Annals of Nuclear Energy 75 (2015) 292–302

Contents lists available at ScienceDirect

Annals of Nuclear Energy

journal homepage: www.elsevier.com/locate/anucene

Review

Safety, security and safeguard

Nasiru Imam Zakariya [a,*], M.T.E. Kahn [b]

[a] Electrical, Electronics and Computer Engineering Department, Cape Peninsula University of Technology, Bellville, South Africa[1]
[b] Centre for Distributed Power and Electronic Systems, Cape Peninsula University of Technology, Bellville, South Africa

ARTICLE INFO

Article history:
Received 5 June 2014
Received in revised form 21 August 2014
Accepted 22 August 2014
Available online 13 September 2014

Keywords:
Safety
Security
Safeguard
Synergy
Threat
Sabotage

ABSTRACT

A physical protection system (PPS) integrates people, procedures, and equipment for the protection of assets or facilities against theft, sabotage and terrorist attacks. Therefore, this paper proposes the use of a systematic and measurable approach to the design of PPS and its emphases on the concept of detection, delay and response. The proposed performance based PPS has the capability of defeating adversaries thereby achieving its targets. Therefore, timely detection of intrusion – based on the use of sensors, signal lines and alarm systems – is a major principle in the proposed system. Also the need for deterrence such as barriers in form of guards, access control, close circuit television (CCTV), strong policy and procedures, then the security culture amongst the facility workers was appropriately discussed. Since nuclear power is considered the only source that can provide large scale electricity with comparatively minimal impact on the environment, the paper also considered base guidelines for the application of PPS in any nuclear and radioactive facilities, followed with the necessity to incorporate inherent safety, security and safeguard (3S) synergy innovation in the physical protection system design and other characteristics that will enhance to reduce the vulnerability of nuclear facilities and materials to theft sabotage and terrorist attacks.

Contents

* Corresponding author. Tel.: +27 619107239/+234 8033104702.
E-mail addresses: 212057189@mycput.ac.za (N.I. Zakariya), khant@cput.ac.za (M.T.E. Kahn).

[1] Present address.

http://dx.doi.org/10.1016/j.anucene.2014.08.051
0306-4549/

1. Introduction

Due to the need and interest in development of nuclear energy capabilities, the potential for malicious use of nuclear and radioactive materials has expanded and heightened. This increase in the nuclear power programs will likely include the construction of a variety of nuclear facilities that could become new potential targets for terrorists and other dangerous actors. According to Boureston and Semmel (2010), an international Symposium held at Vienna, Austria between March 30-April 3, 2009 noted availability of credible evidence that terrorists are interested in acquiring and using nuclear material to build a rudimentary nuclear explosive device, and in constructing a radiological dispersal device that could be used to sabotage nuclear facilities or places where radioactive substances are used, stored, or transported. Also, the physical protection against the theft or unauthorized use of nuclear material and against the sabotage of nuclear material and facilities by individuals or groups of persons has become a matter of increased concern nationally and internationally (Carmona, 2005). Similarly, as a result of a greenhouse gas emission and the need to increase energy demand, a global trend to introduce nuclear power into both developed and emerging countries has been growing. This also increases concern from the international society about the consequences and impact on the non-proliferation regime. Therefore, introducing non-proliferation mechanisms in an efficient and effective manner will require not only a balance between peaceful use of nuclear energy and nuclear non-proliferation, but also inter-cooperation among the 3S practices and implementation (Rojavin et al., 2011). Therefore, fostering a 3S understanding and culture will be important for establishing a stable foundation from which to successfully implement and sustain nuclear energy programs and maintain their public acceptance. Though nuclear industry maintains very high safety standards, the potential for an unintentional reactor malfunction and release of radioactive materials into the environment represents a significant risk. This risk is also associated with the medical use of radioactive materials, as well as storage and transport of spent nuclear fuels.

2. Physical security and protection

The Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225) document of International Atomic Energy Agency (IAEA) has long been considered as the internationally accepted standard for nuclear physical protection, and the practical complement to the Convention on the Physical Protection of Nuclear Material. However, it is not a legally binding instrument as such, but it is given legally binding effect in some bilateral nuclear safeguards agreements that prescribe Information Circular (INFCIRC/225) as the standard to be applied to nuclear material supplied under such agreements (Everton et al., 2010). The physical protection which is also referred to as physical security consists of a variety of measures to protect nuclear facilities and material against sabotage, theft, diversion, and terrorist attacks. The United States Nuclear Regulatory Commission (USNRC) and its licensees use a graded approach for physical protection, consistent with the significance of the facilities or material to be protected. In so doing, the USNRC establishes the regulatory requirements and assesses compliance, and licensees are responsible for providing the protection (USNRC, 2013a,b). Accordingly, the nuclear facilities that require physical protection include nuclear reactors, fuel cycle facilities, and spent fuel storage and disposal facilities.

2.1. Physical Protection System (PPS)

A PPS integrates people, procedures, and equipment for the protection of assets or facilities against theft, sabotage, and terrorist attacks. Hence, the design of an effective PPS requires a methodical approach in which the designer weighs the objectives of the PPS against available resources and then evaluates the proposed design to determine how well it meets the objectives. Without this kind of careful assessment, the PPS might waste valuable resources on unnecessary protection or, worse yet, fail to provide adequate protection at critical points of the facility (Xu et al., 2014; Garcia, 2008; Nuclear Security Science and policy Institute-NSSPI, 2014a,b). However, theft, sabotage, and terrorist attacks at a facility may be prevented in two ways: by deterring the adversary or by defeating the adversary. Deterrence occurs by implementing measures that are perceived by potential adversaries as too difficult to defeat. It makes the facility an unattractive target, so the adversary abandons or never attempts an attack. Examples of deterrents are the presence of security guards in parking lots, adequate lighting at night, posting of signs, and the use of barriers, such as bars on windows. These are features that are often implemented with no additional layers of protection in the event of an attack. Therefore, deterrence can be very helpful in discouraging attacks by adversaries. However, it is less useful against an adversary who chooses to attack anyway. According to Bakr and Hamed (2009), the ultimate goal of a PPS is to prevent the accomplishment of overt or covert malevolent actions. Typical objectives are to prevent sabotage of critical equipment, deter theft of assets or information from within the facility, and protect people. A PPS must accomplish its objectives by either deterrence or a combination of detection, delay and response. Fig. 1 below is a design and evaluation process for PPS. The process starts with determining objectives, then designing a system to meet the objectives. It ends with an evaluation of how well the system performs compared to the objectives.

Adversaries can be classified into three categories, outsiders, insiders and outsiders working in collusion with insiders (IAEA, 2008; Garcia, 2008). Accordingly, each class of adversary with the full range of tactics of deceit, force, stealth, or any combination of these should be expected. Deceit is the attempted defeat of a security system by using false authorization and identification, force is the overt, the forcible attempt to overcome a security system and stealth is any attempt to defeat the detection system and enter the facility covertly. For any given facility there may be several threats, such as a criminal outsider, a disgruntled employee, competitors, or some combination of these, so the PPS must be designed to protect against all of these threats. Therefore, the best option in designing a new PPS is to combine such elements as

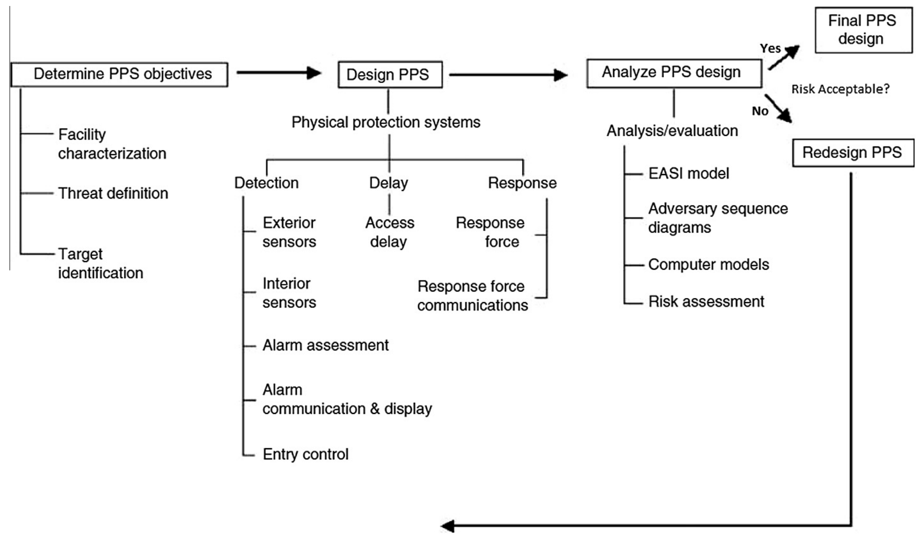

Fig. 1. Design and evaluation process for physical protection systems (Garcia, 2008; NSSPI, 2014a,b).

