities for the development, use and maintenance of the DBT. This implementing guide describes a DBT; identifies and recommends the roles and responsibilities of organizations that should be involved in the development, use and maintenance of a DBT; describes how to conduct a national threat assessment as a precursor to a DBT; explains how a DBT can be developed; explains how a DBT is incorporated into a State's nuclear security regime;

NSS 11: Security of Radioactive Sources, 2009

There are concerns that terrorist or criminal groups could gain access to high activity radioactive sources and use these sources maliciously. The IAEA is working with Member States to increase control, accounting and security of radioactive sources to prevent their malicious use and the associated potential consequences. Based on extensive input from technical and legal experts, this implementation guide sets forth guidance on the security of sources and will serve as a useful tool for legislators and regulators, physical protection specialists, and facility and transport operators, as well as for law enforcement officers.

NSS 12: Educational Programme in Nuclear Security, 2010

Higher education plays an essential role in nuclear security capacity building. It ensures the availability of experts able to provide the necessary competencies for effective national nuclear security oversight of nuclear and other radioactive material and to establish and maintain an appropriate nuclear regime in a State. This guide presents both the theoretical knowledge and the practical skills necessary to meet the requirements described in the international framework for nuclear security.

NSS 13: Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5), 2011

This publication, Revision 5 of Nuclear Security Recommendation on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225), is intended to provide guidance to States and their competent authorities on how to develop or enhance, implement and maintain a physical protection regime for nuclear material and nuclear facilities, through the establishment or improvement of their capabilities to implement legislative and regulatory programmes.

NSS 14: Nuclear Security Recommendations on Radioactive Material and Associated Facilities, 2011

The purpose of this publication is to provide guidance to States and competent authorities on how to develop or enhance, implement and maintain a nuclear security regime for facilities dealing with radioactive material and associated activities. This is to be achieved through the establishment or improvement of their capabilities to implement a legislative and regulatory framework to address the security of radioactive material, and of associated facilities and activities, in order to reduce the likelihood of malicious acts involving such material.

NSS 15: Nuclear Security Recommendations on Nuclear and Other Radioactive Material out of Regulatory Control, 2011

This publication presents recommendations for the nuclear security of nuclear and other radioactive material that is out of regulatory control. It is based on national experience and practices and guidance publications in the field of security as well as the nuclear security related international instruments. The recommendations include guidance for States with regard to the nuclear security of nuclear and other radioactive material that has been reported as being out of regulatory control as well as of material that is lost, missing or stolen but has not been reported as such, or has been otherwise discovered.

NSS 16: Identification of Vital Areas at Nuclear Facilities, 2013

This publication provides detailed guidance with regard to the identification of vital areas at nuclear facilities. It presents a structured approach to identifying those areas that contain equipment, systems and components to be protected against sabotage.

NSS 17: Computer Security at Nuclear Facilities, 2011

This publication provides guidance specific to nuclear facilities on implementing a computer security programme and evaluating existing programmes. The use of computer systems to cover an increasing range of functions at nuclear facilities introduces new vulnerabilities that could seriously endanger nuclear security if not addressed in a rigorous and balanced manner.

NSS 18: Nuclear Security Systems and Measures for Major Public Events, 2012

This publication provides an overview, based on practical experience and lessons learned, for establishing nuclear security systems and measures for major public events. It covers technical and administrative nuclear security measures for developing the necessary organizational structure, developing plans, strategies and concepts of operations, and making arrangements for implementing the developed plans, strategies and concepts.

NSS 19: Establishing the Nuclear Security Infrastructure for a Nuclear Power Programme, 2013

This publication provides guidance on the actions to be taken by a State in implementing an effective nuclear security infrastructure for a nuclear power programme. The topics covered are: development of national policy and strategy; common nuclear security measures; infrastructure issues relating to nuclear and other radioactive material; associated facilities; and cooperation with other States.

NSS 20: Objective and Essential Elements of a State's Nuclear Security Regime, 2013

This IAEA Nuclear Security Series publication provides nuclear security fundamentals, recommendations, and supporting guidance for Member States to assist them in implementing new nuclear security regimes, or in reviewing and if necessary strengthening existing ones. It serves as guidance for Member States with respect to their activities in relation to binding and non-binding international instruments.

