2017 International Nuclear Atlantic Conference - INAC 2017
Belo Horizonte, MG, Brazil, October 22-27, 2017
ASSOCIAÇÃO BRASILEIRA DE ENERGIA NUCLEAR – ABEN

Agência Brasileira do ISBN
ISBN 978-85-99141-07-6

INCREASING THE EFFECTIVENESS OF THE PHYSICAL PROTECTION SYSTEM ON A NUCLEAR FACILITY

Antonio C. A. Vaz[1] and Thadeu N. Conti[2]

[1]Centro do Reator de Pesquisas-CRPq
Instituto de Pesquisas Energéticas e Nucleares (IPEN / CNEN - SP)
Av. Professor Lineu Prestes 2242
05508-000 São Paulo, SP
acavaz@ipen.br

[2]Centro de Engenharia Nuclear-CEN
Instituto de Pesquisas Energéticas e Nucleares (IPEN / CNEN - SP)
Av. Professor Lineu Prestes 2242
05508-000 São Paulo, SP
tnconti@ipen.br

ABSTRACT

The malicious use of radioactive material could be devastating, particularly in the case of a nuclear explosive device, it could be unpredictably disruptive resulting in the dispersal of radioactive material, like it was in the Fukushima Daiichi Nuclear Power Plant disaster. Physical Protection System (PPS) 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 of using radioactive material for malicious acts. PPS is an integrated system of people, equipment and procedures used to protect nuclear facilities and radioactive sources against threat, theft or sabotage. In the operator's perspective, this paper study factors influencing the performance of a PPS in a nuclear facility suggesting ways to increase the system effectiveness. The human factor, the physical and the psychological work environment has a large impact on how personnel perform their work and comply with nuclear security requirements. Apathy and corporatism are two human behaviors that collaborate negatively and make decrease the effectiveness of any PPS. Job satisfaction reduces the probability that personnel will become less reliable and/or obstructive in extreme cases an insider threat. Managers must recognize individual and group needs and the relationship among personnel so that they may motivate personnel by creating a supportive working environment that reduces workplace stress. An effective PPS can result in a significant increase in the effectiveness of the security of radioactive material and associated facilities.

1. INTRODUCTION

This paper describes studied factors influencing the performance of PPS in a nuclear facility, from the operator's perspective.

The nuclear facilities includes each part of nuclear fuel cycle: mining, milling, processing, conversion, enrichment, nuclear fuel fabrication, reactor operation, electrical generation or other energy products, reprocessing to recover fissile material, storage of reprocessed fissile material and final storage for all waste [1]. A security system should be designed by the operator’s security professionals to deter opponents from committing a malicious act or to minimize through detection, delay and response the likelihood of an opponent succeeding in completing such a malicious act. Such an act would consist of a sequence of actions by one or

more adversaries (threat) to obtain access to a source (target) either in order to commit an act of sabotage or another malicious act, or in order to remove the source without authorization [2].

Physical protection measures must be addressed and implemented during all stages of the nuclear fuel cycle [3]. Appropriate measures should be put in place to ensure that nuclear security requirements are met so that uranium cannot be removed for unauthorized purposes. These measures should also cover potential failure of the prevention measures to detect and respond to criminal or unauthorized acts with nuclear security implications [4].

2. OBJECTIVE

The objective of this paper is to present ways to increase the effectiveness of the physical protection system in a nuclear facility, from the operator's perspective, considering as priority the technical and human factors.

3. METHODOLOGY

The operator should prepare a security plan as part of its application to obtain a license. The security plan should be based on the threat assessment or the design basis threat (DBT) and should include sections dealing with design, evaluation, implementation, maintenance of the Physical Protection System (PPS) and emergency plans. They should have the primary responsibility for implementing and maintaining security measures for radioactive sources in accordance with national requirements and IAEA recommendations. Also, operators should ensure that their personnel and their contractors are suitably trained and meet the regulatory requirements, which should include trustworthiness [5].