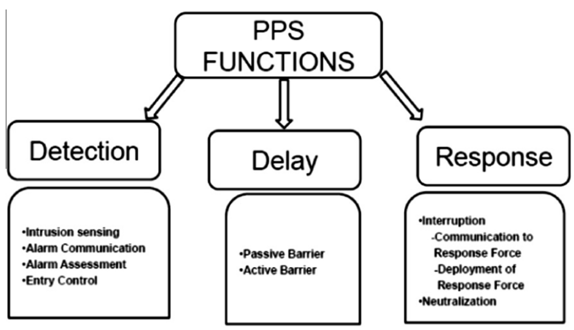

Fig. 2. Functions of physical protection system (Brayon, n.d.).

fences, barriers, sensors, procedures, communication devices, and security personnel in order to achieve the protection objectives necessary. The overall design should meet its objectives within the operational, safety, legal, and economic constraints of the facility. The primary functions of a PPS are detection, delay and response by security personnel and an effective PPS must accomplish these objectives by either deterrence or a combination of detection, delay and response (Garcia, 2008).

Detection: This is the discovery of an adversary action, which includes sensing of covert or overt actions. The measures of effectiveness for the detection function are the probability of sensing adversary action and the time required for reporting and assessing the alarm.

Delay: Delay can be accomplished by personnel, barriers, locks, and activated delays. It is the slowing down of adversary progress. Response personnel can be considered elements of delay if they are in fixed and well-protected positions.

Response: This consists of the actions taken by the response team to prevent adversary success. This may include both interruption and neutralization. Interruption is defined as a sufficient number of response personnel arriving at the appropriate location to stop the adversary's progress while Neutralization describes the actions and effectiveness of the responders after interruption.

Fig. 2 below is the graphical view on the function of PPS:

Similarly, according to IAEA (1999) and Nuclear Security Science and policy Institute-(NSSPI) (2014a,b), a country's objectives for physical protection system are as follows:

(a) To establish conditions which would minimize the possibilities for unauthorized removal of nuclear material and/or for sabotage; and
(b) to provide information and technical assistance in support of rapid and comprehensive measures by the country to locate and recover missing nuclear material and to cooperate with safety authorities in minimizing the radiological consequences of sabotage.

2.2. Concept and requirements of PPS design

According to Gandhi and Kang (2013), design concepts traditionally applied to nuclear safety such as defense in depth, single failure criteria, redundancy and diversity; fail safe criteria, passive systems are also applicable to nuclear security as well. These safety designs and systems can potentially reinforce protection against malicious acts. Therefore, application of these concepts to nuclear security means that would-be perpetrators of nuclear sabotage must compromise several layers of safeguards in order to cause radiological release. However, it is the responsibility of every country to establish and maintain the risk associated to the removal and sabotage of nuclear materials and facilities and this can be achieved through the risk management of physical protection regime which involves assessing the threat and the potential consequences of malicious acts, then developing a legislative, regulatory framework which ensures that appropriate and effective physical protection measures are put in place (IAEA, 2011a,b). The fundamental principles of risk management for physical protection design are as follows:

1. Defense in depth.
2. Security culture.
3. Quality assurance.
4. Confidentiality.
5. Contingency.

2.2.1. Defense in depth

Defense in depth in nuclear security is based on the PPS, which serves to detect, delay and respond effectively in attempts to harm a nuclear facility, nuclear material accounting system and to protect, control against insider and outsider threats. According to Kim and Kang (2012) the concept of defense in depth applies as much in nuclear security as to nuclear safety. At the design level of nuclear facilities, defense in depth relates to physical protection that reflects the concept of several layers (IAEA, 2011a,b) and methods of protection such as structural, technical, personnel and organizational that may need to be circumvented by an adversary in order to achieve his objectives. For instance, an incidence of Fukushima Nuclear Power Plant disaster which occurred March 11 2011, resulting in a meltdown of three of the plant's six nuclear reactors was as a result of insufficient defense in depth provisions for tsunami hazards. The failure occurred when the plant was hit by a tsunami triggered by the magnitude 9.0 Tōhoku earthquake. The tsunami waves overwhelmed the defenses of the Fukushima Dai-ichi facility, which were only designed to withstand tsunami waves of a maximum of 5.7 m high as against the larger waves that impacted the facility estimated to be over 14 m high (IAEA, 2011c). Therefore, a prime aspect of the principle of defense in depth however is the successive layers of protection that must be independent to each other and be sufficient to prevent harm occurring which should cover all layers of protection: management systems and cultures, site selection, design incorporating safety margins, diversity and redundancy with appropriate attention to quality and reliability requirements, operating systems, accident and emergency arrangements.

2.2.2. Security culture

IAEA (2012) and Khripunov (2012) have defined nuclear security culture as the assembly of characteristics, attitudes and behavior of individuals, organizations and institutions which serves as a means to support and enhance nuclear security. A literature review revealed that there is no accepted ways of measuring security culture that can be used outside narrow domains such as the nuclear industry and the security culture to organizational performance (Malcolmson, 2009). Although specific research on security culture has been limited, he has noted that relationships do exist between security culture and organizational security metrics. Therefore, understanding and then enhancing the security culture within organizations where security is a critical success factor is likely to lead to those organizations being better able to achieve their primary goals and maintain their reputation. According to Centre for Nuclear Non-Proliferation and Disarmament-CNND (2013), there are six groups of actors responsible for the proper development of security culture. These are countries, organizations, managers in organizations, personnel, public and the international community who fulfil the different tasks relevant for the realization of nuclear security culture through dialogue and coordination.

2.2.3. Quality assurance

According to USNRC (2013b), quality assurance (QA) comprises all planned and systematic actions that are necessary to provide adequate confidence that a structure, system, or component will perform satisfactorily in service. Attributes of a QA program include procedures, recordkeeping, inspections, corrective actions, and audits. The QA program is an interdisciplinary management tool that provides a means for ensuring that all work is adequately planned, correctly performed and assessed. It includes the organizational structure, functional responsibilities, levels of authority and interfaces for those managing, performing and assessing the adequacy of work providing a systematic approach for accomplishing work with the ultimate goal of doing the job right the first time (IAEA, 1996).

2.2.4. Confidentiality

This is the concept and the property that information is not made available or disclosed to unauthorized individuals, entities, or processes. Computer security objectives are commonly defined as protecting the confidentiality, integrity and availability attributes of electronic data or computer systems and processes. Therefore by identifying and protecting these attributes in data or systems that can have an adverse impact on the safety and security functions in nuclear facilities, the security objectives can be achieved. Otherwise, there will be an impact on the organization, which may take various forms, such as breaches of nuclear security, impaired safety, and impaired operation of the activities, loss of customer confidence or financial losses (IAEA, 2011a,b).