NSS 21: Nuclear Security Systems and Measures for the Detection of Nuclear and Other Radioactive Material out of Regulatory Control, 2013

This publication provides guidance to Member States for the development of, or improvement of nuclear security systems and measures for the detection of criminal or unauthorized acts with nuclear security implications involving nuclear and other radioactive material out of regulatory control. It describes the elements of an effective nuclear security detection architecture which is comprised of an integrated set of nuclear security systems and measures, and is based on an appropriate legal and regulatory framework for the implementation of the national detection strategy.

Forth coming IAEA Nuclear Security Series Publications

1. Security of Nuclear Material in Transport
2. Protection and Confidentiality of Sensitive Information in Nuclear Security
3. Radiological Crime Scene Management
4. Nuclear Forensics in Support of Investigations
5. Development of a National Nuclear Forensics Library
6. Threat Assessment and Risk-informed Approach for Implementation of Nuclear Security Measures for Nuclear and Other Radioactive Material out of Regulatory Control
7. Methodology to Detect Illicit Trafficking of Nuclear and Other Radioactive Material Across Borders

(Adopted from http://www-ns.iaea.org/security/)

Shri Anil Upreti *completed his B.Tech in Electrical Engg. from U P Technical University in 2004. He joined BARC training school in 2005. Currently he is working as Scientific Officer "E" in Control Instrumentation Division of BARC. He is involved in design and development of various sub-systems of Physical Protection System e.g. Web enabled Access Control System, Electric Fence & Vibration Fence based PIDS, Day Night Video Surveillance System etc. Currently he is working in the areas of Fiber Optic based PIDS and Explosive detection and Multisensor Data Fusion.*

Global Centre for Nuclear Energy Partnership (GCNEP)[1]

L.R. Jangra

GCNEP, Electronics and Instrumentation Group, Bhabha Atomic Research Centre, Mumabi 400 085;
E-mail: lrjangra@barc.gov.in

Introduction

The application of nuclear energy has been expanding worldwide driving the need to develop nuclear systems that are intrinsically safe, secure, and proliferation resistant, as well as address the residual risk by means of physical security measures. In the margins of the Nuclear Security Summit held in April 2010 at Washington DC, USA, our Hon'ble Prime Minister, Dr. Manmohan Singh, announced setting up of a Global Centre as an initiative to share India's strengths and insights in the field of nuclear safety, security, and advanced nuclear and radiation technologies with the international nuclear community, and to establish a platform for facilitating broad-ranging partnership through research, training and international seminars by Indian and international experts on topical issues. The Global Centre for Nuclear Energy Partnership - GCNEP - announced by our honorable Prime Minister is visualized to be a state of the art facility for conducting research and development and design of systems (that are intrinsically safe, secure, proliferation resistant and sustainable), along with allied training schemes, and involving international participation from the IAEA and other interested foreign partners.

The Government of India has since approved in September 2010 the establishment of Global Centre for Nuclear Energy Partnership (GCNEP) at village Jasaur Kheri and Kheri Jasaur, near Bahadurgarh, Haryana, (about 45 km from Delhi airport). The land for the centre has been acquired and the master plan of the Centre is ready. The Phase-I construction of the centre will commence soon.

Objectives

The primary objectives of GCNEP are: (i)To pursue design studies and analysis of advanced nuclear energy systems with features to achieve intrinsically enhanced safety, security, proliferation resistance and sustainability; (ii) To carry out research and development in radiation monitoring including development of detectors and systems, to develop decision support systems for nuclear emergency management, to conduct radiation transport, shielding, dispersion modeling and impact assessment studies, to impart training to and certification of personnel in radiation protection principles and safety practices, to maintain and update radiation protection standards; (iii) To provide state of the art research, development and demonstration and training facilities in the application of radio-isotopes and radiation technologies; (iv) To promote the R&D activities for evolving new methodologies in nuclear material accounting and control (NMA&C; NUMAC), to establish an advanced infrastructure and demonstration facility for human resource development in the practices of nuclear material accounting and control; (v) To impart training on application of physical protection system and response procedure, enhance physical security of nuclear facilities by developing and deploying most modern technological tools including information security, and to provide facilities for test and evaluation of sensors and systems used for physical security.