Implementation of PPS measures against unauthorized removal of nuclear and other radioactive material in use and storage, as well as the measures against sabotage of nuclear facilities and nuclear material in use and storage, are necessary for ensuring the protection of people and the environment throughout the lifetime of the facilities.

These are the technical and human factors to be considered to increase the PPS effectiveness in a nuclear facility:

2.1. Design Basis Threat

A Design Basis Threat (DBT) is a comprehensive description of the motivation, intentions and capabilities of potential opponents against which PPS are designed and evaluated. Such definitions permit security planning on the basis of risk management [6]. A DBT is derived from credible intelligence information and other data concerning threats. It is used in a regulatory system to achieve appropriate allocations of resources for the protection of nuclear material and nuclear facilities against malicious acts by potential opponents (from inside and outside of the facility) that could result in dire consequences, particularly radiological consequences like in the Fukushima Daiichi Nuclear Power Plant disaster recently [7] or consequences of proliferation; however a DBT can also be used to protect any asset with associated high potential consequences [8]. This involves considering factors about potential opponents, such as class, capabilities, and range of tactics. A list of necessary information

about opponents includes: motivation, potential goals based upon targets, tactics and numbers and capabilities. Information should be sought for regional, national, and international threats, depending on the mission and location of the facility. Sources for this information include: intelligence sources, crime analysis, studies, professional organizations, published literature, government directives and legislation [9].

2.2. Defense in Depth

The Defense in Depth (DiD) is a classical defensive philosophy currently applied to a variety of technical fields, including nuclear facilities where this concept is widely applied, chemical industries, Information and Communication Technology (ICT), transport, and many others. It deals with slowing down the progression of a threat against a target by using multiple and independent levels of protection (or lines of defense), designed to compensate for the failure of one or more defenses, ensuring that the risks are kept acceptable. Concerning the current practices for the DiD implementation and the rationale for its evolution, there is a shared recognition that the reinforcement of DiD is the key to improve the security of future installations for all types of technologies and industries. Within this context, the results of Probabilistic Safety Assessment (PSA) plays a key role in the demonstration of both the robustness of the design and security, supporting the verification that DiD principles are correctly implemented. A key issue, still open, is related to the link that must be put in place to provide the DiD with probabilistic success criteria through PSA insights [10]. The DiD philosophy in PPS is put into practice through the following diagram (Figure 1).

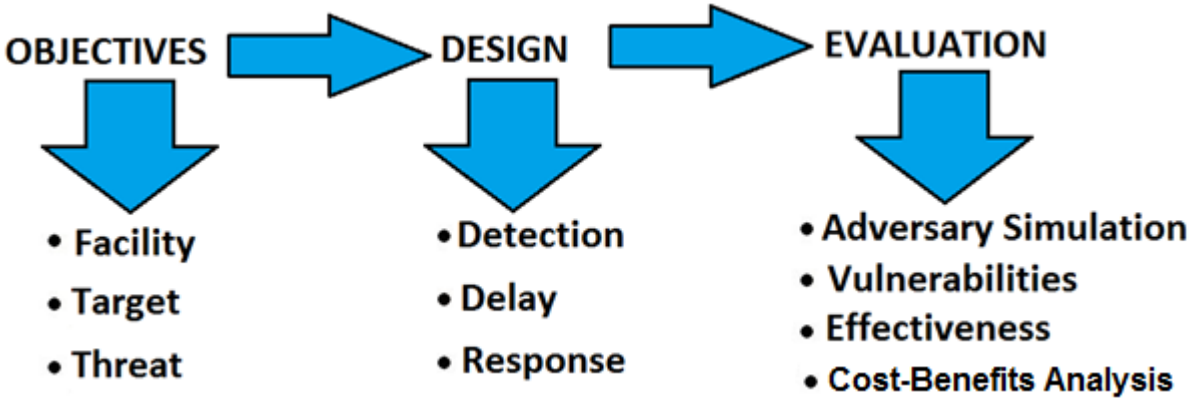

Figure 1: Physical Protection System diagram for design and evaluation

The process works in three steps: setting the objectives, designing the system and ending with an evaluation of the system performance in function of its objectives.