2.2.5. Contingency

According to Gandhi and Kang (2013), a contingency plan can be seen as a sort of upstream radiological emergency plan. It is designed to secure a site before mitigation actions are taken. The contingency plan is also referred to as disaster planning. Statistics provided by Price Waterhouse Coopers reveal that 90 percent of all companies that experience a computer disaster with no pre-existing survival plan go out of business within 18 months (Krupa, 2003). However, if a flood, fire, or hurricane occurred at an organization's site, one would hope employees at this facility know what to do. More importantly, if there was unrecoverable damage to systems, there should be a contingency plan that gives accurate instruction on how to recover from disaster in a specific amount of time.

3. Safety, security and safeguard

Endo (2009) noted that the quest for nuclear power should be welcomed from the perspectives of achieving energy security and combating global warming, but this should not be without reservation because great number of nuclear reactors could increase problems and risks in terms of safety, security, and safeguards, and careful consideration must be given to these three aspects when introducing nuclear power generation to alleviating these. Therefore, the 3Ss stand out as the major prerequisites for the peaceful use of nuclear energy. Safety was the first to gather interest internationally and to be systematically established, followed by safeguards. Nuclear security is to a certain degree included in the concepts of safety and nuclear non-proliferation, but it has come to be treated as an independent concept.

3.1. Nuclear safety

The main principle of safety regulation is to protect the population and the environment from radiation and other hazards caused by the operation of nuclear power plants and other nuclear facilities at all stages of life cycle, as well as storage, transportation and radioactive materials utilization including spent nuclear fuel and radioactive waste, at the same time safety is adherence limits of radiation exposure to personnel, population and environment, and abidance by established rules, regulations and safety standards (IAEA, 2014). Nuclear Safety concerns both the risks of radiation under normal conditions and those arising risks from incidents or due to loss of control over the operation of nuclear reactor, chain reaction, radioactive source or any other source of radiation. Therefore, safety main aim is on the transparency of the information and this is due to the necessity of sharing feedback on experience, and thereby to prevent occurrences of incidents or accidents at one nuclear power plant from being repeated at others. According to Endo (2009), nuclear safety can be divided by focus into the safety of plant design and operation and the safety of material handling, and by phenomenon into safety for the prevention of radioactive exposure and safety for the prevention of critical accidents.

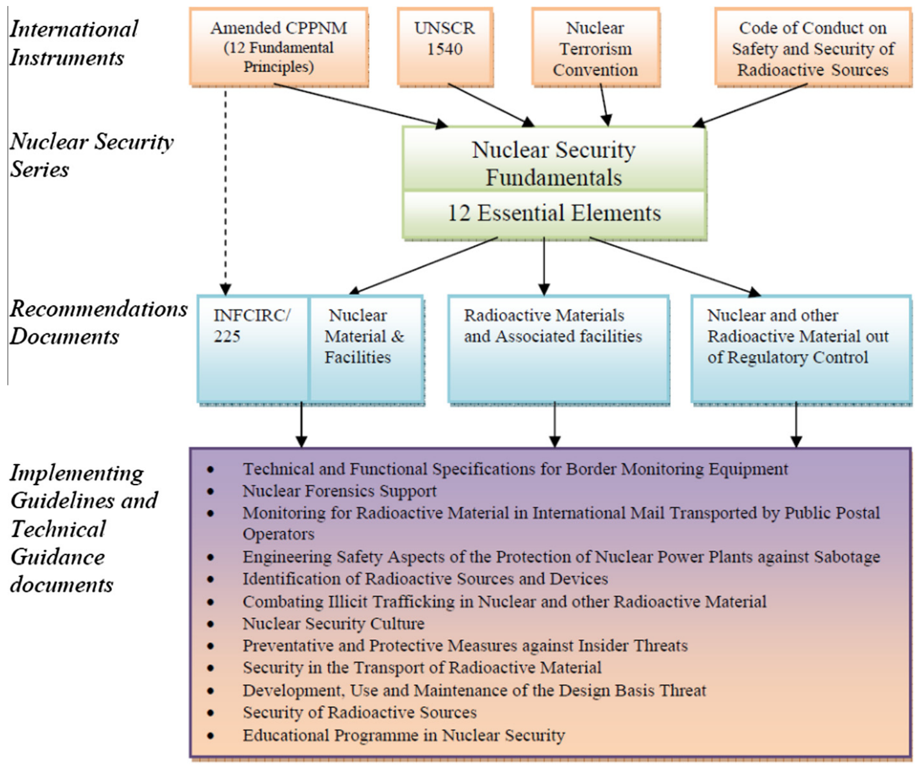

Fig. 3. The Global Nuclear Security Regime (Everton et al., 2010; CNND, 2013).

3.2. Nuclear security

According to CNND (2013), nuclear security means measures designed to address the risks associated with theft and trafficking in nuclear and radiological materials, sabotage of nuclear facilities, and the danger of terrorists acquiring and using it for a nuclear weapon. The global advances in recent time on nuclear security are still inadequate. Therefore, effective nuclear security must be of a concern globally. This is quite necessary because a major nuclear security incident would have far-reaching consequences. Doyle (2008) noted that the security of nuclear materials is the responsibility of the country that possesses them and they have a variety of approaches to this task. There are no legally binding requirements for maintaining high level standards of security, nor is there any multinational authority that inspects and evaluates the effectiveness of nuclear safeguards in each country. However, there is a Convention on the Physical Protection of Nuclear Material to which nearly all countries with nuclear materials are party. These countries agree to follow technical guidelines for adequate physical protection of nuclear materials during storage and transportation. IAEA provides these guidelines to all countries through its document on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Rev.4) but does not require inspections or enforcement of the convention. Amano (2013), the Director General of IAEA highlighted that the risk that nuclear or other radioactive material could be used in criminal or intentional unauthorized acts remains a matter of concern internationally and continues to be regarded as a threat to international security. It is well recognized that the responsibility for nuclear security rests entirely with each country and that appropriate and effective national systems for nuclear security are vital in facilitating the peaceful use of nuclear energy and enhancing global efforts to combat nuclear terrorism. Significant growth is anticipated over the coming years in the use of nuclear applications in general and nuclear power programmes in particular by several countries.

3.3. Global nuclear security architecture

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 – ad hoc and voluntary cooperative measures. As in Fig. 3 above, the main global components are (Everton et al., 2010; CNND, 2013):

- The Convention on the Physical Protection of Nuclear Material (CPPNM) (1980) which applies primarily to the protection of nuclear material in international transport and the CPPNM Amendment (2005) which extends the convention's application to protection of nuclear material in domestic use and of facilities against sabotage;
- The International Convention for the Suppression of Acts of Nuclear Terrorism (ICSANT) (2007),
- United Nations Security Council Resolution (UNSCR) 1540 (28 April 2004),
- IAEA guidance documents like INFCIRC/225/Rev.5 and INFCIRC/153 and various multilateral, regional and bilateral agreements and initiatives. The Physical Protection of Nuclear Material (INFCIRC/225) and its subsequent amendments to Rev.4 are IAEA documents on guidelines and recommendations to protect nuclear facilities and nuclear materials against intentional cases of theft, sabotage or mishandling during transportation. But Rev.5 update is designed to cope with emerging threats to nuclear materials especially nuclear terrorism with new standards for nuclear security in compliance to CPPNM – 2005. However, the reason for the review was the desire to harmonize the structure of Rev.5 with the amended CPPNM which is the parallel development in physical protection standards through the IAEA's Nuclear Security Series and to accommodate the changed in threat environment following the terrorist attacks on the United States in 2001. While INFCIRC/153, according to (Parsick and Sanborn (1994), is an IAEA guidance document

for Non Proliferation Treaty (NPT) verification which serves as an element of a special nuclear materials production cut-off convention. Its safeguards objective is the ability to detect diversion which is achieved by verifying country's nuclear material accounting system. However, a non-nuclear weapons country signatory to the NPT must periodically report of all transfers and inventories of nuclear material to the IAEA for which it will verifies the reports by auditing the records and by independent observations, including measurements of the material presented to the inspectors.
- The Fundamental Principles of Physical Protection of Nuclear Material and Nuclear Facilities.