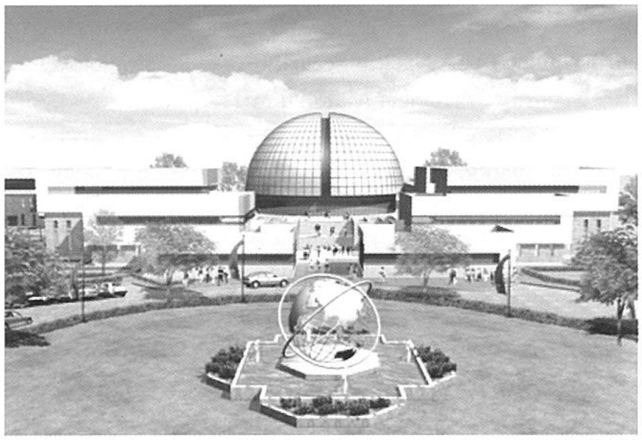


Fig. 1 GCNEP Main Building (Architect's view)

There are five schools to take up various programmes to achieve the above objectives.

- School of Nuclear Security Studies (SNSS)
- School of Nuclear Material Characterization Studies (SNMCS)
- School of Radiological Safety Studies (SRSS)
- School of Advanced Nuclear Energy System Studies (SANESS)
- School for Studies on Applications of Radioisotopes and Radiation Technologies (SSARRT)

The following section provides a brief overview of mission and objectives, various activities, and programmes envisaged under the abovementioned five schools.

School of Nuclear Security Studies (SNSS)

The mission of SNSS is to impart training to security forces on application of physical protection systems and response procedures, to enhance physical security of nuclear facilities by developing and deploying most modern technological tools including information security, and to provide facilities for test and evaluation of sensors and systems used for physical security.

[1](www.gcnep.gov.in)

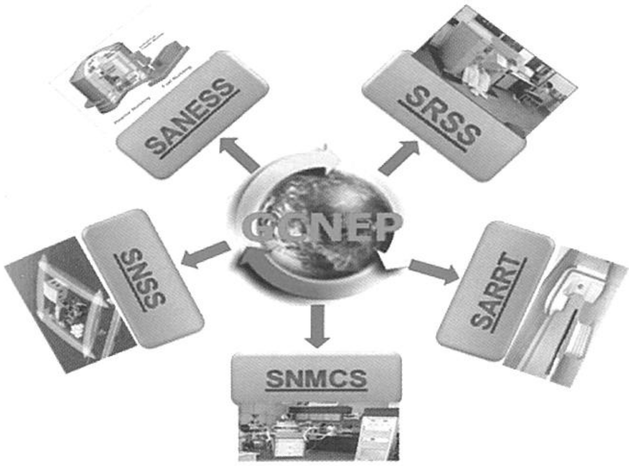


Fig. 2 *Five Schools of GCNEP*

Programme Modules to be developed for this school are: (i) Formal Education and training; (ii) Technological tools for physical security; (iii) Personnel reliability studies; (iv) Vulnerability studies; (v) Seismic monitoring; and (vi) Test and evaluation of sensors and systems.

The SNSS will be involved in carrying out research and development in the frontier areas of Security Equipment, Systems and Sensors and in performance testing and evaluation of systems and sensors. It will be involved in training of security force, guard force personnel, plant personnel on Security aspects, carry out table top and near real time simulated and field exercises. The school will also be involved in computer and information security in nuclear fuel cycle activities, computer security for nuclear security systems and sensors.

The SNSS will take up R&D in the area of, (i) Sensors and systems for security applications, (ii) Systems for personnel and material access control, intrusion detection, (iii) Personnel reliability studies, (iv) Surveillance, Video Analytics and advanced video tools, (v) Explosives and other contraband detection, (vi) Radiation Detection Equipment, (vii) Vulnerability Studies, (viii) Nuclear Security Computer Simulation, and (ix) Secure Transportation. The school will set up facilities/sites like, (i) Outdoor Test Bed, (ii) Barrier Technology Test Site, (iii) Vehicle Access Control Test Site, (iv) Hypothetical Nuclear Facility, and (v) Virtual Reality Simulation for national and international users.

As a part of its activities, the Centre will impart training to security agencies/forces in the field of application of physical protection system and response procedures; address enhanced physical security of nuclear materials and facilities by developing/deploying modern technological tools including information security, and provide facilities for test and evaluation of sensors and systems used for physical protection systems.

