Enhancing Nuclear Security System of Irradiation Facility SIBO INRA/Tangier Morocco

Mouhib Mohammed[1], Chentouf Mouad[2], Guessous Amina[3] and Rostislav Vlaev[4]

1. INRA/CRRA/URTNEQ, Tangier, Morocco

2. INRA/CRRA, Tangier, Morocco

3. Faculté des Sciences IBN TOFAIL Kenitra, Morocco

4. 3TECH, Rabat, Morocco

Abstract: Around the world, radioactive sources have been widely used for decades to benefit humankind; industry food; health，etc. However, the malicious use of radiological sources poses a significant threat globally. As Irradiation facility for research the goal of this paper is to show a case study of application of nuclear security and nuclear security culture code of contact in irradiation facility using cobalt 60. And it will show the necessary work done to achieve the goal of protection of radioactive material and continue working in safe conditions. This objective could not be achieved without the collaboration of all department involved in security and nuclear safety. In this work we applied the nuclear security and nuclear security culture procedures in order to define the type of system used to achieve the global objective in accordance with Global Threat Reduction Program to reduce the threat of a RDD (Radiological Dispersion Device) in collaboration with The United States Department of Energy's NNSA (National Nuclear Security Administration). The objective of this paper is to share a local experience in upgrading security with return of experience in practice and very good collaboration with general direction of national security and all departments involved in security and nuclear safety.

Key words: Security, nuclear, irradiation, safety, radiological, cobalt 60.

1. Introduction

Around the world, radioactive sources have been widely used for decades to benefit humankind—to diagnose and treat illnesses, monitor oil wells and water aquifers, irradiate food to eliminate microbes, and for many other uses. However, the malicious use of radiological sources poses a significant threat globally.

IAEA (International Atomic Energy Agency) code of conduct on safety and security of radioactive sources is a prime example of this trend [1]. One of the basic principles of this code is, "Every State should establish an effective national legislative and regulatory system of control over the management of radioactive sources and over any other activity involving radioactive sources which entails a significant risk to individuals or the environment." According to this code such a system should, among other things, minimize the likelihood of a loss of control and provide for rapid response to regain control over sources that are no longer under control.

GTRI (Global Threat Reduction Initiative) [2] plays a major role in providing global partners with the ability to do this.

The goal of this paper is to show a case study of application of this code of contact in irradiation facility using cobalt 60 [3]. And it will show the necessary work done to achieve the goal of protection of radioactive material and continue working in safe conditions. This objective could not be achieved without the collaboration of all department involved in security and nuclear safety.

Corresponding author: Mouhib Mohammed, engineer researcher, research field: energy irradiation technology.

2. Nuclear Security and Nuclear Security Culture

2.1 Nuclear Security

Nuclear security is the prevention and detection of, and response to, theft, sabotage, unauthorized access, illegal transfer or other malicious acts involving nuclear or other radioactive substances or their associated facilities. It should be noted that "nuclear security" includes "physical protection", as that term can be understood from consideration of the physical protection objectives and fundamental principles, improvised nuclear explosive devices; and/or radioactive material to cause harm to individuals or the environment, including the construction of RDDs (radiological dispersal devices) and REDs (radiological exposure devices) [4]. Such threats could also include: the dispersal of radioactive material through the sabotage of facilities in which radioactive material can be found or of such material in transport. These could be outsider/insider threats. The political and economic consequences, and the impact upon human health and the environment, of the malicious use of radioactive material could be devastating, particularly in the case of a nuclear explosive device, and could be unpredictably disruptive in the case of malicious acts resulting in the dispersal of radioactive material.

2.2 Nuclear Security Culture

Nuclear security culture plays an important role in ensuring that individuals, organizations and institutions remain vigilant and that sustained measures are taken to prevent and combat the threat of sabotage or using radioactive material for malicious acts.