Objectives – The first step of the diagram is a comprehensive description of the facility, threats definition and targets identification.
Design – Of the equipment and devices are working together to improve performance of detection, delay and response elements.
Evaluation – A simulation of the opponent action (opponent/adversary simulation) is necessary to determine of vulnerabilities and the effectiveness of the system.
Cost-Benefit – This is a very important analysis to be considered, managing the risk and benefit of nuclear resources is a policy consideration that must be addressed. Consideration

should be given to the risks and costs of protection completed for other non-nuclear resources of similar consequence [9].

2.3. Detection, Delay and Response

The PPS philosophy is 'defense in depth' and the hardware is the elements of: detection, delay and response. Considerable reliance should be placed upon security technology to provide early warning of the entry of an adversary to the site or the secured area. Intruder detection systems used for the protection of radioactive sources should therefore not only be properly specified but also tested for performance upon installation, maintained at regular intervals by competent persons, and tested at intervals specified by the system operator. Response comprises mitigation of consequences, prevention of serious consequences and bringing a situation under control. Planning shall consider the dependencies of the various areas. In the planning of detection and delay, for example, the time needed to arrange response shall be taken into account. Security personnel shall conduct random patrols of the area to detect a potential threat. The detection, delay and response are systems and equipments working together inside the protection layers (Figure 2) that there are among limited, protected and vital areas [11]. Detection, delay, and response are all required functions of effective PPS; these functions must be performed in this order and within a length of time that is less than the time required for the opponent to complete their task. Inside the protection layers are the PPS elements: sensors, barriers, cameras, guards, fence, wall, door, gate, windows and so on.

Off site – They are areas out of facility.
Limited area – Designated area containing a nuclear facility and nuclear material to which access is limited and controlled for physical protection purposes [1].

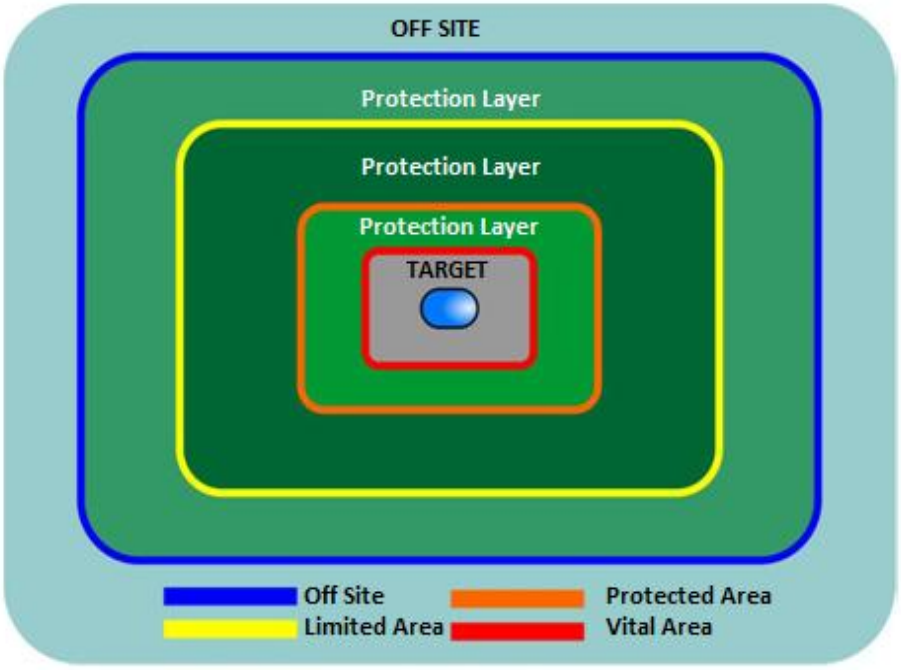

Figure 2: Protections layers between off site and vital area

Protected area – Area inside a limited area containing nuclear material and/or sabotage targets surrounded by a physical barrier with additional physical protection measures [1].
Vital area – Area inside a protected area containing equipment, systems or devices, or nuclear material, the sabotage of which could directly or indirectly lead to high radiological consequences [1].