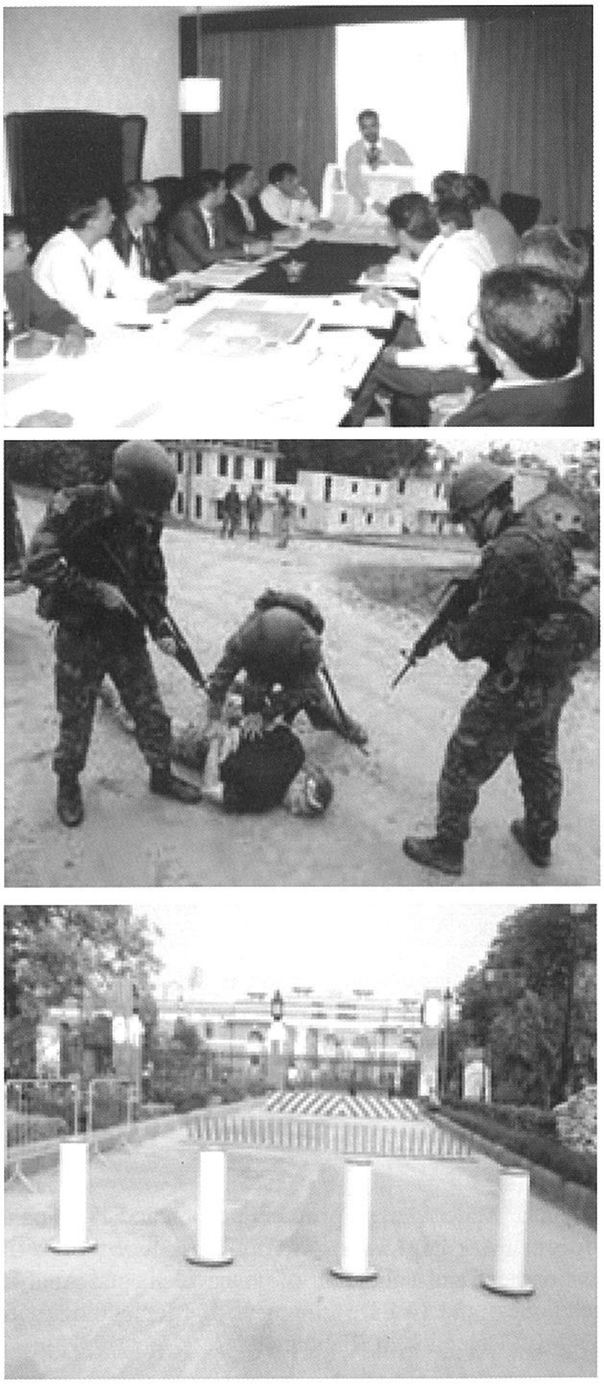


Fig. 3 SNSS will carry out table top and field exercises

School of Nuclear Material Characterization Studies (SNMCS)

The Mission of SNMCS is: (i) to promote the R&D activities for evolving new methodologies to detect and ascertain the causes for unaccounted losses of nuclear materials on a timely basis; (ii) to establish teaching and training facility for the effective implementation of safeguards including nuclear material accounting & control and its practices at national as well as international level; (iii) to establish an advanced infrastructure and demonstration Facility for human resource development in the practices of