The term "nuclear security culture" [5] refers to the beliefs, understandings and practices that the people engaged in a nuclear organisation—from the Board to the general workforce—bring to its security. If they believe that security threats are real, understand that it

is every individual's responsibility to contribute to the security of the whole organisation, and take security responsibilities seriously as part of their daily practices, they are part of an organisation in which a robust culture of security has taken root. In an organisation with a strong security culture, staffs who observe an anomaly or hear something suspicious report it unhesitatingly to their supervisors. If they make a mistake themselves, they willingly own up to it, seek to understand how it occurred, and work actively to improve their performance. If they need more equipment or training to improve security, they feel justified in asking for it—and are likely to receive it. If they have ideas or suggestions for how security can be improved, they are willing to share them with their managers and colleagues because they know such contributions are encouraged, respected and rewarded. While many factors are at play in creating a culture of security, one factor stands out as having special importance: the support of leadership. In organisations with a strong security culture, leaders demonstrate that they take security seriously through their actions, not just their words. They set up policies and procedures that encourage the active participation of all employees in contributing to security. They reward those who come forward, and actively promote a collaborative culture in which security issues are discussed openly, teamwork in finding solutions is encouraged, and corrective actions are implemented quickly. They also conduct periodic assessments of the security culture in their organization to determine what state it is in and, if necessary, take proactive steps to improve it.

The factors that influence culture are essentially the same, whether referring to safety culture, security culture, or a culture of workplace collaboration. They consist of:

2.2.1 Beliefs, Principles and Values.

The essential factors that Shape Your Culture Your organisation's security culture is built on the foundation of the beliefs, principles and values of its board,
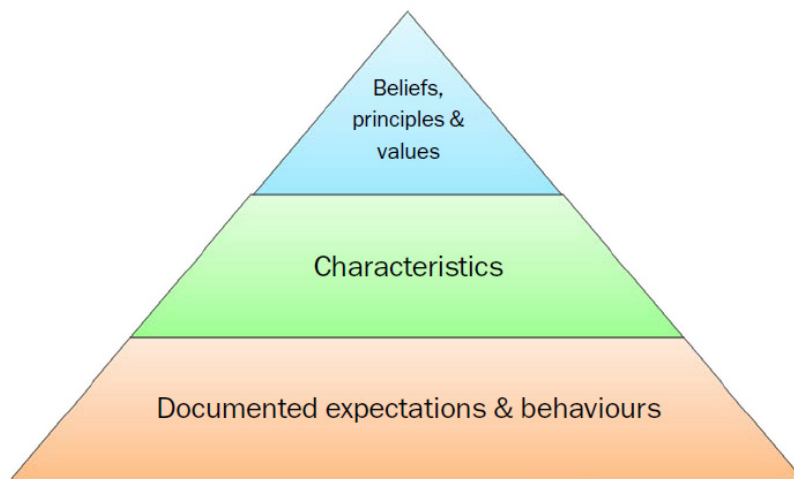
Fig. 1   Security management system.

managers and workforce. These factors are located at the top of the diagram because they are the ultimate sources of actions.

(1) Beliefs

Consisting of ideas that each of us accepts as true, the authors are not born with beliefs; rather, they are our deep-seated, personal responses to life's lessons and experiences. Organisations, also develop beliefs as a result of experience and reflection.

(2) Principles

Top-of-mind statements are, arising from beliefs that drive organizational behaviour.

(3) Values

Articulate aims, desires and goals arise from our beliefs. In a nuclear organisation, security is the responsibility of every person in the organisation. All employees have a duty to challenge, question and report on security issues.

2.2.2 Characteristics

In a strong culture, beliefs, principles and values give rise to a set of good practices known as characteristics.

Nuclear security demands that employees have the qualifications, skills, knowledge and training they need to contribute to organisational security at a high level of professional competence.

(1) Integration

Security processes must be properly integrated with safety, emergency planning, operations, human resources, strategic planning and all other aspects of an organisation's management framework.

(2) Learning and Improvement

A strong nuclear security culture grows out of a commitment to continual learning and improvement. Applying best practices and lessons learned from within the organisation, as well as from other organisations, is an inherent part of this process. Regular self-assessments help the entire organisation understand why any security lapses have occurred and what to do to prevent similar lapses in the future.

2.2.3 Documented Expectations and Behaviours

The third factor influencing nuclear security culture is documented expectations and behaviours. Each of the characteristics identified above requires specific kinds of behaviours from managers and staff members. A key senior leadership responsibility is to document these expectations and behaviours in the organisation's Security Management System.

(1) Setting Documented Expectations

A Security Management System defines an organisation's security policies, individual roles and responsibilities, standard operating procedures, and performance measurements. The system also specifies security-related training and qualification requirements for specific areas of concern, such as information security, personnel screening and

response to emergencies. Management needs to decide how it will encourage and measure staff trustworthiness, assure quality, manage change and obtain feedback. It needs to create contingency plans and drills, develop self-assessments and keep records. Finally, it needs to develop ways to interact with the regulator and work with other organisations in the sector. All of these considerations become part of the Security Management System.