2.4. Systems and Equipment

The communication, surveillance, alarm and access control equipment (and devices) belonging to security arrangements shall be tested and serviced at intervals determined in the nuclear facility's instructions. In provision against failures, measures shall be planned in advance to ensure the adequate functionality of security arrangements. All equipment and devices must be assessed during Emergency Exercise (EEx) [3].

The objectives of surveillance measures are to ensure that the activities of any authorized employee are always monitored by at least one other experienced, authorized employee in order that unauthorized acts on the part of one can be immediately detected and reported, it´s best known as 'two person' rule [12].

2.5. Quality Management

Quality assurance policies and quality assurance programs should be established and implemented with a view to providing confidence that specified requirements for all activities important to physical protection are satisfied [5]. Management systems and quality systems are oriented toward continual improvement and reliability, while accommodating the diversity of the global nuclear facility community. Systems, procedures, processes and components are designed with the flexibility required to respond to changes and advances over time.

2.6. Emergency Plan

Emergency plans to respond to unauthorized removal of nuclear material or sabotage of nuclear facilities or nuclear material, or attempts thereof, should be prepared and appropriately exercised by all license holders and authorities concerned [5]. Emergency plans to respond to unauthorized removal of nuclear material or sabotage of nuclear facilities or nuclear material, or attempts thereof, should be prepared and appropriately exercised by all license holders and authorities concerned.

Plans for security, and measures to prepare for threats, shall be prepared in cooperation with the appropriate police authorities. Mitigation of consequences also includes initiation of the emergency organization's operation. A threat with objective or potential consequence of compromising facility safety shall be classified as an emergency situation in accordance with the emergency plan. During an Emergency Exercise (EEx) scenario the Emergency Plan must be assessed.

2.7. Training and Qualification

Nuclear facility personnel shall be appropriately familiarized with security control and procedures contributing to the implementation of these at the workplace. The mental and

physical capability of shift managers and other security personnel shall be ensured every year based on an assessment conducted by occupational health care. In the annual training events and demonstration tests (practice and theory), shift managers and other security personnel shall demonstrate their capability to carry out their physical security tasks correctly and safely. An access or visiting pass shall not be granted if a physician or other health care professional has established that a person is inclined to, for example, violent behavior, vandalism or the misuse of intoxicating substances, or mental or has other potentially dangerous illnesses. Visitors, a restricted number at a time, may only be allowed to the plant area or the protected area in the company of a person authorized for such a task. The host shall guide and supervise the visitors during the entire visit [12].

2.8. Security Culture

All organizations involved in implementing physical protection should give due priority to the security culture, to its development and maintenance necessary to ensure its effective implementation in the entire organization [5]. An effective nuclear security culture is dependent on proper planning, training, awareness, operation and maintenance, as well as on people who plan, operate and maintain PPS. Even a well designed system can be degraded if the procedures necessary to operate and maintain it are poor, or if the operators fail to follow procedures. Ultimately, therefore, the entire nuclear security regime stands or falls because of the people involved and their leaders. Consequently the human factor must be addressed in any effort to enhance the existing nuclear security culture [13].

The human factor is generally a contributor to all nuclear security related incidents as well as malfunctions related to activities involving radioactive material. They include deliberate malicious acts, unintentional personnel errors as well as ergonomic issues related to the design and layout of software and hardware, inadequate organizational procedures and processes and management failures. Individual understanding of and commitment to roles and responsibilities, commitment to continuous improvement, and management commitment are of great importance to nuclear security [14]. In this regard, leadership and management are vital components.

The characteristics of nuclear security culture are the beliefs, attitudes, behavior and management systems, the proper assembly of which leads to more effective nuclear security. The foundation of nuclear security culture is a recognition by those who have a role to play in regulating, managing or operating nuclear facilities or activities or even those that could be affected by these activities that a credible threat exists and that nuclear security is important [15]. Apathy [16] and corporatism [17] are two human behaviors very present at all levels of our society; they need to be overcome because they negatively affect the effectiveness of any PPS.