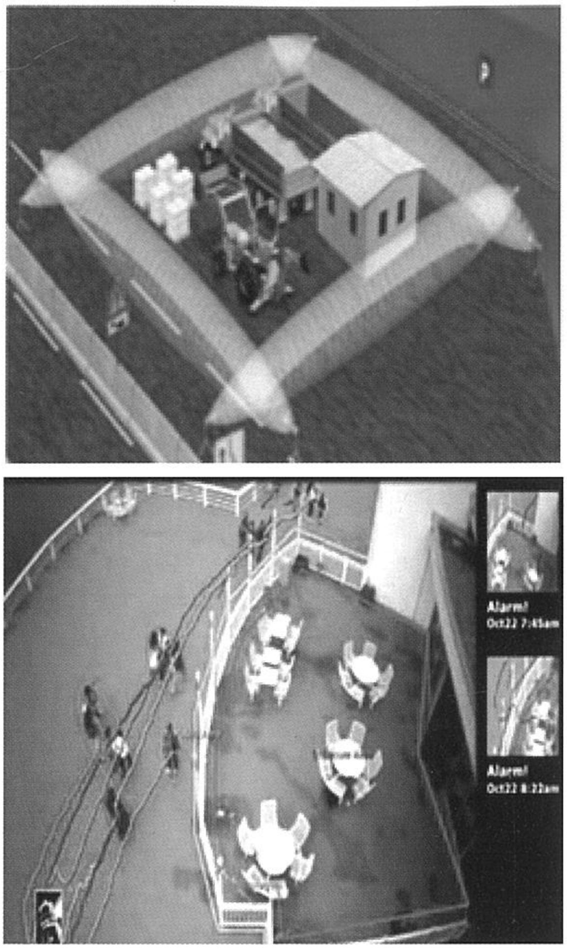


Fig. 4 R&D on sensor and systems will be part of SNSS activities

NMA&C; and (iv) to create a versatile secured data management system for NMA&C .

The program modules planned for this school are: (i) Methodology for Destructive and Non-Destructive Analysis of Nuclear Material; (ii) Formal Education and Training on Nuclear Material Accounting and Control; (iii) Development and validation of Trace Elemental Analysis Techniques; and (iv) Development of Methodologies for Low level Detection of Radionuclides.

School of Radiological Safety Studies (SRSS)

The mission of SRSS is: (i) R&D on radiation detection systems and dosimetry, (ii) impact assessment of radioactivity releases (integrated with GIS), (iii) Nationwide Radiation background mapping, (iv) Safety of Radioactive and Nuclear Material, (v) Emergency preparedness and response, (vi) Medical management of radiation emergencies, and (vii) Field exercises on radiological safety and emergency response.

Programme modules planned for SRSS are: (i) Formal Education, Training and public awareness, (ii) Response to RDD, RED and other radiological emergencies, (iii) Radiation Mapping by mobile monitoring systems, (iv) Source search, detection, identification, assessment and

Fig. 5 The GCNEP campus (Architect's view)

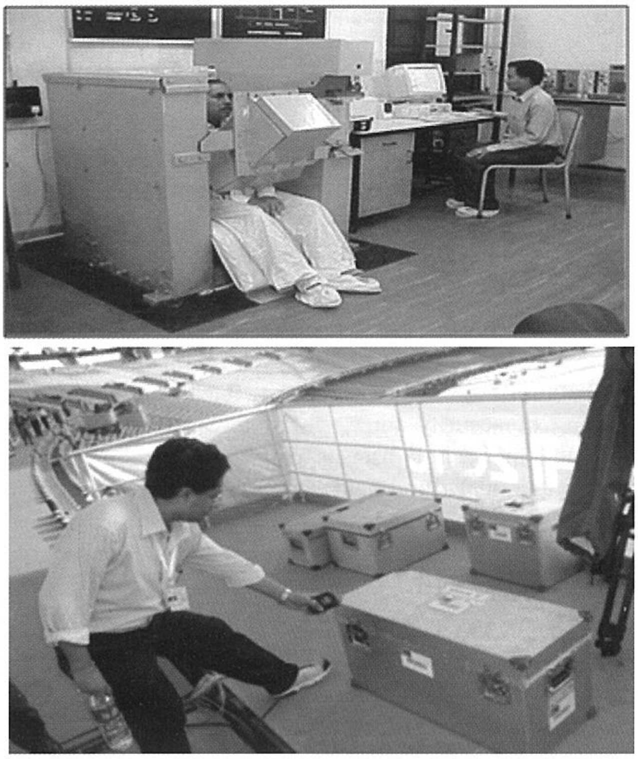


Fig. 6 Training on source search will be part of SRSS activities

recovery, (v) Lessons learned from nuclear and radiological accidents, and (vi)Studies on dispersion of atmospheric and aquatic releases.

Training on radiological safety will be carried out for, i) National Disaster Response Force (NDRF); ii) State Police; iii) Fire Fighters; iv) Civil Defence; v) DAE-ERTs; vi) Medical Professionals, Paramedical staff; vii) Import/Export Agencies, Frontline Officers; viii) RSO for Nuclear Facilities, Medical Institutes, Industries and Research Centres.