However, the 12 essential elements for an effective and appropriate nuclear security regime that should be reasonably and practically applied are as follows (IAEA, 2013b):

1. State responsibility:
   It is the responsibility of a country to meet the objective of the country's nuclear security regime thereby establishing, implementing, maintaining and sustaining a nuclear security regime applicable to nuclear material, other radioactive material, associated facilities, and associated activities under its jurisdiction.
2. Identification and definition of nuclear security responsibilities:
   Various responsibilities such as regulatory bodies and those competent authorities related to border control and law enforcement should be identified and defined for appropriate integration and coordination of responsibilities for the sake of oversight to ensure the continued appropriateness of the nuclear security regime.
3. Legislative and regulatory framework:
   Establish competent authorities, including regulatory bodies, with adequate legal authority to fulfill their assigned nuclear security responsibilities.
4. International transport of nuclear material and other radioactive material:
   Ensuring that nuclear material and other radioactive material are adequately protected which extends to the international transport thereof, until that responsibility is properly transferred to another country.
5. Offences and penalties including criminalization:
   To define appropriately under nuclear security regime measures for offences or violations under domestic laws or regulations for criminal or intentional unauthorized acts involving or directed at nuclear material, other radioactive material, associated facilities or activities.
6. International cooperation and assistance:
   A nuclear security regime provides cooperation and assistance between countries directly or through IAEA or other international organizations by either assistance or cooperation in providing timely information as appropriate to affected countries concerning criminal or intentional unauthorized acts involving nuclear and radioactive material.
7. Identification and assessment of nuclear security threats:
   The nuclear security regime ensures identification and assessment of nuclear security threats, both internal and external including their credibility, regardless of whether the targets are within or outside the country's jurisdiction.
8. Identification and assessment of targets and potential consequences:
   A nuclear security regime ensures that targets under the country's jurisdiction are identified, assessed and it is up to date maintained to determine if protection from nuclear security threats is required should the targets be compromised.
9. Use of risk informed approaches:
   A nuclear security regime uses risk informed approaches in the conduct of nuclear security related activities that are based on a graded approach and defense in depth such as in the allocation of resources for nuclear security systems and nuclear security measures.
10. Detection of nuclear security events:
    A nuclear security regime ensures that nuclear security systems and nuclear security measures are in place at all appropriate organizational levels to detect and assess nuclear security events and to notify the relevant competent authorities so that appropriate response actions can be initiated.
11. Planning, preparedness and response to a nuclear security event:
    A nuclear security regime ensures that relevant competent authorities and authorized persons are prepared to respond appropriately, at local, national, and international levels to nuclear security events by developing arrangements and response plans and periodically exercising, testing, and evaluating the plans for effectiveness by relevant competent authorities and authorized persons with the aim of ensuring timely implementation of comprehensive measures.
12. Sustaining a nuclear security regime:
    A nuclear security regime ensures that each competent authority, authorized person and other organizations with nuclear security responsibilities contribute to the sustainability of the nuclear security regime and this can be achieved by developing, implementing and maintaining appropriate and effective integrated quality management systems in nuclear security matters.

The need for effective nuclear security has been widely recognized. So far, three Nuclear Security Summit (NSS) have been held. One was on 12–13 April 2010 in Washington, DC and the second was 26–27 March 2012 in Seoul. The third is at Hague, Netherlands on 24 and 25 March 2014 (CNND, 2013). Likewise, the Nuclear Security Series are International Atomic Energy Agency (IAEA) publications 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.

3.4. Safeguard

The primary role of IAEA Department of Safeguards – DOS (2014) is to deter the proliferation of nuclear weapons. It does so in two ways: by providing credible assurances that States are honoring their international obligations, thus helping to build international confidence, and by being able to detect early any misuse of nuclear material or technology, thereby alerting the world of potential proliferation. In achieving this, the Department applies various technical measures to verify the correctness and the completeness of the declarations made by States about their nuclear material and activities. IAEA safeguards are an essential component of the international security system. Accordingly, safeguards by design is defined as an approach whereby international safeguards requirements and objectives are fully integrated into the design process of a nuclear facility, from initial planning through design, construction, operation, and decommissioning. This process is not unique to international safeguards and it represents good project management to include safeguards requirements in the overall design and construction process. By including awareness of all regulatory issues, including international agreements that concern international safeguards, project management can schedule consideration at the appropriate time and level of detail and subsequently reduce the project risk

(IAEA, 2013a). Therefore, it is important to understand that nuclear safeguards are a means of reassurance whereby non-nuclear weapons states demonstrate to others that they are abiding by their peaceful commitments. They prevent nuclear proliferation in the same way that auditing procedures build confidence in proper financial conduct and prevent embezzlement. Their specific objective is to verify whether declared nuclear material remains within the civil nuclear fuel cycle and is being used solely for peaceful purposes or not. Also, non-nuclear-weapons state parties to the non proliferation treaty (NPT) agree to accept technical safeguards measures applied by the IAEA. These require that operators of nuclear facilities maintain and declare detailed accounting records of all movements and transactions involving nuclear material. Almost 900 nuclear facilities and several hundred other locations in 57 non-nuclear-weapons countries are subject to regular inspection (WNA, 2013). Similarly, their records and the actual nuclear material are audited. Inspections by the IAEA are complemented by other measures such as surveillance cameras and instrumentation. The aim of traditional IAEA safeguards is to deter the diversion of nuclear material from peaceful use by maximizing the risk of early detection. At a broader level they provide assurance to the international community that countries are honoring their treaty commitments to use nuclear materials and facilities exclusively for peaceful purposes. In this way safeguards are a service both to the international community and to individual countries, which recognize that it is in their own interest to demonstrate compliance with these commitments. According to Boyer and Schanfein (2008), the IAEA defines in the model comprehensive safeguards agreement (CSA) in INFCIRC/153, the technical aim of safeguards as the timely detection of diversion of significant quantities of nuclear material from peaceful nuclear activities to the manufacture of nuclear weapons or of other nuclear explosive devices or for purposes unknown, and deterrence of such diversion by the risk of early detection. Therefore the relationship between safety, safeguards and security is safeguards addresses "peace", nuclear safety as addressing "safety" and nuclear security as spanning both peace and "safety" (Endo, 2009). The term safeguards in relation to peaceful uses referred to institutional, legal, and technical mechanisms to prevent the misuse of nuclear technologies and nuclear materials for military applications. Nuclear technology has dual-use technology with both peaceful and military applications. Concerns about the misuse of peaceful applications of nuclear energy were at first focused on the country's seeking nuclear weapons. The first concepts for restricting nuclear energy to peaceful purposes were proposed in the context of a broad international agreement under the auspices of the newly formed United Nations (Tape and Pilat, 2008).

4. Nuclear safety and nuclear security synergy

Alger (2008) noted that nuclear safety refers to the prevention and mitigation of nuclear accidents and the harmful effects of radiation on human health and the environment while nuclear security refers to the physical protection of nuclear materials and equipment from theft or tampering. During the Fukushima accident of March 2011 and the connection between nuclear security and nuclear safety, it was considered that sustained efforts are required to address the issues of nuclear safety and nuclear security in a coherent manner that will help ensure the safe and secure peaceful uses of nuclear energy (IAEA-NSS, 2012). Hence, during 2012 Seoul NSS of March 2012, synergy between safety and security was one of the main directions of discussion. Based on the official Seoul Summit Communiqué, safety measures and security measures have in common the aim of protecting human life and health and the environment. Moreover, nuclear security and nuclear safety measures should be designed implemented and managed in nuclear facilities in a coherent and synergistic manner. According to IAEA (2014), there is no exact distinction between the general terms safety and security. In general, security is concerned with malicious or negligent actions by humans that could cause or threaten harm to other humans; safety is concerned with the broader issue of harm to humans and the environment from radiation, irrespective of the cause. Therefore, safety matters are transparent with the use of probabilistic safety analysis while security matters are confidential and threat based judgment is used. Fig. 4 shows the Venn diagram for safety nuclear and security synergy.