2.9. Emergency Exercise (EEx)

EEx is the best tool for evaluating emergency procedures and human behavior. In order to demonstrate the effectiveness of nuclear security, the licensee shall draw up an exercise program and accordingly, hold exercises related to security at regular intervals, however, no less frequently than once a year [18, 19].

Annual exercises shall be taken to practice procedures in compliance with the security plan and the security standing order in a threatening situation. Regular exercises shall also be arranged with the authorities concerned. In drawing up the exercise programmed, co-operation exercises and their number shall be agreed upon with the police authority taking into account the various police special groups [3].

Table-top exercises, simulations and practical exercises, for example, shall be used as exercise methods. In the exercises, situations shall be included with a simultaneous accident and nuclear security related threat [20]. Through a credible scenario the sequence simulation of the opponent is created from off site to target (Figure 3).

2.10. Vulnerability Assessment

A vulnerability assessment (VA), also known as security assessment is a method for evaluating PPS. It is a systematic appraisal of the effectiveness of a security system for protection against an assessed threat.

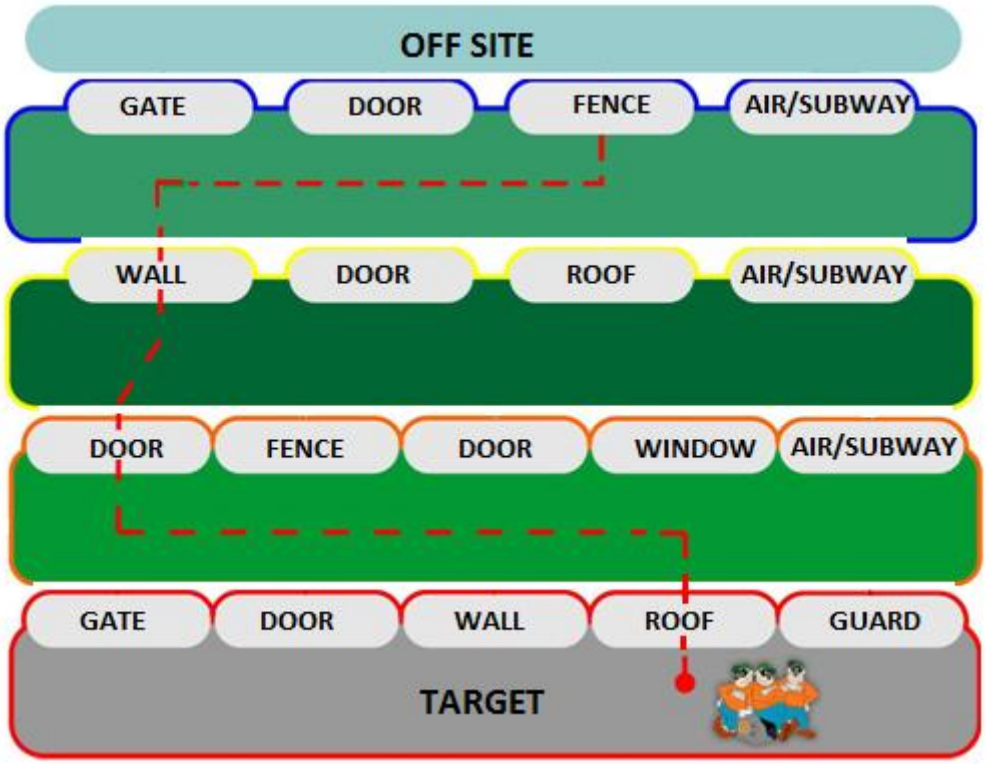

Figure 3: Opponent sequence simulation

The VA can be specific or general in nature, can be conducted locally by the operator or by the regulatory body, and can be used to help the development of regulations by the regulatory body or for demonstrating regulatory compliance of the operator. Risk analysis shall refer to examinations performed by using systematic measures in order to identify threats, problems, and vulnerabilities, surveying the causes and consequences thereof, and assess the related risks. The probability of opponent detection is checked and the time diagram is plotted (Figure 4) [21, 8].