School of Advanced Nuclear Energy Systems Studies (SANESS)

The mission of SANESS is to pursue design studies and analysis of advanced nuclear energy systems with features to achieve intrinsically enhanced safety, security, proliferation

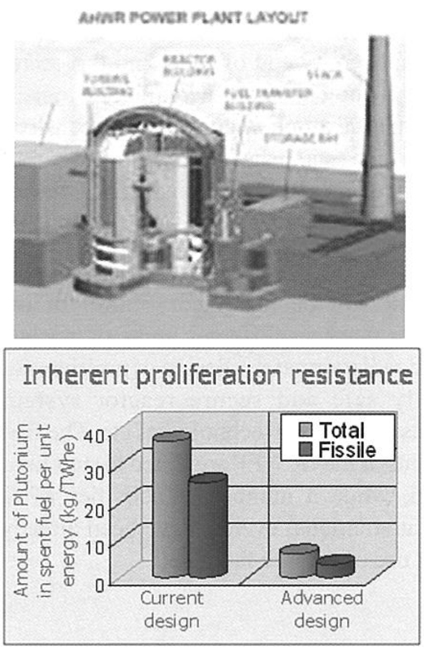


Fig. 7 Typical topics of interest to SANESS

resistance and sustainability. Program modules planned to be taken up under SANESS are: (i) Reactor systems and applications; (ii) Fuel cycle studies; (iii) Accelerator driven systems (ADS); (iv) Risk assessment studies; (v) Emergency planning and management; and (vi) Sustainability parameters assessment .

The R & D focus of this school are (i) Advanced, intrinsically safe, secure, proliferation resistant and sustainable nuclear energy systems (ii) Non electrical applications such as sea-water desalination, hydrogen production and industrial heating (iii) Thorium fuel technologies (iv) Accelerator Driven Sub-critical Reactor System (v) Probabilistic Safety based Studies (PSA).

The training focus will be on (i) Different aspects of Safety, Security and Proliferation Resistance (ii) Evaluation of performance indicators in safety, security and proliferation resistance (ii) Regulatory process, safety culture, radiation protection, nuclear law.

School for Studies on Application of Radioisotopes and Radiation Technologies (SARRT)

The mission of SARRT is to provide state-of-the-art research, development, demonstration and training facilities in the field of application of radioisotopes and radiation technologies. The program modules planned under this school are: (i) Formal education and training; (ii) Radiation processing of food commodities; (iii) Value addition to healthcare, medical and herbal products; (iv) Radiation induced enhancement in properties for creating advanced materials; (v) Industrial radiography and tomography using gamma and X-rays; (vi) Radiotracer and isotope use for high technology systems and managing water resources; and vii) Waste water treatment.