(2) Promoting Desired Behaviour

Good security practices begin at the top. The board and senior management must have a clear understanding of their own roles and responsibilities with respect to security, know when and how to use their authority, make decisions and provide management oversight.

They must also determine how they will motivate and improve staff performance and the degree to which staff will be involved in the decision-making process. Finally, they must develop and carry out an effective communication program to promote security awareness, build understanding, and facilitate communication on security topics among colleagues and between staff and management. Topics for ongoing discussion include emerging threats, professional conduct, personal accountability, vigilance, and adherence to procedures, opportunities for improvement, and teamwork and cooperation. Nuclear security culture can be improved by periodically conducting an independent oversight, or audit, process that generates a holistic view of security performance. Increasingly, an assessment of security performance is included in periodic audits conducted by national and international regulators. It is also useful for the organisation itself to conduct work group audits to ensure that they meet the requirements of the documented Security Management System.

Using the best practices for improving security culture and nuclear security guidelines we have after several meeting with involved department in nuclear security and with collaboration with States Department of Energy's NNSA (National Nuclear Security Administration) [6]. The security system has been defined and installation of equipment and procedures started in the Irradiation facility SIBO (Station d'ionisation de boukhalef).

3. Irradiation Facility SIBO (Station d'Ionisation de Boukhalef)

The facility is a panoramic irradiator with dry store of cobalt 60 in a container used also as transport container in the first loading. It is the first one in Morocco and was installed in 1995 [7], in order to introduce this technology in Morocco the characteristic of this facility are:

Irradiation Cell:

6.1 m length

5.8 m width

2.6 m heigth

Three exposition systems have been installed around the source:

6 big turn tables for high doses

3 small turn tables adjustable in two dimensions for medium doses

1 turn table for low doses
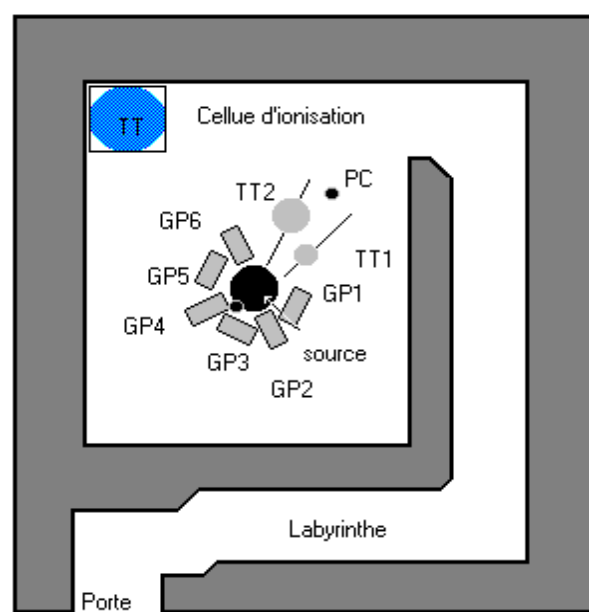
Type of the storage flask: SV-68 B(U) type.

Fig. 2   Irradiation cell with turn table system.

4. Installation and Up-Grading of Security System

The security requirements contained are based on the performance objectives from IAEA Nuclear Security Series No. 11 Security of Radioactive Sources for Security Level A, and the practices and policies of the NNSA GTRI (Global Threat Reduction Initiative).

This system has been installed in different phases the first one was with only two cameras in 2002.

The objective of this task is to implement security enhancements at the site [8]. The enhanced security systems will be incorporated into the existing site access control system, intrusion detection system, and CCTV system.

The main work done concerns the Irradiator Building and CAS (Central Alarm Station) with installation of specified equipment in police control station and concern:

(1) Installation of a hardened (steel) door of substantial construction to replace the entrance door to the control room.

(2) Installation of an electro-magnetic locking mechanism on the irradiator room door and the door to the control room.

(3) Installation of a dual credential biometric access control device on the door to the irradiator and the door to the control room.

(4) Installation of security window film on the windows in the control room. There shall also be security grating on the interior windows to prevent access.