- Delay Time (TT) – the time produced by the barriers to the proposed path for analysis.
- Response time (RT) – the time expected for the response force to stop the opponent's action.
- Detection Time (DT) – the time spent between the detection of the opponent and the beginning of action of the force response.
- Opponent Time (AT) – the time spent by the opponent to perform his action.
- Critical Detection Point (CDP) – the critical moment of detection because there is the risk of force response arriving after the end of the opponent's action.
- First detection time (T0) – the time that could indicate a nuclear security event (threat) starts.
- Action time (TA) – the time when response force starts the action to interrupt the opponent action (threat).

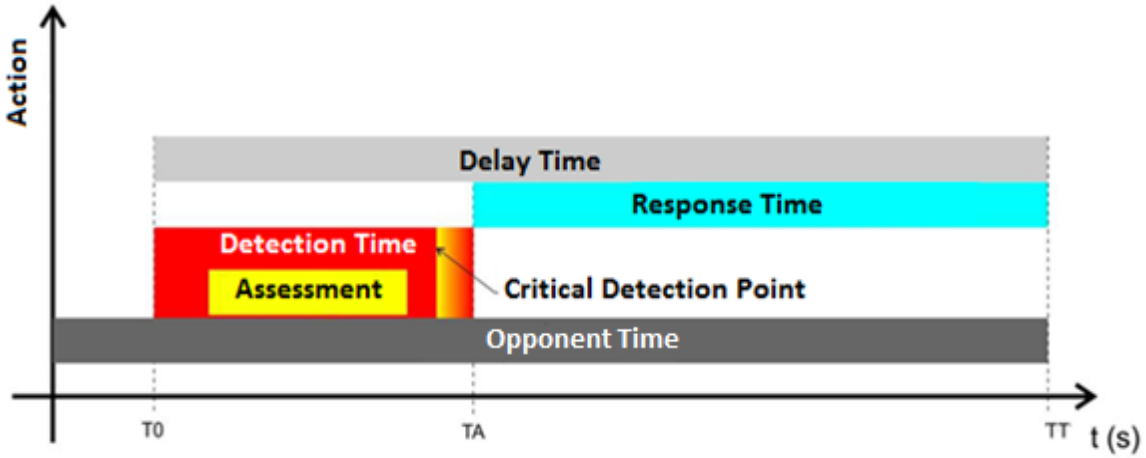

Figure 4: Time diagram of a Physical Protection System

2.11. Increasing the Effectiveness

To increase the effectiveness of the PPS it is necessary to create measures to decrease the time of action of the opponent (Figure 5) and make guards' response time sufficient to interrupt the opponent's action. It is necessary that the delay time be much less than the time of action of the enemy. The opponent must be kept away from vital area [22].
For a PPS with high effectiveness DT + RT must be << AT. This is possible by:

1. Improving the detection system in the limited area.
2. Increasing TT by inserting barriers between the threat and the target.
3. Increasing the numbers of barriers.
4. Decreasing the action time of response force.
5. Increasing the resistance of existing barriers.

The technical factor works according to the PPS design when the human factor does not interfere with the operation of the system.

"Two person" rule implementation is necessary to avoid insider threat and sabotage on the facility.

Figure 5: Increasing the effectiveness of the Physical Protection System

4. CONCLUSIONS

To increase the effectiveness of the Physical Protection System it is necessary from the conception of the Design Basis Treat until the system operation has obtained high performance of all the parties involved. Plans and procedures should always be up-to-date. The installed equipment must be of the latest technologies. As for the human factor, it is important that the people involved in the system be qualified, well trained and be part of a strong security culture. Attempting to increase the effectiveness of the Physical Protection System considering only the technical factor does not reflect the true quality of the system, it is important to create standards for evaluation of the human factors involved.