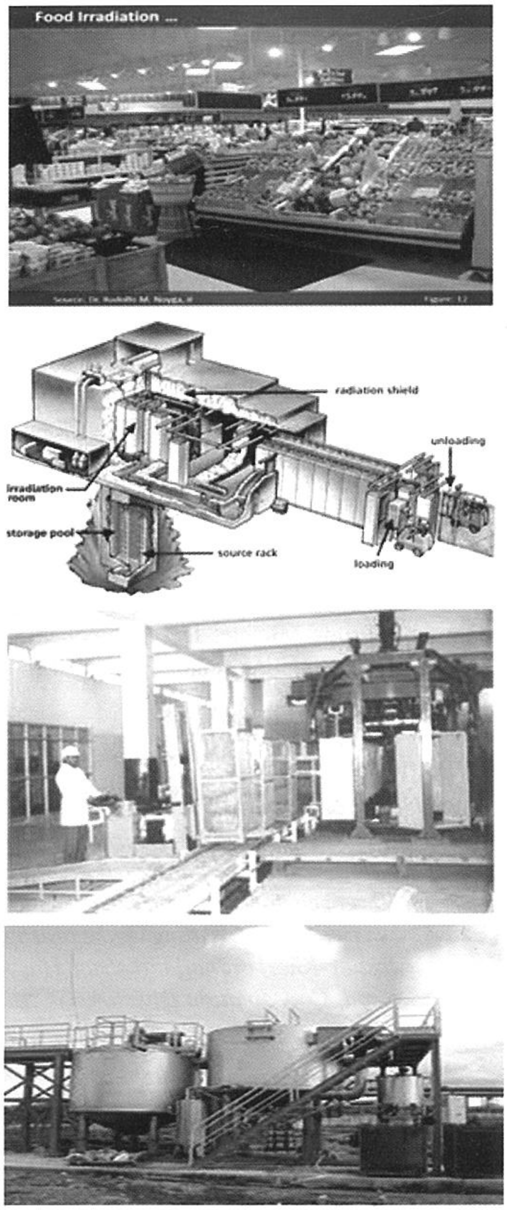


Fig. 8 Typical topics of coverage by SARRT Activities

The R &D focus of SARRT will be on, (i) Industrial Applications, like radiography, radiotracers, radiation processing of materials, (ii) Medical applications, like nuclear medicine, radiometric assays, radiation sterilization, (iii) Food & Agriculture, for radiation processing of food products and mutation breeding, and (iv) Isotope Hydrology.

GCNEP Common Infrastructure & Facilities

In addition to the facilities being set up under individual schools, a few facilities are planned to be set up as common facility like (i) Food / Industrial Irradiator, (ii) Virtual Reality Laboratory, (iii) Computation Cluster, (iv) Conference Hall, (v) Interactive Distance Teaching (Electronic Class Room), (vi) Linkage to National Knowledge Network (NKN), and (vii) Residential complex along with an international guest house.

DAE Outreach Programme Cell

In addition to above, DAE Outreach Programme Cell will also be set up for publicising technologies developed by DAE for societal applications. GCNEP has taken major initiative towards enhancing public awareness and acceptance of nuclear energy programme - with a particular focus on students and faculty of engineering, pharmaceutical, nursing, management and basic science colleges and higher secondary schools.

Present Status of GCNEP

The activities of the Centre have already been initiated, at hired premises, by conducting Training Programmes/ Workshops in the areas of Nuclear Security, Radiological Safety, Safeguards, Radiation Technology Applications for Food Security, and Public Awareness. In the year 2013, ten such programmes were conducted. MOUs with US, Russia, France and the IAEA have been signed and exchange visits for collaborative programmes are going on.

Honourable Prime Minister Dr. Manmohan Singh is scheduled to lay the foundation stone of the GCNEP in early January 2014[1]. It is expected that the first phase construction will be completed by end of 2015 and the center will start functioning at the site soon thereafter. A transit office for shifting some of the operation of the centre very near to the site has also been established. GCNEP will also start offering training programmes from the transit office till the first phase of construction is complete.

Concluding Remarks

GCNEP will be the major centre for international collaborative work in different areas of nuclear security, nuclear and radiation safety, design of proliferation resistant, intrinsically safe and secure reactor system, various applications of radiation technologies etc. The first buildings in the campus of the GCNEP are slated to start functioning by early 2016, while a number of activities of the Centre, including international events, have been already launched by making use of off-site facilities.

Shri L. R. Jangra *obtained his B. Sc. Engg. (Hons) Degree in Electrical Engineering from NIT Kurukshetra (then REC) in 1982. He is from 26th batch of BARC Training School and joined Reactor Control Division in the year 1983. He has designed and developed reactor protection and control systems for nuclear research & power reactors. He is an expert in the area of Reactor C&I, safety critical systems review and audit. Presently, he is working for setting up the prestigious Global Centre for Nuclear Energy Partnership (GCNEP) at village Jasaur-Kheri in Jhajjar district, Haryana. He is Member-Secretary, Program Implementation Group and also Head, Coordination Division, GCNEP.*

[1](performed on 3rd January, 2014)

RNI MAHENG / 2002 / 7152

For Limited Circulation Only

Printed & Published by :
Dr. Rajesh Pai, Secretary, Indian Association of Nuclear Chemists and Allied Scientists (IANCAS)
(Registration No. MAH 232/1984 GBBSD) on the behalf of IANCAS, C/o. Radiochemistry Division,
Bhabha Atomic Research Centre, Mumbai 400 085.

Printed at
Perfect Prints, 22/23, Jyoti Industrial Estate, Nooribaba Dargah Road, Thane 400 601.
Tel. : (022) 2534 1291Telefax : (022) 2541 3546, E-mail : perfectprints@gmail.com

Edited by
Dr. N. Ramamoorthy
Bhabha Atomic Research Centre, Department of Atomic Energy, Mumbai