Gandhi and Kang (2013) have noted that there are many common linkages between safety and security as shown in Fig. 4 above and it is important to treat nuclear safety and security as interrelated subjects, mutually reinforcing and fully integrated. Hence, the synergy between the two should be maximized. Consideration should also be given to the facts that although some safety systems can enhance security, at times security systems have been seen to interfere with safety practices and vice versa. Hence, it is essential that an integrated approach towards nuclear safety and security be adopted. This study describes the similarities and differences between nuclear safety and security. Further, it suggests the ways and methods to increase the synergy between nuclear safety and security. A key difference between nuclear safety and security is intentionality. Accidents related to nuclear safety are unintentional, whereas nuclear security incidents are clearly intentional and undertaken with a specific motive. While safety culture promotes transparency and openness, security culture requires confidentiality. A well-developed safety culture requires that employees share information liberally, but a well-developed security culture requires that the employees share information with the relevant authorized personnel only. Safety culture and security culture should not be merged and yet, they should not be set in opposition to each other. Operators should attempt to integrate the safety-security interface into the core operations of nuclear facilities. Safety and security measures must be built into a plant in all its phases, from design and construction, through operation, to decommissioning and dismantlement. According to Kim and Kang (2012), to ensure that nuclear facilities do not endanger the public, it is time to think in terms not of nuclear safety, or nuclear security, but of a combined approach called nuclear safety-security. Although safety and security programs have different requirements, they overlap in key areas and could support and enhance one another. Moreover, nuclear facilities could improve safety-security in technical ways, including more secure emergency electrical supplies, better security for control rooms, and at new plants, reactor containment structures built to survive attacks by terrorist flown airplanes. At the institutional level, regulators could strengthen the safety-security interface by requiring it to be built into the life cycle of nuclear plants, from design to dismantlement. Similarly, International Nuclear Safety Group-INSAG (2010a,b) highlighted that the events taken into account differ in each sphere but safety evaluations focus on risks arising from unintended events initiated by natural occurrences (such as earthquakes,

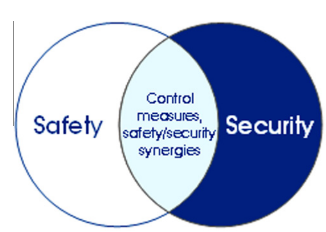

Fig. 4. Synergy of safety and security (IAEA, 2014; Batra and Nelson, 2012).

tornadoes, or flooding), hardware failures, other internal events or interruptions (such as fire, pipe breakage, or loss of electric power supply), or human mistakes (such as the incorrect application of procedures, or incorrect alignment of circuits). In the case of security, the risks, or events arising from malicious acts carried out with the intent to steal material or to cause damage. Security events are therefore based on intelligent or deliberate actions carried out purposely for theft or sabotage and with the intention to circumvent protective measures. Safety and Security should be coordinated from the conceptual stages of development, through infrastructure building, sitting, design, and operation and decommissioning. All systems and procedures should be examined to both safety and security with the aim of ensuring that an optimal balance is achieved. An effective change control process should be put in place to ensure that any proposed changes of design, layout or procedures are thoroughly evaluated to verify that they do not jeopardize safety or security. Therefore, the principle of optimization of protection, applicable to both safety and security, is based on the idea that radiation risks must be kept as low as reasonably as achievable (ALARA), taking social and economic factors into consideration.

According to Kim and Kang (2012), the following areas have been identified in which synergy between safety and security could be maximized:

(1) Legal and regulatory framework.
(2) Responsibility.
(3) Design concepts and criteria.
(4) Graded approach.
(5) Operating principles.
(6) Emergency response.
(7) Training and education.

4.1. Legal and regulatory framework

According to Gandhi and Kang (2013), a legislative and regulatory framework is required to ensure sufficient oversight of installations, deal with potential radiological risks and implement safety as well as security requirements.

4.2. Responsibility

The responsibility of a country lies more on the security than the safety related issues hence, in the assessment of threats and Design Basis Threat (DBT), both of which serve as the basis for the design of the physical protection system for a nuclear facility. But the prime responsibility of the operator is on the safety of the facility (Gandhi and Kang, 2013).

4.3. Design concepts and criteria

Nuclear power plants are designed by applying the defense in depth principle for both safety and security. Certain design criteria imposed for safety purposes may serve to reinforce security. As an example, the single failure criterion applied to safety systems requires the nuclear power plant to be designed with a sufficient level of redundancy and/or diversification to ensure that safety functions are maintained even if one set of equipment in the system fails. This design feature is helpful for security purposes as well. Therefore, with the application of this criterion, aggressors must compromise several targets in the nuclear power plant in order to cause a radiological release (INSAG (2010a,b)).

4.3.1. Design Basis Threat (DBT)

A postulated accident that a nuclear facility must be designed and built to withstand without loss to the systems, structures, and components necessary to ensure public health and safety (USNRC, 2014; Kim and Kang, 2012). According to IAEA (2009a,b), a physical protection system is designed to prevent adversaries from successfully committing a malicious act. To ensure that this objective is met, the designer for physical protection should understand the conditions under which the protection system must perform. A clear description of these threats defines these conditions and is therefore an essential prerequisite for reasonably assured and effective physical protection. Therefore a DBT is a tool that provides a common basis for planning for physical protection by the operator and approval of its physical protection plan by the competent authority for nuclear security.

4.3.2. Design Basis Accident (DBA)

According to Sienicki (2011), nuclear power plants are designed to maintain their integrity and performance of safety functions for a bounding set of normal operational events as well as abnormal events that are expected to occur or might occur at least once during the lifetime of the plant. In addition, they are designed to maintain performance of safety functions for a set of DBA that involve failures that are possible but unlikely to occur during the plant lifetime. The plant design incorporates redundant safety systems which meet requirements for inspection and testing to assure their performance when required. An example of a DBA for a Light Water Reactor (LWR) is the loss of electrical power from the electrical grid. The plant design includes redundant safety systems to shut down the nuclear chain reaction in the core as well as redundant multiple diesel generators that will start automatically to provide the electricity needs with an electrical power backup from batteries to assure core cooling to remove the decay heat generated in the core.

4.3.3. Passive system

Schultz (2012) noted that from an engineering perspective, the best safety systems are those that require no user intervention to operate. Rather, they are engineered to trip automatically under specific conditions and by the use of only natural forces such as gravity, buoyancy, convection, and conduction to drive flows. Such safety systems are known as passive safety in the nuclear industry. However, these techniques have only recently been included in real reactor designs and only a handful of recently opened nuclear power stations around the world are currently using this technology. Similarly INSAG (2010a,b) also highlighted that the use of passive systems to avoid human errors may make it more difficult for potential aggressors to tamper with these systems. Accordingly, new passive safety systems have been proposed in the advanced reactor designs and by using all passive safety systems, a ten-fold increase in reactor safety is possible. Safer, simpler and intelligent engineering systems that are easier to operate and maintain which will reduce significantly the potential for serious human errors and eventually lead to even more economical nuclear power systems (Ishii et al., 2003). According to IAEA (2009a,b), another motivation for the use of passive safety systems is the potential for enhanced safety through increased safety system reliability.