It is essential that consideration be given to the cost-benefit analysis because the cost of a severe nuclear accident is always extremely high.

ACKNOWLEDGMENTS

The authors would like to thank CNEN and IAEA for their support.

REFERENCES

1. "Nuclear Security Series Glossary" *Version 1.3, IAEA, November, pag.16*, Vienna, Austria (2015).
2. "Nuclear Security Series" *No.11 pg. 7, item 3.3., IAEA*,Vienna, Austria (2014)
3. A.C.A. Vaz and T.N. Conti, "How Nuclear Security Team Conducts Emergency Exercise at IEA–R1 Reactor", International Nuclear Atlantic Conference – INAC, Recife-PE, Brazil, November 24-29 (2015).
4. "Educational Programme in Nuclear Security", *Publishing Section–IAEA, Technical Guidance-International Atomic Energy Agency – IAEA*, Vienna, Austria (2010)
5. "Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision – 05)", *Publishing Section, Recommendation-International Atomic Energy Agency – IAEA*, Vienna, Austria (2011).

6. "Development, Use and Maintenance of Design Basis Threat", *International Atomic Energy Agency – IAEA, Nuclear Security Series No. 10*, Vienna, Austria (2009).
7. "The Fukushima Daiichi Accident*". Report by the Director General, IAEA*, Vienna, Austria (2015).
8. "Security of radioactive Sources", *Implementing Guide, IAEA*, Vienna, Austria (2009).
9. M. L. Garcia, *The Design and Evaluation of Physical Protection System*, Elsevier science, Boston-U.S.A, pp. 22 (2001).
10. L. Chierici1, G. Luigi Fiorini, S. La Rovere, P. Vestrucci, "The Evolution of Defense in Depth Approach: A cross Secto rial Analysis", *Open Journal of Safety Science and Technology*, 6, 35-54, France, Italy (2016).
11. A. C. A. Vaz and T. N. Conti, "Implementation and Evaluation of the Physical Protection System of the IEA-R1 Research Reactor ", *International Nuclear Atlantic Conference - INAC November 24-29"*, Recife, PE, Brazil, (2013).
12. "Preventive and Protective Measures Against Insider Threats", IAEA – Nuclear Security Series-No. 08, Vienna, Austria (2006).
13. "Code of Conduct on the Safety of Research Reactors", *Publishing Section, International Atomic Energy Agency – IAEA*, Vienna, Austria (2006).
14. "Security Culture in Nuclear Installations", *Publishing Section–International Atomic Energy Agency – IAEA*, Vienna, Austria (2008).
15. "Glossario-Segurança Nuclear", Divisão de Normas – DINOR, Comissão Nacional de Energia Nuclear – CNEN, *Rio de Janeiro,* R.J, Brazil (2012).
16. Michael P. Coole "The Theory of Entropic Security Decay: The Gradual Degradation in Effectiveness of Commissioned Security Systems". Cowan University-Australia (2010)
17. S. Huluban, "Corporatist Features of the Security Sector in Democratizing Countries: Cross- Regional Analysis of Brazil and Romania", *Master Theses,* Eastern Illinois University, Charleston, Illinois, U.S.A (2003).
18. "Preparedness and Response for a Nuclear or Radiological Emergency", *Publishing Section, International Atomic Energy Agency – IAEA*, Vienna, Austria (2006)
19. "Proteção Física de Unidades Operacionais da Área Nuclear", Norma CNEN NE-2.01, http://appasp.cnen.gov.br/seguranca/normas/pdf/Nrm201.pdf
20. " Security of a Nuclear Facility", file:///C:/Users/acavaz.IP/Downloads/YVL_A.11e%20(1).pdf
21. " Development of a Vulnerability Assessment Code for a Physical Protection System: Systematic Analysis of Physical Protection Effectiveness (SAPE)", https://www.kns.org/jknsfile/v41/JK0410747.pdf
22. " Identification of a Vital Area at Nuclear Facilities", http://wwwpub.iaea.org/MTCD/Publications/PDF/Pub1505_web.pdf