(5) Installation of a color CCTV system appropriate for the environmental conditions providing video surveillance of the area of the irradiator, outside the entrance door to the irradiator room, and the control room. Cameras shall be focused on the exterior and interior.

(6) Installation of BMS (Balanced Magnetic Switches) tamper.

(7) Installation of dual technology (passive infrared and microwave) motion sensors.

(8) Installation of fixed duress buttons and providing mobile duress buttons for the staff.

(9) Installation of a TID (IR Barrier or BMS switch) on the irradiator cap to detect any unauthorized tampering with the irradiator.

(10) Installation of a strobe light and local siren that will annunciate in the vicinity of the room at a level exceeding 100 decibels (dB).

(11) Installation of a prox card access control system on the front door to the building, which utilize an electro-magnetic locking system with an emergency release on the inside of the door. The access control system (dual credential requiring prox card and pin access).

(12) Installation of an exterior intrusion detection system on the fence surrounding the perimeter of the irradiator building. Allow for the detection of an intruder as well as assessment during daytime and night time conditions.

(13) Replace the pedestrian gate with a turnstile system. The turnstile shall have an automated prox card access control system. This shall utilize a dual credential authorization requiring prox and pin number to grant access. The turnstile allows only one person to enter at a time.

(14) Automate the vehicle gate by installing an automatic closure device on the gate. This only is opened from the CAS.

(15) Installation of static vehicle bollards on the inside of the gate to prevent a vehicle from ramming the gate to gain access to the irradiator building.

(16) Program the electro-magnetic door locks in a manner that the irradiator door cannot be opened unless all other doors are closed and locked.

(17) Installation of color CCTV camera appropriate for the environmental conditions (sealed camera or in environmental housing) providing video surveillance.

(18) Replacing the door to the CAS with a hardened steel door and utilizing an electro-magnetic lock with an
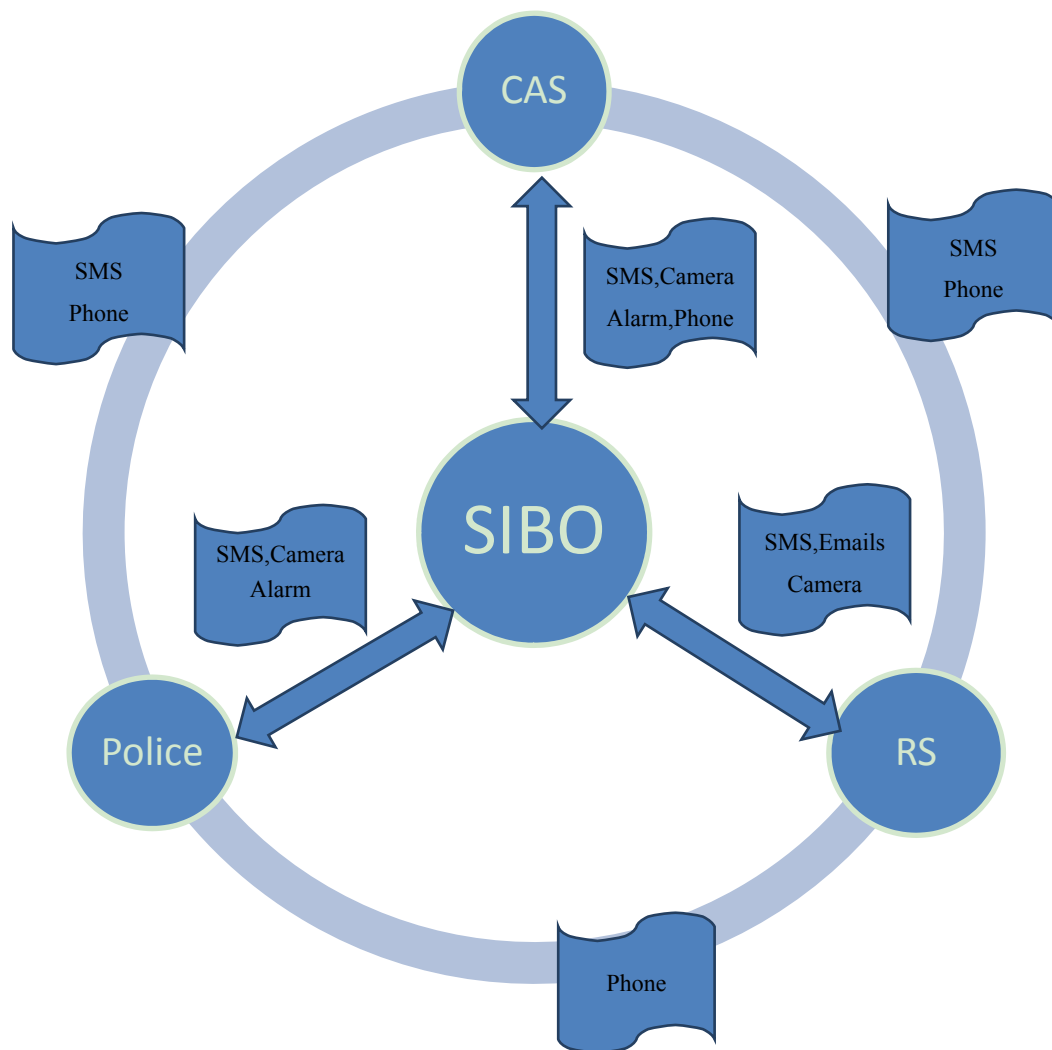
Fig. 3   Communication between Police, Cas and Responsibility of safety in the facility.