4.4. Graded approach

This is a concept of evaluating the threat, its relative attractiveness, nature of the nuclear material and the associated potential consequences (IAEA, 2011a,b). It is the measure, when implementing nuclear safety and security, to ensure that important safety and security requirements are observed more stringently. Therefore, their requirements should be commensurate with the potential hazard of the facility and proportional measures for prevention and mitigation should be undertaken to minimize radiological risks to society and the environment. These requirements should be applied to sitting, design, operation, utilization, modification, training and qualification, emergency preparedness, and regulatory supervision (Gandhi and Kang, 2013).

4.5. Operating principles

Coordination is needed in developing operating procedures, especially when conflicts are unavoidable; the matter should be resolved based on the philosophy of minimizing the overall risk to the public (Shokr, 2014). Coordination is necessary so that compensatory measures do not undermine the necessary balance between safety and security (e.g., compromising security surveillance systems during maintenance operation should be avoided). However, verifying the status of the facility on periodical basis is very necessary, which may either results in the need for modernization or refurbishment, updating of procedures and documents, and revision of the safety analysis including DBA or DBT. Similarly, in access control, consideration should be given for the requirements for safety and security. While facilitated access is needed for emergency teams but it may be controlled for security purposes. Some areas within the reactor facility may be subjected to special physical protection system while it should be possible to be accessed for evacuation of personnel in case of emergency. Likewise, Safety procedures in some cases may slowdown transport of materials, while the duration of transport should be minimized for security purposes.

4.6. Emergency response

The challenges in this area are very similar, regardless of whether the initiating event was on safety or security. The principal aim is to mitigate the event and its radiological consequences, thereafter to address non-radiological issues, through consistent and authoritative provision of information to the public. Coherent initial assessment, crisis and consequence management are needed, which can therefore only be achieved through coordinated and effective preparedness involving all relevant authorities and organizational response. Though, there are different tendencies between safety-related and security-related events (Batra and Nelson, 2012). The most critical type of emergency of a nuclear plant is an off-site emergency where members of the public may get affected and to cope with such an off-site emergency, detailed response plans are required to be put in place. It is also mandatory for the power plant operators to periodically conduct on-site and off-site emergency exercises. No new or existing power plant or radiation facility will be permitted by the regulatory board to operate unless preparedness plans are in place for the postulated emergency scenarios. According to INSAG (2010a,b), security plans for a nuclear power plant should encompass not only the prevention of malicious acts, but also the specification of effective response measures (contingency plans), for example including securing a site. Similarly, there is an obvious need to ensure that the security plan is compatible with and complementary to the safety plan. Therefore, this is necessary to ensure that coordination is organized among both safety and security responders as part of overall emergency planning.

4.7. Training and education

Training is an essential component in building and sustaining capacity in national nuclear security systems. The IAEA offers a wide variety of international, regional, sub-regional and national training courses and workshops which draw upon international guidelines and recommendations published by the IAEA and international best practices (Global Nuclear Safety and Security Network-GNSSN, 2014).

5. Nuclear safety, security and safeguard synergy

Suzuki et al. (2010) have noted that the 3S initiative is to raise awareness of 3S worldwide and to assist countries in setting up nuclear energy infrastructures that are essential cornerstones of a successful nuclear energy program. The goals of the 3S initiative are to ensure that countries already using nuclear energy or those planning to use nuclear energy are supported by strong national programs in safety, security, and safeguards not only for reliability and viability of the programs, but also to prove to the international audience that the programs are purely peaceful and that nuclear material is properly handled, accounted and protected for. An inclusion of security and safeguards in conjunction with safety is important for overcoming growing security threats and increasing proliferation risks. It should be noted that coordination between each "S" is lacking because they are developed independently in response to historical events and because they are often regulated by different institutions. Communication between 3S organizations and cultures is deficient. Nuclear safety-related accident information is shared by all countries and safety culture concepts of "safety first" and "defense in depth" are well established. In contrast, incident information for nuclear security events is generally not shared because of the inherent need for secrecy. The human factor greatly contributes to human error in safety, as well as to all nuclear security events, which can be traced to unintentional personal errors as well as deliberate malicious acts. It is incumbent on leadership and management to resolve issues related to complaints about inadequate organizational procedures and management failure. Therefore, establishing strong cultural norms, strict codes of behaviour and enforceable penalties are important for deterring intentional acts by organizations or individuals. According to Kroening et al., 2012, in the design of new or operation of already existed nuclear facilities, there are several equally important elements for each "S", like confinement, containment, and protection of nuclear materials in the form of 3S synergy as shown in Fig. 5 below. Passive and inherent mechanisms, such as double-entry doors, could satisfy both security and safety objectives, and sharing nuclear facility process data systems could enhance the efficiency of safeguards and safety. According to Hanks (2013), in a nuclear reactor containment structures are designed to prevent the release of radioactive materials during an emergency for protecting the public thereby improving safety of the facility. The containment barriers designed into other facilities such as a mixed oxide fuel fabrication (MOX) facility also serves as protection to the public. More so, these containment structures provides security barrier to terrorist directed towards taking control of nuclear material that might be used for their activities. Furthermore, facility containment design information is verified as part of an IAEA safeguards approach, in ensuring that nuclear material is not removed without detection. Accordingly, at the Three Mile Island (TMI) nuclear power plant (NPP) accident of 1979, new techniques

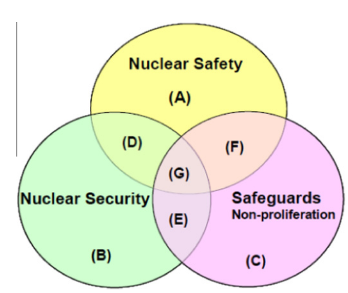

Fig. 5. The Venn diagram of sets of 3S (Suzuki et al., 2010; Batra and Nelson, 2012; Kroening et al., 2012).

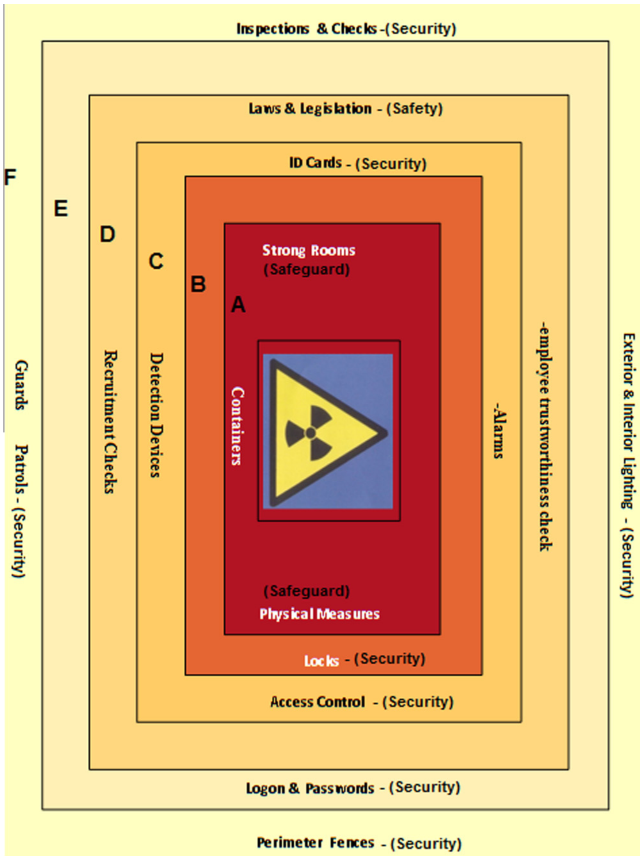

Fig. 6. PPS Layout for nuclear facility.

for locating radioactive materials disbursed throughout the reactor primary system were developed in order to determine nuclear material accountancy (safeguards) and minimize human exposure to radiation (safety). Security measures were also taken to mitigate malicious acts during removal and transportation of the damaged nuclear fuel.

The relationships between 3S as in Fig. 5 are shown below:

A = Emergency core cooling system for nuclear power plant.

B = Barrier at the facility entrance.

C = Authenticated apparatus.

D = Double-entry doors to keeping lower pressure than the atmosphere pressure and prevent radioactive release.

E = Management of nuclear material using containment and surveillance by the use of CCTV and guarding troops.

F = Management of nuclear material for criticality and accounting control.

G = Possible monitoring camera for multipurpose use, such as joint use of equipment.

Based on the concept of 3S synergy as illustrated in this paper, I hereby proposed the PPS design for nuclear facility as shown in Fig. 6 below: The design is made of six (6) different layers of protection (A–F) before the source containment.

A = Strong room with the Source container (Safeguard).

B = barrier made of locks to the strong room (Security 1).

C = detection devices made of Access control for authentication to critical offices with the use of identity cards or any other identification objects (Security 2).

D = law and legislation (Safety).

E = log on password authentication for main office entrance (Security 3).

F = fence, security lights and guard troops (Security 4).

6. Conclusion

Activities such as the operation of nuclear installations, the medical uses of radiation, the production of fuel cycle, transport, and use of radioactive material and the management of radioactive waste must therefore be subject to standards of 3S. The IAEA Nuclear Security Series provides nuclear security fundamentals, recommendations, implementation and technical guidance for member countries to assist them in the new nuclear security regimes or in reviewing and without any doubt peaceful use of nuclear energy. Therefore, to achieve this three elements of 3S, their synergy must be integrated into the design, installation, operation, maintenance and management of Nuclear and radiological facilities which will therefore increase the level of confidence in the safe operation and the fear of sabotage of nuclear facilities, theft of nuclear and radiological materials, trafficking and the danger of terrorists acquiring and using it for a nuclear weapon. Safety measures and security measures must be designed and implemented in an integrated manner so that security measures do not compromise safety and safety measures do not compromise security. Since both are for protecting human life, health and the environment the role of safeguards and the role of PPS with its six fundamental principles of graded approach, security culture, quality assurance, confidentiality, contingency and defense in depth needs to be taking into consideration as well.

References

ALGER, J., 2008. A guide to global nuclear governance. safety, security and non-proliferation. The Centre for International Governance Innovation (CIGI), Ontario, Canada, <http://www.cigionline.org/sites/default/files/a_guide_to_nuclear_power.pdf>, (May 2014).

Amano, Y., 2013. Nuclear Security Plan 2014–2017. IAEA press, Austria, Vienna, <http://www.iaea.org/About/Policy/GC/GC57/GC57Documents/English/gc57-19_en.pdf>, (May 2014).

Bakr, W.F., Hamed, A.A., 2009. Radiological Regulations and Emergency Division. National Centre for Nuclear Safety and Radiation Control. Journal of Physical Security 3 (1), 9–16, >,http://jps.anl.gov/Volume3/Paper3_Bakr_and_Hamed.pdf>, (May 2014).

Batra, A., Nelson, P., 2012. Safety, Safeguards and Security in Indian Civil Nuclear Facilities, Of Literature Otherwise Not Discussed. NSSPI, India, p. 8, 40–48, <http://nsspi.tamu.edu/media/1354465/threesreport_nsspi.pdf>, (June 2014).

Boureston, J., Semmel, A.K., 2010. The IAEA and Nuclear Security: Trends and Prospects, the Stanley Foundation. Muscatine, USA, >,http://psaonline.org/downloads/The%20IAEA%20and%20Nuclear%20Security.pdf>, (May 2014).

Boyer, B., Schanfein, M., 2008. International Safeguards Inspection: An Inside Look at the Process. In: Doyle, J. (Ed.). Nuclear Safeguards, Security, and Non-proliferation Achieving Security with Technology and Policy Elsevier Inc, Burlington, USA.

Brayon, F.C.M., n.d. Physical Protection Principles, Atomic Energy Licensing Board (AELB), Selangor, Malaysia. <http://www.aelb.gov.my/events/lamanweb2/docs/5%20%20Physical%20Protection%20Prinsiples%20%282%29.pdf>, (May 2014).

Carmona, L.V., 2005. The International Regime on the Physical Protection of Nuclear Material and the Amendment to the Convention on the Physical Protection of Nuclear Material. Nuclear Law Bulletin, 1–18, <https://www.oecd-nea.org/law/nlb/nlb-76/031_045.pdf>, (May 2014).

CNND, 2013. Nuclear Weapons: The State of Play. In: Thakur, R. Evans, G (Eds.), Chapter 3, Paragon, Canberra, Australia. <http://cnnd.anu.edu.au/files/2013/state-of-play-report/12305-State-of-Play-report-4-internals-FA2-B.pdf>, (May 2014).

DOS, 2014. Delivering effective Nuclear Verification for World Peace, Safeguards, IAEA, Vienna, Austria. <http://www.iaea.org/safeguards/index.html>, (May 2014).

Doyle, J., 2008. Nuclear Safeguards, Security, and Non-proliferation Achieving Security with Technology and Policy. Elsevier Inc, Burlington, USA.

Everton, C., Bayer, S, Carlson, J., 2010. Australian Safeguards and Non-Proliferation Office. Barton, Australia, <https://www.dfat.gov.au/asno/publications/developments-in-the-iaea-INFCIRC225.pdf>, (May 2014).

ENDO, T., 2009. Countries Planning to Introduce Nuclear Power Generation and the 3Ss – Making the 3Ss an International Standard, ICNND, Barton, Australia. <http://www.icnnd.org/Documents/endo_3s_int_standard.pdf>, (May 2014).

Gandhi, S., Kang, J., 2013. Nuclear safety and nuclear security synergy. Elsevier, pp. 1–5.

Garcia, M.L., 2008. Physical Protection. In: Doyle, J. (Ed.), Nuclear Safeguards, Security, and Non-proliferation Achieving Security with Technology and Policy. Elsevier Inc, Burlington, USA.

GNSSN, 2014. Education and Training, para, 2, Atomic Energy Agency. <http://gnssn.iaea.org/Pages/education_training.aspx>, (June 2014).

Hanks, D.H., 2013. Managing Safety, Security, and Safeguards (3S) Relationship: A National Regulatory Authority Perspective United States Nuclear Regulatory Commission, 54th Annual Meeting of Institute of Nuclear Materials Management, Palm Desert, July 14–18, Deerfield, Illinois, USA.

IAEA-NSS, 2012. Seoul Communiqué, paragraph 6, p. 1–6. <https://www.nss2014.com/sites/default/files/documents/seoul_communique_final.pdf>, (May 2014).

IAEA, 1996. Quality Assurance for Safety in Nuclear Power Plants and other Nuclear Installations-Code and Safety Guides Q1-Q14, Management, p. 8 and 13, IAEA, Vienna, Austria. <http://www.lei.lt/insc/quality/PDF-Files/SS-50-C-SG-Q-CD.pdf>, (June 2014).

IAEA, 1999. The Physical Protection of Nuclear Material and Nuclear Facilities, Objectives, p. 4, Vienna, Austria. <http://www.iaea.org/Publications/Documents/Infcircs/1999/infcirc225r4c.pdf>, (May 2014).

IAEA, 2008. Preventive And Protective Measures against Insider Threats, Objective and Scope, p. 2, IAEA, Vienna, Austria. <http://www-pub.iaea.org/MTCD/publications/PDF/pub1359_web.pdf>, (May 2014).

IAEA, 2009. Development, Use and Maintenance of The Design Basis Threat, Purpose of a Design Basis Threat, pp. 7–8, IAEA, Vienna, Austria. <http://www-pub.iaea.org/MTCD/publications/PDF/Pub1386_web.pdf>, (June 2014).

IAEA, 2009. Passive Safety Systems and Natural Circulation in Water Cooled Nuclear Power Plants, Introduction, p. 1, IAEA, Vienna, Austria. <http://www-pub.iaea.org/MTCD/Publications/PDF/te_1624_web.pdf>, (June 2014).