emergency release on the inside of the door and a proximity access control device with keypad to assure two levels of authentication.

(19) Construction of fences around the irradiator building, this fences replacing the previous one topped with razor wire.

(20) Installation of a remote monitoring station at the local police. This accepts all video and sensor alarms from the site.

An alarm management system (Fig. 3) is capable of integrating all sensor alarms and CCTV video and also incorporate the CCTV images with the capability of opening images on the screen for assessment purposes. This system also sents encrypted video and alarm information to the Tangier police dispatch center.

5. Conclusion

With this security system all procedures in nuckear security cultures are applied and it was also an opportunity to for real exercise during the upgrading of cobalt 60 done in the facility including transport of cobalt 60.

Also a specific procedure for the insider threat has been introduced in the system. During the last two years many works have been done on the facility

concerning the upgrading of cobalt 60, upgrading of safety and technical control of the facility, upgrading of security of the facility. This work has been done following the latest regulation and Norms using the latest technology and using 20 years work experience in the field.

This combined system upgraded in security and safety and processing purpose offers a new largest system with the best of each one and can give a specific global solution to similar facility witch needs to upgrade the control system.

References

[1] IAEA (International Atomic Energy Agency), Nuclear Security Series No. 11 Security of Radioactive Sources for Security, IMPLEMENTING GUIDE Vienna 2009, IAEA publication 2009.

[2] The Practices and Policies of the NNSA. Workshop in tangier 2016.

[3] IAEA (International Atomic Energy Agency), Manual on panoramic gamma irradiators IAEA PRSM. IAEA publication 1996.

[4] IAEA (International Atomic Energy Agency), Safety Glossary Nuclear Safety and Security 2016 REVISION-2007 Edition, IAEA publication.

[5] World Institute for Nuclear Security WINS, Nuclear Security Culture Rev 2 September 2011 (A WINS International Best Practice Guide.

[6] GTRI (Global Threat Reduction Initiative), us department of energy.

[7] Mouhib Mohammed Inra Radioprotection et dosimetrie de la station d'ionisation de Boukhalef SIBO Crra- PTN Tanger Maroc September 1997 (Annual report–Rapport de titularisation).

[8] Mouhib Mohammed – Influence de quelques paramètres sur le débit de doses à différentes positions de la source radioactive Et élaboration d'un logiciel sous Windev permettant d'intégrer toutes les données relatives aux conditions de traitement des différents produits dans la station SIBO Inra – Crra- URTNEQ Tanger Maroc 2003. Thesis for Professional promotion to Engineer Chef.

[9] 2012. Failure Mode and Effects Analysis FMEA. John Wiley & Sons.

[10] IAEA (International Atomic Energy Agency), Standards for Protecting People and the Environment Preparedness and Response for a Nuclear or Radiological Emergency. 2013. IAEA Safety Standards Rev.

[11] [Jean Pierre Vckoff, Développement Rapide des Application RAD Méthodes et out ils , les règles à respecter dans le développement d'applications client-serveur (S&S Masmillan 1996).

[12] F Scott Barker, Microsoft Access 2000 Programmation edition 2000 (F. Scott Barker's Microsoft Access 2000 Book)

[13] Pham Thu Quag J Gonn, Réussir la conduite de projet Informatique.