IAEA, 2011a. Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5), p. 14, IAEA, Vienna, Austria. <http://www-pub.iaea.org/MTCD/publications/PDF/Pub1481_web.pdf> (June 2014).

IAEA, 2011b. Computer Security at Nuclear Facilities, Definitions, p. 2, 60 and 68, IAEA, Vienna Austria. <http://www-pub.iaea.org/MTCD/Publications/PDF/Pub1527_web.pdf>, (June 2014).

IAEA, 2011c. IAEA International Fact Finding Expert Mission of the Fukushima Dai-Ichi NPP Accident Following The Great East Japan Earthquake and Tsunami, IAEA, Vienna Austria. <http://www-pub.iaea.org/MTCD/meetings/PDFplus/2011/cn200/documentation/cn200_Final-Fukushima-Mission_Report.pdf>, (17 August 2014).

IAEA, 2013a. International Safeguards in Nuclear Facility Design and Construction. IAEA Press, Austria, Vienna, <http://www-pub.iaea.org/MTCD/Publications/PDF/Pub1600_web.pdf>, (May 2014).

IAEA, 2013b. Objective and Essential Elements of a State's Nuclear Security Regime Nuclear Security Fundamentals, IAEA Nuclear Security Series No. 20, IAEA, Vienna, Austria.

IAEA, 2014. Concepts and terms, Complementarity of safety and security, IAEA, Vienna, Austria. <http://www-ns.iaea.org/standards/concepts-terms.asp>, (May 2014).

IAEA, 2012. Nuclear Security Culture, IAEA Nuclear Security Series No. 7, Nuclear Security and Nuclear Security Culture, p. 3, IAEA, Vienna, Austria. <http://www-pub.iaea.org/MTCD/publications/PDF/Pub1347_web.pdf>, (June 2014).

INSAG, 2010. The interface between safety and security at nuclear power plants, Purpose and Scope, p. 3, 13, IAEA, Vienna, Austria. <http://www-pub.iaea.org/MTCD/Publications/PDF/Pub1472_web.pdf>, (May 2014).

INSAG, 2010. The Interface Between Safety And Security at Nuclear Power Plants, Design, p. 15, Vienna, Austria. <http://www-pub.iaea.org/MTCD/Publications/PDF/Pub1472_web.pdf>, (June 2014).

Ishii, M., Revankar, S.T., Downar, T., Xu, Y., Yoon, H.J., Tinkler, D., Rohatgi, U.S., 2003. Modular and Full Size Simplified Boiling Water Reactor Design with Fully Passive Safety Systems, Significance of the Project, p. 1, Brookhaven National Laboratory, Uptown, NY, USA. <http://www.osti.gov/scitech/servlets/purl/811897>, (June 2014).

Kim, D., Kang, J., 2012. Where nuclear safety and security meet. Sage Pub. 68 (1), 86–93, p. 1–9, <http://bos.sagepub.com/content/68/1/86.full.pdf+html>, (May 2014).

Khripunov, I., 2012. Nuclear and Radiological Security Culture: A Post-Seoul Summit Agenda, Security as a Subset of Organizational Culture. CITS, University of Georgia, USA, p. 8, <http://cits.uga.edu/uploads/documents/postseoul.pdf>, (June 2014).

Kroening, M., Sednev, D., Chumak, D., 2012. Nondestructive Testing At Nuclear Facilities as Basis For The 3S Synergy Implementation, 7th International Forum (IFOST), p. 1–4. <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6357725>, (June 2014).

Krupa, A.S., 2003. The Oversight of Physical Security and Contingency Planning. SANS Institute, UK, <http://www.sans.org/reading-room/whitepapers/recovery/oversight-physical-security-contingency-planning-557>, (June 2014).

Malcolmson, J., 2009. What is Security Culture? Does it differ in content from general Organizational Culture? Security Technology, 43rd Annual 2009 International Carnahan Conference, October 5–8. <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5335511>, (June 2014).

NSSPI, 2014. Nuclear Safeguard Education Portal, Physical Protection Systems, NSSPI, Texas, USA. <http://nsspi.tamu.edu/nsep/reference-modules/technical-safeguards-terminology/physical-protection-systems/physical-protection-systems>, (May 2014).

NSSPI, 2014b. Nuclear Safeguard Education Portal, Introduction to Physical Protection Systems. NSSPI, Texas, USA, p. 1–32. <http://nsspi.tamu.edu/nsep/courses/physical-protection-systems/introduction/introduction-to-physical-protection-systems>, (May 2014)..

Parsick, R., Sanborn, J., 1994. INFCIRC/153 as the Basis for Verification of a Special Nuclear Materials Production Cut-off Convention. Brookhaven National Laboratory, <http://www.osti.gov/scitech/servlets/purl/79010>, (15 August 2014).

Rojavin, Y., Seamon, M.J., Tripathi, R.S., Papadimos, T.J., Galwankar, S., Kman, N., Cipolla, J., Grossman, M.D., Marchigiani, R., Stawicki, S.P.A., 2011. Civilian nuclear incidents: an overview of historical, medical, and scientific aspects. Journal of Emergencies, Trauma, and Shock 4 (2), 1–17, <http://www.ncbi.nlm.nih.gov/pmc/articles/PMC3132367/>, (May 2014).

Schultz, I., 2012. Passive Nuclear Safety Technology, Introduction. Stanford University, California, USA, <http://large.stanford.edu/courses/2012/ph241/schultz1/>, (June 2014).

Shokr A. M., n.d. Synergy between Nuclear Safety and Security for Research Reactors, Operating Principles, p. 14–16, IAEA, Vienna, Austria. <http://www-ns.iaea.org/downloads/ni/training/rr-presentations-pdf/synergy-between-safety-and-security-for-rr.pdf>, (June 2014).

Sienicki, J., 2011. Energy Engineering and Systems Analysis, Design Basis and Severe Accidents. Argonne National Laboratory, Lemont, Illinois, USA, <http://www.ne.anl.gov/pdfs/nuclear/design_basis_and_severe_accidents_sienicki.pdf>, (June 2014).

Suzuki, M., Izumi, Y., Kimoto, T., Naoi, Y., Inoue, T., Hoffheins, B., 2010. Investigating 3S Synergies to Support Infrastructure Development and Risk-Informed Methodologies for 3S by Design, Nuclear Non-proliferation Science and Technology Centre, Japan, Atomic Energy Agency 2-4 Shirane, Shirakata, Tokai-mura, Naka-gun, pp. 319–1195, Japan, <http://www.iaea.org/safeguards/Symposium/2010/Documents/PapersRepository/064716080619958803977.pdf>, (May 2014).

Tape, J., Pilat, J., 2008. Nuclear Safeguards and the Security of Nuclear Materials. In: Doyle, J. (Ed.), Nuclear Safeguards, Security, and Non-proliferation Achieving Security with Technology and Policy. Elsevier Inc, Burlington, USA.

USNRC, 2013. Physical Protection, US.gov, Washington, USA. <http://www.nrc.gov/security/domestic/phys-protect.html>, (May 2014).

USNRC, 2013. Quality Assurance for New Reactors, US Govt., Washington, USA. <http://www.nrc.gov/reactors/new-reactors/oversight/quality-assurance.html>, (June 2014).

USNRC, 2014. Design basis accident, US. Govt., Washington, USA. <http://www.nrc.gov/reading-rm/basic-ref/glossary/design-basis-accident.html>, (June 2014).

WNA, 2013. Safeguards to Prevent Nuclear Proliferation, World Nuclear Association, London, UK. <http://www.world-nuclear.org/info/Safety-and-Security/Non-Proliferation/Safeguards-to-Prevent-Nuclear-Proliferation/>, (May 2014).

Xu, P., Deng, Y., Su, X., Chen, X., Mahadevan, S., 2014. An evidential approach to physical protection system design, Vol. 65. Elsevier, Science Direct, p. 125–137.